НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО
ІНФОРМАЦІЙНОГО ПРОСТОРУ

ПУСТОВІТ ОЛЕКСАНДР СЕРГІЙОВИЧ

УДК 519.1 + 519.72

ЗАСТОСУВАННЯ ТЕОРІЇ ЕКСТРЕМАЛЬНИХ ГРАФІВ ДО СУЧАСНИХ ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Спеціальність 05.13.06 – Інформаційні технології

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня

кандидата технічних наук

Київ – 2021

Дисертацією є рукопис.

Робота виконана на в Інституті телекомунікацій і глобального інформаційного простору Національної академії наук України

Науковий керівник: доктор фізико-математичних наук, професор
Устименко Василь Олександрович,
Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України,
завідувач відділу інформаційної безпеки

Офіційні опоненти: доктор фізико-математичних наук, професор
Петравчук Анатолій Петрович
Київський національний університет імені Тараса Шевченка,
завідувач кафедри алгебри і математичної логіки механіко-математичного факультету

доктор технічних наук, доцент
Семко Віктор Володимирович,
Національний авіаційний університет,
професор кафедри комп'ютеризованих систем управління факультету кібербезпеки, комп'ютерної та програмної інженерії

Захист дисертації відбудеться «9» грудня 2021 року о 13 годині на засіданні спеціалізованої вченої ради Д 26.255.01 в Інституті телекомунікацій і глобального інформаційного простору НАН України за адресою: 03186, м. Київ, Чоколівський бульвар, буд. 13, к.601.

З дисертацією можна ознайомитись у бібліотеці Інституту телекомунікацій і глобального інформаційного простору НАН України за адресою: 03186, м.Київ, Чоколівський бульвар, буд. 13.

Автореферат розісланий « » листопада 2021 року.

Учений секретар СВР Д 26.255.01
к.т.н., ст. дослідник О.Г. Лебідь

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми дослідження. Сучасний стан розвитку суспільства характеризується різким зростанням інформаційних потоків не тільки в засобах масової інформації, але й у сфері виробництва, науки, культури. Стрімке вдосконалювання комп'ютерних технологій позначилося й на принципах побудови захисту інформації.

Проблема захисту інформації з'явилася ще задовго до появи комп'ютерів. З самого початку свого розвитку системи інформаційної безпеки розроблялися для військових відомств. Розголошення такої інформації могло привести до величезних людських жертв, тому конфіденційності в системах безпеки приділялася особлива увага. Очевидно, що надійно захистити повідомлення й дані від розголошення і перехоплення може тільки повне їхнє шифрування.

На сьогоднішній час у галузі захисту інформації має місце велика кількість розробок, для яких відсутній системний аналіз, і тому їх часом неможливо порівняти між собою.

В наш час відбувається криза теорії кібербезпеки викликана неспроможністю сучасних інструментів захисту інформації відповісти зростаючим потребам організацій працюючих у Глобальному Інформаційному просторі.

Одна з таких вимог коротко названа Викликом Великих Даних (Big Data Challenge), вона викликана експоненційним зростом працюючих Інформаційних Систем та обсягами інформації при обробці та потребує значно швидших алгоритмів захисту великих множин даних.

Інший виклик пов’язаний з протидією кібертероризму та кіберагресії. Визнаним фактом є перелік успішних кібертерористичних атак, які підтримуються організаціями з практично необмеженими фінансовими та обчислювальними ресурсами.

Квантові комп’ютери матимуть спроможність вирішувати теоретичні проблеми недоступні сучасним детермінованим комп’ютерам.

Національний Інститут стандартизації технологій Сполучених Штатів Америки оголосив тендер на виявлення найкращих відомих нових алгоритмів асиметричної криптографії з публічним ключем для їх постквантової сертифікації. Такі алгоритми розбиваються на класи криптосистем, що спираються на:

- теорію кодування (Code based Cryptography),
- теорію решіток (Lattice based Cryptography),
- поліноміальні функції від багатьох змінних (Multivariate Cryptography),
- супереліптичні криві (Superelliptic curves),
- функції хешування (Hash functions Cryptography).

В березні 2019 завершився перший раунд цього тендеру, під час другого раунду спеціалісти зі стандартизації виконують дослідження властивостей відібраних у 2019 році алгоритмів.

У липні 2020 року розпочався третій раунд для остаточного подальшого дослідження вже вибраних алгоритмів. В області криптографії від багатьох змінних для подальшого дослідження відбираються лише цифрові підписи на

зразок олії та оцту. Їх не можна використовувати як алгоритми шифрування. Цей факт мотивує різні, ніж загальнодоступні напрямки криптографії від багатьох змінних.

На сьогоднішній день питання побудови нових алгоритмів захисту інформації розглядається вітчизняними та багатьма зарубіжними фахівцями та науковцями. Можна назвати дослідників зі Швейцарії (J. Rozenberg , G. Maze , C. Monico), Сполучених Штатів Америки (T. Shaska, V. Shpilrain, A. Myasnikov, D. Kahrobei та інші), Російської Федерації (D. Moldovjan, A.. Moldovjan, D. Grigoriev, I. Ponomarenko, V. Roman'kov), Великої Британії (S. Blackburn, S Galbraith), Іспанії (J. Lopez Ramos, J. Gutierez) та інших країн.

В Україні займаються як хеш функціями (І. Горбенко, Р. Олійников., О. Казимиров, В. Руженцев, О. Кузнєцов, Ю. Горбенко та інші) так і теоретичною криптографією з використанням алгебро-комбінаторних об'єктів (В. Устименко, М. Савчук, О. Фаль, В. Задірака, А. Напрієнко, А. Олійник та інші).

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота пов'язана з вирішенням науково-технічних задач, сформульованих в Стратегії кібербезпеки України, затвердженої Указом Президента України №96/2016 від 27.01.2016 р., в Стратегії національної безпеки України, затвердженої Указом Президента України № 287/2015 від 26.05.2015 р., а також в «Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» затвердженому Наказом №660 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 02.12.2014 р. Дисертаційна робота виконана у рамках науково-дослідних робіт: «Аналіз складних нелінійних динамічних систем, що використовуються у новітніх телекомунікаційних технологіях перетворення, збереження та захисту інформації» (№ держреєстрації: 0112U002714), «Розробка методів захисту інформації що використовують новітні досягнення екстремальної теорії графів» (№ держреєстрації: 0112U007444), «Створення програмно-інформаційних засобів інформаційно-аналітичного забезпечення мережецентричних ситуаційних центрів» (№ держреєстрації: 0221U104666).

Мета і задачі дослідження. Метою дисертаційної роботи є розв'язання нових постквантових задач захисту інформації. А саме:

- розробка і створення унікальних протоколів обміну ключів,
- розробка і створення залежних дайджестів електронних документів для автентифікації нових постквантових криптосистем шифрування,
- розробка і створення нових швидких потокових алгоритмів з відпірністю атак лінеаризації.

Об'єктом дослідження є Марковський процес блукання на алгебраїчних графах та задач дослідження його криптографічних властивостей.

Предметом дослідження є криптографічні прототипи, що будуються за екстремальними графами та графами-експандерами.

Методи дослідження. При вирішенні поставлених задач у дисертаційній роботі було використано методи Екстремальної теорії графів, Теорії скінченних геометрій та Теорії символьних обчислень разом із методами некомутативної криптографії та прикладної алгебраїчної геометрії.

Для задач симетричної криптографії (потокове шифрування та створення дайджестів електронних документів) використовувались обчислювальні методи. При дослідженні властивостей (швидкодія, степені змішування) вживались статистичні методи.

Наукова новизна одержаних результатів. Новими результатами, отриманими в дисертаційній роботі є:

1) вперше в термінах теорії алгебраїчних графів та графів-експандерів створено криптографічно стійкі постквантові швидкі алгоритми для хешування великих файлів у дайджесту заданих розмірів, який буде чутливим до будь-яких змін символів у файлі;

2) вперше розроблені алгоритми створення чутливих дайджестів електронних файлів для виявлення кібератак на віртуальні організації з покращеним на 45% показником аваланч ефекту;

3) вперше в термінах Алгебраїчної Геометрії запропоновано нову парадигму, в якій теорія алгебраїчних графів та некомутативна алгебра використовується для розробки та впровадження нових несиметричних інструментів криптографії (протоколи, криптосистеми, інструмент контролю доступу), стійких до кібератак супротивника у постквантову епоху;

4) вперше в термінах теорії алгебраїчних графів створено алгоритми використання напівгрупи над скінченними комутативними кільцями для розробки швидких потокових алгоритмів шифрування зі зростаючим простором відкритих текстів;

5) вперше теорію скінченних геометрій використано для створення алгоритмів електронного підпису криптографії від багатьох змінних, які замість публічних ключів використовують протоколи некомутативної криптографії.

Результати дисертаційних досліджень реалізовані й впроваджені в:

Київському університеті імені Бориса Грінченка в рамках навчальних дисциплін «Методи побудови та аналізу криптосистем», «Математичні методи криптографії» та впроваджені в програмно-апаратне забезпечення «Центру технологій захисту інформаційних активів» при розгортанні Лабораторії криптографічного та технічного захисту інформації.

ТОВ «Алгорітм –Х» у програмно-апаратне забезпечення при створенні алгоритмів захисту мереж ситуаційних центрів та алгоритмів виявлення кібератак.

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У статтях написаних у співавторстві з керівником дисертаційної роботи, здобувачу належить: в [2] – імплементація потокового алгоритму шифрування над спеціальними кільцями, дослідження їх властивостей як теоретичними методами, так і з використанням комп’ютерної симуляції, [3] – імплементація потокових алгоритмів створення дайджестів для спеціальних комутативних кілець (скінченні поля, арифметичні кільця за модулем та булевих кілець), вивчення параметрів для цих алгоритмів та рівня відповідного аваланч ефекту, [5] – імплементація публічних ключів визначених за графами, використання комп’ютерної симуляції для дослідження розміру ключа, швидкодії та властивостей змішування, [6] – імплементація протоколів обміну ключами,

визначеними за стабільними групами перетворень афінного простору та їх розширень до криптосистеми типу Ель Гамаля. Вивчення властивостей нових криптосистем за результатами комп'ютерної симуляції. У працях [7]-[18] – презентація виників комп'ютерної симуляції та теоретичних властивостей запропонованих алгоритмів.

