Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

«Допущено до захисту»

В.о. завідувача кафедри БІСТ

Мелкозьорова О.М.

_____

«_____» _____ 2024 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Дослідження та порівняльний аналіз смарт-карток на основі RFID та NFC технологій у контексті кібербезпеки»

Оцінка «_____»

Голова ЕК

Лемешко О.В. _____

Керівник к.т.н. Єсіна М.В.

Рецензент к.н.т.Бобух В.А.

Виконавець: студентка групи КБ-42

Матвєєва Є.Д.

Харків – 2024

РЕФЕРАТ

Пояснювальна записка до бакалаврської дипломної роботи містить 44 сторінок, 7 рисунків, 4 таблиці, 4 додатки, 26 джерел посилань.

Метою роботи є проведення детального дослідження та порівняльного аналізу сучасних смарт-карток на базі технологій RFID та NFC.

Об’єкт дослідження – смарт-картки на основі технологій RFID та NFC.

Предмет досліджень – використання технологій RFID та NFC у смарт-картках, зокрема їх рівень кібербезпеки та заходи захисту від потенційних загроз і атак.

У роботі розглядається порівняльний аналіз технологій RFID і NFC, які є дослідженням двох систем безконтактної ідентифікації, призначених для передачі даних та інформації, аналізуються основні характеристики та застосування RFID і NFC, такі як дальність передачі, швидкість зчитування, типи використання, вартість і безпека. Робота спрямована на визначення ключових відмінностей та переваг кожної технології, вивчення моделей загроз, потенційних вразливостей та засобів забезпечення безпеки для смарт-карток з використанням цих технологій.

Здійснення огляду та аналізу допоможе сформувати інформативну базу для подальшого дослідження та розробки рекомендацій, щодо підвищення кібербезпеки використання смарт-карток.

Ключові слова: ВРАЗЛИВОСТІ, ЗАГРОЗИ, ЗЧИТУВАЧ, КІБЕРБЕЗПЕКА, МІКРОЧІП, МІТКА, ПОРІВНЯЛЬНИЙ АНАЛІЗ, РАДІОХВИЛІ, РЕКАОМЕНДАЦІЇ, СМАРТ-КАРТКИ, NFC ТЕХНОЛОГІЯ, RFID ТЕХНОЛОГІЯ.

ABSTRACT

The explanatory note to the master's project contains 44 pages, 7 figures, 4 tables, 4 appendices, and 26 references to sources.

The purpose of the work is to carry out a detailed study and comparative analysis of modern smart cards based on RFID and NFC technologies.

The object of research is smart cards based on RFID and NFC technologies.

The subject of research is the use of RFID and NFC technologies in smart cards, particularly their level of cyber security and protection measures against potential threats and attacks.

The paper considers a comparative analysis of RFID and NFC technologies, which are a study of two contactless identification systems designed for data and information transmission, the main characteristics and applications of RFID and NFC are analyzed, such as transmission range, reading speed, types of use, cost and security. The work aims to identify each technology's key differences and advantages, studying threat models, potential vulnerabilities, and security measures for smart cards using these technologies.

Conducting a review and analysis will help to form an informative base for further research and development of recommendations for improving the cyber security of smart card use.

Keywords: VULNERABILITIES, THREATS, READER, CYBER SECURITY, MICROCHIP, TAG, COMPARATIVE ANALYSIS, RADIO WAVES, RECOMMENDATIONS, SMART CARDS, NFC TECHNOLOGY, RFID TECHNOLOGY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ....6
ВСТУП....7
1. ТЕХНОЛОГІЇ NFC ТА RFID: ПРИНЦИП РОБОТИ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ....9
1.1 Історія розвитку смарт-карток та основні принципи роботи....9
1.2 Принципи роботи технологій NFC та RFID....11
1.2.1 Технологія RFID....11
1.2.2 Технології NFC....14
1.3 Порівняльний аналіз переваг та недоліків технологій NFC та RFID....15
1.3.1 Переваги та недоліки технологій RFID та NFC....17
1.4 Приклади стандартів технологій NFC та RFID....19
2. ОГЛЯД, АНАЛІЗ ТА ДОСВІД ВИКОРИСТАННЯ RFID ТА NFC ТЕХНОЛОГІЙ, RFID ТА NFC СМАРТ-КАРТОК НА МІЖНАРОДНОМУ ТА НАЦІОНАЛЬНОМУ РІВНЯХ....21
2.1 Розвиток технологій RFID та NFC на міжнародному рівні, їх розповсюдження та застосування у різних країнах світу....21
2.1.1 Приклад використання технології RFID у світі....23
2.1.2 Приклад використання технології NFC у світі....23
2.2 Застосування смарт-карток з технологіями RFID та NFC у різних галузях на міжнародному рівні....24
2.3 Вивчення успішних та неуспішних проектів впровадження смарт-карток на базі RFID та NFC на національному рівні....26
2.4 Аналіз технічних та організаційних аспектів використання смарт-карток з технологіями RFID та NFC....28
3. МОДЕЛІ ЗАГРОЗ, ПОРУШНИКА ТА БЕЗПЕКИ ДЛЯ RFID ТА NFC ТЕХНОЛОГІЙ....32
3.1 Типи атак на смарт-картки....32

3.1.1 Безконтактні смарт-картки з унікальними форматами обміну даними 35
3.2 Ризики втрати конфіденційності даних через використання смарт-карток 37
3.3 Засоби захисту від атак на смарт-картки з технологіями RFID та NFC ..39
ВИСНОВКИ 42
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 45
ДОДАТОК А 49
ДОДАТОК Б 54
ДОДАТОК В.....60

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

BFSI – Banking, financial services and insurance

DoS – Denial of Service (відмова в обслуговуванні)

IoT – Internet of Things (Інтернет речей)

MITM – man in the middle (людина посередині)

NFC – Near Field Communication (комунікація ближнього поля, зв’язок ближнього поля)

RFID – Radio Frequency Identification (радіочастотна ідентифікація)

ІС – інформаційна система

ПЗ – програмне забезпечення

ВСТУП

У нашому технологічно орієнтованому світі одними з технологій, які стали невід'ємною частиною повсякденного життя, є технологія RFID (Radio Frequency Identification) і NFC (Near Field Communication). Ці технології зробили революцію в тому, як ми отримуємо доступ до інформації та послуг, але вони мають і свої проблеми, що створює нові виклики в галузі кібербезпеки.

Смарт-картки, що використовують ці технології, стають все більш поширеними у різних сферах життя, включаючи транспорт, фінанси, медицину, торгівлю, корпоративний доступ та інші. Зростання популярності смарт-карток базується на їх здатності забезпечувати безконтактну та швидку обробку даних, що в свою чергу забезпечує зручність для користувачів та підвищує ефективність різних процесів. Однак, разом зі збільшенням використання смарт-карток зростає і ризик зловживання та атак з боку зловмисників. Такі картки стають об'єктом цільових кібератак через можливість перехоплення даних або несанкціонованого доступу до об'єктів, конфіденційної інформації.

У новому звіті про ринок смарт-карток від дослідницької компанії Marketsandmarkets зазначено, що до 2026 року цей сектор досягне 16,9 млрд доларів, а середньорічний темп зростання буде становити 4,0% з 2021 по 2026 рік [19].

Безконтактна смарт-карта включає вбудований захищений контролер або аналогічний інтелектуальний компонент, внутрішню пам'ять та невелику антену, яка зв'язується із зчитувачами через безконтактний радіочастотний (RF) інтерфейс.

Технології радіочастотної ідентифікації (RFID) або зв'язку ближнього поля (NFC) в основному використовуються для застосування з безконтактними смарт-картками та картками доступу. Пандемія Covid-19 позитивно вплинула на ринок безконтактних смарт-карток, оскільки Всесвітня організація охорони здоров'я (ВООЗ) та уряди всього світу виступають за використання безконтактних рішень

для різних цілей, щоб забезпечити соціальне дистанціювання для стримування поширення коронавірусу. Безконтактні смарт-карти забезпечують простоту, швидкість та зручність для користувачів.

Впроваджені смарт-карти у всіх секторах довели свою високу ефективність у боротьбі з крадіжками та шахрайством. Державні проекти, такі як Aadhar карта в Індії, стимулюють попит на смарт-карти для використання в ряді секторів. Більше того, очікується, що проблеми безпеки, особливо у громадській сфері, сприятимуть зростанню ринку безконтактних карток доступу.

Однак, разом зі збільшенням використання смарт-карток зростає і ризик зловживання та атак з боку зловмисників. Такі картки стають об’єктом цільових кібератак через можливість перехоплення даних або несанкціонованого доступу до об’єктів, конфіденційної інформації.

Тому, кібербезпека смарт-карток набуває все більшої актуальності і вимагає комплексного підходу до її забезпечення. Дослідження та аналіз заходів захисту стають невід’ємною частиною розробки та впровадження сучасних систем безпеки, оскільки вони спрямовані на запобігання можливим загрозам та захисту важливих даних від несанкціонованого доступу.

Метою цієї роботи є проведення об’єктивного дослідження та порівняльного аналізу смарт-карток на базі технологій RFID та NFC у контексті їхньої кібербезпеки. Ці дослідження допоможуть виявити потенційні загрози та вразливості цих технологій, а також розробити ефективні заходи захисту для забезпечення безпеки та конфіденційності даних, збережених на смарт-картках.

Основні завдання дослідження включають вивчення стану сучасних технологій RFID та NFC, аналіз їхнього застосування у смарт-картках та ідентифікацію потенційних загроз для кібербезпеки. Крім того, в рамках роботи будуть розглянуті різні моделі атак та методи захисту, які можуть бути використані для забезпечення безпеки смарт-карток.

1. ТЕХНОЛОГІЇ NFC ТА RFID: ПРИНЦИП РОБОТИ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ

1.1 Історія розвитку смарт-карток та основні принципи роботи

Смарт-картки виникли як результат поєднання потужності мікропроцесорних технологій з можливостями карткових систем. Початкові випадки використання карткових систем відносяться ще до середньовіччя, коли торговці та управляючі використовували великі картонні картки для фіксації товарів, обліку операцій та інших фінансових транзакцій. Проте справжній прорив у розвитку цих систем стався у другій половині XX століття.

У 1970-х роках виникли перші мікропроцесорні картки, які мали здатність зберігати та обробляти інформацію на самій картці. Ці картки мали обмежену потужність та використовувалися головним чином для простих завдань, таких як контроль доступу та зберігання особистої інформації.

У наступному десятилітті з розвитком мікроелектроніки та бездротових технологій з’явилися бездротові смарт-картки. Технології NFC та RFID стали основою для цих нових поколінь карток. NFC, що базується на радіочастотних полях, забезпечує безконтактну передачу даних на короткі відстані, що робить його ідеальним для застосувань, таких як безготівкова оплата та контроль доступу. З іншого боку, RFID, історія якого налічує понад півстоліття, також використовує радіочастотні поля, але має більші дальності передачі, що робить його ефективним для сфер логістики, інвентаризації та слідкування за товарами.

Сьогодні смарт-картки об’єднують у собі мікропроцесорні та бездротові технології, надаючи користувачам широкий спектр можливостей. Вони застосовуються в різних галузях, починаючи від громадського транспорту та закінчуючи фінансовими послугами та охороною об’єктів.

Розробка цієї ідеї в Україні розпочалася у 2003 році, але на той момент втілити її не вдалося. Повноцінна розробка пластикових безконтактних карток розпочалася у 2011 році. Цей проект належить компанії MasterCard, його названо PayPass. У 2012 році був запропонований альтернативний варіант компанією Visa, відомий як PayWave [3].

Успішне впровадження безконтактних технологій в Україні підтверджується зменшенням черг у магазинах, прискоренням роботи з терміналами самообслуговування (наприклад, IBox) та швидкими сплатами товарів і послуг за допомогою карт (наприклад, Monobank).

Смарт-картки, вигляд яких нагадує візитівку або кредитку (рис. 1.1) [27], насправді мають унікальні можливості завдяки інтегрованій схемі. Ці вироби відрізняються за такими ключовими аспектами:

- тип інтегральної схеми, яка використовується;
- метод зчитування та передачі даних;
- сфера використання.

Щодо типу інтегральної мікросхеми, існують різні види смарт-карток:

- картки пам’яті, які зазвичай використовуються для зберігання обмеженого обсягу інформації, наприклад, для проведення платежів на невеликі суми, що є актуальним для транспорту або паркування;
- мікропроцесорні карти, які також призначені для зберігання інформації, але відрізняються підвищеним рівнем захисту;
- карти з криптографічною логікою, що забезпечують захист інформації від несанкціонованого доступу та підробки підписів.

Безконтактні RFID-картки працюють за принципом зчитування даних за допомогою подачі живлення на мікросхему, що вбудована всередині системи.

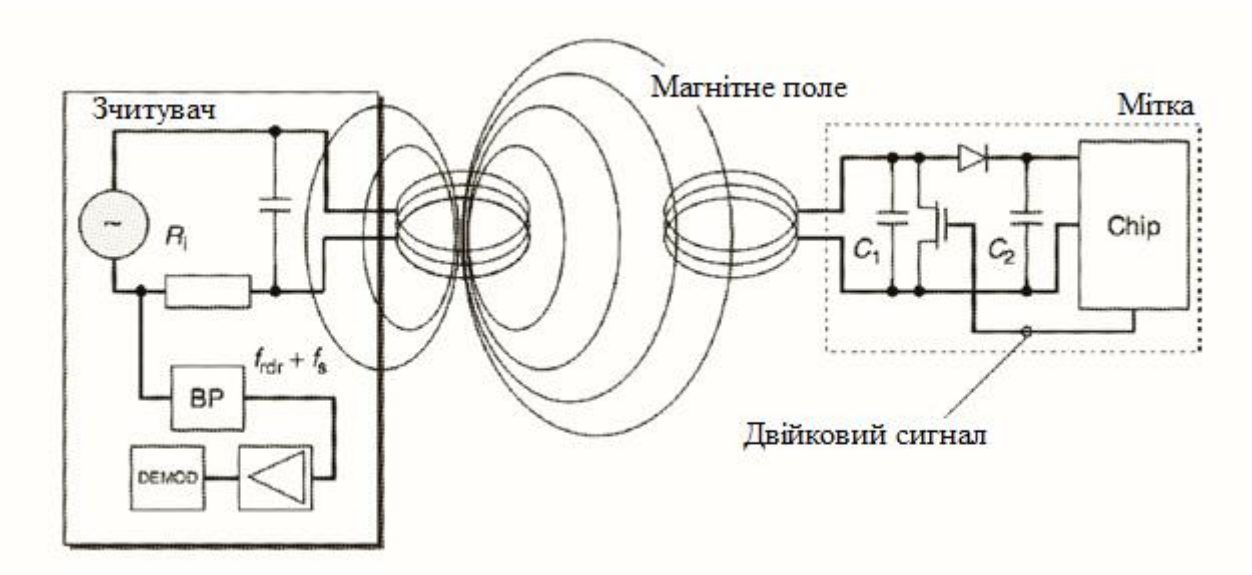


Рисунок 1.1 – Схема роботи смарт-картки

1.2 Принципи роботи технологій NFC та RFID

Технології NFC та RFID забезпечують бездротовий обмін даними між пристроями та об'єктами без прямого фізичного контакту. Ці технології дозволяють передавати інформацію на короткі відстані, зазвичай до 10 см для NFC і від кількох сантиметрів до кількох метрів для RFID, і ідеально підходять для застосувань, де обмін даними має бути швидким і зручним. Вони використовуються в багатьох галузях, включаючи безконтактні платежі, ідентифікацію, логістику та контроль доступу [2].

Технології NFC та RFID базуються на бездротовому обміні даними через радіочастотний сигнал, але вони мають різні принципи роботи та застосування.

1.2.1 Технологія RFID

RFID (Radio Frequency Identification) – це бездротова технологія, яка використовує радіохвилі для ідентифікації та відстеження об’єктів. Застосовується мікрочип всередині тега для зберігання даних. Для прийому та передачі інформації використовуються RFID мітки та RFID зчитувачі. Зовнішній зчитувач сканує пам’ять RFID-мітки та обробляє отримані дані. Програмне

забезпечення відповідає за цілісну роботу системи. Методи автоматичної ідентифікації об’єктів з кожним роком використовуються все частіше. RFID мітки можна класифікувати на активні та пасивні, залежно від наявності живлення.

Активні RFID-мітки мають у собі джерело енергії для забезпечення нею, у той час як пасивні RFID-мітки забезпечують подачу енергії за допомогою радіохвиль, що передаються пристроєм, що зчитує. Активні генерують сигнали на далеких відстанях, оскільки мітка має власне джерело енергії [17].

Пасивні RFID-системи мітки потребують живлення від зчитувача, щоб передати сигнал (причому на коротку відстань до 20 см).

На рис. 1.2 представлено базову схему роботи RFID технології [28].

Рисунок 1.2 – Базова RFID система

RFID може використовуватися в різних галузях промисловості, тваринництві, медицині, бібліотеках та логістиці (рис. 1.3) [29]. В основному роздрібному секторі вказана технологія також відіграє роль у запобіганні крадіжкам. Для пошуку та зчитування інформації з RFID-мітки в RFID-системах

немає необхідності у прямій видимості маркованого об’єкта або контакті мітки та зчитувача. Пошук та зчитування міток можуть виконуватися навіть через упаковку або на відстані від 20 см до 300 м [16].

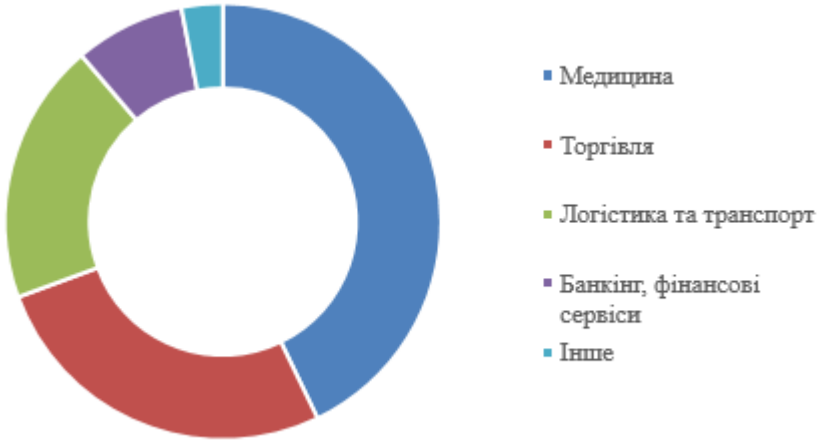


Рисунок 1.3 – Сфери використання технології RFID на 2023 рік

Принципи роботи RFID по своїй суті є удосконаленим алгоритмом радіолокаційного визначення "свій-чужий". Апаратно-програмний технічний комплекс для автоматичного пошуку відмінностей використовує радіохвилі певної частоти. Дані зберігаються в спеціальній мітці (тегу), яку можна приймати, а потім розшифрувати дистанційно за допомогою спеціальних зчитувачів. Технологія має досить простий механізм роботи: інформація записується за допомогою радіохвиль на мікрочип, дані надходять на зчитувач за допомогою радіосигналу вбудованої антени; визначення випромінювальної частоти, налаштування і зчитування відомостей здійснюється автоматично за допомогою сканера.

Як і штрих-коди, мітки RFID можна використовувати для швидкої ідентифікації об’єкта, однак, на відміну від штрих-кодів, кілька міток можна сканувати одночасно й без необхідності фізичного огляду етикетки, таким чином скорочуючи час, витрачений на управління запасами. RFID-мітки також можуть містити набагато більше інформації, ніж штрих-коди, і створювати більш точну

ідентифікацію предметів, відстежувати, контролювати та зберігати дані. Завдяки невеликому розміру RFID-мітки розміщуються в повсякденних предметах, таких як паспорти, бібліотечні книги, одяг і платіжні картки.

Попит на радіочастотну ідентифікацію (RFID) з'явився ще на початку 21-го століття. Однак, система постійно вдосконалюється, використовується для маркування та автоматичної ідентифікації продукції. Але перелік функцій RFID набагато ширший. За допомогою сучасної технології можна ідентифікувати та контролювати рух маркованих об'єктів – як живих, так і неживих.

1.2.2 Технології NFC

NFC – це високочастотна (13,56 МГц) технологія бездротового зв'язку, яка дає змогу двом електронним пристроям взаємодіяти один з одним, коли вони знаходяться на відстані приблизно 4 см, що робить NFC більш адаптивним, ніж RFID, і, крім того, доступним для всіх за допомогою смартфонів. Вона вже широко використовується для безконтактної оплати та контролю доступу, наприклад, у громадському транспорті, але одна з нових можливостей цієї технології полягає в «розумній упаковці» та «розумному маркетингу». NFC можна використовувати для обміну цифровим вмістом, а також для підвищення залучення клієнтів. Розмістивши тег NFC у продукті, клієнти можуть відсканувати тег, щоб дізнатися більше про товар, взяти участь у конкурсах або легко змінити замовлення [18].

NFC – це унікальна безпечна технологія, яка забезпечує виняткову взаємодію з клієнтами та тепер відкрита як для Android, так і для IOS, що надає безмежні можливості щодо залучення та задоволення клієнтів.

Основні принципи безпеки NFC включають:

- обмеження відстані зв'язку;
- використання безпечного протоколу передачі даних;
- обмеження суми платежу;

- захист від копіювання чипу.

Такі заходи роблять безпечним використання технології NFC для різних видів операцій.

Технологія NFC має достатньо широке застосування у різних сферах, таких як, мобільні платежі (дозволяє здійснювати безконтактні платежі за допомогою смартфонів або спеціальних NFC-карток), доступ до об’єктів (для безконтактного відкриття дверей, проходу на транспорт або доступу до офісних приміщень), інтерактивний маркетинг (для створення інтерактивних маркетингових заходів, таких як «розумні» постери або візитівки, які можуть передавати інформацію про товар або посилання) тощо (рис. 1.4) [30].

Рисунок 1.4 – Сфери використання NFC технологій

1.3 Порівняльний аналіз переваг та недоліків технологій NFC та RFID

Порівняльний аналіз переваг та недоліків кожної технології є важливим кроком у виборі найбільш підходящого рішення для конкретного застосування. RFID та NFC відрізняються у своїх можливостях та обмеженнях.

Технологія RFID відома своїми можливостями, щодо широкої автоматизації та ефективності в управлінні логістикою та інвентаризації. Вона може працювати на значні відстані. Однак вартість впровадження системи RFID може бути дуже високою, а деякі системи також можуть мати обмежену дальність зчитування.

Технологія NFC відрізняється своєю зручністю та безпекою, забезпечуючи швидкий та безпечний обмін даними між пристроями. Однак його робоча дальність зчитування та сумісність можуть обмежити його використання у деяких сценаріях.

Порівняльний аналіз також включає оцінку технічних характеристик кожної технології, таких як швидкість передачі даних, можливість одночасного оброблення багатьох міток або пристроїв, витрати на інфраструктуру та підтримку. Так RFID може використовуватися в різних галузях промисловості, тваринництві, медицині, бібліотеках та логістиці. В основному роздрібному секторі вказана технологія також відіграє роль у запобіганні крадіжкам. Для пошуку та зчитування інформації з RFID-мітки в RFID-системах немає необхідності у прямій видимості маркованого об’єкта або контакті мітки та зчитувача. Пошук та зчитування міток можуть виконуватися навіть через упаковку або на відстані від 20 см до 300 м.