Апробація результатів роботи. Основні положення і результати досліджень доповідалися та обговорювалися на Міжнародних конференціях «Groups and Actions, Geometry and Dynamics», Kyiv, 2016, «Сучасні інформаційні технології управління навколишнім середовищем, природокористування та заходи в надзвичайних ситуаціях» Київ, 2017, 2018, 2019, 2020, 2021; Міжнародній Алгебраїчній конференції 2019 та 2021.; Міжнародній математичній конференції присвяченій 60-річчю кафедри алгебри та математичної логіки Національного Київського університету ім. Т. Шевченка; 3-й Міжнародній науково-практичній конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем, Київ, 2020; Міжнародній конференції «Modern Stochastics», Київ, 2021; Federated conference on Computer Science and Information Systems, Sofia, 2021 (digital library); Міжнародній конференції «Cybersecurity Providing in Information and Telecommunication system», Київ, 2021 (індексується в Scopus); Міжнародному науковому симпозіумі «Питання оптимізації обчислень» (ПОО-XLVI), Київ, 2019; Міжнародному науковому симпозіумі «Питання оптимізації обчислень» (ПОО-XLVII), Львів, 2021.

Публікації. За результатами дисертаційної роботи опубліковано 19 наукових праць, 6 наукових статей, написаних у співавторстві й опублікованих у наукових спеціалізованих фахових виданнях України, 1 наукова праця, що входить до наукометричної бази SCOPUS. Разом з тим основні наукові результати додатково відображені у 13 тезах доповідей на науково-практичних конференціях. Із праць, що опубліковано у співавторстві, у дисертаційній роботі використано виключно ті результати, які одержано здобувачем особисто.

Обсяг і структура дисертації. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, п'яти розділів, загальних висновків, списків використаних джерел (в кінці кожного розділу основної частини дисертації) і має 155 сторінок основного тексту, 9 рисунків, 9 таблиць. Список використаних джерел містить 176 найменувань. Загальний обсяг дисертаційної роботи – 160 сторінок.

ОСНОВНИЙ ЗМІСТ

У **вступі** обгрунтовано актуальність теми, сформульовано мету і завдання досліджень, визначено наукову новизну та практичне значення роботи, наведено відомості про публікації, апробацію та впровадження результатів роботи.

У першому розділі розглядаються задачі класичної криптографії від багатьох змінних, що пов'язані зі створенням криптографічних ключів. Коротко оглянуто виники міжнародного тендеру NIST (інституту стандартизації інформаційних технологій Сполучених Штатів Америки) на створення

постквантових публічних ключів для розв'язання задач безпечного обміну інформації та постквантових алгоритмів електронного підпису.

Напрямок криптографії від багатьох змінних у цьому тендері конкурує з напрямками алгоритмів, що базуються на решітках, криптосистем, що використовують коди захисту від шумів, криптосистем, що використовують супереліптичні криві та алгоритмів побудованих з використанням хеш функцій.

В липні 2020 року розпочався останній третій раунд цього проекту. Результати відбору в галузі алгоритмів захисту обміну інформації (шифрування) не сприятливі для класичної криптографії від багатьох змінних – жодний з алгоритмів цього класу не залишився у списку кандидатів на переможця.

Зазначимо, що класична криптографія від багатьох змінних використовує відображення простору шифрограм степені 2. Це мотивує дослідження криптосистем від багатьох змінних, що базуються на відображеннях необмеженої степені або таких, що задають взаємно-однозначну відповідність.

Саме цьому напрямку і присвячено перший розділ дисертації. У ньому визначені основні алгебраїчні об'єкти криптографії від багатьох змінних. Це перш за все афінний простір вимірності n над скінченним комутативним кільцем K (алфавітом для текстів).

Варто зазначити, що більшість файлів, які обробляються, створено у бінарному алфавіті розміру 256, текстові файли (з розширенням .txt) використовують алфавіт розміру 128. Саме тому вибір кілець F_2^8 (скінченні поля розміру 256 та 128), Z_2^8, Z_2^7 (арифметичні кільця за модулем 256 та 128) $B(8,2), B(7,2)$ (булеві кільця порядків 256 та 128) є популярним для алгоритмів шифрування. Використовуються також більш загальні випадки $K = F_{2^m}, K = Z_{2^{2m}}, K = B(m,2)$.

Як правило файл задається вектором символів K визначеної довжини n. Тому простір відкритих текстів ототожнюється з афінним простором K^n елементи якого можна додавати та множити на скаляр з K.

Функція шифрування криптографії від багатьох змінних є нелінійним поліноміальним перетворенням цього простору вигляду $x_i \to f_i(x_1, x_2, \dots, x_n) = y_i, i = 1,2, \dots, n$, де кожен f_i є елементом комутативного кільця $K[x_1, x_2, \dots, x_n]$ всіх поліномів з коефіцієнтами з K від змінних $x_1, x_2, \dots, x_n$. Вектор $(x_1, x_2, \dots, x_n)$ відповідає відкритому тексту, вектор $(y_1, y_2, \dots, y_n)$ – шифрограмі. Многочлени f_i визначають ендоморфізм кільця $K[x_1, x_2, \dots, x_n]$, що переводить x_i у f_i.

Афінна напівгрупа Кремони $CS_n(K)$ всіх таких ендоморфізмів є найважливішим об'єктом криптографії від багатьох змінних. Для створення публічних ключів як правило використовують автоморфізми, що утворюють афінну групу Кремони $CG_n(K)$.

На відміну від класичної криптографії алгоритми з публічним ключем, імплементації яких присвячена робота, використовують підгрупу Ейлерівських перетворень $ES_n(K)$ вигляду $x_i \to x_1^{a(i_1,1)} x_2^{a(i_2,2)} \dots x_n^{a(i_n,n)}, i = 1,2, \dots, n$. Жодне з таких перетворень не є взаємно-однозначним відображенням афінного

простору на себе. В $ES_n(K)$ виділяється підгрупа бієктивних перетворень $EG_n(K)$ многовиду $(K^*)^n$, де K^* – мультиплікативна підгрупа елементів кільця.

Представлено імплементації кількох алгоритмів шифрування з публічним ключем створених за наступною схемою. Кодуюче відображення F обирається спеціального вигляду $E \cdot G$, де E належить $ES_n(K)$, G є елементом $CG_n(K)$, означає композицію відображень. Ендоморфізм E є відображення степені $\alpha \cdot n$, де $\alpha > 0$. G обирається як елемент малої степені α ($\alpha = 2$ або $\alpha = 3$).

Наприклад було розглянуто ситуацію, коли: «Кореспонденти (Аліса та Боб) у стандартній криптографічній термінології працюють з простором відкритих текстів $(K^*)^n$ та простором шифрограм K^n.

Передбачається, що Аліса (власник публічного ключа) використовує алгоритми генерації E та G. Вона має також алгоритм обчислення прообразу довільного $\bar{b}$ з K^n для відображення G, тобто елементу x для якого $G(x) = b$. Крім того для довільного $\bar{c}$ з $(K^*)^n$ Аліса має можливість обчислити $E^{-1}(c)$.

Публічним ключем є стандартна форма відображення $F: x_i \to f_i$, тобто набір поліномів f_i заданий їх коефіцієнтами заданими списком у лексикографічному порядку. Кількість таких коефіцієнтів для кожного i оцінюється як n^α ($\alpha = 2$ або $\alpha = 3$).»

Описано алгоритм генерації елементів $EG_n(K)$ за допомогою спеціальних твірних, так званих генераторів Жордана Гауса. В якості G обирається елемент стабільної підгрупи X степені α у групі $CG_n(K)$, тобто підгрупи, де максимальна степінь автоморфізму дорівнює α.

Побудова таких підгруп є важкою алгебраїчною задачею. Степінь композиції двох відображень з ймовірністю 1 буде мати степінь α^2. Тобто конструктивне завдання стабільних груп є важкою алгебраїчною задачею.

Вибрано конструкції, що пов’язані з алгебрами Лі типу Каца-Муді. Вони визначаються над довільним полем F за допомогою узагальненої матриці Картана. Скінченновимірні алгебри відповідають матрицям Картана визначеними діаграмами $A_n, B_n, C_n, D_n, F_4, E_6, E_7, E_8$ та G_2. Всі інші діаграми визначають алгебри Лі нескінченної вимірності.

Використано конструкцію графу Шуберта $\Gamma_{ij}(A, F)$ що є дводольним графом визначеним за узагальнено матрицею Картана та двома різними вершинами i та j її діаграми. Конструкції графу дозволяє заміну поля F на довільне комутативне кільце K.

Отже маємо граф $\Gamma_{ij}(A, F)$ або в інших позначеннях граф $\Gamma_{ij}(D, K)$, де D – діаграма Картана.

Множина точок *P(D)* графу $\Gamma_{ij}(D, K)$ ототожнюється з афінним простором K^n скінченної вимірності або ж з K^∞. Шляхи на графах $\Gamma_{ij}(D, K)$ та $\Gamma_{ij}(D, K[x_1, x_2, \dots, x_n])$ визначають стабільну групу Кремони *G(D,K)*.

Для криптографічних застосувань в роботі вибрані класична родина діаграм A_n разом з діаграмою $\widetilde{A_1}$ (розширена діаграма для A_1). Для побудови публічних ключів використовуються стабільні групи квадратичних перетворень $G(A_n, K)$ та групи кубічних перетворень *GA(n,K)* що будуються за родиною графів *A(n,K)* пов’язаних з діаграмою $\widetilde{A_1}$. Описано алгоритми генерації цих груп.

Було продемонстровано на прикладі, де публічний ключ будувався за наступною схемою: «

1. Аліса вибирає граф $\Gamma_{ij}(A_m, K)$ або $\text{ГА}(D_m, K)$. Вона буде працювати з простором K^n визначеним множиною точок графа П.
2. Аліса вибирає перетворення G степені α ($\alpha = 2$ або $\alpha = 3$), що належить групі $G_{ij}(A_m, K)$ або *GA(n,K)* та обчислює G^{-1}.
3. Аліса генерує елемент *E* групи $EG_m(K)$ та його оберненим E^{-1}.
4. Вона обчислює стандартну форму перетворення $F = E \cdot G$ вигляду $x_i \to p_i(x_1, x_2, \dots, x_n),\ i = 1,2, \dots, n$ та розміщує її в інтернеті. Отже публічний користувач Боб може користуватися цією формою.

Шифрування: Боб створює свій текст $(p_1, p_2, \dots, p_n)$ в алфавіті $K^* \subset K$. Він обчислює $F(p_1, p_2, \dots, p_n) = C \in K^n$ та надсилає це Алісі.

Дешифрування: Аліса обчислює $^1C = G^{-1}(c) \in (K^*)^n$. Після цього вона відновлює p як $E^{-1}(\bar{c})$.

Зауважимо, що кількість одночленів у квадратичному публічному ключі оцінюється величиною $O(n^3)$. Степінь публічного відображення дорівнює *O(n),* тому складність алгоритму кодування є $O(n^4)$. У випадку кубічного ключа маємо складність $O(n^5)$.

Стабільність перетворення G дозволяє Алісі обчислити G^{-1} за поліноміальний час. Постквантовий статус алгоритму забезпечуються складністю апроксимації відображення лінійної від n степені та густини $O(n^2)$ або $O(n^3)$. Зауважимо, що перетворення *F* не є бієкцією.»

Поліноміального алгоритму апроксимації функції з такими властивостями навіть при умові використання квантового комп'ютера разом зі звичайною машиною Тюрінга не знайдено.

Інші публічні ключі розглядаються у розділі 4. Він присвячений алгоритмам, що ґрунтуються на бієктивних відображеннях необмеженої степені.

Треба відзначити, що згадані вище перетворення *E* та *G* є бієкціями на многовидах $(K^*)^n$ та K^n відповідно. На прикладі згадуваної ситуації було показано, що: «Аліса може вигенерувати E лінійної степені $\alpha n, \alpha > 0$. Алгоритм будує E як суперпозицію елементів Жордана-Гауса $E_i, i = 1,2, \dots, l$ для яких вона досить швидко обчислює обернені E_i^{-1}. Аліса пересилає стандартну форму *E* до Боба.

Кореспонденти працюють з простором відкритих текстів $(K^*)^n$. Боб створює свій явний текст в алфавіті K^*. Аліса одержує шифрограму $C = E(p)$. Вона декодує послідовно застосовуючи $E_l^{-1}, E_{l-1}^{-1}, \dots, E^{-1}$.

Безпека цього публічного ключа базується на задачі знаходження оберненого перетворення для елемента групу $EG_n(K)$. Ця задача залежить від вибору комутативного кільця *K*. Алгоритм імплементовано для випадків $K = F_{2^t}$ (скінченне поле характеристики 2) та $K = Z_{2^t}$ (кільце лишків за модулем 2^t).»

На сьогоднішній день розв'язання згаданої вище задачі за поліноміальний час не побудовано. Отже відповідна криптосистема може розглядатися як кандидат у постквантові алгоритми.

Слід відзначити, що перетворення G не може безпосередньо використовуватися для створення публічного ключа. Зі стабільності групи випливає, що G^{-1} має степінь α ($\alpha = 2$ або $\alpha = 3$). Це дає змогу супротивнику проводити так звані атаки лінеаризації, які відбудують обернене перетворення за час $O(n^7)$ ($\alpha = 2$) або ж за $O(n^{10})$.

Саме тому у розділі 4 розглядаються більш загальні перетворення $\tilde{G}$ простору K^n, побудовані у термінах шляхів на графах $G_{i,j}(A_n, K)$ та $G(A_n, K[x_1, x_2, \dots, x_n])$ або ж *A(n,K)* та $A(n, K[x_1, x_2, \dots, x_n])$.

Перетворення $\tilde{G}$ має лінійний степінь *O(m)*, але обернене до нього $\widetilde{G^{-1}}$ має експоненційний степінь. Виникає так звана степенева прірва. Алгоритм генерації $\tilde{G}$ використовує розклад цього перетворення у композицію елементів, для яких прообраз обчислюється за $O(m^2)$.

Отже при використанні стандартної форми $\tilde{G}$ як публічного ключа Аліса може декодувати за час $O(m^3)$. На сьогоднішній час алгоритму для обчислення прообразу $\tilde{G}$ не побудовано.

Далі у четвертому розділі також описані криптосистеми, що використовують стандартну форму відображення вигляду $\widetilde{EG}$. Як і криптосистеми з розділу 1 у цих алгоритмах простір явних текстів $(K^*)^m$ відрізняється від простору шифрограм K^n.

Такі публічні ключі безпечні у порівнянні з описаними в розділі 1, вони використовують трохи повільний алгоритм шифрування (для Боба) та декодування для Аліси.

Зазначимо, що кожен з алгоритмів з приватним ключем у публічних ключах з розділу 1 може бути перетворений у потоковий алгоритм шифрування, який розглядається у розділі 2.

У другому розділі було імплементовано потоковий алгоритм та детально досліджено вибрану функцію шифрування *G* з алгоритму, що використовує властивості графів *A(n,K)*.

Було розглянуто інформацію про ці графи та їх проективну границю *A(K)*, що використовується в алгоритмі. Граф $A(F_q)$ є нескінченним q – регулярним деревом. Задання графу $A(F_q)$ вирішує проблему презентації графу рівняннями у Гільбертовому просторі F_q.

Графи *A(n,K)* належать до класу лінгвістичних графів типу (1, 1, (n-1)), які визначено як дводольні графи з множинами точок і прямих K^n, такі що точка $(x_1, x_2, \dots, x_n)$ є інцидентною до прямої $[y_1, y_2, \dots, y_n]$ тоді і тільки тоді, коли виконуються наступні співвідношення:

$$\alpha_2 x_2 + \beta_2 y_2 = f_2(x_1, y_1)$$
$$\alpha_3 x_3 + \beta_3 y_3 = f_3(x_1, x_2, y_1, y_2)$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots.$$
$$\alpha_n x_n + \beta_n y_n = f_n(x_1, x_2, \dots, x_{n-1}, y_1, y_2, \dots, y_{n-1})$$

де f_i – поліноми від зазначених змінних.

Застосування графів до задач шифрування було запропоновано В.О. Устименком у 1998 році. Саме лінгвістичні графи типу (1, 1, (n-1)) було використано у перших алгоритмах шифрування. Граф *A(n,K)* задається

рівняннями $x_2 - y_2 = y_1 x_1,\ x_3 - y_3 = x_1 y_2,\ x_4 - y_4 = y_1 x_3, \dots, x_n - y_n = y_1 x_{n-1}$, (для парного n) або $x_n - y_n = x_1 y_{n-1}$ (n – непарне).

Перші координати x_1 і y_1 точок і прямих лінгвістичного графа називають кольорами вершин. Для шифрування використовується лінгвістична властивість графу: кожна вершина має єдиного сусіда визначеного вигляду.

Наприклад, було розглянуто ситуацію: «Природний алгоритм шифрування у просторі K^n визначається таким чином. Будується шлях у графі визначених кольорами $\alpha_1, \alpha_2, \dots, \alpha_s$. Нехай $N_\alpha(\bar{x})$ – це оператор сусіда вершини *x*, що має колір $x_1 + \alpha$. Шлях виглядає як $(x) = (x_1, x_2, \dots, x_n)$ (початкова точка загального вигляду $v_1 = N_{\alpha_1}(x), v_2 = N_{\alpha_2}(v_1), \dots, v_s = N_{\alpha_s}(v_{s-1})$.

Припустимо, що кореспонденти (Аліса і Боб) мають інформацію про граф та стрічку $\alpha_1, \alpha_2, \dots, \alpha_s$ ненульових елементів кільця. Вони ототожнюють відкритий текст з $(x_1, x_2, \dots, x_n)$, вважають $\alpha_1, \alpha_2, \dots, \alpha_s$ гаслом та $v_s = (y_1, y_2, \dots, y_n)$ шифрограмою. Щоб запобігти повторенню векторів використовують умову $\alpha_i \neq \alpha_{i+2},\ i = 1, 2,$ ... на гасла.»

У перших роботах з імплементації таких алгоритмів було використано відомі лінгвістичні графи *D(n,K)* (Устименко, 2001) та графи Венгера *W(n,K).*

Був імплементований алгоритм на графах *A(n,K)* та вивчені властивості такого шифрування для випадків комутативних кілець $K = F_q$ (скінченне поле розміру $q, q > 2$) $K = Z_{2^m}$ (арифметичне кільце лишків за модулем 2^m) та *K=B(m,2)* (Булеве кільце розміру 2^m).

Серед властивостей слід згадати факт, що при умові $s < [\frac{n+5}{2}]$ різним гаслам відповідають різні шифрограми. Цей факт справджується комп'ютерною симуляцією. У випадку довільного кільця K відображення шифрування є нелінійним, його степінь дорівнює 3.

Поліноміальна природа шифрування використана у його криптоаналітичному дослідженні. Цей факт було використано М. Клісовським, який довів, що атака лінеаризації потребує $O(n^3)$ перехоплених пар відкритий текст/відповідна шифрограма. Складність такої атаки становить $O(n^{10})$. Тобто при шифруванні стрічки довжиною 1000 знаків алфавіту K потрібна кількість перехоплень є пропорційною 1000 млн.

Швидкодію імплементованих алгоритмів подано у таблицях. Визначена також густина кодуючого перетворення від багатьох змінних, тобто кількість d одночленів у кубічному відображенні вигляду $x_i \to f_i, i = 1, 2, \dots, n$. Аліса та Боб можуть вживати безпечно цей алгоритм $\leq \frac{d}{2n}$ рази, тоді супротивник не зможе інтерполювати відображення, навіть маючи повний перелік пар відкритий текст/відповідна шифрограма.