У свою чергу NFC більше використовується в мобільних платежах, транспорті, контролі доступу. NFC може зчитувати інформацію лише в діапазоні до 5 см. Технічний прийом, що розглядається, дуже поширився і впровадився в сферу мобільних платежів. Великі платіжні платформи, такі як Google Pay, Samsung Pay, Apple Pay та Fitbit Pay, всі засновані на мітках NFC для зчитування даних [20]. Пристрої, які підтримують NFC, можна використовувати як різні документи. Наприклад, як паспорт або електронне посвідчення особи. Воно може використовуватися всіма видами смарт-карт. Можна зробити транспортні карти, карти ключі та карти для входу в систему. NFC також може використовуватися і в соціальних мережах, для обміну фотографіями, відео, файлами та забезпечити доступ до розрахованих на багато користувачів мобільних ігор.

RFID технологія підтримує лише односторонній зв’язок. Оскільки зчитувач отримує радіохвилі від мітки для зчитування даних. Завдяки електромагнітній індукції, що створюється, RFID-мітка отримує енергію та активує мікрочип

усередині. Мікрочип активується та посилає радіохвилі на зчитувач, який отримує та зчитує дані. Після електромагнітної індукції між ними активна мітка RFID активно посилатиме радіохвилі зчитувачу. На відміну від RFID, NFC вимагає наявності двох комунікаційних пристроїв на відстані кількох сантиметрів один від одного та прямої лінії зв'язку з об'єктом зчитування. NFC може зчитувати лише одну мітку один раз. Крім того, NFC може надавати як односторонній, так і двосторонній зв'язок. Він може використовуватися як пристрій для зчитування або як мітка [12].

1.3.1 Переваги та недоліки технологій RFID та NFC

До основних переваг технології RFID можна віднести:

- високу швидкість зчитування та передачі даних: зчитувач автоматично зчитує десятки пристроїв на секунду, дозволяє перезаписувати та вносити додаткову інформацію;
- зниження впливу людського фактору: автоматичне сканування та запис даних без втручання людини;
- швидкий пошук міток без прямої видимості: діапазон читання радіотега становить 10 метрів і більше, можливе приховане розміщення пристрою та його читання через упаковку;
- безпеку та конфіденційність відомостей: чип має унікальний ID, записані відомості можуть бути засекречені;
- стійкість до агресивних середовищ: мітки розпізнаються через пару, воду, шар бруду, фарби, олії; інформація перекачується за будь-яких умов, стійкість до високих тисків та температур;
- альтернативу іншим видам маркувань: використання в різних середовищах та умовах.

Що стосується недоліків, то можна виділити наступні пункти:

- залежність від електромагнітних перешкод: мітки недоступні для

зчитування у пошкодженому вигляді;

- обмежена відстань зчитування: не всі мітки зчитуються з великої відстані;
- вплив вологи: мітки схильні до негативного впливу вологи.

У NFC технології список переваг буде наступним:

- безпека при близькому контакті: ускладнює перехоплення конфіденційної інформації, низьке споживання енергії;
- швидкі безконтактні платежі: ідеально підходить для швидких безконтактних платежів, імпульс триває 0,1 секунди;
- складна технологія: дозволяє виконувати операції читання/запису;
- різноманітність застосувань: підтримка однорангового обміну, читання карт та смарт-плакатів.

До недоліків відносяться:

- обмежена відстань роботи: працює на малих відстанях (до 10 см);
- невисока швидкість передачі: максимальна швидкість передачі близько 400 кбіт/с;
- не підходить для передачі великих файлів: не може конкурувати з Bluetooth або Wi-Fi в передачі великих файлів.

Вибір між RFID та NFC залежить від конкретних потреб і умов використання. RFID підходить для ситуацій, де потрібне зчитування на великій відстані без прямої видимості, ідеально підходить для логістики, інвентаризації та управління запасами. Проте його висока вартість і чутливість до електромагнітних перешкод можуть стати недоліками.

NFC, зі своєю здатністю до швидких і безпечних транзакцій на коротких відстанях, є оптимальним вибором для безконтактних платежів, доступу до приміщень та обміну даними між пристроями. Вбудована підтримка в смартфонах робить її зручною та економічною, але обмежена дальність і низька

швидкість передачі даних обмежують її використання для великих файлів.

1.4 Приклади стандартів технологій NFC та RFID

Як вже було вище зазначено, NFC та RFID технології мають широке застосування у різних сферах використання. NFC розробляється на основі технології RFID, тобто за своєю природою вони майже однакові та засновуються на передачі сигналу між об’єктами з одним і тим самим розташуванням.

Стандарти цих технологій визначають набір специфікацій та правил, що дозволяють різним виробникам створювати пристрої, що зможуть співпрацювати між собою безпосередньо та ефективно. Це забезпечує сумісність між пристроями різних брендів та робить можливим застосування цих технологій у багатьох галузях. Завдяки стандартам, користувачі можуть використовувати різні пристрої та системи без необхідності у комплексному перекомпонуванні або додатковому програмуванні.

ISO 15693 – це міжнародний стандарт для застосунків, заснованих на технології RFID. Стандарт визначає інтерфейс та специфікації передачі даних для смарт-тегів та зчитувачів, що працюють на частоті 13,56 МГц. Максимальна відстань зчитування міток, що відповідають цьому стандарту, становить 2 метри. Мінімальний робочий діапазон становить 0,15 А/м, а максимальний – 5 А/м. Метод кодування між зчитувачем та міткою використовує імпульсивну модуляцію положення імпульсу і підтримує два режими кодування (256 вибору 1 режиму і 4 вибору 1 режиму) [15]. Кодування даних смарт-мітки для зчитувача відбувається у манчестерському коді (двійковому коді без постійної складової, в якому значення переданого біта визначається напрямком зміни логічного рівня в середині обумовленого заздалегідь часового інтервалу), залежно від того, як налаштований сигнал. Швидкість передачі даних також варіюється. Як показано у табл. 1.2, мітки підтримують як високошвидкісний, так і низько швидкісний зв’язок.

Іншим міжнародним стандартом RFID є ISO 14443. Стандарт визначає передачу та характеристику цієї передачі даних для технологій NFC і RFID, що працюють на частоті 13,56 МГц. Заглиблюючись у принцип стандарту, він визначає передачу даних між двома зчитувачами та мікросхемою ближнього поля: тип A і тип B. Стандарт підтримує передачу даних від 106 кбіт/с до 848 кбіт/с.

Стандарт ISO 14443 в основному застосовується у сферах управління персоналом та ідентифікації за допомогою мікрочипів ближнього радіусу дії.

Основними галузями застосування є картки, управління членством, картки для покупок, електронні документи тощо [9].

Таблиця 1.2 – Продукти стандарту ISO/IEC 15963

Продукт	Опис
Кадровий канал	Є найтиповішим продуктом стандарту ISO 15693. Він підтримує розпізнавання смарт-міток в одномірний та/або двомірній орієнтаціях. Стандартна відстань зчитування міток становить більше 120 см. Вони широко використовуються в таких сферах, як ідентифікація особистості, управління бібліотеками, контроль доступу, відстеження товарів, боротьба із підробками, логістика тощо.
Все спрямований канал	Підтримує тривимірне зчитування міток, відстань між каналами може досягати понад 90 см, підтримує EAS, режим виявлення AFI, підтримує офлайн-застосунок та паралельне використання декількох антен, може автоматично підраховувати та відображати кількість людей, що входять та виходять.
Розумна полиця для книг	Інтелектуальна книжкова полиця – це високопродуктивна система управління книгами в режимі реального часу для бібліотек, що використовує технологію RFID для ідентифікації книг на рівні одиниць, а також виконує такі функції, як відстеження книг, інвентаризація, запити на книги, статистика.

2. ОГЛЯД, АНАЛІЗ ТА ДОСВІД ВИКОРИСТАННЯ RFID ТА NFC ТЕХНОЛОГІЙ, RFID ТА NFC СМАРТ-КАРТОК НА МІЖНАРОДНОМУ ТА НАЦІОНАЛЬНОМУ РІВНЯХ

2.1 Розвиток технологій RFID та NFC на міжнародному рівні, їх розповсюдження та застосування у різних країнах світу

На міжнародному рівні, технології RFID та NFC відіграють ключову роль у вдосконаленні різноманітних аспектів бізнесу та побуту. RFID, як бездротова технологія ідентифікації, стала необхідною для ефективного управління логістикою, ведення інвентаризації та забезпечення безпеки в різних галузях, включаючи виробництво, роздрібну торгівлю, транспортні послуги та охорону. Її застосування поширюється від відстеження товарів у постачальницькому ланцюжку до контролю доступу до будівель і транспортних систем.

На міжнародному рівні відбувається активна розробка стандартів і протоколів для цих двох технологій, що сприяє їх впровадженню в різних країнах і секторах. Крім того, заохочуються дослідження та інновації для нових застосувань, які можуть розширити використання RFID і NFC в тому числі у виробництві, охороні здоров’я, транспорті та інших секторах. Цей безперервний розвиток і розширення сфер застосування робить RFID і NFC ключовою технологією в цифровій трансформації сучасного суспільства.

Розповсюдження та застосування технологій RFID та NFC відрізняються в різних країнах світу в залежності від технічного розвитку, економічних факторів та культурних особливостей. Однак, ці технології стають все більш популярними та широко використовуються в усьому світі (рис. 2.1) [31].

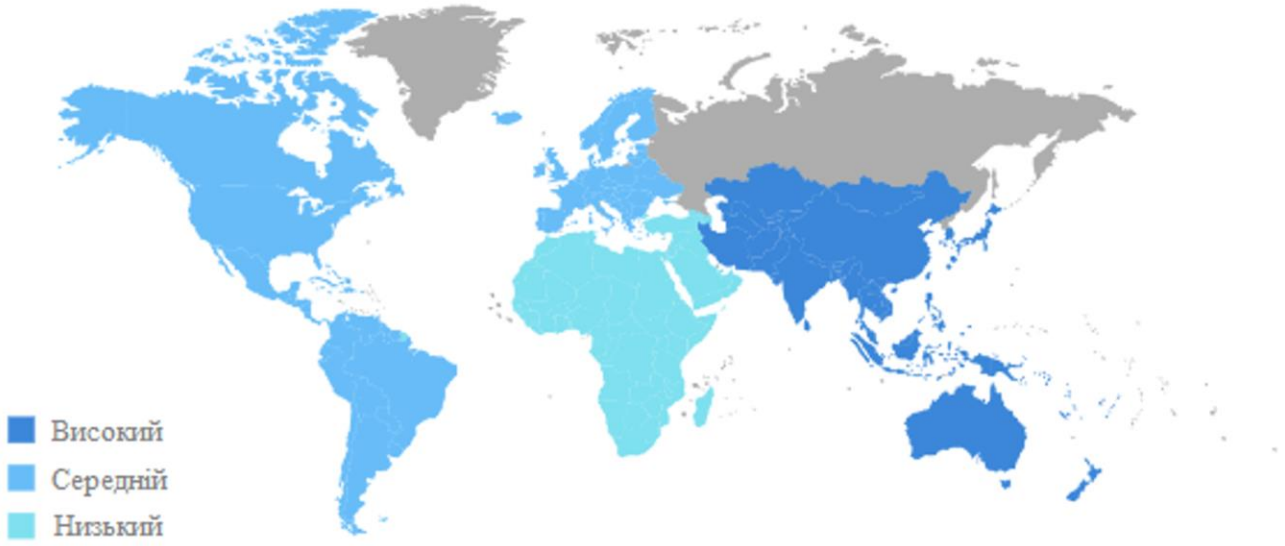


Рисунок 2.1 – Міжнародний ринок смарт-карток

У розвинених країнах, таких як Сполучені Штати Америки, Японія, країни Західної Європи, RFID та NFC широко використовуються в різних галузях, таких як:

- логістика (впроваджується технологія RFID для відстеження товарів та оптимізації логістичних процесів);
- платіжні системи та транзакції (міжнародні банки та фінансові установи впроваджують технологію NFC в банківських картках та мобільних застосунках для зручних та безпечних бездротових платежів);
- транспортні системи (для громадського транспорту використовують технологію NFC для безконтактної оплати проїзду. Так, наприклад, у Лондоні система оплати транспорту "Oyster Card" використовує NFC-карти, які можна просто притримати біля читача під час входу та виходу з транспорту, щоб здійснити оплату);
- контроль доступу (міжнародні корпорації та установи використовують RFID технологію для контролю доступу до своїх приміщень чи об’єктів. У таких системах кожен співробітник або гість може мати RFID картку або браслет, який дозволяє або обмежує їхній доступ до різних зон або приміщень) тощо.

Загалом, хоча рівень розповсюдження та застосування технологій RFID та NFC може варіюватися в різних країнах, їхнє значення та потенціал у сучасному світі надзвичайно великі, і ці технології продовжують широко розвиватися та застосовуватися в усьому світі.

2.1.1 Приклад використання технології RFID у світі

Італійське містечко Мільяніко, що в провінції К'єті, є успішним прикладом використання технології RFID для оцифрування і автоматизації обліку управління відходами. Як і багато інших італійських міст, в Мільяніко за останні кілька років активно розвивалась модель Pay as You Throw (PAYT). Це модель ціноутворення для утилізації твердих побутових відходів. З користувачів стягується ставка в залежності від кількості та типу відходів, які вони викидають. Статистика за 2021 рік показує, що в чверті італійських міст вже працює модель PAYT. Система збору сміття, заснована на RFID технології, протягом багатьох років демонструє хороші результати: відсоток сировини, що переробляється, доходить до 70%, а деякі райони досягають і 85%, як, наприклад, місто Мільяніко [5]. Згідно системи PAYT, сміттєві баки й мішки ідентифікуються мітками радіочастотної ідентифікації, а співробітники зі збору отримують зчитувачі міток або браслети для сканування. Скануючи мітку, співробітник фіксує і передає в систему дані про всі види відходів, що потрапили в конкретний сміттєвий контейнер: вторинну сировину, органічні і несортовані відходи або надзвичайно небезпечні компоненти. Використання системи надає можливість отримувати більш об'єктивні дані, допомагає мінімізувати людську помилку і зменшити кількість претензій. Важливо відзначити, що нова технологія дозволить жителям краще опанувати сортування сміття і переглянути свої звички.

2.1.2 Приклад використання технології NFC у світі

Один із реальних прикладів використання технології NFC спостерігається у Стокгольмі, Швеція, де впроваджується система велопрокату під назвою

"Stockholm City Bikes". Ця система дозволяє мешканцям та відвідувачам міста орендувати велосипеди для короткострокового використання.

Кожен велосипед обладнаний спеціальним замком з технологією NFC. Користувачам, які бажають орендувати велосипед, потрібно просто доторкнутися своєю NFC-карткою або NFC-смартфоном до замка на велосипеді. Це активує систему та дозволяє користувачеві відкрити замок і взяти велосипед. Після закінчення користування велосипедом, користувач повертає його на будь-яку з установлених станцій у місті та знову використовує свою NFC-картку або смартфон для повернення велосипеда та завершення прокату [6].

Ця система дозволяє мешканцям та відвідувачам міста легко та зручно користуватися велосипедами для поїздок по місту, сприяючи активному способу життя та зменшенню викидів CO_2. Технологія NFC у цьому випадку допомагає автоматизувати процес оренди та повернення велосипедів, роблячи його більш ефективним та зручним для користувачів.

2.2 Застосування смарт-карток з технологіями RFID та NFC у різних галузях на міжнародному рівні

Смарт-картка (чип-картка або інтелектуальна карта) – це пластикова карта, в яку вбудована електроніка, яка дозволяє зберігати та обробляти дані. Основна особливість смарт-карток полягає в тому, що вони мають мікрочип або мікропроцесор, який може виконувати різноманітні функції, від зберігання особистої інформації до виконання операцій з фінансами або контролю доступу.

До основних характеристик смарт-карток належать:

- зберігання даних (смарт-картки можуть зберігати різні типи інформації, такі як особисті дані, фінансові дані, медичні записи, доступові коди та інше);
- обробка даних (завдяки вбудованому мікропроцесору смарт-картки можуть виконувати різні обчислення та операції безпеки над збереженими даними);

- безпека (смарт-картки зазвичай мають вбудовані механізми захисту, такі як шифрування даних та використання паролів, для захисту інформації від несанкціонованого доступу);
- безконтактна технологія (деякі смарт-картки можуть працювати за безконтактним принципом, використовуючи технології, такі як RFID або NFC, що дозволяє зчитувати та записувати дані без прямого контакту з карткою);
- різноманітність застосувань (смарт-картки застосовуються у багатьох галузях, включаючи фінансові послуги, громадський транспорт, охорону здоров'я, програми лояльності, ідентифікацію та контроль доступу).

У загальному, смарт-картка – це універсальний інструмент для зберігання та обробки різних видів інформації, що забезпечує зручність, безпеку та ефективність у багатьох сферах діяльності.

Використання смарт-карток з технологіями RFID та NFC дозволяє підвищити ефективність, зручність та безпеку в різних сферах діяльності. Однією із ключових переваг є швидке та безпечне проведення транзакцій без необхідності фізичного контакту з платіжним терміналом чи іншим пристроєм. Наприклад, у фінансових послугах, використання безконтактних смарт-карток дозволяє клієнтам швидко розраховуватися за товари та послуги, зменшуючи час очікування в черзі та покращуючи загальний досвід покупки.

У галузі громадського транспорту, смарт-картки дозволяють пасажирам оплачувати проїзд швидко та зручно, просто наблизивши картку до читача при вході та виході з транспортного засобу. Це спрощує процес та допомагає зменшити затори на зупинках, що підвищує загальний рівень обслуговування населення.

У сфері безпеки та доступу, смарт-картки забезпечують більш високий рівень автентифікації осіб і контролю доступу до об'єктів. Вони можуть бути інтегровані з системами моніторингу та відстеження, що дозволяє оперативно реагувати на будь-які недоречні події та забезпечує безпеку приміщень та

обладнання.

Крім того, смарт-картки використовуються у програмах лояльності та системах охорони здоров’я для ідентифікації користувачів та забезпечення надійного зберігання та обміну особистої інформації. Це сприяє зручності та точності управління клієнтськими даними та поліпшує якість обслуговування.

2.3 Вивчення успішних та неуспішних проектів впровадження смарт-карток на базі RFID та NFC на національному рівні

Національний рівень використання смарт-карток на базі технологій RFID та NFC відзначається різноманітністю ініціатив у різних галузях. Завдяки постійному розвитку технологій та зростанню інтересу до безконтактних комунікаційних технологій, смарт-картки стають все більш популярними і використовуються в різних сферах життя. Вони забезпечують не лише зручність для користувачів, а й підвищують ефективність бізнес-процесів, забезпечують безпеку та прискорюють різноманітні транзакції і взаємодії. Такий широкий спектр застосувань відображає різноманіття викликів та можливостей, що відкриваються завдяки впровадженню цих технологій у національному масштабі, створюється багато проектів, що відповідно використовують по максимуму ці технології. Будь-який проект можу бути як успішним, так і навпаки – зазнати невдачі.

Одним із таких успішних прикладів може бути проект в галузі охорони здоров’я, де смарт-картки використовуються безпосередньо для зберігання медичної інформації та ідентифікації пацієнтів. Наприклад, у Сингапурі була створена програма HealthHub. Це інтегрована платформа електронного здоров’я, що дозволяє мешканцям зберігати свої медичні записи на спеціальних смарт-картках та легко отримувати доступ до них у будь-який час. HealthHub надає різноманітні функції та сервіси, включаючи доступ до електронних медичних записів, планування прийому до лікаря, моніторинг показників здоров’я, онлайн-

консультації з лікарями, інформаційні ресурси про захворювання та здоровий спосіб життя, а також інструменти для ведення здорового способу життя, включаючи програми фітнесу та харчування.

Одним із ключових аспектів HealthHub є партнерство з різними медичними установами, лікарями та провайдерами послуг, що дозволяє користувачам швидко та зручно отримувати доступ до медичних послуг, незалежно від їх місця перебування чи графіку. Крім того, програма також пропонує інструменти для відстеження та аналізу показників здоров'я, що допомагає користувачам краще розуміти їх стан здоров'я та приймати більш обізнані рішення щодо свого здоров'я.

Безконтактні смарт-картки широко використовуються для контролю доступу до приміщень урядових установ, бізнес-центрів та інших об'єктів. Так, наприклад, в США програма TWIC (Transportation Worker Identification Credential) використовує безконтактні смарт-картки для ідентифікації та контролю доступу працівників, які працюють у транспортній галузі. Смарт-картка TWIC містить унікальні ідентифікаційні дані працівника, такі як фотографія, біометричні дані (наприклад, відбитки пальців) та іншу інформацію, необхідну для перевірки особи та його прав доступу. Карта використовує технології RFID або NFC для безконтактного зчитування, що дозволяє швидко та зручно перевіряти особу та її статус.

Успішне впровадження програми TWIC дозволяє підвищити рівень безпеки в транспортній галузі, контролюючи доступ працівників до критичних об'єктів та ресурсів. Програма допомагає зменшити ризик незаконного доступу або терористичних загроз у транспортних вузлах та портах.

Проте, існують і приклади неуспішного використання смарт-карток у програмах ідентифікації та контролю доступу. Наприклад, деякі системи можуть стикатися з технічними проблемами, такими як непрацездатність читачів карток або несправності в програмному забезпеченні. Також можуть виникати проблеми

з безпекою даних, якщо картки не захищені від крадіжки чи копіювання. Один з прикладів неуспішного використання смарт-карток у сфері ідентифікації та контролю доступу можна побачити в Індії з їхньою програмою Aadhaar [19].

Aadhaar – це ідентифікаційна система, яка використовує унікальні біометричні та особисті дані кожної особи для видання 12-значного ідентифікаційного номера. Однак, програма стикається з кількома проблемами, серед яких:

- Проблеми з безпекою даних: інформація у системі Aadhaar може бути підвернена ризику порушення приватності та зловживання через нестабільність системи безпеки даних.
- Технічні недоліки: інколи читачі біометричних даних не працюють належним чином, що призводить до затримок у використанні карток та надає недостатню ефективність при реєстрації або перевірці особи.
- Проблеми доступу: іноді люди можуть мати обмежений доступ до послуг або важкість використання карток через технічні або інфраструктурні обмеження.
- Відсутність дублювання: у разі втрати або пошкодження картки можуть виникнути проблеми із втратою доступу до важливих послуг.

Ці проблеми створюють значні виклики для програми Aadhaar у Індії, що вказує на важливість ретельного розроблення та впровадження смарт-карток у програмах ідентифікації та контролю доступу.

2.4 Аналіз технічних та організаційних аспектів використання смарт-карток з технологіями RFID та NFC

Використання смарт-карток з технологіями RFID та NFC вимагає уважного управління з організаційної та технічної точок зору. Організації повинні ретельно спланувати процес впровадження цих технологій, враховуючи різноманітність проектів та їхніх вимог.