Важливою категорією інформаційного простору є довіра до документів. Легко побачити, що навіть користування надійними засобами шифрування не забезпечує повної довіри до документів, тому що треба рахуватися із шумами у каналах та проблемами безпечного збереження файлів у електронних сховищах, де документи можуть бути підроблені, пошкоджені комп'ютерними вірусами, технічними помилками в роботі обчислювальної техніки та інше. Останнім часом постійно зростає загроза потужних кібертерористичних атак на сховища, їх наслідки це не тільки виток інформації, але й ушкодження або

фальсифікування документів. Зрозуміло, що після виявлення кібератаки потрібно робити аудит усіх файлів системи.

Для задач виявлення кібератак, верифікації та автентифікації документів потрібні так звані залежні від ключів хеш-функції (автентифікаційні коди повідомлень або МАСи) які залежать. від гасла. Хеш-функція потрібна для генерації скомпенсованої форми оригінального документа довільно обраного розміру. Таку форму називають хешем або дайджестом документа, її використовують у різних криптографічних застосуваннях. Хеш-функція *h* працює з файлом довільного розміру *n*, її значення має фіксований розмір.

Криптографічно стабільна функція хешування *f* повинна забезпечувати: практичну неможливість вибору пари посилань *x* та *z* таким самим значенням хеш-функції. Для дайджесту документа, створеного залежною від ключа хеш-функцію (MAC) використовують символ HMAC. Коли користувачі хочуть безпечно обмінятися кореспонденцією, перевіряючи хто є дійсним автором листа, так і відсутність змін при пересилці, вони разом обирають спільний MAC. При цьому користуються спільною схемою симетричного шифрування.

Крім криптографічної стабільності дуже важлива швидкодія та високий показник аваланч ефекту. Цей ефект вимірюється таким чином. Обчислюється HMAC для генерованого файлу, змінюється довільний його біт та обчислюється HMAC для зміненого файлу, після цього робиться побітове порівняння отриманих дайджестів. Для практичного вживання МАСу потрібно, щоб статистичні дослідження показали, що поєдина зміна символу приводить до зміни 40% бітів HMACу незалежно від розміру файлів, що генеруються.

Нехай $F(K)$ - простір потенційно нескінченних текстів в алфавіті *K*, який являє сукупність всіх кортежів виду $(a_1, a_2, ..., a_k), a_i \in K$ різної довжини k. Будемо вважати, що *K* є скінченним комутативним кільцем та ототожнювати $F(K)$ з напівгрупою із наступним множенням $(a_1, a_2, ..., a_k) \circ (b_1, b_2, ..., b_s) = (a_1, a_2, ..., a_k, b_1 + a_k, b_2 + a_k, b_s + a_k)$. Нехай $F'(K)$ буде піднапівгрупою всіх слів парної довжини. Позначимо через $S(K^n)$ скінченну напівгрупу всіх поліноміальних відображень простору K^n в себе.

Теорема. Для кожного натурального m≥2 існує гомоморфне відображення $\psi : F'(K) \to S(K^m)$ таке, що його образ $\psi(F'(K))$ утворює групу *G* кубічних поліномів ступеня 3.

Відображення, що задовольняє умовам теореми будується конструктивно в термінах теорії дискретних динамічних систем, визначених за алгебраїчними графами з екстремальними властивостями. Ці методи дозволяють одержати таку нижню оцінку порядку конструктивно побудованої групи: $|G| \geq 2^{4n}$. Зазначимо, що твердження визначає рідкісний математичний об'єкт. Суперпозиція двох кубічних відображень з великою ймовірністю буде мати ступінь 9, трьох – 27, чотирьох – 81, а у побудованій групі всі ці добутки обмежені числом 3. Ця група вже вживалася для побудови криптографічних алгоритмів з приватним ключем та протоколів обміну ключами.

Третій розділ присвячено задачам симетричної криптографії, а саме, потоковому шифруванню та створенню чутливих дайджестів електронних документів, що залежать від ключа.

Симетрична криптографія не є частиною постквантової криптографії, але при дослідженні захищеності алгоритмів також потрібно розглядати можливість атак супротивника з використанням квантового комп'ютера. У випадку дайджестів вже визначено поняття постквантової стабільності алгоритму.

Критичним параметром симетричних алгоритмів є швидкодія, тому що розміри інформації для обробки постійно зростають, потрібно рахуватися з викликом Великих Даних. Потокові алгоритми симетричного шифрування потрібно підтримувати безпечними протоколами обміну ключів. Популярний протокол Діффі-Хеллмана вже не витримує атак з використанням квантового комп'ютера.

Для створення МАСу було використано не саму групу *G*, а відображення ψ, що її визначає, разом з афінними *A* та *B* перетвореннями групи Кремони за правилом $g: x \to A\psi(x)B$. Не важко побачити, що ψ – природній оператор компресії даних який відображає нескінченну множину $F'(K)$ усіх слів парної довжини в алфавіті *K* на скінченну множину $S(K^m)$. На вихід подається список координат *g(x)*, до яких двічі застосовано оператор повного диференціалу. Комп'ютерна симуляція дозволила обчислити дуже високий аваланч ефект у межах 97-99%. Для прикладу в МАСу російських дослідників інтервал аваланч ефекту оцінюється як 47-50%.

Наприклад було розглянуто ситуацію, коли: «Нехай $(a_1, a_2, ..., a_n)$ документ представлений в алфавіті *K* після перемішування з деяким псевдовипадковим словом сталої довжини. Будемо вважати, що число *n* парне. Користувачі обирають розмір дайджесту $m, m < n$ та $m = O(1)$ або ж $m = O(n)$ разом з ключем, що складається зі зростаючої послідовності натуральних чисел $i(1), i(2), ..., i(m-1)$ та невиродженої матриці *M* складеної з елементів кільця лишків Z_{256}. Вони утворюють вектор $u = (v_1, v_2, ..., v_m)$, де $v_1 = a_1 + a_2 + ... + a_n, ..., v_j = v_{j-1} - a_{i(j-1)}$. Потім обчислюється кубічне відображення $F = \psi_m(a_1, a_2, ..., a_n)$, яке кореспонденти застосовують до вектора *u*. Отриманий вектор-рядок $F(u)$ множиться на матрицю *M*. Вектор $w = F(u)M$ вважаємо дайджестом документу.

Зазначимо, що значення $F(u)$ обчислюється за допомогою рекурсивного алгоритму, його складність визначається як $O(mn)$ і співпадає зі складністю створення дайджесту.

Цей базовий алгоритм легко модифікувати без змінення складності обчислень. Зокрема:

1) Можна представити слово $(a_1, a_2, ..., a_n)$ у вигляді конкатенації скінченної кількості слів $z_1, z_2, ..., z_t$ парної довжини. Потім обрати послідовність слів вигляду $u_1, u_2, ..., u_k$, де $u_i \in \{z_1, z_2, ..., z_t\}$ таку, що кожне z_i у цій послідовності зустрічається не менше ніж один раз. Далі обчислюється значення у добутку $u_1, u_2, ..., u_k$ у розглянутій вище напівгрупі слів $F'(K)$. Алгоритм модифікується заміною кубічного відображення $\psi(a)$ на $\psi(y)$. При умові всім відомого розбиття файлу криптографічна стабільність такого дайджесту буде залежною від проблеми розкладу $\psi(y)$ у добуток перетворень $\psi(z_i)$ з аффінної групи Кремони. Зазначимо, що поліноміального алгоритму для розв'язання цієї проблеми на

звичайному або квантовому комп’ютері на сьогоднішній день не знайдено. Насправді ця задача виникає за умов неповної визначеності, бо відоме тільки значення $\psi(y)$ на деякому залежному від файлу векторі. Зрозуміло що розбиття a на підслова z_i та послідовність u_j слід вважати частиною спільного ключа для кореспондентів.

2) Можна обчислювати v_1 як добуток виразів $2a_i+1$ та одержувати v_i діленням v_{i-1} на $2a_{i(j-1)}+1$.

3) У варіанті 2 можна замінювати v_i на його непарні степені $k, k<128$. Тоді ці степені слід вважати параметрами ключа.»

Імплементовані випадки зручні для їх використання у технології blockchain, де потрібні дайджести у вигляді послідовності бітів або ж нулів та одиниць.

Виники імплементації створення алгоритмів дайджестів містяться в розділі 3.8. Проілюструємо швидкодію алгоритмів.

Програми імплементовано на мові C++. Час її роботи залежить від параметрів комп'ютера. Ми використали звичайний персональний комп'ютер з процесором Pentium 3.00 GHz, 2GB пам'яті RAM та системи Windows 7. Для провадження комп’ютерних експериментів з базовим алгоритмом, описаним у розділі 4, було обрано групу GA(n,K), та розширені матриці M, які обчислюються за час O(m), де m – розмір дайджесту.

Для вимірювання аваланч ефекту дайджест представлявся у символах бінарного алфавіту. Швидкодія алгоритму в секундах, виміряна на файлах різного типу подається нижче.

Таблиця 1 – Швидкодія алгоритму створення дайджестів

Розмір файлу, Мегабайт	Розмір дайджесту (у бітах)						
	256	384	512	640	768	896	1024
4,0	1,36	2,03	2,74	3,43	4,12	4,81	5,52
16,1	4,94	7,40	9,90	11,09	14,88	16,99	19,82
38,7	11,60	17,39	23,20	29,03	34,84	40,65	46,46
62,3	18,54	27,80	37,10	46,38	55,68	64,94	74,22
121,3	36,24	54,35	72,52	90,63	108,76	126,89	145,02
174,2	51,22	77,72	103,66	129,40	155,53	181,42	207,34

Четвертий розділ присвячено побудові криптосистем з публічним ключем криптографії від багатьох змінних, що спираються на відображення необмеженої степені на відміну від першого розділу розглядається випадок бієктивних відображень. Ейлерівські перетворення афінного простору або поліноміальні відображення генеровані за лінгвістичними графами розглядаються окремо, як самостійні методи шифрування.

Використано більш загальні лінгвістичні графи типу *(k, k, n-k)* вершини яких мають визначений першими *k* координатами вектору з простору K^n, де *K* – довільне комутативне кільце.

Визначено напівгрупи та групи *SL(K)* та *GL(K)*, що відповідають парі лінгвістичних графів *L(K)* та $L(K[x_1, x_2, \dots, x_n])$. Вони утворені поліноміальними перетвореннями простору K^n, що використовується як простір відкритих текстів над алфавітом *K*.

Ці алгебраїчні об'єкти отримуються як гомоморфні образи напівгрупи утвореної наборами $\bar{f} = (f_1, f_2, \dots, f_{2s})$ поліноміальних відображень простору K^n. Композиція такого елементу з набором $(g_1, g_2, \dots, g_{2t})$ задається формулою $(f_1, f_2, \dots, f_{2s}, g_1(f_{2s}), g_2(f_{2s}), \dots, g_{2t}(f_{2s}))$.

Відповідний гомоморфізм L_η лінгвістичного стискання практично визначає функцію з секретом $F = L_\eta(\bar{f})$ на просторі K^n. Це означає, що коли $\bar{f}$ відомо, то деякий прообраз *F* ефективно обчислюється за поліноміальний час.

Для імплементації публічних ключів вибрано Подвоєні Графи Шуберта, що відповідають алгебрам Лі над діаграмою A_{2k+1} з виділеними вершинами *k* та *k+1*.

При певних умовах на набір $\bar{f}$ відповідні відображення простору K^{k+k^2} має лінійну степінь $O(k^2)$ та поліноміальну від *k* густину k^d, де *d* – деяка стала. Зауважимо, що при d=4 густина буде квадратичною функцією від вимірності $n = k + k^2$. Таким чином можна створити публічний ключ, що визначається стандартною формою вигляду *G=PFQ*, де *P* та *Q* елементи афінної групи $AGL_n(K)$.

Публічний користувач (Боб) може її використовувати та кодувати зі швидкістю $O(n^3)$. Аліса має розклад на *P, F* та *Q* і набір $\bar{f}$. Це дозволяє процес декодування виконати за час $O(n^2)$.

Конструктивно будуються відображення *G* зі степеневою прірвою, тобто з оберненим елементом експоненційної степені. Такий вибір *G* призводить до того, що супротивник не може здійснювати атаки лінеаризації.

Інший клас публічних ключів будується на Ейлерівських відображеннях. У цьому випадку Аліса генерує кілька відображень $E_1, E_2, \dots, E_s$ типу Жордана-Гауса. Вона обчислює їх композицію у стандартній формі *G*.

Задача знаходження оберненого перетворення для Ейлерівського елементу загального положення розв'язуються методами як класичного так і засобами постквантового аналізу. Це обумовлює пост квантовий статус такого алгоритму.

У четвертому розділі наведені приклади публічних ключів, побудованих на комбінації Ейлерівського перетворення з відображенням лінійної степені, що є побудованим за лінгвістичним графом над комутативним кільцем *K*.

Такі криптосистеми також задаються стандартною формою. Аліса та Боб працюють з простором відкритих текстів $(K^*)^n$ та простором шифрограм K^n. Їх особливістю є нестабільність перетворення генерованого за лінгвістичним графом. Саме тому криптоаналіз таких публічних ключів значно складніший у порівнянні з криптосистемами описаними у першому розділі. Швидкодії цих постквантових алгоритмів представлені у таблицях.

Широковідомий алгоритм Діффі Хеллмана широко використовувався у задачах обміну ключів симетричних алгоритмів шифрування (одноразовий блокнот, потокові та блокові алгоритми шифрування). Різні шляхи для заміни цього протоколу розглядаються у не комутативній криптографії, де робляться спроби замінити циклічну групу F_q^* не комутативним алгебраїчним об'єктом, використати кілька генераторів замість одного та довести пост квантовий статус протоколу, спираючись на складність відомої проблеми, що не розв'язується за поліноміальний час з використанням як машини Тюрінга так і теоретичного квантового комп'ютера.

Дослідження у цьому напрямку далекі до завершення. До останнього часу напівгрупи та групи перетворень афінного простору над комутативним кільцем не використовувалися у не комутативній криптографії у зв'язку зі швидким зростом степені та густини при перемноженні елементів.

У п'ятому розділі абстрактні схеми протоколів обміну ключів доводяться до рівня алгоритмів у випадках Подвоєних графів Шуберта, напівгрупи всіх Ейлерівських перетворень та групи визначеною за стабільними кубічними групами *GA(n,K)*. Приведено Tahoma протокол, назва якого походить від tame homomorphism, тобто гомоморфізму який можна обчислити за поліноміальний час.

Було доведено, що проективна границя *A (n, q), n = 2, 3, ...* збігається з T_q є дерево, зображено на рисунку 1.

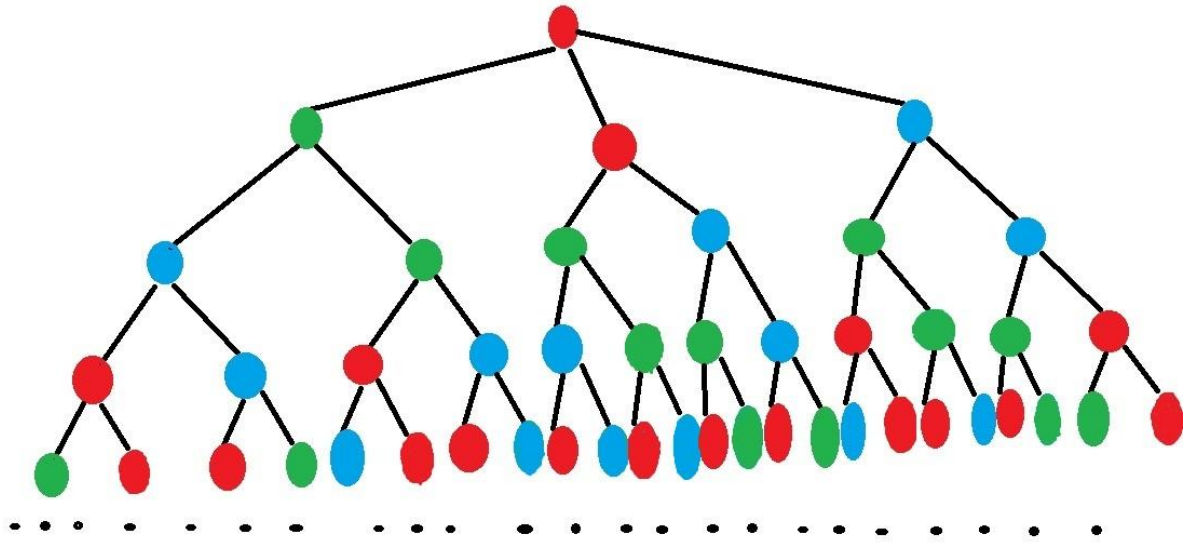

Рис.1 Розфарбоване дерево за *A(n,K)* графа

Ця конструкція дозволяє представити T_q як q - регулярний дводольний граф з точками виду$(p) = (p_1, p_2, \dots, p_i, \dots)$ та прямими $[l] = [l_1, l_2, \dots, l_i, \dots]$, де лише скінченне число координат p_i та l_i відмінні від нуля, а точка *(p)* і пряма

[l] є інцидентними тоді і тільки тоді, коли виконуються наступні співвідношення:

$p_2 - l_2 = l_1 p_1, p_3 - l_3 = p_1 l_2, p_4 - l_4 = l_1 p_3, \dots, p_{2s} l_{2s} = l_1 p_{2s-1}, p_{2s+1} l_{2s+1} = p_1 l_{2s-1} \cdots$

Проекції *(p)* та *[l]* на $(p_1, p_2, \dots, p_3)$ та $[l_1, l_2, \dots, l_n]$ визначають гомоморфізм графа на графі *A (n, q)* із множиною точок та прямих, ізоморфним до $(F_q)^n$ та інцидентності, заданою *n-1* першими рівняннями у визначенні T_q.

Можна замінити скінченне поле *F* у наведеній вище конструкції для довільного комутативного кільця *K* з одиницею і отримати нескінченний граф T_K разом із дводольним графом *A (n, K)*, для якого дві копії K^n утворюють множини розподілів. Якщо *K* - кільце цілісності (без дільників нуля), то $T_K = A(K)$- це також нескінченне дерево, але існування нульових дільників призводить до появи циклів на цих графах.

Перші координати $\dot{\rho}$ *(p)* = p_1 та $\dot{\rho}$ *([l])* = l_1 - це природні кольори точок *(p)* та *[l]* графів *A (n, K)* і *A (K)*.

Має місце наступна лінгвістична властивість. Для кожної вершини *v* існує єдиний сусід *u* вибраного кольору $\dot{\rho}$ *(u)* = *a*.

Нехай $N_a(v)$ є оператором знаходження сусіда *v* з кольором *a*. Прогулянка на графі *A (n, K), n = 2,3, ...* довжиною *m*, стартує у даній точці $p = (p_1, p_2, ..)$, може бути заданою точкою *p* та послідовністю *a (1), a (2) ,..., a (m)*, кольорів інших вершин. Шлях є послідовність:

$$(p), v_1 = N_{a(1)}(p), v_2 = N_{a(1)}(v_1), \dots,$$

$$v_m = N_{a(m)}(v_{m-1})$$

Ми називаємо рядок *(a (1), a (2), .., a (m))* напрямком прогулянки. У випадку парного *m* ми розглядаємо перетворення ${}^nC\big(a(1), a(2), \dots, a(m)\big)$з K^n у себе, визначене наступним чином.

Візьмемо список змінних $x_1, x_2, \dots, x_n$ і розглянемо нове кільце $K[x_1, x_2, \dots, x_n]$ (вже нескінченне) разом з новим графом $A(n, K[x_1, x_2, \dots, x_n])$, заданим тими ж рівняннями, що й у випадку *A (n, K)*. Але вже з нескінченними множинами точок і прямих.

Візьмемо спеціальну початкову точку $(x) = (x_1, x_2, \dots, x_n)$ нового графу і напрямок заданий кольорами $x_1 + a(1), x_1 + a(2), \dots, x_1 + a(m)$ та обчислимо наступний шлях у новому графі

$(x), v_1 = N_{a(1)+x(1)}(p), v_2 = N_{a(2)+x(1)}(v_1), \dots, v_m = N_{a(m)+x(1)}(v_{m-1})$, де $x_1 = x(1)$.