Планування та впровадження смарт-карток вимагає детального аналізу і стратегічного підходу. Перш за все, потрібно визначити мету використання смарт-карток і визначити, які завдання вони мають вирішувати. Далі необхідно обрати відповідну технологію – RFID або NFC – залежно від потреб і можливостей організації.

Після вибору технології необхідно вибрати надійного постачальника смарт-карток та обладнання для них. Важливо обрати постачальника з досвідом і гарною репутацією, щоб уникнути проблем з якістю та обслуговуванням. Далі необхідно розробити програмне забезпечення для смарт-карток, яке відповідало б потребам організації. Це може включати в себе програми для обліку сплати, контролю доступу, ідентифікації користувачів та інші функції.

Забезпечення безпеки особистих даних користувачів є критично важливою складовою використання смарт-карток. Організації повинні приділяти належну увагу заходам захисту даних, щоб уникнути можливих порушень і втрати довіри користувачів. В першу чергу, необхідно застосовувати сучасні методи шифрування для захисту інформації, що зберігається на смарт-картах. Це дозволить унеможливити несанкціонований доступ до особистих даних та інформації про транзакції. Додатково, організації повинні ретельно контролювати доступ до систем, які обробляють дані зі смарт-карток. Це включає в себе встановлення строгих прав доступу та моніторинг дій персоналу з метою виявлення можливих загроз безпеці. Поряд з цим, важливо постійно вдосконалювати заходи захисту відповідно до змін у загрозах та технологіях. Регулярні аудити безпеки допоможуть виявити слабкі місця в системі та прийняти необхідні заходи для їх усунення.

Для успішного впровадження смарт-карток необхідно забезпечити їхню сумісність з існуючими системами управління доступом, обліку сплати, системами безпеки та іншими внутрішніми системами організації. Це означає, що організація повинна ретельно розглянути, як смарт-картки інтегруються з

існуючими системами, щоб забезпечити їхню взаємодію та співпрацю. Наприклад, якщо організація використовує систему контролю доступу на основі біометричних даних, смарт-картки повинні бути інтегровані з цією системою, щоб дозволити доступ користувачам за допомогою картки та їхніх біометричних даних. Крім того, інтеграція з існуючими системами також може включати синхронізацію даних між різними системами, щоб забезпечити їхню актуальність та консистентність. Наприклад, інформація про користувачів, яка зберігається на смарт-картках, повинна бути відображена в системі обліку сплати, щоб забезпечити точність фінансової інформації та ефективне управління рахунками користувачів.

Для досягнення успішної інтеграції з існуючими системами, організація повинна мати чіткий план впровадження, який враховує всі аспекти інтеграції, включаючи технічні, функціональні та організаційні аспекти. Також важливо провести відповідне тестування та валідацію інтеграції, щоб переконатися, що всі системи працюють разом належним чином і задовольняють потреби організації.

Технічна підтримка виконує ключову роль у забезпеченні безперебійної роботи системи смарт-карток на основі технологій RFID та NFC. Організації повинні мати належно підготовлений технічний персонал, який буде відповідати за підтримку та обслуговування смарт-карток.

Основні завдання технічної підтримки включають в себе виявлення та усунення будь-яких технічних проблем, що виникають у процесі використання смарт-карток. Це може включати в себе діагностику проблем, відновлення роботи карток після втрати зв’язку або пошкодження, а також відновлення доступу до даних, якщо вони втрачені або пошкоджені. Крім того, технічна підтримка також включає в себе оновлення програмного забезпечення смарт-карток та забезпечення їхньої сумісності з оновленнями інших систем організації. Це може включати в себе встановлення нових версій драйверів, патчів безпеки або програмного забезпечення, які покращують функціональність та безпеку

смарт-карток.

Впровадження нової технології смарт-карток на базі технологій RFID та NFC може вимагати тренінгу користувачів. Організації повинні забезпечити належний тренінг для персоналу, щоб вони могли ефективно користуватися смарт-картками. Тренінг користувачів включає в себе ознайомлення з основними принципами роботи смарт-карток, їхніми можливостями та обмеженнями. Це може включати в себе навчання користувачів, як правильно наближати картки до читачів, як використовувати різні функції та сервіси, які доступні за допомогою смарт-карток, а також як забезпечити безпеку своїх даних під час використання карток. Тренінг також може включати в себе навчання персоналу, як правильно використовувати програмне забезпечення, пов’язане із смарт-картками, як відслідковувати використання карток та звітувати про них, а також як взаємодіяти з технічною підтримкою у разі виникнення проблем.

Важливим елементом тренінгу є інформування користувачів про будь-які зміни у політиці використання смарт-карток, включаючи правила безпеки та конфіденційності даних. Крім того, періодичні нагадування та оновлення тренінгу можуть бути корисними для забезпечення того, що персонал завжди залишається інформованим та вміє ефективно користуватися смарт-картками.

3. МОДЕЛІ ЗАГРОЗ, ПОРУШНИКА ТА БЕЗПЕКИ ДЛЯ RFID ТА NFC ТЕХНОЛОГІЙ

3.1 Типи атак на смарт-картки

Загалом, перелік можливих атак на смарт-картки випливає з їхніх функцій. До них відносяться автентифікація, зберігання ключової інформації та криптографічні операції в довіреному середовищі. Безконтактні смарт-картки поділяються на дві категорії:

- Смарт-картки, що використовують ISO/IEC 14443 як транспортний рівень і спеціальні власні протоколи для взаємодії на прикладному рівні. До цієї категорії відносяться картки сімейства Mifare, HID iCLASS тощо.
- Смарт-карти, які використовують ISO/IEC 14443 як транспортний рівень і ISO/IEC 7816-4 у поєднанні з іншими прикладними протоколами для взаємодії на прикладному рівні (прикладний протокол блок даних, APDU). До цієї категорії відносяться всі банківські картки, смарт-картки, власниками яких є закриті ключі електронних підписів та інші продукти.

Мотиви атак на смарт-картки поділяються на декілька категорій:

- Фінансові крадіжки (використовування вкрадених або підроблених смарт-карток для вчинення фінансових шахрайств, таких як витягнення грошей з банкоматів або здійснення платежів на ім’я потерпілого).
- Уособлені атаки (отримання доступу до комп’ютерних систем або інших пристроїв контролю доступу, використовуючи смарт-картку як проміжну мету. Наприклад, зловмисник може намагатися використати картку доступу для отримання доступу до конкретної комп’ютерної системи для отримання конфіденційної інформації).

- Напад на приватне життя (отримання більшого обсягу інформації про особу, ніж те, що передбачено протоколом. Наприклад, зловмисник може намагатися здійснити атаку на особисте життя, щоб отримати доступ до особистої інформації про користувача смарт-картки, такої як ім’я, адреса або інші конфіденційні дані).
- Атаки, коли зловмисник прагне популярності (привернення уваги або підвищення репутації зловмисника. Наприклад, зловмисник може намагатися зламати смарт-картку з метою демонстрації своїх навичок або для того, щоб отримати популярність серед інших хакерів або в Інтернет-спільноті).

Окрім того, атаки можна класифікувати відносно часу їхнього проведення – можна використовувати фази життєвого циклу смарт-картки (рис. 3.1) [20]. У такому випадку класифікація таких атак буде мати наступний вигляд:

- атаки на етапі розробки смарт-карток;
- атаки на етапі виробництва смарт-карт;
- атаки на етапі застосування смарт-карт.

Рисунок 3.1 – Життєвий цикл виробництва смарт-картки

У рамках забезпечення безпеки смарт-карти виділяють три основні рівні атаки: соціальний, фізичний і логічний.

Атаки на соціальному рівні це, насамперед, атаки на людей, які мають відношення до смарт-карт, незалежно від їх фази життєвого циклу. Організаційні заходи безпеки грають тут ключову роль у відверненні і виявленні таких атак, тоді як технічні заходи стають вторинними. Наприклад, установка непрозорих екранів по обидва боки від клавіатури може убезпечити від перехоплення PIN-коду. Однією з організаційних мір безпеки щодо програмістів смарт-карт може бути регламентація у правових документах процесу розробки та використання відкритих процедур. Ступінь безпеки в цьому випадку буде визначатися секретними ключами.

Атаки на фізичному рівні потребують фізичного доступу до апаратних засобів мікроконтролера смарт-карти, що ускладнює завдання для зловмисника і вимагає складного технічного обладнання. Ці атаки можуть бути статичними або динамічними. У статичних атаках зловмисник не потребує працюючого мікроконтролера і не обмежується часом, тоді як динамічні атаки передбачають наявність працюючого мікроконтролера, спеціального вимірювального обладнання і високу швидкість обробки даних. Основні види фізичних атак представлені у таблиці 3.1.

Таблиця 3.1. – Основні види фізичних атак

Вид атаки	Опис
Пасивні	Пасивні атаки, такі як атаки за енергоспоживанням (SPA і DPA) [21], атаки за часом [22] і атаки за електромагнітним випромінюванням, ґрунтуються на спостереженнях за різними фізичними параметрами, які модулюються ключовою інформацією. Ці атаки досить добре вивчені та розглянуті у відкритій літературі, проте існує система заходів для їх запобігання.
Активні без проникнення	Активні атаки без проникнення, такі як диференціальні атаки на основі наведення апаратних помилок (DFA) [23] та енергетичні атаки, ґрунтуються на створенні випадкових апаратних помилок під час виконання криптоалгоритму та їх подальшому аналізі.

Продовження таблиці 3.1.

	Ці атаки можуть включати маніпуляцію тактовими сигналами, постачання мікросхем енергії, вплив лазером або пучком електронів та інші методи. На відміну від пасивних атак, для DFA поки що не існує добре відпрацьованої практичної моделі захисту. Однак фірми-виробники смарт-карт активно працюють над розробкою таких моделей і конкретних механізмів захисту.
Активні з проникненням	Активні атаки з проникненням, такі як атаки на основі проб, включають проникнення в саму мікросхему. Ці атаки можуть комбінуватися з різними методами зняття корпусу мікросхеми та шарового доступу до топології кристала (методи обробки), та іншими атаками. Навички виконання активних атак з проникненням зазвичай є лише у невеликої кількості комерційних та правоохоронних організацій, і лише маленька частина цієї інформації зазвичай публікується.

Атаки на логічному рівні зазвичай базуються на класичному криптоаналізі, використанні відомих несправностей операційної системи смарт-карти та впровадженні "троянських коней" у виконавчий код програми смарт-карти. За статистикою, ці атаки часто виявляються найбільш успішними.

На практиці зазвичай здійснюються атаки змішаного типу.

3.1.1 Безконтактні смарт-картки з унікальними форматами обміну даними

Дії зловмисника можуть бути спрямовані на втручання в обмін даними між передавачем і приймачем. До цієї категорії належать такі типи атак: підслуховування, "людина посередині" (MITM), відмова в обслуговуванні (DoS). Атаки цієї категорії не є успішними, оскільки стандарти ISO/IEC 18000-3 та ISO/IEC 14443 не передбачають криптографічного захисту. У цьому випадку успіх дій зловмисника залежить від близькості місця розташування та досконалості обладнання хакера. У різних дослідженнях при пасивному прослуховуванні були досягнуті відстані від 2-3 м до 18 м [10, 11]. Якщо при пасивному прослуховуванні відсоток успішності перехоплення всієї переданої інформації при розміщенні пристрою для прослуховування на картці зі стандартною робочою відстанню 10 см, то зрозуміло, що перехоплення всієї

інформації, що передається, є абсолютним. Однак, здійснити повномасштабну MITM-атаку неможливо через фізичні обмеження, такі як швидкість поширення радіохвиль і час відгуку обладнання.

Хорошим прикладом в цьому випадку є Opal Card (рис.3.2) [18], одна з найпоширеніших смарт-карт в Австралії, яка використовується для оплати громадського транспорту. Opal Card має свій унікальний формат обміну даними, що використовується для зчитування та запису інформації про подорожі.

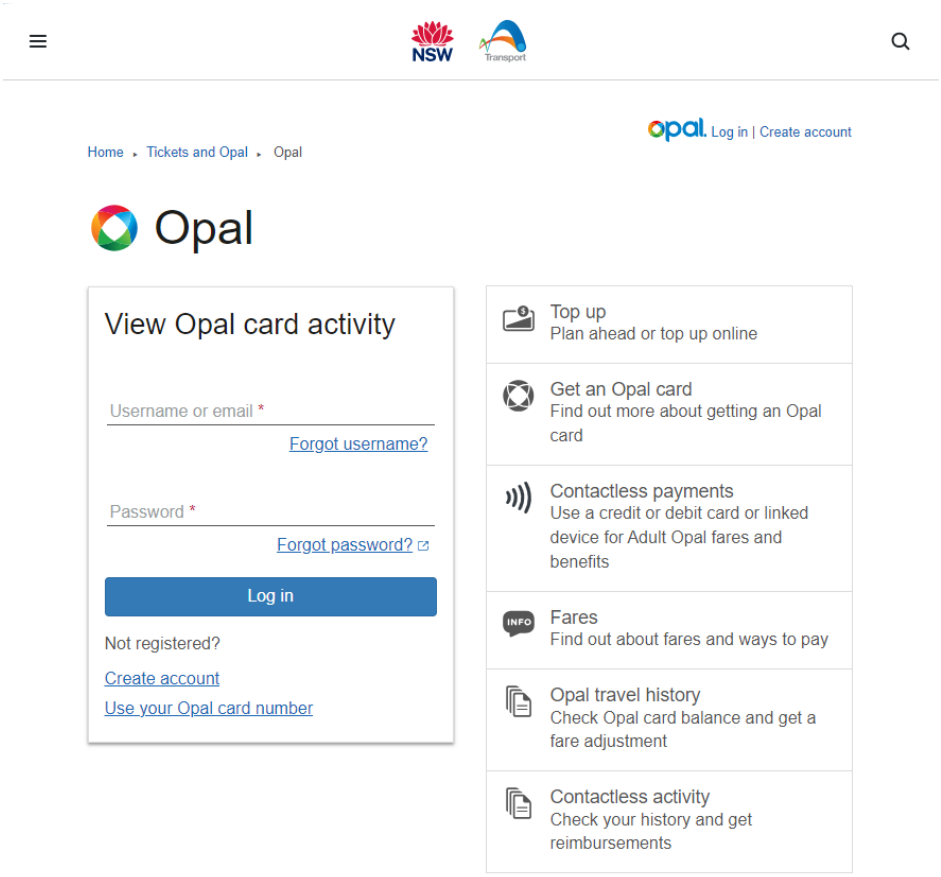


Рисунок 3.2 – Сторінка входу/реєстрації для користувачів Opal Card

Хоча Opal Card використовується для безконтактного проходу через турнікети та оплати послуг громадського транспорту, вона також може бути предметом атак зловмисників, які спрямовані на перехоплення та зміну даних, що передаються між карткою та читачем. Атаки такого роду можуть включати підслуховування, MITD і DoS, які можуть бути виконані з використанням

спеціального обладнання та програмного забезпечення.

Однак, стандарти безпеки Opal Card передбачають захист від таких атак. Наприклад, дані на картці можуть бути зашифровані алгоритмами шифрування, які ускладнюють можливість перехоплення та розшифрування інформації [18]. Крім того, використання автентифікації та авторизації дозволяє перевіряти легітимність користувача та запобігає несанкціонованому доступу до даних на картці.

Австралійська компанія Transport for NSW, відповідальна за систему Opal, регулярно вдосконалює та покращує безпеку карток, враховуючи потенційні загрози та вразливості. Наприклад, вони можуть оновлювати програмне забезпечення на картках для виправлення виявлених вразливостей або впроваджувати нові методи шифрування для підвищення рівня захисту даних. Тим не менш, заходи захисту, розроблені виробником, спрямовані на мінімізацію цих ризиків та забезпечення безпеки користувачів.

3.2 Ризики втрати конфіденційності даних через використання смарт-карток

Використання смарт-карток може належно спростити і поліпшити багато аспектів побуту та бізнесу, проте воно також пов’язане з ризиками, які потребують уважного розгляду та заходів захисту. Необережне використання смарт-карток може призвести до витоку конфіденційної інформації, несанкціонованого доступу до систем та фінансових втрат. Тому важливо вживати всі необхідні заходи безпеки та ретельно вивчати потенційні ризики перед впровадженням цієї технології.

Крадіжка та втрата смарт-карток, особливо тих, що мають технології RFID та NFC, може стати серйозним ризиком для безпеки та конфіденційності. У випадку втрати або крадіжки карти, зловмисники можуть мати доступ до конфіденційної інформації, яка зберігається на ній. Це може стати початком

широкомасштабної ідентифікаційної або фінансової крадіжки.

Якщо картка використовується для безконтактних платежів, втрата чи крадіжка відповідно може призвести до фінансових втрат для власника. Зловмисники можуть використовувати втрачену або викрадену карту для проведення транзакцій без дозволу власника, що може призвести до непередбачуваних витрат і збитків.

Перехоплення даних є не менш серйозною проблемою, пов’язаною із використанням смарт-карток, особливо тих, що використовують технології RFID та NFC. Так зловмисники можуть використовувати спеціальне обладнання, таке як RFID-сканери або NFC-читачі, для перехоплення безконтактних сигналів, що передаються між карткою та зчитувачем.

Деякі картки можуть мати вразливості в протоколах передачі даних, що можуть бути використані зловмисниками Ця вразливість може дозволити їм отримати доступ до конфіденційної інформації, яка зберігається на картці, або навіть використовувати картку для несанкціонованого доступу до систем або приміщень. Наприклад, якщо зловмисники змінюють або перехоплюють дані, що передаються між карткою та зчитувачем, вони можуть зламати систему безпеки та отримати доступ до обмежених ресурсів або інформації.

Соціальний інжиніринг представляє собою ще один значний ризик. Зловмисники можуть використовувати різні методи соціального інжинірингу для отримання доступу до смарт-карток або конфіденційних даних, шляхом маніпуляції користувачів та використання психологічних трюків. Наприклад, зловмисники можуть намагатися переконати користувачів надати їм особисту або фінансову інформацію, шляхом вигадування вигідних пропозицій або створення ситуацій, що вимагають негайного реагування. Вони також можуть використовувати психологічний тиск або маніпуляцію, щоб змусити користувачів виконати їхні вимоги. Основні форми соціального інжинірингу подані у табл. 3.2.

Таблиця 3.2 – Форми соціального інжинірингу із прикладами атак стосовно смарт-карток

Форма	Опис
Фішингові атаки через електронну пошту або текстові повідомлення	Зловмисники можуть надсилати підроблені електронні листи або повідомлення, вигадуючи, що вони є представниками банку або іншої фінансової установи, та просити отримати конфіденційну інформацію про смарт-картку, таку як номер карти або коди безпеки.
Підроблені веб-сайти або застосунки	Зловмисники можуть створювати підроблені веб-сайти або мобільні застосунки, які виглядають як офіційні системи управління смарт-картками, та запитувати від користувачів конфіденційну інформацію.
Телефонні шахрайства	Зловмисники можуть здійснювати телефонні дзвінки, вигадуючи себе представниками банку чи іншої організації, і намагатися переконати власника смарт-картки надати їм конфіденційну інформацію або здійснити платежі за допомогою підробленої інформації.
Фізичний доступ до картки	Зловмисники можуть намагатися викрасти смарт-картку безпосередньо з власником або використовувати скримери, щоб перехопити дані з картки під час її використання в банкоматах або платіжних терміналах.
Фізична підміна картки	Зловмисники можуть намагатися фізично підмінити смарт-картку у власника або використовувати спеціальне обладнання для крадіжки даних з картки, наприклад, за допомогою скримерів або інших пристроїв.

3.3 Засоби захисту від атак на смарт-картки з технологіями RFID та NFC

Сучасні технології RFID та NFC, які використовуються в смарт-картках, дозволяють безпечно проводити безконтактні транзакції та ідентифікувати осіб. Проте, разом із зручністю використання цих технологій приходять і ризики безпеки. Зловмисники можуть намагатися перехопити інформацію зі смарт-карток для вчинення шахрайства або крадіжки фінансових даних.

Одним із основних заходів безпеки використання смарт-карток є криптографічні протоколи. Саме використання шифрування даних допомагає ускладнити спроби перехоплення інформації, переданої між карткою та зчитувачем. Протоколи діляться на протоколи простої та строгої автентифікації,

а також протоколи з розголошенням нульових знань (ZK-протоколи).

Найбільш вразливими є протоколи простої автентифікації та однією з таких вразливостей є те, що після передачі пред'явником свого пароля, перевірник може використовувати цей пароль і виступати в ролі пред'явника. У той час як протоколи строгої автентифікації є більш безпечними, оскільки пред'явник зобов'язаний продемонструвати знання секретного ключа, і передана інформація не може бути прямо використана перевірником. ZK-протоколи були розроблені для вирішення проблеми та спрощення процедури автентифікації, але не зниження рівня її безпеки. Такі протоколи дозволяють демонструвати знання секрету, але при цьому перевірник не може отримати додаткову інформацію про секрет пред'явника. Вони можуть застосовуватися в системах, де вимагається висока безпека, таких як системи на основі смарт-карт, але вони вимагають значних обчислювальних ресурсів та пам'яті, що підвищує вартість смарт-карт [20].

Іншим заходом безпеки можна виділити фізичні заходи захисту. Вони можуть включати застосування спеціальних оболонок або футлярів для смарт-карток, які додатково захищають картку від фізичних пошкоджень, зношення та втрати. Деякі фізичні заходи захисту можуть включати встановлення механічних перешкод (або механізмів блокування), що ускладнюють доступ до смарт-картки без дозволу. Крім того, виробники смарт-карт іноді вбудовують в картки додаткові захисні елементи, такі як мікрочипи або сенсори, які можуть виявляти спроби несанкціонованого доступу або використання картки. Ці елементи можуть активувати спеціальні заходи безпеки, такі як блокування доступу до даних чи автоматичне повідомлення про можливу крадіжку або втрату картки.

Безумовно, що доволі важливим методом захисту буде також запровадження додаткових методів автентифікації: вони можуть також включати використання двофакторної або багатофакторної автентифікації, де для доступу до картки потрібно успішно пройти не лише одну, а кілька ступенів перевірки.

Наприклад, крім введення PIN-коду або сканування біометричних даних, може також вимагатися підтвердження через мобільний застосунок або відправка SMS-коду на зареєстрований телефон [14]. Також, для вдосконалення безпеки можуть застосовуватися додаткові методи ідентифікації, такі як розпізнавання голосу, сканування радужки ока або визначення геолокації користувача. Ці методи можуть бути використані як додаткові шари захисту, що також ускладнюють доступ до картки для несанкціонованих осіб і підвищують загальний рівень безпеки користувача.

Останнім, але не менш важливим є також процес моніторингу і виявлення, що дозволяє вчасно виявляти незвичайну активність та реагувати на можливі загрози. Якщо розбирати більш детально, то ці системи виявляють незвичайні патерни використання, несподівані зміни місцезнаходження картки або надзвичайні транзакції, що можуть свідчити про можливу крадіжку або несанкціонований доступ. Вони включають аналіз даних з різних джерел, таких як журнали транзакцій, журнали входів та виходів, а також інформація з внутрішніх та зовнішніх джерел. Це дозволяє операторам системи швидко реагувати на будь-які підозрілі події та приймати заходи для їх усунення. Додатково до цього, системи моніторингу можуть включати елементи штучного інтелекту та машинного навчання, які дозволяють автоматично виявляти відмінності та аномалії в активності користувачів смарт-карток і надавати рекомендації щодо подальших заходів для забезпечення безпеки даних.