Визначимо ${}^nC\big(a(1), a(2), \dots, a(m)\big)$, де (*a (1), a (2) ,..., a (m)*) напрямок з $\sum$(K) як перетворення $P = K^n$, що задано формулою $x_1 \to x_1 + a(m)$, $x_2 \to g_2(x_1, x_2)$, $x_3 \to g_3(x_1, x_2, x_3), \dots, x_n \to g_n(x_1, x_2, \dots, x_n)$ де $(x_1 + a(m), g_2, g_3, \dots, g_m)$ вершина v_m нового графу.

Таким чином візьмемо поліноміальне перетворення ${}^nC\big(a(1), a(2), \dots, a(m)\big)$ з K^nу себе, що надсилає *(x)* до V_m. Це перетворення задається правилом $(x) \to (g_1, g_2, \dots, g_n) = v_m$.

Ми бачимо, що кожна прогулянка від точки до точки *w* по вершинах такого графа, розпочата у вибраному початку (точка 0), може бути задана напрямком, який є кортежем виду $w = (a_1, a_2, \dots, a_{2s})$ з $a_i \in K$.

З таким напрямком ми пов'язуємо кортеж ${}^nC(w) = (g_1, g_2, \dots, g_n)$, де $g_i \in R = [x_1, x_2, \dots, x_n]$. Можна довести, що максимальний ступінь $g_i \in R$ такий, що ступінь $\deg(g_i)$ дорівнює 3. Ми ідентифікуємо цей кортеж з відображенням ${}^nC(w)$ виду $x_i \to g_i(x_1, x_2, \dots, x_n)$, *i = 1,2 , ..., n*, що є бієктивним поліноміальним перетворенням афінного простору $(K)^n$.

Натуральна композиція прогулянок з 0 формально може бути задана наступним правилом.

Для $w = (a_1, a_2, \dots, a_{2s})$ та $u = (u_1, u_2, \dots, u_{2t})$ їх композиція *w∘u* є кортежем $(a_1, a_2, \dots, a_{2s}, a_{2s} + u_1, a_{2s} + u_2, \dots, a_{2s} + u_{2t})$.

Нехай $\sum$ *(K)* - напівгрупа всіх напрямків із введеною вище операцією. Це напівпрямий добуток вільної напівгрупи над алфавітом *K* та адитивною групою *(K, +)*, ∑(K) можна розглядати як модифікацію вільного добутку *(K, +)* із собою.

Неважко перевірити, що композиція ${}^nC(w)$ та ${}^nC(u)$ збігається з ${}^nC(w \circ u)$. Отже, перетворення, ${}^nC(w)$, *w*$\epsilon\sum$ *(K)* утворюють підгрупу *GA (n, q)* групи $AutK[x_1, x_2, \dots, x_n]$, яка діє на афінному просторі $(K)^n$ як група $CG((K)^n$ (афінна група Кремони) всіх бієктивних поліноміальних відображень $(K)^n$ у себе. Це означає, що відображення $\acute{\eta}_n$*:* $\sum$ *(K)* $\to$ *GA (n, K),* що посилає *w* на ${}^nC(w)$, є гомоморфізмом, а її образ *GA (n, K)* є стабільним 3-го ступеня, тобто кожне поліноміальне відображення з цієї групи має степінь 3.

Протокол Тахома (скорочення від «Tame homotorphism»). Він використовує прихований гомоморфізм $\acute{\eta}_n$ з $\sum$ *(K)* у $GA_n(K)$.

Це було продемонстровано на прикладі, де: «Аліса вибирає параметри *n* та *m* і слова-напрямки $w_1, w_2, \dots, w_k$, *k> 1* та слово *u* скінченної парної довжини з $\sum$ *(K)*.

Нехай $u = (a_1, a_2, \dots, a_s)$. Назвемо $Rev(u) = (-a_s + a_{s-1}, -a_s + a_{s-2}, \dots, -a_s + a_1, -a_s)$ як зворотним напрямком для *u*. Неважко зрозуміти, що $\eta_n(uRe\, v(u))$ є одиницею афінної напівгрупи Кремони $CG(K^n)$ всіх бієктивних перетворень простору.

Аліса вибирає афінне перетворення $T_1 \in AGL_n(K)$ і $T_2 \in AGL_m(K)$ в "загальному положенні" і обчислює T_1^{-1} разом з T_2^{-1} . Вона утворює $F_i = T_1\acute{\eta}_n\big(uw_iRe\, v(u)\big)T_1^{-1}$ та $G_i = T_2\acute{\eta}_m\big(zw_iRe\, v(z)\big)T_2^{-1}$ для *i = 1,2, ..., k.*

Вона посилає Бобу пари (F_i, G_i), *i = 1,2, ... k.*

Він використовує формальний алфавіт $\{x_1, x_2, \dots, x_n\}$ для написання слова $x_{i(1)}^{k(1)} x_{i(2)}^{k(2)} \dots\ x_{i(s)}^{k(s)}$ скінченної довжини *s*. Боб обчислює спеціалізації $F = F_{i(1)}^{k(1)} F_{i(2)}^{k(2)} \dots F_{i(s)}^{k(s)}$ та $G = G_{i(1)}^{k(1)} G_{i(2)}^{k(2)} \dots G_{i(s)}^{k(s)}$ степені 3. Він посилає *F* до Аліси, але зберігає *G* для себе.

Аліса повинна відновити стандартну форму перетворення *G* з відомого *F*. Вона знає, що стандартна проекція *A (n, K)* на *A (m, K)* індукує гомоморфізм μ з *GA (n, K)* на *GA (m, k)*, для якого $\mu\big(\acute{\eta}_n(w_i)\big) = \acute{\eta}_m(w_i)$. Елемент *F* дорівнює $T_1\acute{\eta}_n(u)\acute{\eta}_n(w_{i(1)}^{k(1)} w_{i(2)}^{k(2)} \dots w_{i(s)}^{k(s)})\acute{\eta}_n(u)^{-1}T_1^1$.

Тож Аліса обчислює $\acute{\eta}_n(w_{i(1)}^{k(1)}w_{i(2)}^{k(2)}\dots w_{i(s)}^{k(s)}) = \mathrm{F}'$ через свої знання про T_1 та u. Вона застосовує μ до F' і отримує $\acute{\eta}_m(w_{i(1)}^{k(1)}w_{i(2)}^{k(2)}\dots w_{i(s)}^{k(s)}) = \mathrm{G}'$. Нарешті Аліса обчислює G як $T_2\acute{\eta}_m(z)G'^{\acute{\eta}_m}\big(Rev(z)\big)T_2^{-1}$. Спільне перетворення колізії G має стандартну форму $x_i \to g_i(x_1, x_2, \dots, x_m,\ i = 1, 2, \dots, m$.

Безпека відповідає проблемі розкладу F на слово генераторів F_i, $i = 1,2,\dots, k$.

Розширення криптосистеми. Кореспонденти двічі виконують операції з алгоритму наведеним вище з різними групами виду $T_1GA(m,K)T_1^{-1}$ і $T_2GA(m,K)T_2^{-1}$, такими що $T_1T_2 \neq T_2T_1$, вони отримують кубічні відображення зіткнень Z, U .

Аліса бере трійки P, Q, w і P',Q', w', де P, Q, P', Q' – елементи $AGL_2(K)$. Вона утворює $G = P\acute{\eta}_m(w)Q$ та $H = P'\acute{\eta}_m(w')Q'$.

Боб шифрує за допомогою $(GH)^t, t = [log_2(m)] + 1$. Аліса розшифровує $(H^{-1}G^{-1})^t$, час шифрування становить $O(m^4t)$. Аліса використовує розкладання відображення шифрування на генератори G і H, а також її знання про потрійні проходи для генераторів та розшифрування за час $O(m\,log_2\,m)$. Примітно, що відображення шифрування має ступінь $\geq m$.

Тому атаки лінеаризації з боку супротивника неможливі. Безпека всього алгоритму ґрунтується на безпеці постквантового алгоритму. Час виконання протоколу – $O(n^{13})$.»

Зауваження 1. Ми можемо використовувати цей алгоритм більш симетрично відповідно до наступного варіанту. Аліса шифрує за допомогою $(H^{-1}G^{-1})^t$ а Боб розшифровує за допомогою свого $(GH)^t$ за час $O(m^4t)$. У нього є відображення G і H, але у них немає потрійних люків.

Результати комп'ютерного моделювання та симуляції. Постквантовий протокол та розширення його виходу за допомогою алгоритму побудови потенційно нескінченної послідовності символів алфавіту було імплементовано для випадку скінченних полів характеристики 2 (F_{2^8}, $F_{2^{16}}$, $F_{2^{32}}$), арифметичних кілець за модулем m, $m = 2^8, m = 2^{16}$, $m = 2^{32}$ та Булевих кілець B(8), B(16), B(32). Отже маємо 27 імплементованих алгоритмів.

Алгоритми побудовано з використанням гомоморфізму $\acute{\eta}_n$ з напівгрупи $\sum(K)$ шляхів на нескінченному дереві степені $|K|$ в афонічну групу Кремони поліноміальних перетворень простору K^n.

Комп'ютерний результат показав, що кількість $N(n,w)$ одночленів $\acute{\eta}_{n(w)}$ залежить тільки від довжини шляху l, а не від кольорів стрічки w. Маємо $N(n,l)=N(n,w)$. Якщо розглянути $N_{A(n,w)}$ визначену як кількість одночленів відображення $A\acute{\eta}_{n(w)}A^{-1}$, де A-невироджена матриця, то це явище (залежить тільки від довжини) залишається. Маємо $N_{A(n,w)} = N_{A(n,l)}$, де l - довжина w.