У роботі смарт-карток ніколи не використовується один метод захисту. Комбінування різних методів забезпечує більш надійну систему безпеки, що й саме удосконалює її.

ВИСНОВКИ

У нашому сучасному світі технології радіочастотної ідентифікації (RFID) та зв’язку ближнього поля (NFC) стали неодмінною складовою. Вони змінили підхід до доступу до інформації та послуг, проте також викликають питання безпеки, що потребують уважного розгляду. Використання цих технологій, які дозволяють безконтактний обмін даними, переважною більшістю сприймається як перевага. Однак, ретельний аналіз також виявляє потенційні загрози та ризики, які пов’язані з їх використанням.

Технологія RFID пропонує декілька переваг традиційними картками з магнітною смугою. По-перше, картки RFID не потребують фізичного контакту зі зчитувачем, що робить їх зручнішими та швидшими у використанні. Вони також довговічніші, ніж картки з магнітною смугою, і можуть зберігати більше даних.

Однак, як згадувалося раніше, картки RFID також становлять загрозу безпеці. Вони можуть бути вразливими до несанкціонованого доступу, клонування та перехоплення. Щоб усунути ці ризики, можна впровадити різні заходи безпеки, наприклад, використання блокуючих рукавів або гаманців RFID, впровадження зашифрованої технології RFID, а також використання суворого контролю доступу та моніторингу.

Одним із головних ризиків безпеки, пов’язаних із картками RFID, є несанкціонований доступ. Технологія RFID розроблена, щоб зробити доступ легшим і зручнішим, але це також означає, що хтось із зчитувачем RFID потенційно може отримати доступ до конфіденційної інформації, навіть не торкаючись картки. Це відомо як "знімання" або "сканування". Зловмисники можуть використовувати невеликі портативні зчитувачі RFID для захоплення інформації з RFID-карт, а власник картки навіть не буде підозрювати про це.

Ще одним ризиком безпеки є клонування. Зловмисники можуть використовувати зчитувач RFID, щоб скопіювати інформацію з незашифрованої картки RFID і створити дублікат картки за кілька секунд. Це створює прогалину в системі безпеки та дозволяє їм отримати доступ до контрольованих зон або робити покупки, використовуючи дані облікового запису іншого.

Нарешті, незахищені карти RFID вразливі до перехоплення. Хакери можуть використовувати складне обладнання для перехоплення та декодування сигналів, що передаються між RFID-карткою та зчитувачем, дозволяючи їм отримати доступ до конфіденційної інформації.

Дослідження показує, що існують певні можливості вдосконалення заходів захисту та розробки нових технологій для забезпечення безпеки смарт-карток. Використання надійного шифрування даних, ефективних методів автентифікації та систем регулярного оновлення програмного забезпечення може допомогти зменшити загрози та ризики, пов’язані з використанням цих технологій.

Використання технології NFC сприяє зручності та ефективності в багатьох аспектах нашого повсякденного життя. Завдяки NFC можна здійснювати безконтактні платежі, використовувати смартфони для проходу через турнікети у громадському транспорті та обмінюватися даними між пристроями з великою швидкістю та зручністю.

Проте, разом із цими перевагами, існують і певні ризики та проблеми з безпекою, пов’язані з технологією NFC. Зловмисники можуть використовувати атаки на NFC для перехоплення конфіденційної інформації, здійснення несанкціонованих транзакцій або навіть відстеження користувачів. Недостатня захищеність даних та вразливості в реалізації пристроїв NFC можуть становити серйозну загрозу для приватності та безпеки користувачів. Відповідне забезпечення безпеки та захисту приватності користувачів від потенційних загроз дозволить максимально використовувати переваги технології NFC без ризику для їхньої особистої інформації та фінансів.

Загальний висновок полягає в тому, що технології RFID та NFC мають великий потенціал для розвитку та використання в різних сферах, але їх впровадження повинно супроводжуватися виваженим підходом до захисту конфіденційності та безпеки даних. Тільки таким чином можна забезпечити безпечне та ефективне використання цих технологій у майбутньому.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Avery Dennison. That's all you need: One NFC tag for endless application. [Електронний ресурс]. – Режим доступу: http://surl.li/qspet.

2. NFC Vs RFID: What's The Difference? [Електронний ресурс]. – Режим доступу: https://wlius.com/blog/rfid-vs-nfc-whats-the-difference/

3. Веб-сайт VISA [Електронний ресурс]. – Режим доступу: https://www.visa.com.ua/pay-with-visa/featured-technologies/contactless-payment.html.

4. ЩО ТАКЕ NFC І ЯК ЦЮ ТЕХНОЛОГІЮ ВИКОРИСТОВУВАТИ? [Електронний ресурс]. – Режим доступу: https://www.itbox.ua/ua/blog/Scho-take-NFC-i-yak-cyu-tehnologiyu-vikoristovuvati/.

5. УПРАВЛІННЯ ВІДХОДАМИ ЗА ДОПОМОГОЮ RFID: ДОСВІД ІТАЛІЇ [Електронний ресурс]. – Режим доступу: https://idcard.com.ua/blog/waste-management-rfid/.

6. City Bikes Stockholm [Електронний ресурс]. – Режим доступу: https://www.tripadvisor.com/Attraction_Review-g189852-d6560699-Reviews-or25-City_Bikes_Stockholm-Stockholm.html

7. Введення в стандарти RFID та NFC [Елекртонний ресурс]. – Режим доступу: http://ua.led-diode.com/info/introduction-to-rfid-and-nfc-standards-41838088.html.

8. Kryzhanovskyi, V.. Listening to NFC at higher harmonic frequencies. / Kryzhanovskyi, V. ., Serhiienko, S. ., Chernov, D. ., & Kryzhanovsky, V. // Radiotekhnika. – 2021. – 1(204). – 99–104. https://doi.org/10.30837/rt.2021.1.204.11

9. Engelhardt, M.. Extending ISO/IEC 14443 type an eavesdropping range using higher harmonics., / Engelhardt, M., Pfeiffer, F., Finkenzeller, K., & Biebl, E. //

Smart SysTech. Erlangen/Nuremberg ,Germany. June 6 2013, VDE, 2013. ISBN:978-3-8007-3521-1.

10. Opal Privacy Policy. [Електронний ресурс]. – Режим доступу: https://transportnsw.info/tickets-opal/opal/opal-privacy-policy.

11. Avail Aadhaar Services. [Електронний ресурс]. – Режим доступу: https://uidai.gov.in/en/my-aadhaar/avail-aadhaar-services.html.

12. Бондаренко М. Ф. Аналіз технологій смарт-карт / М. Ф. Бондаренко, М. Г. Заросилова // Прикладная радиоэлектроника : науч.-техн. журн. – Х. : ХНУРЭ, 2011. – Т. 10, № 2 – С. 264–270. Режим доступу: https://openarchive.nure.ua/server/api/core/bitstreams/efafda42-f821-4fd4-a67d-c80772c44586/content.

13. What is the Difference Between NFC and RFID? [Електронний ресурс]. – Режим доступу: https://www.globalpaymentsintegrated.com/en-us/blog/2020/04/21/what-is-the-difference-between-nfc-and-rfid#:~:text=RFID%20tags%20can%20generally%20be,few%20centimeters%20of%20each%20other.

14. R. Kilani. Mobile Authentication with NFC enabledSmartphones. / R.Kilani, K.Jensen. // Aarhus University, 2012. - 101 URL:http://ojs.statsbiblioteket.dk/index.php/ece/article/download/21229/18718 ISSN: 2245-2087.

15. Damgani Kh. Investigating Attacks to Enhance Security and Confidentiality in RFID Systems Using Security Bit Method / Damgani, Kh., Hosseinian, H., & Damgani, L. // Conference on Engineering and Innovation (KBEI), Tehran, Iran, February 28 - March 1 2019, 833-838 pp.

16. Обговорення системи ідентифікації радіочастотної ідентифікації [Електронний ресурс]. – Режим доступу: https://ua.joyful-printing.net/info/discussion-on-rfid-radio-frequency-identificat-31689814.html.

17. AutoID Technology: RFID & Smart Labels. [Електронний ресурс]. – Режим доступу: https://www.industrialrfid.com/rfid/technology.

18. How Near Field Communication (NFC) Works. [Електронний ресурс]. – Режим доступу https://electronics.howstuffworks.com/nfc1.htm.

19. Як працює технологія наближення NFC [Електронний ресурс]. – Режим доступу: https://www.marketsandmarkets.com/Market-Reports/near-field-communication-nfc-market-520.html.

20. Contactless / Mobile Payment Statistics in Belgium [Електронний ресурс]. – Режим доступу: https://www.xorlogics.com/tag/nfc-technology/.

21. Kocher P. Differential Power Analysis. / Kocher, P., Jaffe, J., Jun, B. // Advances in Cryptology – CRYPTO 1999. Heidelberg, Berlin. December 16. Springer, 1999. - 388–397 pp. https://doi.org/10.1007/3-540-48405-1_25.

22. Kocher P. Timing attacks on Implementations of Diffie-Hellman, RSA, DSS, and other systems. / Kocher P. // Advances in Cryptology — CRYPTO’96. CRYPTO 1996.. Heidelberg, Berlin. July 13. Springer, 2001. – 104-113 pp. https://doi.org/10.1007/3-540-68697-5_9.

23. Biham E. Differential fault analysis of secret key cryptosystems. / Biham, E., Shamir, A. // Advances in Cryptology – CRYPTO'97. CRYPTO 1997. Heidelberg, Berlin. May 17. Springer, 1999. -513-525 pp. https://doi.org/10.1007/BFb0052259.

24. Kuznetsov A. Research of Computational Complexity of Cost Functions in S-boxes Generation Problems / A. Kuznetsov, S. Kandii, N. Poluyanenko, E. Frontoni, Y. Matvieieva // 2022 IEEE 9th International Conference on Problems of Infocommunications Science and Technology, PIC S and T , Kyiv, October 10-12 2022 - Kyiv: IEEE, 2022. - с. 465–469. https://ieeexplore.ieee.org/document/10238530 DOI:10.1109/PICST57299.2022.10238530.

25. Krasnobaev V. Mathematical Model of the Reliability of a Computer System Operating in the Residual Class System, Based on Dynamic Redundancy / V. Krasnobaev, O. Bagmut, A. Kuznetsov, Y. Matvieieva // UkrMiCo 2021 – 2021 IEEE

International Conference on Information and Telecommunication Technologies and Radio Electronics, Odesa, November 2021 – 03 December 2021, – Odesa: IEEE, 2021. – с. 61–66 https://ieeexplore.ieee.org/document/9716636 DOI: 10.1109/UkrMiCo52950.2021.9716636.

26. Kuznetsov A. Optimization of the WCF Cost Function to Generate Nonlinear Substitutions / A. Kuznetsov, Y. Gorbenko, N. Poluyanenko, S. Kandiy, Y. Matvieieva // Radiotekhnika. – 2022. – 2(209), 16–28 pp. https://doi.org/10.30837/rt.2022.2.209.02.

27. B. Oertel. Security Aspects and Prospective Applications of RFID Systems / B.Oertel, M. Evers-Wolk, B. Debus, V. Handke // German Federal Office for Information Security (BSI) – January 2005 - Berlin, Germany - Swiss Federal Laboratories for Materials Testing and Research, Empa + IZT - https://www.researchgate.net/publication/258275664_Security_Aspects_and_Prospective_Applications_of_RFID_Systems

28. Piotr F. Borowski. Digitization, Digital Twins, Blockchain, and Industry 4.0 as Elements of Management Process in Enterprises in the Energy Sector / Piotr F. Borowski // Energies – March 2021. – 14(7), 1885 pp. https://doi.org/10.3390/en14071885

29. RFID технологія для автоматизації обліку [Електронний ресурс]. - https://remonline.ua/blog/rfid-technology/

30. NFC Technology - Essentials & Insights [Електронний ресурс]. - https://www.st.com/content/st_com/en/support/learning/essentials-and-insights/connectivity/nfc.html

31. Ринок смарт-карток 2020-2026; Прогноз зростання та звіт про частку промисловості [Електронний ресурс]. - https://uk.eturbonews.com/ринок-смарт-карток-2020-2026-прогноз-зростання-звіт-про-частку-галузі/

ДОДАТОК А

Research of computational complexity of cost functions in S-boxes generation problems

Alexandr Kuznetsov
Department of Political Sciences, Communication and International Relations, University of Macerata, Macerata, Italy, Department of information systems and technologies security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine, JSC "Institute of Information Technologies", Kharkiv, Ukraine
kuznetsov@karazin.ua
https://orcid.org/0000-0003-2331-6326

Nikolay Poluyanenko
Department of information systems and technologies security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine, JSC "Institute of Information Technologies", Kharkiv, Ukraine
nlfsr01@gmail.com
https://orcid.org/0000-0001-9386-2547

Serhii Kandii
Department of information systems and technologies security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine, JSC "Institute of Information Technologies", Kharkiv, Ukraine
sergeykandy@gmail.com
https://orcid.org/0000-0003-0552-8341

Yevheniia Matvieieva
Department of information systems and technologies security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
belka.j.0507@gmail.com
https://orcid.org/0000-0001-8801-2185

***Abstract* — The generation of non-linear substitutions (S-boxes) is an important task in the design of cryptographic algorithms with a secret key. The properties of S-boxes determine the cryptographic strength of symmetric ciphers against various attacks, for example, linear and differential cryptanalysis. In addition, substitutions must be random in order to be resistant to algebraic cryptanalysis methods. Many authors explore the problem of generating random S-boxes. The most effective technique is heuristic search, which is based on the use of various cost functions (special heuristics). Heuristic search consists of iteratively modifying a randomly generated substitution. At each iteration, the value of the cost function is calculated, the search continues until a substitution is found that minimizes the cost function. In this article we explore several options for cost functions and evaluate the complexity of their calculation. We estimate the number of iterations required by the heuristic search to generate S-boxes with given cryptographic indicators as well as the computational complexity of generation taking into account the complexity of calculating the cost function.**

Keywords—component; formatting; style; styling; insert (key words)

I. Introduction

Most block and stream ciphers include substitution blocks or S-blocks which are chosen to satisfy a number of cryptographic criteria [1]–[3]. S-blocks are important components of modern cryptographic algorithms. Their research has been carried out for many years [4]–[9].

The development of various cryptosystem attacks over the years has led to the development of criteria for resistance to such attacks. An important unconditional criterion of cipher stability is the high nonlinearity of the S-block used [10]–[13]. These criteria provide some protection against attacks related to linear cryptanalysis.

Known methods of synthesis of non-linear substitution nodes with the necessary stability indicators can be conditionally divided into three classes: random generation methods, algebraic methods and heuristic methods [6], [9], [14], [15].

The first class includes methods based on random generation procedures followed by the selection of replacement nodes that meet the specified criteria. Their advantage lies in the obvious simplicity of practical implementation. Another advantage is the random nature of the formed S-blocks, that is, the absence of such disadvantages as linear loss and algebraic simplicity of representation. A significant disadvantage is the rapid decrease in search efficiency - finding replacement nodes with high nonlinearity with increasing dimensionality quickly becomes an impossible task [4], [16], [17].

Algebraic methods belong to the second class. Their advantage is low computational complexity, which allows for the synthesis of non-linear nodes of substitutions of arbitrary dimensions. The second advantage of this class of methods is good (main) indicators of cryptographic stability of the generated replacement nodes, such as high nonlinearity and low autocorrelation [11], [18], [19]. However, these methods have a number of disadvantages:

1) the obtained S-blocks have a non-random nature, that means that they have a linear loss (all component Boolean functions and their linear combinations are equivalent to each other) [5], [20];

2) the simplicity of the algebraic representation of S-blocks in a binary field which gives a potential vulnerability to algebraic cryptanalysis of the ciphers that use them [21]–[24];

3) the number of possible S-blocks obtained by such an algebraic method is strictly limited;

978-x-xxxx-xxxx-x/22/$31.00 ©2022 IEEE

4) reduction in the efficiency of the synthesis of S-blocks with high (main) stability indicators with increasing dimensions, i.e., the difference between the optimal calculated values of stability indicators and the obtained ones increases significantly. The issue of building replacement nodes with optimal stability indicators is open to this day.

Methods of random generation have proven themselves well in the basis of heuristic algorithms [4], [9], [14]. These algorithms are built on iterative approaches to the synthesis of S-blocks - at each step of the iteration, the method tries to improve some objective function that is related to nonlinearity and generally improves it using certain heuristics.

This work is devoted to the comparison of the most promising (in our opinion) objective functions (taking into account the minor modifications proposed by us) in terms of calculation speed. The calculation time directly affects each step of the search algorithm and the total time of the S-block formation algorithm.

II. Related works

The public literature contains an extensive review of articles on evolutionary computing related to the design and construction of S-boxes with good cryptographic properties.

In 2005 Clark proposed a new cost function for the evolution of S-boxes combined with simulated annealing to produce S-boxes with non-linearity values up to 102 [25]. We examine its slightly modified version - using a coefficient $1/4$:

$$WHS = \sum_{b=1}^{255}\sum_{i=0}^{255}\left|\frac{|WHT[b,i]|-X}{4}\right|^R,$$

where WHT – (Walsh–Hadamard transform) Walsh–Hadamard spectral coefficients;

i – loop over all component functions and their linear combinations;

b – loop over all linear functions;

X i R – parameters with valid values.

In 2016, Pychek presented a new cost function for the evolution of strongly nonlinear bijective S-blocks [26]. Picek's cost functions PCF:

$$PCF = \sum_{i=0}^{N-1} 2^{-i} H(S)_{2^i},$$

where $H(S)_k$ – the number of coefficients of the Walsh-Hadamard distribution whose absolute value is in the position k (corresponds to the position $|4\cdot k|$, the Walsh-Hadamard spectrum of the S-block S).

In 2020 Freire-Echevarria published [27] his interpretation of the objective function based on the Walsh–Hadamard spectral coefficients. Cost function (Freyre-Echevarría cost functions) WCF (slightly modified version - using the coefficient $1/4$):

$$WCF = \sum_{b=1}^{255}\sum_{i=0}^{255}\prod_{\substack{j=start\\ j+=step}}^{end}\frac{1}{4}\cdot\left||WHT[b,i]|-j\right|$$

where, $start, step, end$ – some integer value, as a rule $start = 0, step = 4$ (based on the multiplicity of the coefficients by four);

In addition to the above objective functions, we investigate two more functions proposed by us [28], [29]:

- function power_max_WHT:

$$\text{power\_max\_WHT} = \sum_{b=1}^{255}\left|\max_b\left(WHT[b,i]\right)-X\right|^R,$$

where $\max_b\left(WHT[b,i]\right)$ – the maximum value of the Walsh–Hadamard spectral coefficients for all component functions and their linear combinations ($i = 0,1,\ldots,255$); X i R – parameters with valid values.

- function *WCFS*:

$$WCFS = \sum_{\substack{b=1\\ |WHT[b,i]|>X}}^{255}\sum_{i=0}^{255}\left(\frac{|WHT[b,i]|-X}{4}\right)^R$$

where X i R – parameters with valid values.

III. Objective function calculation pseudocode

To understand the cost of computer time for the calculation of each of the listed functions, we will present the pseudocode that we used during their calculation. Please note that during the calculation, the nonlinearity of the S-block was set in parallel in the target functions.

A. Clark's WHS cost function:

```
sum = 0
for by b for all 255 linear combinations (except zero)
   spectre[0..255]← calculate the Walsh-Hadamard spectrum
   for by i for all 256 values of the Walsh-Hadamard spectrum
      max_spectre← finding the maximum element in the spectrum
      tmp = | | spectre[i] | - X | / 4
      val = 1
      for from 1 to R, perform exponentiation
         val = val * tmp
      end for
      sum = sum + val
   end for
end for
nonlinearity = 128 - max_spectre/2
return sum value
```

B. WCF Freire-Echevarria cost function:

```
sum = 0
for by b for all 255 linear combinations (except zero)
   spectre[0..255]← calculate the Walsh-Hadamard spectrum
   for by i for all 256 values of the Walsh-Hadamard spectrum
      max_spectre← finding the maximum element in the spectrum
      val = 1
      for by j from start to end with step
```

```
            tmp = | | spectre[i] | - j | / 4
            val = val * tmp
        end for
        sum = sum + val
    end for
end for
nonlinearity = 128 - max_spectre/2
return sum value
```

C. C. Pichek's cost function PCF

```
sum = 0
for by b for all 255 linear combinations (except zero)
    spectre[0..255]← calculate the Walsh-Hadamard spectrum
    for by i for all 256 values of the Walsh-Hadamard spectrum
        max_spectre← finding the maximum element in the spectrum
        histogram [ | spectre[i] |/4]++ // build a spectrum distribution histogram
    end for
    sum = 0
    max_val = max_spectre/4
    mult = 1
    for by i from 0 to N
        sum = mult * histogram[max_val]
        mult = mult/2
        max_val = max_val-1
    end for
end for
for from max_spectre/4 iterations (implementation of the requirement that sum increases significantly with increasing nonlinearity)
    sum = 8 * sum
end for
nonlinearity = 128 - max_spectre/2
return sum value
```

D. Our proposed power_max_WHT function:

```
sum = 0
for by b for all 255 linear combinations (except zero)
    spectre[0..255]← calculate the Walsh-Hadamard spectrum
    for by i for all 256 values of the Walsh-Hadamard spectrum
        max_spectre_b← finding the maximum element in a spectrum of 256 elements
    end for
    max_spectre← finding the maximum element in the spectrum
    max_spectre_b = | max_spectre_b – X |
    val = 1
    for from 1 to R, perform exponentiation
        val = val * max_spectre_b
    end for
    sum = sum + val
end for
nonlinearity = 128 - max_spectre/2
return sum value
```

E. Our proposed WCFS function:

```
sum = 0
for by b for all 255 linear combinations (except zero)
    spectre [0..255]← calculate the Walsh-Hadamard spectrum
    for by i for all 256 values of the Walsh-Hadamard spectrum
        max_spectre← finding the maximum element in the spectrum
        val = 1
        if spectre[i] > X
            tmp = (| spectre[i] | - X) / 4
            val = 1
            for from 1 to R, perform exponentiation
                val = val * tmp
            end for
        end if
        sum = sum + val
    end for
end for
nonlinearity = 128 - max_spectre/2
return sum value
```

IV. Conditions of Performing a Computer Experiment

The computation time was averaged over 500,000 individual runs of the objective function. As parameters for each objective function, those with which the average number of iterations for finding a bijective S-block with nonlinearity 104 was the smallest (according to our experiments) were chosen, namely:

- Clark's WHS cost function: $R = 12;\ X = 0$.
- Freire-Echevarria's WCF cost function: $start = 0$; $step = 4$; $end = 28$.
- Pichek's PCF value function: $N = 11$.
- Our proposed power_max_WHT function: $R = 4;\ X = 36$.
- Our proposed WCFS function: $R = 4;\ X = 11$.