Функцію $N_{A(n,l)}$ розглянуто у таких трьох випадках:

Випадок 1

A – розріджена матриця, $O(n)$ ненульові записи

Випадок 1
A – розріджена матриця, $O(n)$ ненульові записи

m	довжина прогулянки з G у ∑(K).				
	16	32	64	128	256
16	5623	5623	5623	5623	5623
32	53581	62252	62252	62252	62252
64	454375	680750	781087	781087	781087
128	360774 1	623714 4	951992 1	1082661 6	1082661 6

Таблиця 2 Кількість одночленів кубічного відображення, індукованого графом $A(m, F_{2^{32}})$

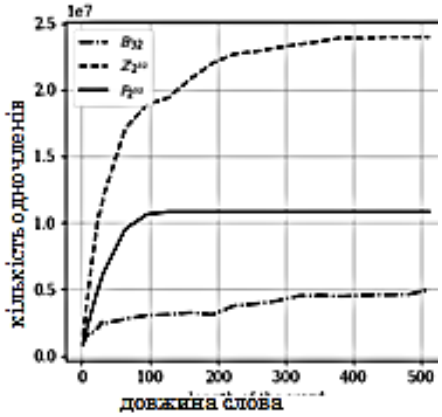

Рис.2 Кількість одночленів кубічного відображення
$G, m = 128 (K = B(32), Z_{2^{32}}, F_q, q = 2^{32})$

m	Довжина прогулянки				
	16	32	64	128	256
16	20	60	128	260	540
32	508	788	1776	3760	7716
64	3198	5858	25251	53196	115148
128	54051	157201	565460	950849	2164057

Таблиця 3 Час генерації для відображення (мс) $A(m, F_{2^{32}})$

Випадок 2
A – матриця в загальному вигляді, n^2 ненульові записи

m	довжина прогулянки з G у ∑(K)				
	16	32	64	128	256
16	6544	6544	6544	6544	6544
32	50720	50720	50720	50720	50720
64	399424	399424	399424	399424	399424
128	3170432	3170432	3170432	3170432	3170432

Таблиця 4 Кількість одночленів кубічного відображення, індукованого графом $A(m, F_{2^{32}})$

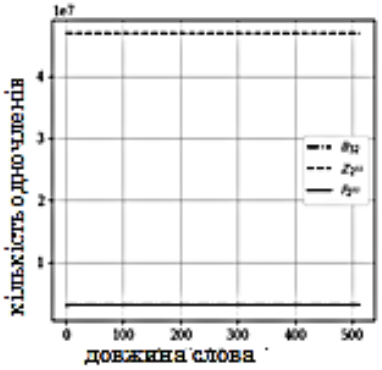

Рис.3 Кількість одночленів кубічного відображення $G, m = 128$
$(K = B(32), Z_{2^{32}}, F_q, q = 2^{32})$

m	довжина прогулянки				
	16	32	64	128	256
16	76	148	288	576	1148
32	1268	2420	4700	9268	18405
64	22144	40948	78551	153784	304240
128	460200	819498	1552277	2970748	5856938

Таблиця 5 Час генерації для відображення (мс) $A(m, F_{2^{32}})$

Випадок 3
A – одинична матриця

m	довжина прогулянки з G у ∑(K)				
	16	32	64	128	256
16	250	250	250	250	250
32	770	1010	1010	1010	1010
64	1810	3074	4066	4066	4066
128	3890	7202	12290	16322	16322

Таблиця 6 Кількість одночленів кубічного відображення, індукованого графом $A(m, F_{2^{32}})$

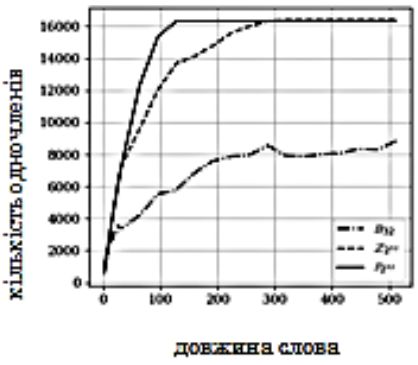

Рис. 4 Кількість одночленів кубічного відображення $G, m = 128$ $(K = B(32), Z_{2^{32}}, F_2, q = 2^{32})$

m	Довжина прогулянки				
	16	32	64	128	256
16	4	12	24	48	96
32	56	152	288	600	1252
64	996	2100	4644	10068	20933
128	15645	33489	74244	167454	364707

Таблиця 7 Час генерації для відображення (мс) $A(m, F_{2^{32}})$

Зазначимо, що теорія лінгвістичних графів визначених за кільцем K типу *(k, k, n-k)* дозволяє будувати родини стабільних напівгруп довільної степені α. Для цієї мети у роботі використовуються Подвоєні Графи Шуберта, тобто дводольні графи точок $(x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ з простору K^{k^2+k} та прямих $[y_1, y_2, \dots, y_k, y_{11}, y_{12}, \dots, y_{kk}]$ та відношенням інцидентності визначеним рівняннями $x_{ij} - y_{ij} = x_i y_j,\ i = 1, 2, \dots, k\ , j = 1, 2, \dots, k.$

Позначимо через ${}^dU(k,K)$ стабільну піднапівгрупу $CS_{k+k^2}(K)$ побудовану за визначенням вище графом. Кожна непорожня власна підмножина J з $\{1,2, \dots, k\} \times \{1,2, \dots, k\}$ визначає індукований підграф $DS_J(k, K)$, якому відповідає d – стабільна напівгрупа ${}^dU_J(k,K)$. Граф $DS_J(k, K)$ є гомоморфним образом $DS(k,K)$. Цей гомоморфізм індукує гомоморфізм η_J між ${}^dU(k,K)$ та ${}^dU_J(k,K)$, який обчислюється за час $O(k^2)$.

Це дає змогу визначити протокол Тахоми за трійкою $({}^dU(k,K), {}^dU_J(k,K), \eta_J)$. Особливе значення має випадок d=2 (квадратичні відображення) тому що складність протоколу для нього найменша і становить $O(n^7)$.

Нехай $E_T = F_T(k, K)$ є поліноміальне відображення з K^n на K^n з секретом T – часткою інформації яка дозволяє обчислювати один з прообразів F_T за час $O(n^s)$, де s є відомою сталою .

У класичній криптографії побудовано вже досить багато родин таких функцій, що є квадратичними відображеннями. Бієктивні функції такі, що без знання секрету T знаходження прообразу є складною задачею з класу NP можна використати для створення публічних ключів шифрування. Не бієктивні

відображення можуть визначати публічні ключі, призначені для цифрового підпису.

Наприклад було розглянуто ситуацію, коли: «Припустимо, що Аліса і Боб використовують Тахома протокол та виробляють квадратичні колізійні відображення G, що визначається на просторі K^n. Аліса має відображення $F_T(n, K)$ разом з секретом. Вона обчислює стандартну форму F' та цієї функції та пересилає $F'+T$ до партнера, Боб відновлює F'.

Тепер Боб та Аліса можуть використати бієктивне F' для шифрування, а не бієктивне F' для задач електронного підпису. Зазначено, що пост квантова безпека Тахома протоколу гарантує приватність F' для Боба. Таку схему можна назвати приватизацією публічного ключа.»

У п’ятому розділі ця схема детально описується для Unbalanced Oil and Vinegar (UOV) систем цифрового підпису. Зазначимо, що UOV один з кандидатів у переможці тендеру NIST PQC. У праці наводиться модифікація цієї системи, що елімінує багато відомих атак супротивника та підвищує її криптостійкість. Постквантовий статус цього модифікованого цифрового підпису ґрунтується на безпеці Тахома протокола.

Тахома протокол можна використовувати для контролю доступу до інформаційної системи (ІС). На прикладі згадуваної ситуації було показано, що: «Припустимо, що Аліса є адміністратором інформаційної системи, а Боб є користувачем ІС. Для користування системою Боб виконує Тахома протокол з Алісою. По закінченню вони мають відображення G на просторі K^n, де K відповідає обраному алфавіту.

Аліса генерує псевдовипадкову послідовність $p = (p_1, p_2, \dots, p_n)$ та пересилає її Бобу. Вона реєструє Боба під гаслом $G(p)$. Боб також обчислює $G(p)$ та входить у систему.»

ВИСНОВКИ

У дисертації розв’язано задачі оптимізації, імплементації та практичного використання математичних алгоритмів методами теорії алгебраїчних графів. Зокрема, задачі моделювання прикладних алгебраїчних об’єктів (графів, відповідних їм груп та напівгруп перетворень визначених над різними некомутативними кільцями, відповідних динамічних систем) розв’язано методами Алгебраїчної Комбінаторики.

Це дозволило розробити комплекс програм для розв’язання різних проблем сучасного захисту інформації з використанням мов Java, C Sharp та C++. У процесі виконання дисертаційної роботи отримано такі основні результати.

1. Задачу про потокове шифрування розв'язано у термінах динамічних систем, визначених за графами $A(n,K)$ та $D(n,K)$ над обраними скінченними кільцями (скінченні поля, Булеві кільця, арифметичні кільця лишків за модулем натурального числа) таким чином, що функція шифрування гарантує наступну властивість: різним гаслам відповідають різні шифрограми обраного відкритого тексту.

2. За допомогою моделювання та комп'ютерної симуляції підібрано параметри при яких зміна одного символу тексту або гасла призводить до зміни 96-98% символів шифрограми. Показник аваланч ефекту покращено на 16-18%.

3. Методами комп'ютерної симуляції та теорії складності алгоритмів проведено криптографічні дослідження атак лінеаризації. Доведено, що для проведення таких атак супротивник повинен перехопити за $1/8n^3 + O(n^2)$ пар відкритого тексту (відповідна шифрограма). При цій умові успішна атака лінеаризації потребує час $O(n^{10})$. Тобто кореспонденти можуть безпечно використовувати незмінне гасло до $1/8n^3 + O(n^2)$ програм, які працюють з різними типами файлів розширення .txt .jpg, .tyf , .avi та інші.

4. Методами теорії Екстремальних графів побудовано швидкі алгоритми створення залежних від ключа дайджестів електронних документів. Використано методи моделювання та комп'ютерної симуляції дозволили підібрати параметри для досягнення високого рівня аваланч ефекту (98%), показник аваланч ефекту покращено на 45%, тому дайджест є чутливим інструментом для виявлення кібератак та подальшого аудиту.

5. Методами Алгебраїчної Геометрії над скінченними комутативними кільцями оптимізовано нові алгебраїчні криптосистеми з публічним ключем. Всі такі криптосистеми базуються на алгебраїчних поліноміальних перетвореннях необмеженої степені на відміну від криптосистем розглянутих NIST (степінь 2 та 3).