Before starting the tests, each function was optimized for the selected parameters, which in some cases led to a time reduction of up to 40%.

The calculation was performed on an Intel Core i5-3210M CPU 2.50GHz personal computer running the 64-bit Windows 7 operating system. The code written in C++ was compiled using Microsoft Visual Studio Community 2022 (64-bit version) in the Release configuration.

V. Obtained Results

Each function first uses a fast Walsh-Hadamard transform to find its spectrum. This operation is the most expensive (in terms of time) and has the same implementation for all functions. That is why we measured the time to calculate the Walsh-Hadamard spectrum and included it in the results as a separate item. Computational times in other functions include the computation time of the Walsh-Hadamard spectrum. The general results of the

averaged time for calculating the objective functions are given in table __.

TABLE I. AVERAGE CALCULATION TIME OF THE OBJECTIVE FUNCTION

Function	the Walsh-Hadamard spectrum	*WHS*	*WCF*	*PCF*	power maxWHT	*WCFS*
Time (sec.)	$6{,}1\cdot10^{-4}$	$8{,}8\cdot10^{-4}$	$8{,}2\cdot10^{-4}$	$7{,}2\cdot10^{-4}$	$6{,}9\cdot10^{-4}$	$10{,}3\cdot10^{-4}$
	100%	144%	134%	118%	113%	169%

If you choose 100% time for calculating the Walsh-Hadamard spectrum, the fastest function is PCF, which requires only 18% additional time to obtain the result. The longest is the WCFS function, which additionally uses 69% of the calculation time.

However, for each objective function, the search algorithm performs a different number of iterations to find a bijective S-block with nonlinearity 104. Table __ shows the average number of iterations for each objective function that we obtained in previous studies, as well as the probability of finding a solution.

TABLE II. AVERAGE NUMBER OF ITERATIONS CONSUMED BY A HILL CLIMBING ALGORITHM WITH DIFFERENT OBJECTIVE FUNCTIONS FOR FINDING A BIJECTIVE S-BLOCK WITH NONLINEARITY 104

Function	*WHS*	*WCF*	*PCF*	power_ max_WHT	*WCFS*
Number of iterations	50 265	53 160	74 868	150 278	49 139
The probability of finding an S-block with $N_f = 104$	≈ 99%	≈ 100%	≈ 98%	≈ 27%	≈ 100%
Average time (t, sec)	44,2	43,6	53,9	більш 120	50,6

Considering the given data, it can be concluded that despite the high calculation speed of the power_max_WHT function, it takes much more time than any other. In addition, in practical application, the specified time will increase significantly (at least 3 times) due to the need to repeatedly run the search algorithm to find a bijective S-block with nonlinearity 104.

The average time ($t, сек$) spent by the program to compute only the objective functions in the hill-climbing search algorithm on a personal computer (the configuration of which is shown above) is given in the last line of Table __. The time was calculated as the product of the average number of iterations times the average function computation time (i.e., using only one thread and not using the parallel computing capability). Visually, the average time spent on the calculation of objective functions for finding a bijective S-block with nonlinearity 104 is shown in Figure __.

Fig. 1. Fig. 1. The average time spent by the program to calculate only the objective functions in the hill-climbing search algorithm

VI. CONCLUSIONS

This work examines the average time for calculating the objective function with optimal parameters. They are compared with each other and the total search time (taking into account only the time of objective function calculations) of the hill-climbing algorithm for finding a bijective S-block with nonlinearity 104.

It has been established that the power_max_WHT function is the fastest (executes in 6.9 seconds), but with it the search algorithm must spend more than a few iterations, so the total time of the algorithm is very long.

Although the other four objective functions showed a discrepancy of 1.5 times the average calculation time (from $7{,}2\cdot10^{-4}$ seconds to $10{,}3\cdot10^{-4}$ seconds), however, taking into account the average number of iterations before finding a bijective S-block with nonlinearity 104, the average calculation time in the search algorithm is somewhat close (from 44 sec. to 54 sec.). The WCF and WHS objective functions have the best results with an average time of 43.6 sec. and 44.2 sec. in accordance.

REFERENCES

[1] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 2018. doi: 10.1201/9780429466335.

[2] A. A. Kuznetsov, O. V. Potii, N. A. Poluyanenko, Y. I. Gorbenko, and N. Kryvinska, *Stream Ciphers in Modern Real-time IT Systems: Analysis, Design and Comparative Studies*. Springer International Publishing, 2022. doi: 10.1007/978-3-030-79770-6.

[3] A. Andrushkevych, Y. Gorbenko, O. Kuznetsov, R. Oliynykov, and M. Rodinko, "A Prospective Lightweight Block Cipher for Green IT Engineering," in *Green IT Engineering: Social, Business and Industrial Applications*, vol. 171, V. Kharchenko, Y. Kondratenko, and J. Kacprzyk, Eds. Cham: Springer International Publishing, 2019, pp. 95–112. doi: 10.1007/978-3-030-00253-4_5.

[4] A. J. Clark, "Optimisation heuristics for cryptology," phd, Queensland University of Technology, 1998. Accessed: May 19, 2021. [Online]. Available: https://eprints.qut.edu.au/15777/

[5] J. E. Fuller, "Analysis of affine equivalent boolean functions for cryptography," phd, Queensland University of

Technology, 2003. Accessed: Apr. 18, 2021. [Online]. Available: https://eprints.qut.edu.au/15828/

[6] L. D. Burnett, "Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography," phd, Queensland University of Technology, 2005. Accessed: May 19, 2021. [Online]. Available: https://eprints.qut.edu.au/16023/

[7] J. Álvarez-Cubero, "Vector Boolean Functions: applications in symmetric cryptography," 2015. doi: 10.13140/RG.2.2.12540.23685.

[8] T. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications: Second edition*. 2017, p. 275.

[9] A. Freyre Echevarría, "Evolución híbrida de s-cajas no lineales resistentes a ataques de potencia," 2020. doi: 10.13140/RG.2.2.17037.77284/1.

[10] K. Nyberg, "Linear Approximation of Block Ciphers," 1994. doi: 10.1007/BFb0053460.

[11] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology — EUROCRYPT '93*, Berlin, Heidelberg, 1994, pp. 55–64. doi: 10.1007/3-540-48285-7_6.

[12] C. Carlet and C. Ding, "Nonlinearities of S-boxes," *Finite Fields and Their Applications*, vol. 13, no. 1, pp. 121–135, Jan. 2007, doi: 10.1016/j.ffa.2005.07.003.

[13] C. Carlet, "Vectorial Boolean functions for cryptography," *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Dec. 2006.

[14] J. McLaughlin, "Applications of search techniques to cryptanalysis and the construction of cipher components," phd, University of York, 2012. Accessed: Aug. 16, 2020. [Online]. Available: http://etheses.whiterose.ac.uk/3674/

[15] A. A. Kuznetsov, I. V. Moskovchenko, D. I. Prokopovych-Tkachenko, and T. Y. Kuznetsova, "HEURISTIC METHODS OF GRADIENT SEARCH FOR THE CRYPTOGRAPHIC BOOLEAN FUNCTIONS," *TRE*, vol. 78, no. 10, 2019, doi: 10.1615/TelecomRadEng.v78.i10.40.

[16] W. Millan, "How to improve the nonlinearity of bijective S-boxes," in *Information Security and Privacy*, Berlin, Heidelberg, 1998, pp. 181–192. doi: 10.1007/BFb0053732.

[17] J. A. Clark, J. L. Jacob, and S. Stepney, "The design of S-boxes by simulated annealing," *New Gener Comput*, vol. 23, no. 3, pp. 219–231, Sep. 2005, doi: 10.1007/BF03037656.

[18] K. Nyberg, "Perfect nonlinear S-boxes," in *Advances in Cryptology — EUROCRYPT '91*, Berlin, Heidelberg, 1991, pp. 378–386. doi: 10.1007/3-540-46416-6_32.

[19] J. Daemen and V. Rijmen, "Specification of Rijndael," in *The Design of Rijndael: The Advanced Encryption Standard (AES)*, J. Daemen and V. Rijmen, Eds. Berlin, Heidelberg: Springer, 2020, pp. 31–51. doi: 10.1007/978-3-662-60769-5_3.

[20] J. Fuller and W. Millan, "Linear Redundancy in S-Boxes," in *Fast Software Encryption*, vol. 2887, T. Johansson, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 74–86. doi: 10.1007/978-3-540-39887-5_7.

[21] G. V. Bard, *Algebraic Cryptanalysis*. Boston, MA: Springer US, 2009. doi: 10.1007/978-0-387-88757-9.

[22] N. T. Courtois and J. Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations," in *Advances in Cryptology — ASIACRYPT 2002*, Berlin, Heidelberg, 2002, pp. 267–287. doi: 10.1007/3-540-36178-2_17.

[23] N. T. Courtois and G. V. Bard, "Algebraic Cryptanalysis of the Data Encryption Standard," in *Cryptography and Coding*, Berlin, Heidelberg, 2007, pp. 152–169. doi: 10.1007/978-3-540-77272-9_10.

[24] A. Biryukov and A. Shamir, "Structural Cryptanalysis of SASAS," *J Cryptol*, vol. 23, no. 4, pp. 505–518, Oct. 2010, doi: 10.1007/s00145-010-9062-1.

[25] J. A. Clark, J. L. Jacob, and S. Stepney, "The design of s-boxes by simulated annealing," in *Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No.04TH8753)*, Jun. 2004, vol. 2, pp. 1533-1537 Vol.2. doi: 10.1109/CEC.2004.1331078.

[26] S. Picek, M. Cupic, and L. Rotim, "A New Cost Function for Evolution of S-Boxes," *Evolutionary Computation*, vol. 24, no. 4, pp. 695–718, Dec. 2016, doi: 10.1162/EVCO_a_00191.

[27] A. Freyre-Echevarría *et al.*, "An External Parameter Independent Novel Cost Function for Evolving Bijective Substitution-Boxes," *Symmetry*, vol. 12, no. 11, Art. no. 11, Nov. 2020, doi: 10.3390/sym12111896.

[28] A. Kuznetsov, N. Poluyanenko, S. Kandii, Y. Zaichenko, D. Prokopovich-Tkachenko, and T. Katkova, "WHS Cost Function for Generating S-boxes," in *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S T)*, 2021, pp. 434–438. doi: 10.1109/PICST54195.2021.9772133.

[29] A. Kuznetsov, N. Poluyanenko, S. Kandii, Y. Zaichenko, D. Prokopovich-Tkachenko, and T. Katkova, "Optimizing the Local Search Algorithm for Generating S-Boxes," in *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S T)*, 2021, pp. 458–464. doi: 10.1109/PICST54195.2021.9772163.

ДОДАТОК Б

Mathematical Model of the Reliability of a Computer System Operating in the Residual Class System, Based on Dynamic Redundancy

Victor Krasnobaev
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
v.a.krasnobaev@gmail.com
https://orcid.org/0000-0001-5192-9918

Alexandr Kuznetsov
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
kuznetsov@karazin.ua
https://orcid.org/0000-0003-2331-6326

Oleksandr Bagmut
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
Oleksandr.bagmut@karazin.ua
https://orcid.org/0000-0003-3241-5756

Yevheniia Matvieieva
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
olga.bulgakova.dp@gmail.com
https://orcid.org/0000-0001-8801-2185

***Abstract*—The article discusses a variant of the mathematical model of the reliability of a computer system (CS) operating in the residual class system (RNS), based on the use of dynamic redundancy. The calculation and comparative analysis of the reliability of the tripled computational structure in the positional number system with an ideal majority element and CS in the RNS with an ideal commutator is carried out. The analysis results showed the following. At the initial stage of the operation of computing systems, the reliability of the CS in the RNS with one control base is higher than the triple positional computing system. At the initial stage of the operation of computing systems, the reliability of the CS in the RNS with one control base is higher than the triple positional computing system. This presupposes the effective use of the COP in the RNS in systems and devices for short-term use. For example, in on-board computers of ballistic missiles and aircraft.**

Keywords—residual class system, dynamic redundancy, mathematical model of the reliability, computer system

I. INTRODUCTION

Note that at present, interest in the use of the residual class system (RNS) is growing again [1]–[3]. It is caused primarily by the following circumstances [4]–[6]:

- the emergence of numerous technological and theoretical publications dedicated to the theory and practice of creating computer systems (CS) and components in the RNS;
- the universal use of mobile processors, which want high data processing performance with little energy consumption;
- no inter-digit transfers in the process of performing arithmetic operations of addition and multiplication of numbers in the RNS allows reducing energy consumption;
- banking configuration demonstrate great interest in RNS, where it is necessary to reliably and reliably process large data arrays in real time, i.e. high-performance tools are required for highly reliable computations with self-correction of errors, which is typical of codes in RNS;
- increasing the density of elements on one chip does not in all cases allow high-quality and complete testing; in this case, the importance of ensuring the fault-tolerant functioning of specialized CS increases;
- the need to use specialized CS to perform a various of operations on vectors that require a high speed of performing integer addition and multiplication operations (matrix multiplication problems, vector scalar product problems, transformation Fourier, etc.);
- the widespread introduction of microelectronics into all spheres of average life has significantly increased the relevance and importance of previously rare, and now such massive scientific and practical tasks as digital processing of signals and images, pattern recognition, cryptography, processing and storage of multi-bit information, etc.; this circumstance requires huge computing resources that exceed existing capabilities;
- the current level of development of microelectronics is approaching the limit of its capabilities in terms of ensuring performance and reliability of existing and future CS and components for real-time processing of large data arrays; nanoelectronics, molecular electronics, micromechanics, bioelectronics, optical, optoelectronic and photonic computers, biological, etc., which are coming to replace it, are still very far from real wide industrial production and application.

The article discusses a variant of the mathematical model of the reliability of a computer system, functioning in the residual class system, based on the use of dynamic redundancy.

The article is structured as follows. Section 2 briefly analyzes recent publications in the subject area. Section 3 provides basic theoretical information about number systems in residual classes. Section 4 is devoted to the presentation of the main results. In particular, a mathematical model of the reliability of a computer system operating in a residual class system is described. It also provides several examples that

clearly demonstrate the proposed solutions, as well as figures and calculations that give an idea of the reliability of a computer system operating in a residual class system. In the "Conclusion" section, the results obtained are summarized, some conclusions and recommendations are stated.

II. Related Works

The problems of constructing computer systems operating in the residual class system have been studied by many authors. In works [4], [6], [7] and many others, the general theoretical provisions of the residual class systems, as well as the techniques for their use in computer systems, were investigated. In works [2], [8] - [11], etc., the possibilities of the residual class system for error correction were investigated. This is a very important property, which was also studied in works [12] - [16]. Articles [17] - [19] are devoted to the study of new techniques for constructing specialized computing devices operating in the system of residual classes. The papers [1], [20] - [23] investigate new directions in computer science devoted to systems of residual classes. For example, in [2] artificial intelligence methods are investigated, in [20] methods of fast Fourier transform are studied, in [21] digital filters are considered, in [22], [23] some cryptography problems using computations in the system of residual classes.

Many works are also devoted to research of methods of increasing the reliability and fault tolerance of computer systems. For example, these are fundamental works [24] - [27], etc. In articles [2], [3], [28] aspects of increasing the reliability of computer systems are investigated, and in [2], [10], [12], [13] issues of fault tolerance of computing devices operating in the system of residual classes. However, the issues of quantifying the probability of failure-free operation of computer systems in residual class systems have not been studied enough.

This article proposes a mathematical model of the reliability of a computer system operating in the residual class system. This model makes it possible to quantify the main indicators of the reliability of the computer system functioning in the residual class system. We also provide several examples with a visual calculation of the probability of no-failure operation of computer systems in residual class systems.

III. Basic Properties of Non-Positional Arithmetic in RNS

First, preliminary, before taking into consideration a version of the mathematical model of the reliability of a CS operating in the residual class system (RNS), we will deal with the consequence of the leading properties of a non-positional number system on the structure and principles of operation of the CS [7]–[9].

A. Independence of the residues.

This property makes it possible to produce a CS in the RNS in the form of a set of independent, parallel operating in time, break computing paths (BT) for data processing, functioning severally of each other agreement with their particular modulus m_i. Thus, the CS operating in the RNS has a modular design, which allows maintenance and elimination of failures and malfunctions of the computing paths by replacing an inoperative VT with an efficient one without interrupting the solution of the problem. The time for the implementation of arithmetic operations in the CS is determined by the time for the implementation of the operation in the BT according to the greatest radix m_i RNS.

In addition, errors arising from failures (failures) of the binary bit circuits in an arbitrary TC of the CS do not "multiply" into neighboring paths (remain within one remainder), which makes it possible to increase the reliability of calculations in the RNS. It does not matter whether there was a single or multiple errors or a burst of errors no longer than $[\log_2(m_i-1)]+1$ binary digits. A mistake that has arisen in the CS in the base m_i is either stored in this path until the end of the calculations, or is self-eliminated in the process of further calculations (for example, by multiplying the remainder of the number by zero). This property of the RNS made it possible to create a unique system for monitoring and correcting errors in the dynamics of the computational process (without stopping the computation process) of the CS with the introduction of a minimum information code redundancy, which is essential for data processing systems operating in real time.

B. Equality of residues.

Note that there is a close relationship between arithmetic codes in RNS and arithmetic AN-codes in a positional number system (PSS). Arithmetic codes in RNS are an advanced development of the known positional arithmetic noise-immune many-residual AN-codes [3], [10], [11].

Based on the procedure for generating numbers in the RNS, it is obvious that any remainder ai of the number $A=(a_1,a_2,\dots,a_n)$ carries information about the entire original number A, which makes it possible by software methods to replace the failed computational path modulo m_i with an operable path modulo m_i (provided that $m_i < m_j$) without interrupting the solution of the problem. Thus, the CS functioning in the RNS having, for example, two control bases, retain their operability in the event of failure of any two computing paths. In the event of failures in the third or fourth paths, the CS continues to execute the computation program with a slight decrease in the computational accuracy, i.e. CS in RNS has the property of gradual degradation. This property determines the characteristic feature of the functioning of the CS in the RNS: a CS, depending on the requirements imposed on it, can have different reliability, accuracy of calculations and speed in the dynamics of the computational process. Thus, in the process of solving the problem, it is possible to vary the reliability of the CS, the reliability, accuracy and speed of calculations. Indeed, let the data be determined by a numerical code represented by a set of bases $\{m_i\}$ $(i=\overline{1,n+k})$ RNS.

It is known that the execution time of arithmetic operations and the accuracy of the solution depends on the number n of information bases, and the reliability of the functioning of the CS and the reliability of calculations depends on the number k of the control bases of the RNS. Let in the process of calculations the need arose to improve the reliability of the functioning of the CS and (or) the reliability of the calculations. In this case, in real time, without interrupting the calculations, the bases $\{m_i\}$ of the RNS are redistributed as follows

$$i=\overline{1,n'+k'}$$

and

$$n'<n,\ k'>k.$$

Moreover,

$$n + k = n^* + k^* = const .$$

In this case, the accuracy of calculations decreases and the speed of performing arithmetic operations increases, which are determined by the number of information bases n'. If there is a need to increase the accuracy of the solution in a separate section of the computed program, then the program is redistributed as follows:

$$i = \overline{1, n^* + k^*} \quad (n + k = n^* + k^* = const).$$

In this case, with an increase in the accuracy of calculations ($n^* > n$), the reliability of the CS (reliability of calculations) decreases and the time for solving this problem increases.

Furthermore, the redistribution of information n and k control bases takes place with the execution of non-modular functions in the RNS (operation of control, correction, comparison, etc.). The time required to perform non-modular operations in the RNS is proportional to the number n of information bases, i.e. the number of bases that determine the accuracy of the calculations.

The transition to computations with lower accuracy makes it possible to increase the speed of the CS. If an ordered ($m_i < m_{i+1}$) RNS is expanded by adding l bases, each of which is larger than the previous base of the original RNS, then the minimum code distance d_{min} is automatically increased by l.

The same can be achieved by decreasing the number n of information bases, i.e. moving on to calculations with less precision. Consequently, there is an inverse relationship between the correcting capabilities of the RNS codes and the computational accuracy. The combined use of the first and second properties of the RNS determines the presence of three types of redundancy in the CS simultaneously: structural, informational and functional.

Based on the idea of structural redundancy, the joint use of the first and second properties makes it possible to synthesize mathematical models of the CS reliability in the RNS, corresponding to the models of constant and dynamic redundancy in the PSS. In this case, the information paths $m_{n+1} \div m_{n+k}$ of the CS plays the role of working elements, and the control $m_{n+1} \div m_{n+k}$ play the role of reserve elements, where k is the number of control (reserve) bases of the RNS.

C. Low bit representation of residues.

This property allows to significantly increase the reliability and performance of the CS. This is achieved both due to the low bit depth of the construction of the CS, and due to the possibility of using (in contrast to the PSS) tabular arithmetic, where the arithmetic operations of addition, subtraction and multiplication are performed practically in one machine cycle. In particular, the small digit capacity of the residuals in the representation of numbers in the RNS makes it possible to choose a wide range of options for system engineering solutions in the implementation of modular arithmetic operations based on the following principles:

- adder principle (based on the use of low-bit binary adders modulo);
- tabular principle (based on the use of read-only memory devices (ROM) of small sizes);
- the principle of ring shift based on the use of ring shift registers.

IV. Mathematical Model of the Reliability of a Computer System Operating in the Residual Class System

Based on the analysis of the possible use of the above three main properties (independence, equality and low bit depth of residuals that determine the non-positional code structure), non-positional arithmetic in the RNS, in comparison with the PSS, has the following significant advantages [13], [17], [29]:

- the ability to parallelize computations at the level of decomposition of the operands, which significantly increases the speed of the CS;
- the possibility of spatial diversity of data elements with the possibility of their subsequent asynchronous independent processing;
- the possibility of tabular (matrix) execution of arithmetic operations of the base set and polynomial functions with a single-cycle selection from the ROM of the result of a modular operation;
- the ability to create a system for monitoring and correcting the CS with effective detection and correction of failures and failures;
- the ability to control and correct errors in the dynamics of the computational process of the CS;
- the possibility of effective use of passive and active fault tolerance based on the operational reconfiguration of the CS structure;
- lower computational and time complexity for individual classes (types) of integer problems;
- manifestation of a special property of the structure of the CS in the RNS, ensuring the absence of the effect of multiplication of errors in the implementation of arithmetic integer operations of addition, subtraction and multiplication;
- the suitability of the structure of the CS in the RNS for carrying out operational diagnostics of blocks and nodes of the calculator;
- the possibility of increasing the reliability of the CS in the RNS due to the efficiency of the simultaneous use of passive and active fault tolerance.

Based on the listed basic properties of the RNS, the probability of no-failure operation of the CS can be represented as the probability of no-failure operation of the CS in the PSS for the case of sliding redundancy with a loaded reserve, taking into account the influence of the listed properties of the RNS. In this case, the formula for determining the probability of no-failure operation of the CS in the RNS will take the form of expression (1).

$$P_{RNS}^{(k)}(t) = \sum_{i=0}^{k} C_{k+n}^{i} P_1^{k+n-i}(t) \sum_{j=0}^{i} (-1)^j C_i^j P_1^j(t) . \qquad (1)$$

Here, on the right-hand side of formula (1), the expression $P_1(t)=exp(-\lambda_1 t)$ is the probability of failure-free operation of the CS data processing path on the largest (least reliable) basis m_{n+k} RNS, and the value λ_1 is the failure rate of the equipment on the largest base m_{n+k}.

Relation (1) can be used to calculate the probability of no-failure operation of the CS in the RNS under the following assumptions:

- This property makes possible to significantly increase the reliability and performance of the CS. This is achieved both because of the low bit depth of the construction of the CS, and due to the possibility of using (in contrast to the PSS) tabular arithmetic, where the arithmetic operations of addition, subtraction and multiplication are performed practically in one machine cycle. In particular, the small digit capacity of the residuals in the representation of numbers in the RNS makes it possible to choose a wide range of options for system engineering solutions in the implementation of modular arithmetic operations based on the following principles: information and control computing paths of the CS are equally reliable (the probability of failure-free operation of all paths is taken to be equal to the probability of failure-free operation $P_1(t)$ of the path on the largest basis m_{n+k} RNS, which has the lowest probability of failure-free operation);
- the possibility of restoring failed CS paths is not taken into account.

Note that the real reliability of the CS in the RNS will be higher than that determined by relation (1), since this formula does not take into account the possibility of replacing one control path on the basis of m_j with one or several inoperable information paths at the same time

$$m_j \geq \prod_{i=1}^{r} m_{k_i},$$

provided where r is the maximum number simultaneously replaced working paths with one control operable path on the base m_j.

Let us carry out a comparative analysis of the reliability of a triple positional CS with an ideal majority element and a CS in an RNS with an ideal fail-safe switch, using the considered reliability model (1). Let us denote by λ_3 the failure rate of the equipment referred to one binary digit (to the unit of the CS bit grid). In this case, the probability of failure-free operation of the equipment, referred to one binary bit of the COP is equal to

$$P_3(t)=e^{-\lambda_3 t}.$$

For a positional l-byte CS, the probability of no-failure operation is equal to

$$P_0(t)=e^{-\lambda_0 t},$$

where

$$\lambda_0=8l\lambda_3, \text{ or } P_0(t)=e^{-8l\lambda_3 t}.$$

It is known that the probability of no-failure operation for a triple majority structure in an PSS containing three computers and an ideal majority element is [24], [30]–[32]:

$$P_M(t)=3P_0^2(t)-2P_0^3(t)=e^{-16\lambda_3 t}(3-2e^{-8\lambda_3 t}). \quad (2)$$

For CS in RNS, the probability of failure-free operation of the path on an arbitrary basis $m_i (i=\overline{1,n+k})$ is equal

$$P_i(t)=e^{-\lambda_i t}$$

or

$$P_1(t)=e^{-\lambda_1 a_{n+k} t},$$

where

$$a_{n+k}=[\log_2(m_{n+k}-1)]+1.$$

The probability of failure-free operation of the CS in the RNS is determined in accordance with expression (1).

Let us give examples of using formula (1) for various RNS.

Let $l=1$ (single-byte CS) and $k=1$.

Then the RNS can be represented as a set of the following bases

$$m_1=3,\ m_2=4,\ m_3=5,\ m_4=7,\ m_5=11.$$

Moreover,

$$\prod_{i=1}^{4} m_i = 420 > 2^8 = 256$$

and

$$\text{GCD}(m_i,m_j)=1 \text{ for } i\neq j.$$

In this case, relation (1) can be written in the form

$$P_{RNS}^{(1)}(t)=5P_1^4(t)-4P_1^5(t)= \\ =e^{-16\lambda_1 t}(5-4e^{-4\lambda_1 t}). \quad (3)$$

We denote $\lambda^*=8\lambda_3$. In this case, expressions (2) and (3) can be written, respectively, in the form

$$P_M(t)=e^{-2\lambda^* t}(3-2e^{-\lambda^* t}), \quad (4)$$

$$P_{RNS}^{(1)}(t)=e^{-2\lambda^* t}(5-4e^{-4\lambda^* t}). \quad (5)$$

In accordance with expression (4) and (5), the values of the probability of no-failure operation are calculated for the triple positional CS in the PSS and for the CS in the RNS.

In Fig. 1 shows the graphs of the $P(\lambda^* t)$ for single-byte CS: non-redundant (I) in the PSS, three-channel redundant (II) CS in the PSS and CS in the RNS (III) with parameters

$$l=1,\ n=4,\ k=1.$$

From Fig.1, it can be seen that a CS in an RNS with one (k = 1) control base (III) is more reliable than a triple positional computing system (II).

In this case, the critical value of the probability of no-failure operation of the CS in the RNS is equal to 0.425, and the critical value of the tripled computing system is equal to 0.5, i.e. the use of the RNS expands the range of values $\lambda^* t$, at which the reliability of the CS in the RNS is higher than the reliability of the CS in the PSS.

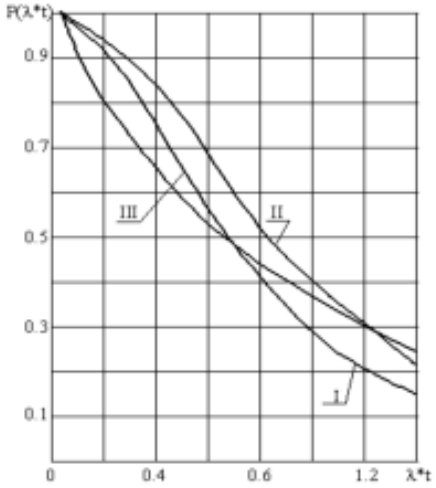


Fig. 1. Graphs of dependencies $P(\lambda^* t)$ of CS reliability, $k=1$

Let $k = 2$.

In this case, the RNS is defined as a set of the following bases:

$$m_1=3,\ m_2=4,\ m_3=5,$$

$$m_4=7,\ m_5=11,\ m_6=13.$$

For a given RNS, expression (1) is written as follows

$$P_{RNS}^{(2)}(t) = P_1^4(t)\left\{P_1^2(t)+6P_1(t)\left[1-P_1(t)\right]+15\left[1-P_1(t)\right]^2\right\}$$

or

$$P_{RNS}^{(2)}(t) = \\ = e^{-2\lambda^* t}\left[e^{-\lambda^* t}+6e^{-0,5\lambda^* t}\left(1-e^{-0,5\lambda^* t}\right)+15\left(1-e^{-0,5\lambda^* t}\right)^2\right]. \quad (6)$$

The graph of function (6) for k = 2 is shown in Fig. 2.

It can be seen from this graph that the CS in the RNS with two control bases (IV) is more reliable than the triple positional computing system (II) and more reliable than the CS in the RNS with one (k = 1) control base (III).

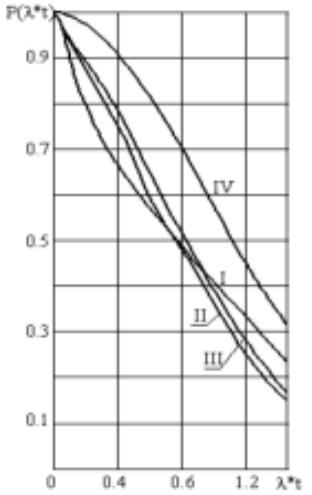


Fig. 2. Graphs of dependencies $P(\lambda^* t)$ of CS reliability, $k=2$

Shown in Fig. 1, 2 dependencies were obtained by calculation using the formulas of the proposed mathematical model. With an increase in the multiplicity of redundancy, the reliability of the CS increases, which corresponds to the provisions of the general theory of reliability [33].

V. Conclusion

The article discusses a variant of the mathematical model of the reliability of a computer system, functioning in the residual class system, based on the use of dynamic redundancy.

The computing and comparative analysis of reliability in terms of the probability of failure-free operation of a triple computing structure in a positional number system with an ideal majority element and a CS in an RNS with an ideal commutator is carried out. The analysis results showed the following. At the initial stage of the operation of computing systems, the reliability of the CS in the RNS with one control base is higher than the triple positional computing system. This presupposes the effective use of the CS in the RNS in systems and devices for short-term use. For instance, in on-board computers of ballistic missiles and aircraft.

References

[1] D. I. Kaplun *et al.*, "Hardware Implementation of Video Processing Device using Residue Number System," in *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, Jul. 2019, pp. 701–704. doi: 10.1109/TSP.2019.8768827.

[2] T.-C. Huang, "Self-Checking Residue Number System for Low-Power Reliable Neural Network," in *2019 IEEE 28th Asian Test Symposium (ATS)*, Dec. 2019, pp. 37–375. doi: 10.1109/ATS47505.2019.000-3.

[3] Y. Zhang, "An FPGA implementation of redundant residue number system for low-cost fast speed fault-tolerant computations," Thesis, 2018. doi: 10.32657/10220/47113.

[4] P. V. A. Mohan, *Residue Number Systems*. Cham: Springer International Publishing, 2016. doi: 10.1007/978-3-319-41385-3.

[5] I. Koren, "THE RESIDUE NUMBER SYSTEM," *Computer Arithmetic Algorithms*, Oct. 08, 2018. https://www.taylorfrancis.com/ (accessed Aug. 16, 2020).

[6] J. O. Tuazon, "Residue number system in computer arithmetic," Doctor of Philosophy, Iowa State University, Digital Repository, Ames, 1969. doi: 10.31274/rtd-180816-2270.

[7] I. Koren, "THE RESIDUE NUMBER SYSTEM," in *Computer Arithmetic Algorithms*, 2nd ed., A K Peters/CRC Press, 2002.

[8] F. Barsi and P. Maestrini, "Error Correcting Properties of Redundant Residue Number Systems," *IEEE Transactions on Computers*, vol. C–22, no. 3, pp. 307–315, Mar. 1973, doi: 10.1109/T-C.1973.223711.

[9] L. Yang and L. Hanzo, "Coding theory and performance of redundant residue number system codes," *Ieee Trans. Inform. Theory*, 1999.

[10] P. V. Ananda Mohan, "Error Detection, Correction and Fault Tolerance in RNS-Based Designs," in *Residue Number Systems: Theory and Applications*, P. V. A. Mohan, Ed. Cham: Springer International Publishing, 2016, pp. 163–175. doi: 10.1007/978-3-319-41385-3_7.

[11] Y. N. Kocherov, D. V. Samoylenko, and A. I. Koldaev, "Development of an Antinoise Method of Data Sharing Based on the Application of a Two-Step-Up System of Residual Classes," in *2018 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, Oct. 2018, pp. 1–5. doi: 10.1109/FarEastCon.2018.8602764.

[12] K. Phalakarn and A. Surarerks, "Alternative Redundant Residue Number System Construction with Redundant Residue Representations," in *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*, Apr. 2018, pp. 457–461. doi: 10.1109/CCOMS.2018.8463305.

[13] D. I. Popov and A. V. Gapochkin, "Development of Algorithm for Control and Correction of Errors of Digital Signals, Represented in System of Residual Classes," in *2018 International Russian Automation Conference (RusAutoCon)*, Sep. 2018, pp. 1–3. doi: 10.1109/RUSAUTOCON.2018.8501826.

[14] P. A. Ramamoorthy and B. Potu, "High-speed ADC using residue number system," in *International Conference on Acoustics, Speech, and Signal Processing*, May 1989, pp. 1063–1066 vol.2. doi: 10.1109/ICASSP.1989.266615.

[15] V. Krasnobaev, O. Reshetniak, T. Kuznetsova, S. Florov, and Y. Kotukh, "Data Control Method, which Presented By Code of Non-Positioning System of Deduction Class Calculation," in *2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Sep. 2019, pp. 1–5. doi: 10.1109/UkrMiCo47782.2019.9165528.

[16] V. Krasnobayev, A. Kuznetsov, A. Yanko, and K. Kuznetsova, "The data errors control in the modular number system based on the nullification procedure," in *Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27-May 1, 2020*, 2020, vol. 2608, pp. 580–593. Accessed: Jul. 02, 2020. [Online]. Available: http://ceur-ws.org/Vol-2608/paper45.pdf

[17] P. V. Ananda Mohan, "Specialized Residue Number Systems," in *Residue Number Systems: Theory and Applications*, P. V. A. Mohan, Ed. Cham: Springer International Publishing, 2016, pp. 177–193. doi: 10.1007/978-3-319-41385-3_8.

[18] G. Pirlo, "Non-Modular Operations of the Residue Number System: Functions for Computing," in *Embedded Systems Design with Special Arithmetic and Number Systems*, A. S. Molahosseini, L. S. de Sousa, and C.-H. Chang, Eds. Cham: Springer International Publishing, 2017, pp. 49–64. doi: 10.1007/978-3-319-49742-6_3.

[19] C. Fan and G. Ge, "A Unified Approach to Whiteman's and Ding-Helleseth's Generalized Cyclotomy Over Residue Class Rings," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1326–1336, Feb. 2014, doi: 10.1109/TIT.2013.2290694.

[20] V. M. Amerbaev, R. A. Solovyev, A. L. Stempkovskiy, and D. V. Telpukhov, "Efficient calculation of cyclic convolution by means of fast Fourier transform in a finite field," in *Proceedings of IEEE East-West Design Test Symposium (EWDTS 2014)*, Sep. 2014, pp. 1–4. doi: 10.1109/EWDTS.2014.7027043.

[21] P. V. An, a Mohan, CDAC, and Bangalore, "Implementation of Residue Number System Based Digital Filters – A Quarterly Publication of ACCS." https://journal.accsindia.org/implementation-of-residue-number-system-based-digital-filters/ (accessed Aug. 16, 2020).

[22] M. Kasianchuk, I. Yakymenko, I. Pazdriy, A. Melnyk, and S. Ivasiev, "Rabin's modified method of encryption using various forms of system of residual classes," in *2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, Feb. 2017, pp. 222–224. doi: 10.1109/CADSM.2017.7916120.

[23] M. Karpinski, S. Ivasiev, I. Yakymenko, M. Kasianchuk, and T. Gancarczyk, "Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes," in *2016 16th International Conference on Control, Automation and Systems (ICCAS)*, Oct. 2016, pp. 1484–1486. doi: 10.1109/ICCAS.2016.7832500.

[24] A. M. Polovko, *Fundamentals of reliability theory*. Published: New York - London: Academic Press., 1968.

[25] "Understanding Redundancy," in *Beyond Redundancy*, John Wiley & Sons, Ltd, 2011, pp. 35–58. doi: 10.1002/9781118104910.ch3.

[26] I. A. Ushakov, Ed., *Optimal Resource Allocation: With Practical Statistical Applications and Theory*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2013. doi: 10.1002/9781118400715.

[27] *Fault-Tolerant Systems*. Elsevier, 2021. doi: 10.1016/C2018-0-02160-X.

[28] D. Radhakrishnan and T. Pyon, "Fault tolerance in RNS: an efficient approach," in *Proceedings., 1990 IEEE International Conference on Computer Design: VLSI in Computers and Processors*, Sep. 1990, pp. 41–44. doi: 10.1109/ICCD.1990.130156.

[29] M. Z. Garaev and A. A. Karatsuba, "THE REPRESENTATION OF RESIDUE CLASSES BY PRODUCTS OF SMALL INTEGERS," *Proceedings of the Edinburgh Mathematical Society*, vol. 50, no. 2, pp. 363–375, Jun. 2007, doi: 10.1017/S0013091505000969.

[30] I. A. Ushakov, "Formulation of Optimal Redundancy Problems," in *Optimal Resource Allocation*, John Wiley & Sons, Ltd, 2013, pp. 33–47. doi: 10.1002/9781118400715.ch2.

[31] M. H. Weik, "computer system fault tolerance," in *Computer Science and Communications Dictionary*, M. H. Weik, Ed. Boston, MA: Springer US, 2001, pp. 274–274. doi: 10.1007/1-4020-0613-6_3420.

[32] V. Krasnobaev, V. Popenko, A. Kuznetsov, and T. Kuznetsova, "Method of Control of Data which is Presented by Residual Classes," in *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S T)*, Oct. 2020, pp. 779–784. doi: 10.1109/PICST51311.2020.9468087.

[33] V. Krasnobaev, M. Zub, T. Kuznetsova, I. Perevozova, and O. Maliy, "Mathematical Model of the Process of Tabular's Implementation of the Operation Algebraic Multiplication in the Residues Class," in *2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Sep. 2019, pp. 1–6. doi: 10.1109/UkrMiCo47782.2019.9165400.

ДОДАТОК В

Optimization of the WCF Cost Function to Generate Nonlinear Substitutions

Alexandr Kuznetsov [1,2,3] [0000-0003-2331-6326], Yuriy Gorbenko [2,3] [0000-0002-0652-8629], Nikolay Poluyanenko [2,3] [0000-0001-9386-2547], Sergey Kandiy [2,3] [0000-0003-0552-8341], Yevheniia Matvieieva [2] [0000-0001-9834-2970]

[1] University of Macerata, Via Crescimbeni, 30/32, 62100, Macerata, Italy
[2] V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
[3] JSC "Institute of Information Technologies", Bakulin St., 12, Kharkiv, 61166, Ukraine

kuznetsov@karazin.ua, gorbenkou@iit.kharkov.ua, nlfsr01@gmail.com, sergeykandy@gmail.com, belka.j.0507@gmail.com

Abstract. Modern encryption algorithms with symmetric key are effective means of ensuring the confidentiality of information. Their reliability and cryptographic strength are ensured by the cryptographic properties of the applied crypto-primitives, in particular, nonlinear substitutions (S-bloxes). This work investigates heuristic methods for generating S-boxes. These methods use special cost functions, which are calculated at each iteration of the search algorithm. The input substitution is formed randomly, then the generation algorithm gradually changes this S-box and minimizes (sometimes maximizes) the cost function. However, the problem of rapid generation of highly nonlinear S-boxes has not yet been solved due to the high computational complexity of iterative search. In particular, for the best known result, more than 65,000 iterations have to be performed to find a bijective 8-bit substitution with a nonlinearity of 104. The WCF (Cost Function of the content of the Walsh-Hadamard spectrum) is used there. We investigate this function and optimize its parameters. Our WCF optimization in combination with the Hill Climbing algorithm significantly reduces the number of iterations. In particular, we demonstrate that to find a substitution with a nonlinearity of 104 on average, we need about 53 thousand iterations of the algorithm. In addition, we were able to increase the success rate of heuristic search. Especially, for our tuning in 100% of cases a bijective S-box with nonlinearity 104 was found.

Keywords: nonlinear substitutions, S-boxes, cost function, generation methods, nonlinearity, Walsh-Hadamard transform

1 Introduction

When designing a cipher with a symmetric key, the generation of cryptographically stable nonlinear substitutions (S-boxes) is a difficult task [1–3]. Firstly, nonlinear substitutions should be random, to wit not to contain simple algebraic constructions,

because this can create the preconditions for effective algebraic cryptanalysis [4, 5]. Secondly, S-boxes have to provide the necessary cryptographic properties that significantly complicate the implementation of various cryptanalytic attacks (differential, linear, statistical, etc.) [3, 6, 7]. Thus, the task of generating nonlinear substitutions is complex and extremely important from the point of view of further improvement of cryptographic algorithms with a symmetric key.

Heuristic techniques are considered to be the most promising for the generation of highly nonlinear S-boxes. They allow iteratively to change the initial random S-box until it does not meet the established criteria. However, the time of such generation may be too long. For instance, for the best known result, the generation of random bijective 8-bit substitutions with a nonlinearity of more than 104 requires more than 65,000 iterations [8, 9]. The aim of this work is to optimize heuristic methods to accelerate the generation of highly nonlinear S-boxes.

2 Related works

In this article, we consider heuristic techniques for generating nonlinear substitutions. Such algorithms include heuristic methods:

- Local Search Algorithm [1, 8–10];
- Hill-climbing Algorithm [8, 11–13];
- Gradient Descent method) [6, 14];
- Simulated Annealing algorythm [12, 15–17] and [10, 18];
- Genetic Algorithm [19–21] etc.

The main task of heuristic techniques is to reduce (or in some cases increase) the value functions, which areassociated with the desired property of the S-box. During the operation of the search algorithm, the characteristics of the current S-box are brought closer to the desired value.

It should be noted that the success of generation is very sensitive to the chosen value function, and hence to the choice of its parameters. Among the known value functions should be noted the most popular:

- Clark's cost functions *WHS* [15] and its modification [10, 18];
- Picek's cost functions *PCF* [8, 22];
- Freyre-Echevarría cost functions *WCF* [8, 9].

Here we consider the WCF cost function, which was proposed in [8, 9]. Using the Hill climbing algorithm [2, 11, 23] and the WCF function, the authors obtained the best known result to date from the generation of 8-bit objective substitutions with a nonlinearity of 104 [8, 9]. The average number of iterations of the search algorithm to find the S-box with nonlinearity 104 was 65,933 [9]. In [9] it is stated that out of 30 independent experiments in 11 cases an S-box with nonlinearity of 104 was found. In another publication of the same authors [8] the average value in 70,596 iterations is given.

In this article, we check the results of [8, 9] and optimize the parameters of the WCF function. We confirm the results from [8, 9] and show that the WCF function can be even more efficient. In our experiments, we obtained the lowest value of the number of iterations for the WCF function and the Hill climbing algorithm. In fact, we have been able to significantly increase the efficiency of heuristic search by reducing the number of iterations.

3 Methods

To search for bijective S-boxes with high nonlinearity, we used the Hill climbing algorithm [8, 11–13]. Climbing a hill is an iterative algorithm that begins its search from some possible point randomly selected in the state space. Then the generation mechanism is consistently applied to find the best solution (in terms of the value of the value function), exploring the neighborhood of the current solution. If a better solution is found, it becomes the current solution. The algorithm terminates when no improvement can be found, and the current solution is considered as an approximate solution to the optimization problem.

Hill-climbing algorithm optimizes the cost function by examining adjacent decision points relative to the current point in the decision space. Below we consider (S, f) example of a combinatorial optimization problem (where S is a set of possible solutions; f is a cost function that should be minimized).

Hill-climbing algorithm (for the minimization problem) can be generalized by the following pseudocode 1:

Hill Climbing Pseudocode

1. Choose the initial solution S_i;
2. Generate solutions S_j from the neighborhood of the current solution S_i;
3. If ($f(S_j) < f(S_i)$), then S_j is the current solution;
4. If ($f(S_j) \geq f(S_i)$) for a certain amount S_j, then finish;
5. Go to step 2.

We have programmed an algorithm for climbing a hill, which simultaneously performs a search in several streams running in parallel. The number of threads is specified in the input parameter thread_count (in our case thread_count = 2). The algorithm starts its work with a substitution that is generated randomly. This substitution is set as the current solution. The current solution is common to all threads. At each iteration of the loop, several (according to the thread_count parameter) new solutions are generated, which are generated by the specified mutation operators. The mutation operator randomly selects $k = 2$ different positions in the substitution S_i and rearranges the elements in the selected positions. The new solution S_j is compared to the current S_i. If you get better than the current one, the solution is set to current.