6. Методами теорії складності досліджено властивості криптосистем типу Ель Гамаля, де інструмент шифрування не надається публічно. Обрані криптосистеми використовують методи некомутативної криптографії. Деякі з криптосистем використовують небієктивне відображення необмеженої степені. Параметри (степінь, густина, період) підібрані так, що відомі методи крипто аналітичних досліджень (бази Ширшова-Грьобнера та інше) не можливо використати.

7. Методами алгебраїчної геометрії оцінено рівень безпеки нових систем електронного підпису, що не спираються на публічні ключі.

8. За рахунок використання генерованих таблиць алгебраїчних операцій швидкодія алгоритмів обміну ключів покращена на порядок. Такі системи використовують складність факторизації нелінійного відображення у добуток відомих генераторів та деякі інші складні проблеми (потенціювання зі спряженості, дискретний логарифм для спеціальних нелінійних перетворень).

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, в яких опубліковано основні результати дисертації:

1. V. Ustimenko, **O. Pustovit**, On effective computations in subsemigroups of affine Cremona semigroup and implentations of new postquantum multivariate cryptosystems, Physico-mathematical modelling and informational technologies, Lviv, vol. 32, 2021, pp. 27-31.

2. V. Ustimenko, **O. Pustovit**, On the implementations of new multivariate public keys based on transformations of linear degree, Conference on Mathematical Foundations of Informatics, Kyiv, 2021, pp. 397-420.

3**. O.S. Pustovit**,V.O Ustimenko, A new stream algorithms generating sensetive digests of digital documents, Mathematical modelling in economics, N3, 2019, 18-35.

4. Устименко В. О., **Пустовіт О. С.** Нові потокові алгоритми для створення дайджесту електронних документів з високим рівнем лавинного ефекту. Математичне та комп'ютерне моделювання, Серія: Фізико-математичні науки, Збірник наукових праць. Випуск 19, Київ, 2019, с. 174-180.

5. **О. Пустовіт**, В. Устименко, Про застосування алгебраїчної комбінаторики до проблем кодування та криптографії, Математичне моделювання в економіці, № 1-2, Київ, 2017, с. 31-39.

6. **О. Пустовіт**, Динамічні системи та їх використання до проблем інформаційної безпеки, Журнал для студентів фізико-математичних етюдів, №10, Київ, 2011, 64-67.

Праці, які засвідчують апробацію матеріалів дисертації:

7. Устименко В.О., **Пустовіт О.С**., On the implementation of postquantum access control protocol based algorithms, 20 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природного використання, заходи в надзвичайних ситуаціях, Київ, 2021, с 42-44.

8. V. Ustimenko, **O. Pustovit**, New cryptosystems of Noncommutative cryptography based on Eulerian semigroups of multivariate transformations, Cybersecurity Providing in Information and Telecommunication Systems 2021, Kyiv, 2021, pp. 18-26. (***індексується в Scopus***)

9. V. Ustimenko, **O. Pustovit**, On new stream algorithms generating sensitive digests of computer files, Federated Conference on Computer Science and Information Systems, Sofia, 2021, pp. 131-135 (***List B, IEEE Digital Library***)

10. V. Ustimenko, **O. Pustovit**, On the implementation of public keys with the usage of algebraic maps of unbounded degree, The 13th International Algebric Conference in Ukraine, Kyiv, 2021, p. 84.

11. V. O. Ustimenko, **O. S. Pustovit**, Dynamical systems based on small world expanding graphs and algorithms to secure big data processing, International conference Modern Stochastics: Theory and Applications V, Kyiv, 2021, pp. 39-40.

12. Устименко В.О., **Пустовіт О. С.**, Про застосування екстремальної теорії графів до створення дайджестів електронних документів з високорівневим аваланч ефектом, 3 Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS) 2-3 квітня 2020, Taras Shevchenko National University of Kyiv.

13. V. O. Ustimenko, **O. S. Pustovit**, On noncommutative cryptography responds to challenges of quantum computer and secure big data processing, International mathematical conference dedicated to the 60th anniversary of the department of algebra and mathematical logic of Taras Shevchenko National University of Kyiv, Book of abstract, Kyiv 2020, p.83.

14. Устименко В.О., **Пустовіт О. С.**, Про нові постквантові алгоритми електронного підпису, що модифікують алгоритми представлені на другий етап NIST сертифікації, Праці 19-ої Міжнародної науково – практичної конференції «Сучасні інформаційні технології управління екологічною безпекою, природокористуванням, заходами в надзвичайних ситуаціях», 2020р., м. Київ, Петропавлівська Борщагівка.(розділ у колективній монографії), с. 57-59.

15. Устименко В.О., **Пустовіт О.С**., Покращена безпека для ГІС з використанням N-зв'язної архітектури та нового графу, який базується на основі потокового шифру, 18 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природного використання, заходи в надзвичайних ситуаціях, Київ, 2019, с. .92-94.

16. Устименко В. О, **Пустовіт О.С.**, Про екстремальні графи, афінну напівгрупу Кремони та нові рішення постквантової криптографії, Міжнародна алгебраїчна конференція, 2019, с. 121-122, Вінниця.

17. **Пустовіт О.С.**, Устименко В. О. Нові алгоритми аудиту електронних документів, їх впровадження та застосування в кібербезпеці, 17 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природокористування, заходи в надзвичайних ситуаціях, Київ, 2018, с. 170-175.

18. В. О. Устименко, **О. С. Пустовіт**, Нова концепція електронного підпису та засоби її реалізації, 16 Міжнародна науково-практична конференція: Сучасні інформаційні технології управління навколишнім середовищем, природокористування, заходи в надзвичайних ситуаціях, Київ, 2017, с. 86-89.

19. В.М. Лахман, **О.С. Пустовіт**, В.О. Устименко, Про реалізацію криптографічного алгоритму, визначеного в рамках груп Kac-Moody над діаграмою $\overline{A_1}$, International mathematical conference Group and Actions: Geometry and Dynamics, Київ, 2016, с. 33

АНОТАЦІЯ

Пустовіт О.С. Застосування теорії екстремальних графів до сучасних проблем інформаційної безпеки. - Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології. – Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України, Київ, 2021.

Дисертаційна робота присвячена вирішенню актуальної науково-практичної проблеми розробки методів захисту інформації, пов’язаних з викликом Великих Даних та появою перших зразків квантового комп’ютера.

Розглянуто новий клас груп та напівгруп перетворень афінного простору K^n, які задовольняють властивості суперпозиції, тобто можливості обчислення добутку n елементів за поліноміальний час $T(n)$. Ці алгебраїчні об’єкти визначаються у термінах спеціальних графів, визначених за комутативним кільцем K. Саме вони є знаряддям для побудови криптографічних алгоритмів у

випадках $K = F_q$ (скінченне поле), Z_m (арифметичне кільце лишків за модулем m), $K = B(m, 2)$ (булеве кільце розміру 2^n).

У роботі детально описано новий потоковий симетричний алгоритм шифрування за відомою родиною графів *A(n,K)* та відповідною групою кубічних перетворень простору відкритих текстів K^n. Швидкість кодування *O(n)* порівняльна зі швидкістю читання файлів. При певному обмеженню на довжину різним гаслам відповідають різні шифрограми.

За виниками комп'ютерної симуляції досліджено властивості змішування. Показано, що атаки лінеаризації потребують $O(n^3)$ перехоплень типу відкритий текст/відповідна шифрограма. Складність атаки лінеаризації становить $O(n^{10})$. Алгоритм підтримано безпечним постквантовим протоколом, безпека якого визначається задачею розкладу перетворення групи Кремони у добуток відомих твірних.

Пропонуються швидкі, постквантово стійкі алгоритми створення дайджестів електронних документів. Описано нові алгоритми з публічним ключем, визначені перетвореннями від багатьох змінних необмеженої степені. Досліджені властивості нових асиметричних алгоритмів шифрування типу Ель Гамаля, визначених постквантовими протоколами. Запропоновано нові алгоритми цифрового підпису, безпека яких також визначено постквантовими протоколами некомутативної криптографії, визначиними у термінах криптографії від багатьох змінних.

Ключові слова: багатоваріантна криптографія, хеш функція, дайджести, цифровий підпис, протоколи обміну ключів, постквантова криптографія, кібербезпека.

ANNOTATION

Pustovit O.S. Application of theories of extreme graphs to modern problems of information security. - Manuscript.

The dissertation for the degree of a candidate of technical sciences on the specialty 05.13.06 «Information technologies.» Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, 2021.

The dissertation, devoted to the solution of a topical scientific and practical problem, reveals the methods of data protection involved in the Big Data call and the first samples of a quantum computer appear.

A new class of groups and semigroups of transformations of the affine space K^n is considered, which satisfy the properties of superposition, ie, the possibility of calculating the product of *n* elements for the polynomial time *T (n)*. These algebraic objects are defined in terms of special graphs defined by the commutative ring *K*. They are the tool for constructing cryptographic algorithms in the cases $K = F_q$ (finite field), Z_m (arithmetic ring of surpluses modulo *m*), $K = B(m, 2)$ (Boolean ring of size 2^n).

The paper describes in detail a new flow symmetric encryption algorithm for the known family of graphs *A (n, K)* and the corresponding group of cubic transformations of the open text space K^n. The encoding speed *O (n)* is comparable to the file read speed. With a certain length restriction, different slogans correspond to different ciphers.

The properties of mixing were investigated based on the results of computer simulation. It is shown that linearization attacks require $O(n^3)$ plaintext / corresponding ciphertext interceptions. The complexity of the linearization attack is $O(n^{10})$. The algorithm is supported by a secure post-quantum protocol, the safety of which is determined by the task of scheduling the transformation of the Cremona group into the product of known generators.

Fast, post-quantum stable algorithms for creating digests of electronic documents are offered. New algorithms with a public key defined by transformations from many variables of unlimited degree are described. The properties of new asymmetric El Gamal-type encryption algorithms defined by post-quantum protocols are investigated. New digital signature algorithms are proposed, the security of which is also determined by post quantum protocols of non-commutative cryptography, defined in terms of cryptography from many variables.

Keywords: multivariate cryptography, hash function, digests, digital signature, key exchange protocols, post quantum cryptography, cybersecurity.