All iterations of the search according to the algorithm of climbing the hill are performed in the inner cycle. Iterations of the inner loop are nested in the outer loop. An external loop is not required for the algorithm to work, it is introduced only to monitor the current state of the search process and optimize the choice of its parameters. The algorithm is considered in more detail in [10].

A bijective 8-bit S-box with nonlinearity $N_f = 104$ was chosen as the target S-box. The following were used as other parameter:

- number of internal cycles - max_inner_loops = 10000;
- maximum number of external cycles - max_outer_loops = 50;
- the maximum number of consecutive external cycles in which no improvement in the value function is performed - max_frozen_outer_loops = 5.

Criteria for stopping the algorithm:

- finding a bijective S-box with nonlinearity 104;
- achieving the maximum number of iterations (corresponds to the value of thread_count x max_inner_loops x max_outer_loops);
- achieving the number of consecutive external cycles in which no improvement of the value function of the value of max_frozen_outer_loops.

4 Research of the WCF cost function

As the main apparatus of analysis and study of the features of the criteria, it is convenient to choose the Fourier transform and Walsh Boolean functions [1, 11, 24].

4.1 Transformation of Walsh-Hadamard function

Denote $\mathbf{x}, \boldsymbol{\omega}$ by binary sets the lengths n above $GF(2)$, and x_i, ω_i - the coordinates of these sets. If, $f(x_1, x_2, \ldots, x_n)$ is a Boolean function of binary variables, then we denote $f'(x_1, x_2, \ldots, x_n) = (-1)^{f(x_1, x_2, \ldots, x_n)}$ by a conjugate function defined on the same set. Functions f and f' unambiguously define each other. The scalar product $\mathbf{x}$ and $\boldsymbol{\omega}$ is an integer function defined as

$$\langle \mathbf{x}, \boldsymbol{\omega} \rangle = \sum_{i=1}^{n} x_i \cdot \omega_i \ .$$

The Walsh transformation of the Boolean function is denoted as

$$W_f\left(f(\mathbf{x}), \omega\right) = \sum_{\mathbf{x} = F_2^n} f(\mathbf{x}) \cdot (-1)^{\langle \mathbf{x}, \omega \rangle} \ .$$

The spectral transformation of the function is denoted by

$$WHT\left(f(\mathbf{x}),\omega\right)=\sum_{\mathbf{x}=F_2^n}(-1)^{f(\mathbf{x})+\langle\mathbf{x},\omega\rangle},$$

and is called the Walsh-Hadamard Boolean transformation.

Spectral transformations allow us to directly assess the balance, nonlinearity and correlation immunity of the Boolean function [1, 11, 24]. In particular, the nonlinearity of the S-box is expressed as:

$$N(S)=2^{n-1}-\frac{1}{2}\cdot\max\left(\left|WHT\right|\right), \quad (1)$$

Where $\max\left(\left|WHT\right|\right)$ is the maximum absolute value in the Walsh-Hadamard spectrum for all component Boolean functions of the S-box.

4.2 Distribution of Walsh-Hadamard spectral coefficients

An example of the values of the Walsh-Hadamard spectral coefficients for a randomly formed bijective 8x8 S-box is presented in Figure 1 (a fragment for 256 values is presented).

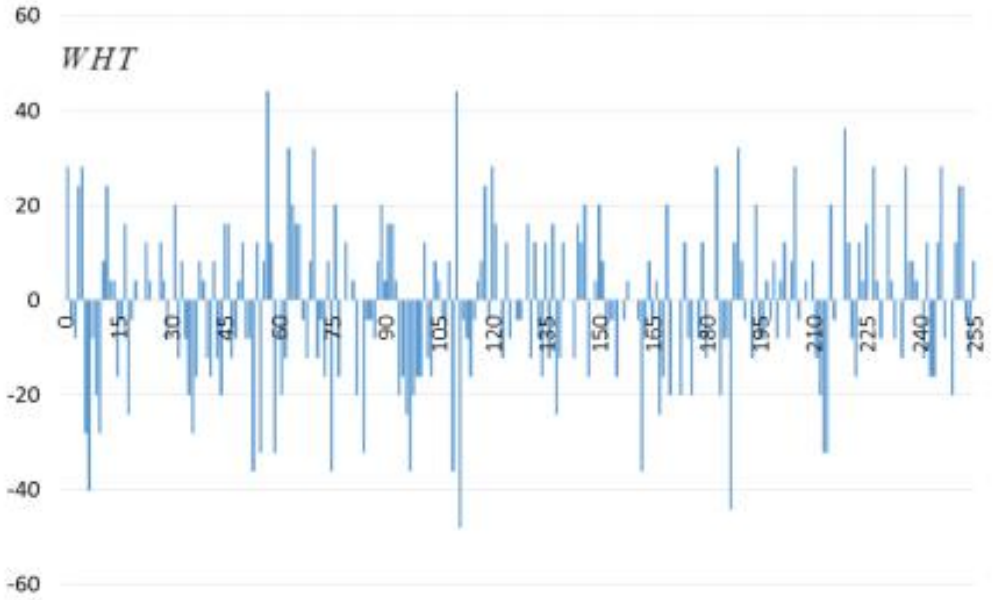


Fig. 1. The first 256 Walsh-Hadamard spectral coefficients for a randomly formed bijective S-box (example)

As you can see for this example, the values WHT vary from - 48 to +57. The change of values WHT always occurs in step 4. The histogram of the distribution of the number of coefficients WHT by their values (for all 65 280 values) is shown in Figure 2. The abscissa line shows the value that WHT takes, and the ordinate - the number of cases value WHT.

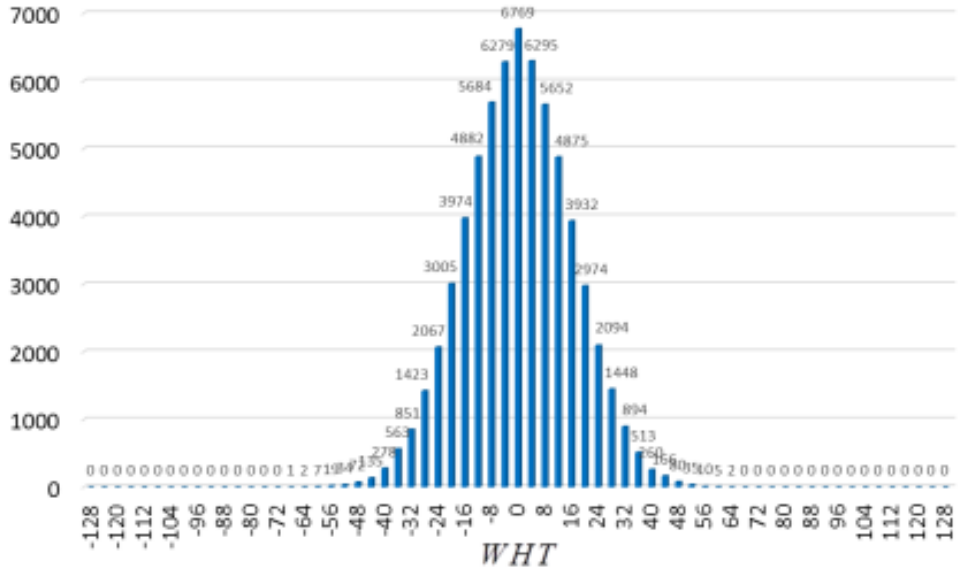


Fig. 2. Distribution of values of Walsh-Hadamard spectral coefficients for a randomly formed bijective S-box (example)

Taking into account (1) we are interested in the maximum value of the spectrum, i.e. $\max\left(\left|WHT\right|\right)$. In the above example, this will be -68, i.e. $N(S)=94$.

When using heuristic algorithms for finding the target S-box is a gradual decrease $\max\left(\left|WHT\right|\right)$, which leads to increased nonlinearity of the S-box. Thus, in Fig. 3 shows the final distribution of quantities by their values at $N(S)=104$. In fig. 4 shows a histogram of changes in the distribution of quantity from the initial state (randomly formed bijective S-box) to the final state. In this experiment, the algorithm of hill climbing was used. A total of 117 WCF enhancements were made. The symbol k indicates the number of received enhancements in the search algorithm.

As we can see from the above results, the form of distribution and its maximum does not change significantly during improvements to the selected search algorithm. Therefore, it seems appropriate to take into account only the part of the distribution of the spectrum of Walsh – Hadamard coefficients, which is close to $\max\left(\left|WHT\right|\right)$ what was realized as a function of the value of WCF.

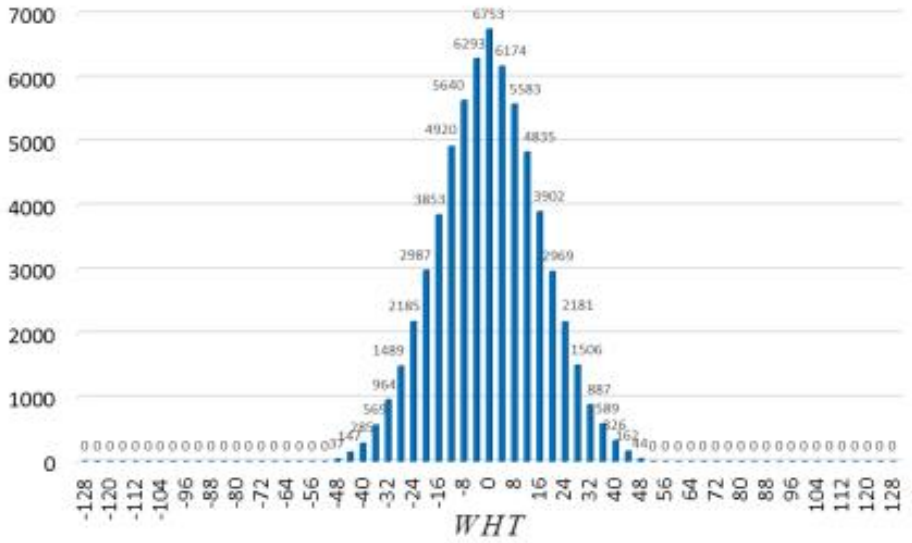


Fig. 3. Distribution of values of Walsh-Hadamard spectral coefficients for the obtained bijective S-box with nonlinearity $N(S)=104$

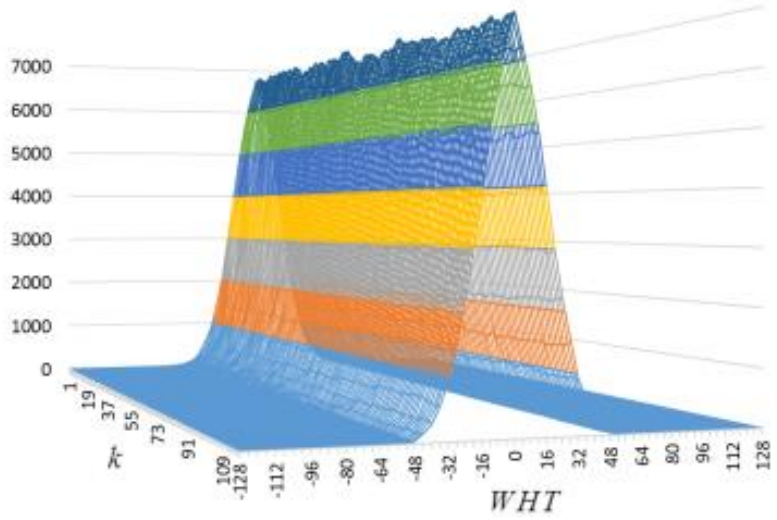


Fig. 4. Histogram of changes in the distribution of Walsh-Hadamard spectral coefficients

4.3 Description of the WCF cost function

The cost function of WCF in the general case has the following form [8, 9]:

$$WCF = \sum_{b=1}^{255}\sum_{i=0}^{255}\prod_{\substack{j=start\\ j+=step}}^{end} \left| |WHT[b,i]| - j \right|, \qquad (2)$$

where:

- WHT – Walsh-Hadamard spectral coefficients;
- $start, step, end$ – some integer values are usually $start = 0, step = 4$ (based on the multiplicity of coefficients WHT of four);
- i – cycle variable for all component functions and their linear combinations;
- b – cycle variable for all linear functions.

For each S-box of size 8x8 there are $256 \cdot 256 = 65536$ values of Walsh-Hadamard spectral coefficients. Moreover, $b = 0$ the first value will always be equal to 256, and the next 255 - zero, so the sum starts with one and the total number of coefficients studied is 65,280

The histogram of the change in the value of the WCF function, which corresponds to the change in the distribution of the Walsh-Hadamard spectral coefficients, is shown in Fig. 5. This diagram is obtained for the parameters $start = 0, step = 4, end = 32$.

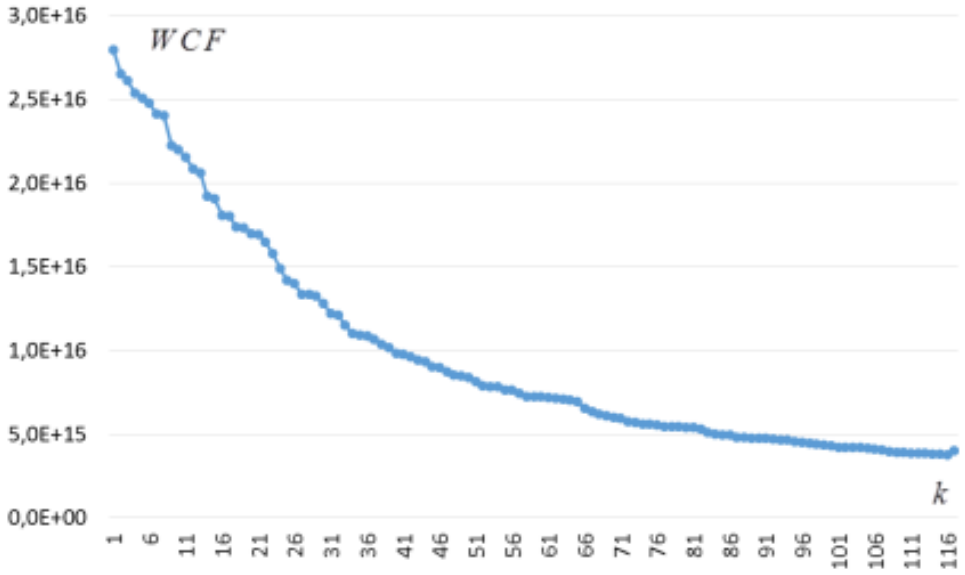


Fig. 5. Diagram of the change in the value of the *WCF* function

The WCF function actually takes as zero the values of the Walsh-Hadamard spectral coefficients and takes into account only their extreme values, the indices of which are modulo greater than the values *end*. Visually, it is presented in Fig. 6, which is obtained from the values of the distribution shown in Fig. 3. The constraints are used in the calculation of the WCF function are applied here and are presented on a logarithmic scale.

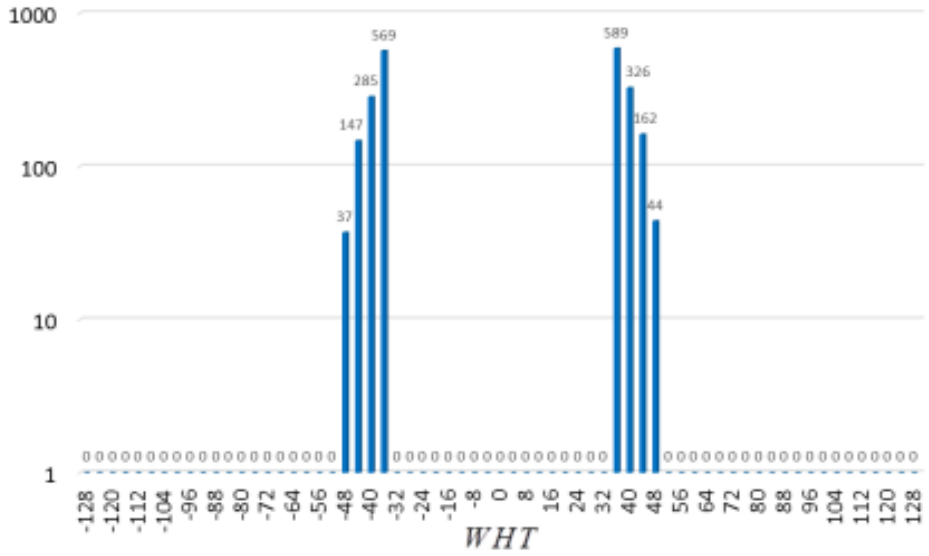


Fig. 6. Distribution of values of Walsh-Hadamard spectral coefficients taken into account in the WCF function for the obtained bijective S-box with nonlinearity $N_f = 104$ (example)

The calculation of function (2) for this example will be performed as follows:

$$WCF = \sum_{b=1}^{255}\sum_{i=0}^{255}\prod_{\substack{j=start\\ j+=step}}^{end} \| WHT[b,i]| - j| =$$

$$= 37\cdot\Big[\big(|-48|-0\big)\cdot\big(|-48|-4\big)\cdot\big(|-48|-8\big)\cdot\big(|-48|-12\big)\cdot\big(|-48|-16\big)\cdot$$
$$\cdot\big(|-48|-20\big)\cdot\big(|-48|-24\big)\cdot\big(|-48|-28\big)\cdot\big(|-48|-32\big)\Big]+$$
$$+147\cdot\Big[\big(|-44|-0\big)\cdot\big(|-44|-4\big)\cdot\big(|-44|-8\big)\cdot\big(|-44|-12\big)\cdot\big(|-44|-16\big)\cdot$$
$$\cdot\big(|-44|-20\big)\cdot\big(|-44|-24\big)\cdot\big(|-44|-28\big)\cdot\big(|-44|-32\big)\Big]+$$
$$+285\cdot\Big[\big(|-40|-0\big)\cdot\big(|-40|-4\big)\cdot\big(|-40|-8\big)\cdot\big(|-40|-12\big)\cdot\big(|-40|-16\big)\cdot$$
$$\cdot\big(|-40|-20\big)\cdot\big(|-40|-24\big)\cdot\big(|-40|-28\big)\cdot\big(|-40|-32\big)\Big]+$$
$$+569\cdot\Big[\big(|-36|-0\big)\cdot\big(|-36|-4\big)\cdot\big(|-36|-8\big)\cdot\big(|-36|-12\big)\cdot\big(|-36|-16\big)\cdot$$
$$\cdot\big(|-36|-20\big)\cdot\big(|-36|-24\big)\cdot\big(|-36|-28\big)\cdot\big(|-36|-32\big)\Big]+$$
$$+589\cdot\Big[\big(|36|-0\big)\cdot\big(|36|-4\big)\cdot\big(|36|-8\big)\cdot\big(|36|-12\big)\cdot\big(|36|-16\big)\cdot$$
$$\cdot\big(|36|-20\big)\cdot\big(|36|-24\big)\cdot\big(|36|-28\big)\cdot\big(|36|-32\big)\Big]+$$
$$+326\cdot\Big[\big(|40|-0\big)\cdot\big(|40|-4\big)\cdot\big(|40|-8\big)\cdot\big(|40|-12\big)\cdot\big(|40|-16\big)\cdot$$
$$\cdot\big(|40|-20\big)\cdot\big(|40|-24\big)\cdot\big(|40|-28\big)\cdot\big(|40|-32\big)\Big]+$$

$$+162\cdot\left[\left(|44|-0\right)\cdot\left(|44|-4\right)\cdot\left(|44|-8\right)\cdot\left(|44|-12\right)\cdot\left(|44|-16\right)\cdot\right.$$
$$\left.\cdot\left(|44|-20\right)\cdot\left(|44|-24\right)\cdot\left(|44|-28\right)\cdot\left(|44|-32\right)\right]+$$
$$+44\cdot\left[\left(|48|-0\right)\cdot\left(|48|-4\right)\cdot\left(|48|-8\right)\cdot\left(|48|-12\right)\cdot\left(|48|-16\right)\cdot\right.$$
$$\left.\cdot\left(|48|-20\right)\cdot\left(|48|-24\right)\cdot\left(|48|-28\right)\cdot\left(|48|-32\right)\right]=4\ 003\ 221\ 743\ 861\ 760.$$

We have got the result $WCF = 4\ 003\ 221\ 743\ 861\ 760$ that corresponds to the last value (if $k = 117$) in fig.5.

From the given example of calculations we see:

1. Walsh-Hadamard spectral coefficients with higher absolute values have much more weight than their "neighboring" lower coefficient. For example, an increase of one in the number of spectral coefficients with a value of 48 is balanced by a decrease in the number of spectral coefficients with a value of 44 by 4 units, or with a value of 40 by 22 units, or with a value of 36 by 220 units;
2. Unlike the WHS value function proposed by Clark in [15], the WCF function does not take into account the central values in the spectrum distribution. That is, it will cause very significant changes in the distribution WHT, the values of which are less than end, will not be taken into account in the WCF function;
3. What matters is not only the maximum value of the spectrum of the Walsh-Hadamard coefficients, but also those following the maximum values. Thus, of the two S-boxes that have the same maximum values of the spectrum of the Walsh – Hadamard coefficients, the S-box that has smaller values of the other values of the spectrum of coefficients taken into account will be selected for the next search.;
4. The value of the WCF function is growing very fast. For example, when selecting $end = 28$ the value of the WCF function of a randomly formed S-box is close to $\sim 1\cdot 10^{15}$, when $end = 32$ close to $\sim 2\cdot 10^{16}$, when $end = 36$ close to $\sim 5\cdot 10^{17}$, and when $end = 40$ the value of the WCF function exceeds 64-bit value (which covers the range from --9 223 372 036 854 775 808 to 9 223 372 036 854 775 807) and requires the use of longer arithmetic, which potentially reduces the performance of the search algorithm.

5 Results of testing and optimization of WCF functions

5.1 Modification of WCF function

To reduce the growth rate of the WCF function and the possibility of its application $end \geq 40$ to 64-bit integers, given the multiplicity of the spectrum of Walsh – Hadamard coefficients by four, you can reduce each factor by 4 times. You can programmatically do this by bitwise shifting the numbers without qualitatively changing the behavior of the WCF function. That is, in the future we will investigate the modified value function of the species:

$$WCF = \sum_{b=1}^{255}\sum_{i=0}^{255}\prod_{\substack{j=start\\ j+=step}}^{end}\frac{1}{4}\cdot\left|\left|WHT[b,i]\right|-j\right|. \qquad (3)$$

This modification reduces the value of WCF in $4^{(end-start)/step}$ times. The value of function (4) for a randomly generated S-box will be:

- For the parameter $end = 28$ close to $\sim 1\cdot 10^{10}$,
- For the parameter $end = 32$ close to $\sim 1\cdot 10^{11}$,
- For the parameter $end = 36$ close to $\sim 5\cdot 10^{11}$,
- For the parameter $end = 40$ close to $\sim 5\cdot 10^{12}$,
- For the parameter $end = 44$ close to $\sim 1\cdot 10^{13}$,
- For the parameter $end = 48$ close to $\sim 5\cdot 10^{13}$,
- For the parameter $end = 52$ close to $\sim 1\cdot 10^{14}$,
- For the parameter $end = 56$ close to $\sim 5\cdot 10^{14}$.

It does not make practical sense to set the value $end > 48$, as it will be appropriate, ie for $N(S) = 104$ the value of the value function WCF = 0.

5.2 Research of the influence of the parameter *end*

To investigate the effect of parameters on the value of the value function (3), we conducted testing. The parameter *end* was changed in the range from 0 to 48 in steps of 4. It does not make sense to change the parameters $start = 0$ and $step = 4$ because of the values that can take the spectrum of Walsh – Hadamard coefficients.

In total, we conducted 100 exams (individual launches of the program to find the target S-box) for each value *end*. We calculated for each series of exams:

- number of successful exams, i.e. cases of finding the target S-box (bijective 8-bit substitution with nonlinearity $N(S) = 104$);
- the number of iterations to find the target S-box (which is proportional to the time spent searching);
- the sequence of changes to the accepted values of the WCF function in the search algorithm and the current value $N(S)$.

In fig. 7 - 14 the test results are showed:

- (a) the number of iterations r that were performed in each exam to find the target S-box;
- (б) distribution of the number of iterations r.

Denote the average number of iterations by the symbol r^{aver}. Summarized test results are shown in table 1.

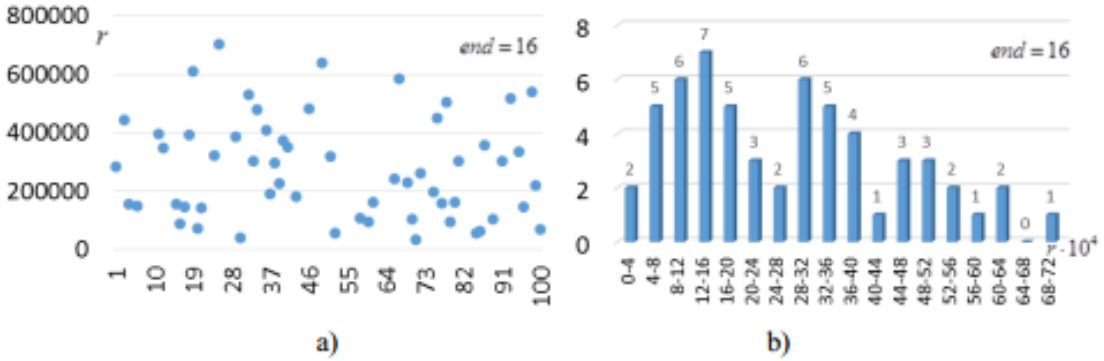


Fig. 7. Test results of Hill climbing algorithm with WCF cost function, $end = 16$

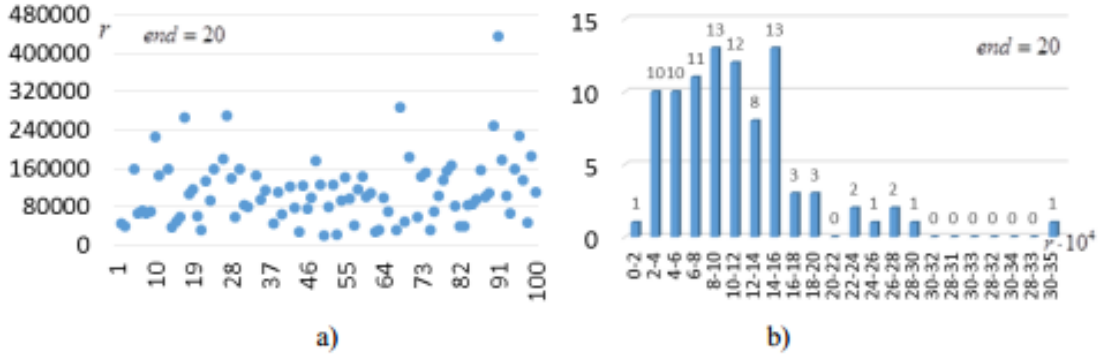


Fig. 8. Test results of Hill climbing algorithm with WCF cost function, $end = 20$

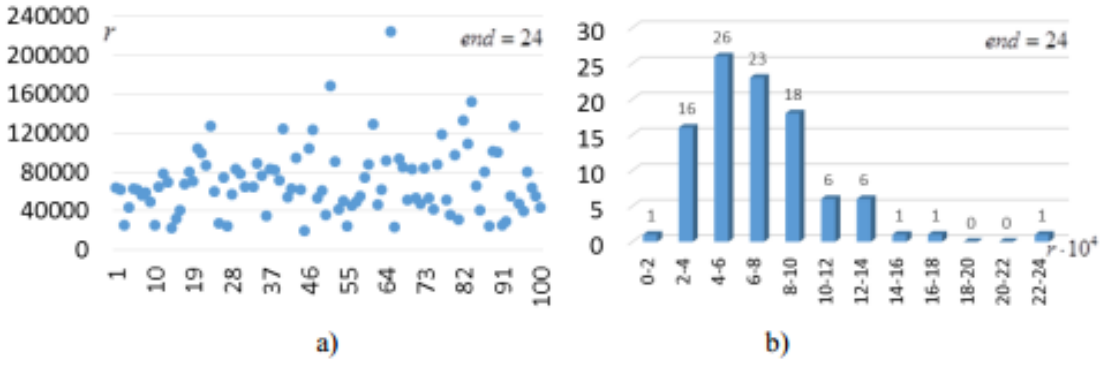
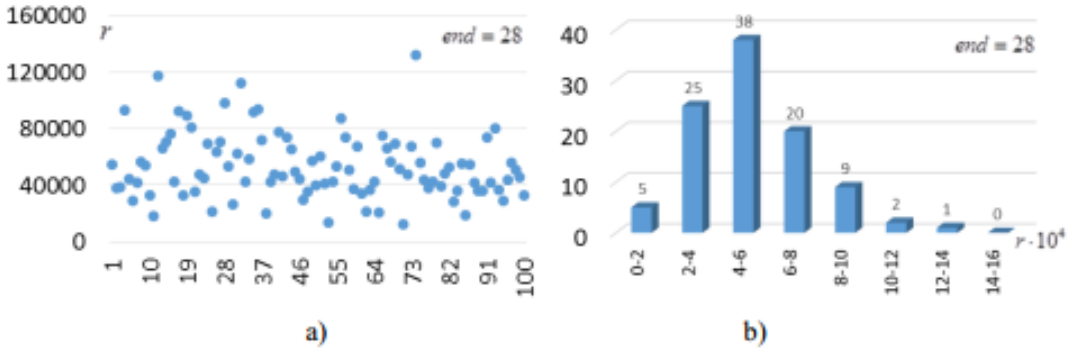
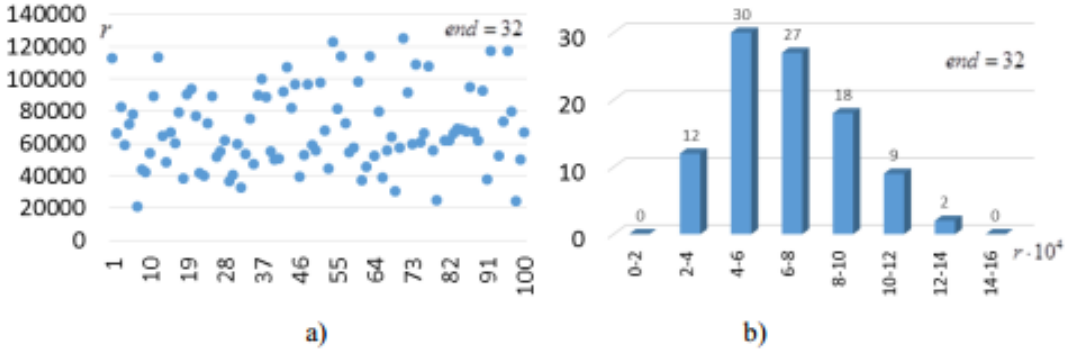


Fig. 9. Test results of Hill climbing algorithm with WCF cost function, $end = 24$



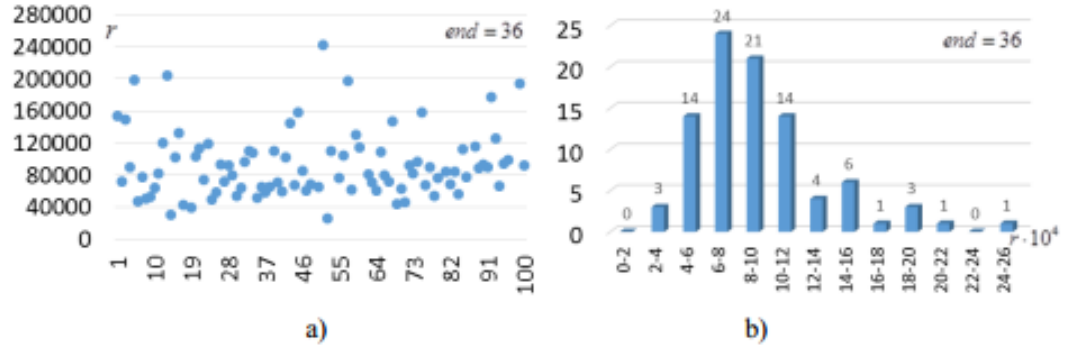
a) b)

Fig. 10. Test results of Hill climbing algorithm with WCF cost function, $end = 28$



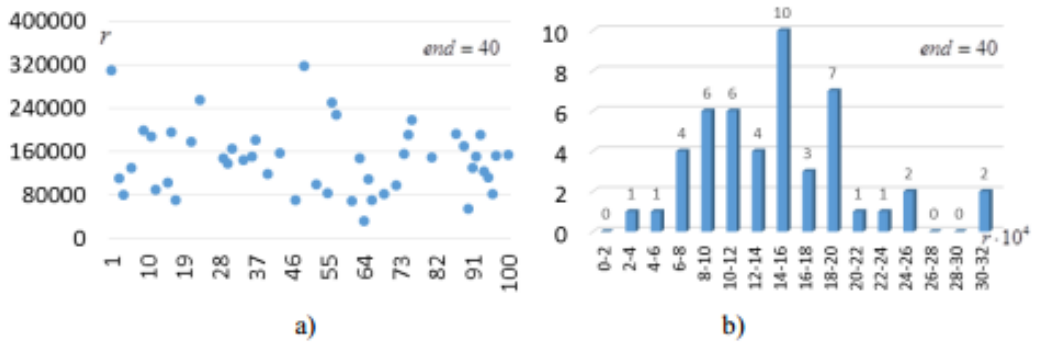
a) b)

Fig. 11. Test results of Hill climbing algorithm with WCF cost function, $end = 32$



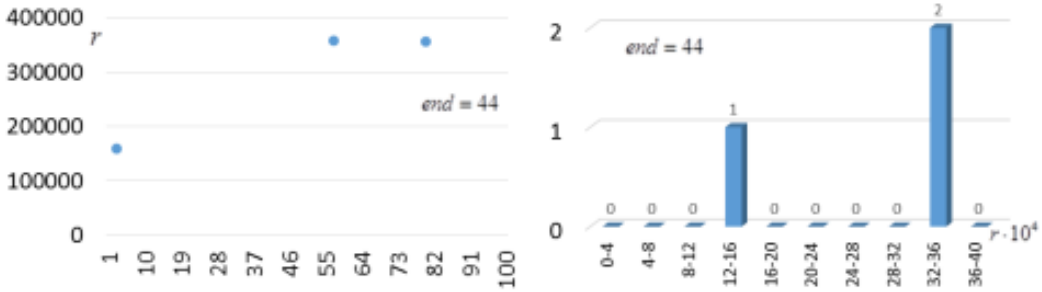
a) b)

Fig. 12. Test results of Hill climbing algorithm with WCF cost function, $end = 36$



a) b)

Fig. 13. Test results of Hill climbing algorithm with WCF cost function, $end = 40$



a) b)

Fig. 14. Test results of Hill climbing algorithm with WCF cost function, $end = 44$

Table 1. Generalized test results of Hill climbing algorithm with WCF cost function for different values *end*

end	Number of found S-boxes	Average number of iterations (r^{aver})
0	0	–
4	0	–
8	0	–
12	0	–
16	58	276 380
20	91	110 770
24	99	69 344
28	100	53 160
32	98	68 855
36	92	92 709
40	48	146 074
44	3	291 568
48	0	–

6 Discussion of results

According to the test results, we received a significant acceleration in the formation of target substitutions. In particular, the average number of iterations was significantly reduced compared to the best result known to date.

The value of $end = 32$ corresponds to the case of the value function, which was proposed and investigated in [8, 9]. According to the results of testing the Hill climbing algorithm in [8], the average number of iterations was $r^{aver} = 70{,}596$. In [9] the same authors published the best result, which is 65,933 iterations. Our rate from Table 1 for $end = 32$ gives an average of 68,855 iterations, which is close to the values from [8, 9]. Therefore, we consider this result confirmed. However, from our results (Table 1) we see that the lowest number of iterations is achieved at $end = 28$. In this case, on average, you need to perform only 53,160 iterations. This is almost 20% better than for the results of [8, 9]. In addition, we have significantly improved the frequency of target substitutions. According to the results of testing in [8], only in 11 cases out of 30 independent experiments was found an S-box with a nonlinearity of 104. For our settings, success was achieved in 100% of cases

Analyzing the second column in Table 1 we also see that for other values of the parameter end the number of found S-boxes is decreasing. However, this is not because the algorithm is unable to find a solution, but because the exit condition is met when the selected stop criterion is reached at max_frozen_outer_loops = 5. In fig. Figures 15 and 16 show examples of successive changes in the values of the WCF cost function and the corresponding nonlinearity values $N(S)$ for $end = 28$ and $end = 40$ during the operation of the search algorithm. As you can see, on average, during the search algorithm, there are 100 to 150 improvements to the values of the WCF cost function.

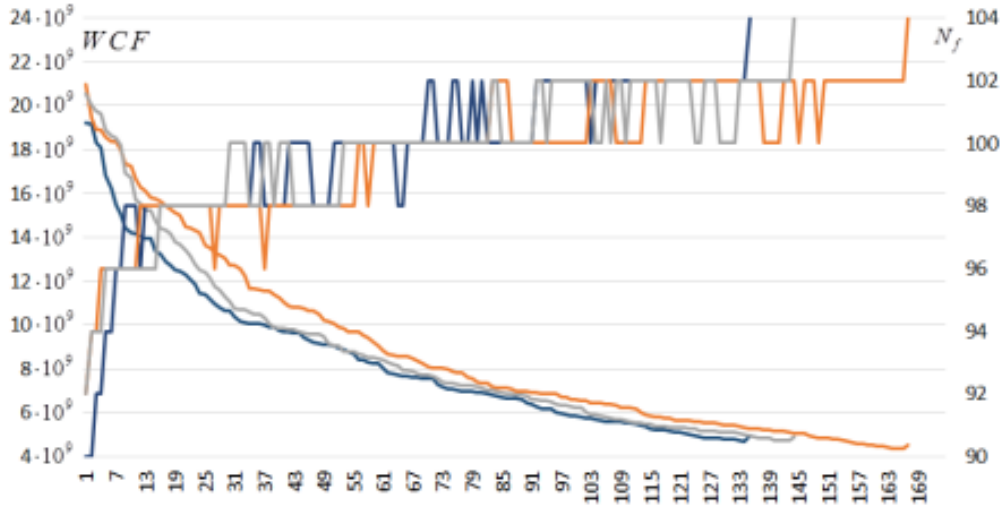


Fig. 15. The sequence of changes in WCF values and $N(S)$, which were recorded with each improvement of the value of the WCF value function, $end = 28$

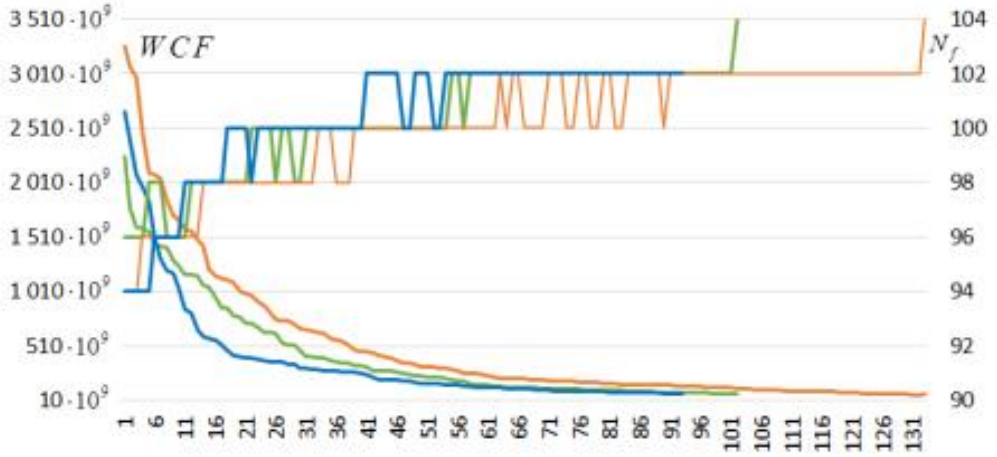


Fig. 16. The sequence of changes in WCF values and $N(S)$, which were recorded with each improvement in the value of the WCF value function, $end = 40$.

7 Conclusions

In this article, we investigated the possibility of forming highly nonlinear S-boxes using an easy-to-implement heuristic hill-climbing algorithm. We used WCF as a cost function.

According to the test results, the results published in [8, 9] were verified and confirmed. In particular, we confirm that the WCF cost function can really speed up the formation of highly nonlinear substitutions. Using the Hill climbing algorithm, we obtained an average value of 68,855 iterations, which is close to the results published in [8] and [9] (65,933 and 70,596, respectively).

It should be noted that in [8, 9] a fixed parameter $end = 32$ was used. We modified the WCF value function and performed extended testing for different values end. According to the test results, the best parameters were determined to have a value $end = 28$ at which a bijective S-box with a nonlinearity of 104 was found in 100% (of the tests). The average number of iterations of the Hill climbing algorithm was 53,160 iterations. This improves the result known from [8, 9] by almost 20%.

References

1. Freyre Echevarría, A.: Evolución híbrida de s-cajas no lineales resistentes a ataques de potencia, (2020). https://doi.org/10.13140/RG.2.2.17037.77284/1.
2. McLaughlin, J.: Applications of search techniques to cryptanalysis and the construction of cipher components, https://etheses.whiterose.ac.uk/3674/, (2012).
3. Álvarez-Cubero, J.: Vector Boolean Functions: applications in symmetric cryptography, (2015). https://doi.org/10.13140/RG.2.2.12540.23685.
4. Bard, G.V.: Algebraic Cryptanalysis. Springer US, Boston, MA (2009). https://doi.org/10.1007/978-0-387-88757-9.

5. Courtois, N.T., Bard, G.V.: Algebraic Cryptanalysis of the Data Encryption Standard. In: Galbraith, S.D. (ed.) Cryptography and Coding. pp. 152–169. Springer, Berlin, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77272-9_10.
6. Rodinko, M., Oliynykov, R., Gorbenko, Y.: Optimization of the High Nonlinear S-Boxes Generation Method. Tatra Mountains Mathematical Publications. 70, 93–105 (2017). https://doi.org/10.1515/tmmp-2017-0020.
7. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N.: Stream Ciphers in Modern Real-time IT Systems. Springer Nature, Cham (2022). https://doi.org/10.1007/978-3-030-79770-6.
8. Freyre-Echevarría, A., Alanezi, A., Martínez-Díaz, I., Ahmad, M., Abd El-Latif, A.A., Kolivand, H., Razaq, A.: An External Parameter Independent Novel Cost Function for Evolving Bijective Substitution-Boxes. Symmetry. 12, 1896 (2020). https://doi.org/10.3390/sym12111896.
9. Freyre Echevarría, A., Martínez Díaz, I.: A new cost function to improve nonlinearity of bijective S-boxes. (2020).
10. Kuznetsov, A., Poluyanenko, N., Kandii, S., Zaichenko, Y., Prokopovich-Tkachenko, D., Katkova, T.: Optimizing the Local Search Algorithm for Generating S-Boxes. In: 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S T). pp. 458–464 (2021). https://doi.org/10.1109/PICST54195.2021.9772163.
11. Burnett, L.D.: Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography, https://eprints.qut.edu.au/16023/, (2005).
12. Ivanov, G., Nikolov, N., Nikova, S.: Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm. In: Pasalic, E. and Knudsen, L.R. (eds.) Cryptography and Information Security in the Balkans. pp. 31–42. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-29172-7_3.
13. Freyre-Echevarría, A., Martínez-Díaz, I., Pérez, C.M.L., Sosa-Gómez, G., Rojas, O.: Evolving Nonlinear S-Boxes With Improved Theoretical Resilience to Power Attacks. IEEE Access. 8, 202728–202737 (2020). https://doi.org/10.1109/ACCESS.2020.3035163.
14. Kazymyrov, O., Kazymyrova, V., Oliynykov, R.: A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent. (2013).
15. Clark, J.A., Jacob, J.L., Stepney, S.: The design of S-boxes by simulated annealing. New Gener Comput. 23, 219–231 (2005). https://doi.org/10.1007/BF03037656.
16. McLaughlin, J.: Applications of search techniques to cryptanalysis and the construction of cipher components, http://etheses.whiterose.ac.uk/3674/, (2012).
17. Wang, J., Zhu, Y., Zhou, C., Qi, Z.: Construction Method and Performance Analysis of Chaotic S-Box Based on a Memorable Simulated Annealing Algorithm. Symmetry. 12, 2115 (2020). https://doi.org/10.3390/sym12122115.
18. Kuznetsov, A., Poluyanenko, N., Kandii, S., Zaichenko, Y., Prokopovich-Tkachenko, D., Katkova, T.: WHS Cost Function for Generating S-boxes. In: 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S T). pp. 434–438 (2021). https://doi.org/10.1109/PICST54195.2021.9772133.
19. Ivanov, G., Nikolov, N., Nikova, S.: Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties. Cryptogr. Commun. 8, 247–276 (2016). https://doi.org/10.1007/s12095-015-0170-5.
20. Kapuściński, T., Nowicki, R.K., Napoli, C.: Application of Genetic Algorithms in the Construction of Invertible Substitution Boxes. In: Rutkowski, L., Korytkowski, M., Scherer, R., Tadeusiewicz, R., Zadeh, L.A., and Zurada, J.M. (eds.) Artificial Intelligence

and Soft Computing. pp. 380–391. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-39378-0_33.

21. Mariot, L., Leporati, A.: Heuristic Search by Particle Swarm Optimization of Boolean Functions for Cryptographic Applications. In: Proceedings of the Companion Publication of the 2015 Annual Conference on Genetic and Evolutionary Computation. pp. 1425–1426. Association for Computing Machinery, New York, NY, USA (2015). https://doi.org/10.1145/2739482.2764674.
22. Picek, S., Cupic, M., Rotim, L.: A New Cost Function for Evolution of S-Boxes. Evolutionary Computation. 24, 695–718 (2016). https://doi.org/10.1162/EVCO_a_00191.
23. Clark, A.J.: Optimisation heuristics for cryptology, https://eprints.qut.edu.au/15777/, (1998).
24. Cusick, T., Stănică, P.: Cryptographic Boolean Functions and Applications: Second edition. (2017).