ВІДГУК

офіційного опонента

професора кафедри комп'ютеризованих систем управління
факультету кібербезпеки, комп'ютерної та програмної інженерії
Національного авіаційного університету
доктора технічних наук, доцента Семка Віктора Володимировича
на дисертаційну роботу Пустовіта Олександра Сергійовича
«Застосування теорії екстремальних графів до сучасних проблем інформаційної безпеки», що подана на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.06 – інформаційні технології

Актуальність обраної теми та зв'язок з науковими програмами

Наукові задачі квантової і постквантової криптографії пов'язані з переглядом традиційних підходів до використання традиційних криптосистем, які використовують методи факторизації цілих чисел та дискретного логарифмування. При цьому потребують розвитку методи некомутативної криптографії, що базується на алгебраїчних об'єктах, таких як групи, напівгрупи, некомутативні кільця та алгебри, методи поліноміальної криптографії від багатьох змінних, прикладної комп'ютерної алгебри та прикладної теорії символьних обчислень.

Актуальними задачами постквантової криптографії є синтез криптографічних алгоритмів (частіше за все з публічним ключем або протоколів обміну ключів), які можуть унеможливлюють реалізацію загроз несанкціонованого доступу до ресурсів квантових обчислювальних систем.

Таким чином, вирішення задачі застосування теорії екстремальних графів до проблем постквантової криптографії та проблемам безпечного процесування великих файлів є важливим та актуальним завданням при створенні новітніх технології захисту інформації.

Зміст дисертаційної роботи та результати досліджень пов'язані з низкою робіт, які виконувались в рамках державних бюджетних програм Інституту телекомунікацій і глобального інформаційного простору НАН України. Зокрема, в рамках науково-дослідних робіт «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).

Загальна оцінка змісту, наукової новизни та практичної значимості, оцінка достовірності та обґрунтованості результатів

Рукопис дисертаційної роботи складається з анотації, змісту, переліку умовних позначень, вступу, 5 розділів, висновків, списку використаних джерел (в кінці кожного розділу основної частини дисертації) та додатків. Обсяг роботи становить 174 сторінок, з них 164 сторінка основного друкованого тексту, 9 рисунків та 9 таблиць. Список використаних джерел містить 215 найменувань.

Зміст роботи відповідає поставленому науковому завданню та сформульованим задачам. Їх рішення є суттю та змістом виконаних досліджень, які відповідають паспорту спеціальності 05.13.06 – "Інформаційні технології" й направлені на дослідження сутності процесів квантової і постквантової криптографії.

*У **вступі*** визначено актуальність, методи та задачі дисертаційної роботи, сформульовано наукову новизну отриманих результатів та визначено їх практичне значення. Автором перелічено наукові програми, плани та теми, з якими пов'язана дисертаційна робота та наведено відомості апробацію і впровадження результатів. Для кожної наукової праці та публікації наведено відомості про особистий внесок автора та подано короткий опис роботи.

В ***першому розділі*** викладено теоретичні відомості та проведено аналіз існуючих методів та концепцій конструкцій алгебраїчної комбінаторики та алгебраїчної геометрії, які можна розглядати як інструментарій розробки криптографічних алгоритмів. Висвітлено зв'язок теорії простих алгебр Лі та більш загальних нескінченновимірних алгебр Каца-Муді для побудови родин алгебраїчних графів, які використовуються для породження поліноміальних груп перетворень векторного простору K^n визначеного над довільним скінченним комутативним кільцем.

Наведено опис алгоритмів конструкції стабільних напівгруп та груп перетворень визначених просторів.

Виходячи з теорії символьних обчислень, запропоновано підхід щодо створення ключа шифрування на основі списку одночленів у лексикографічному порядку. Враховуючи властивості Ейлерівського перетворення, показано, що суб'єкти обміну шифрограмами використовують криптосистему з множиною відкритих текстів та простором шифрограм. Такі особливості гарантують постквантовий статус криптосистеми.

Другий розділ присвячено задачам шифрування симетричної криптографії з використанням стабільних кубічних груп, які будуються за відомими екстремальними графами.

Розглянемо стійкість нового потокового алгоритму шифрування кубічними поліноміальними перетвореннями. Визначено, що симетрична криптосистема принципово відрізняється від криптосистеми з публічним

ключем. Її дефініція вимагає повної відкритості алгоритму, а безпека ґрунтується на приватному ключі, відомому кожному з двох кореспондентів.

Показано, що завдяки лінійній складності алгоритму шифрування забезпечується лінійна швидкість процесу шифрування, Досліджена структура формального опису кодуючого відображення.

В ***третьому розділі*** розглянуто задачу створення залежних від ключа шифрування хеш функцій (автентифікаційних кодів документів),що дозволяє уявити електронний документ у вигляді дайджесту (малого документу). Такий підхід дозволяє забезпечити криптографічну стабільність, що означає NP- складність задачі підробки дайджесту, а постквантова стабільність унеможливлює підробку електронного документу з використанням квантового комп'ютера.

В розділі описані нові постквантово стабільні алгоритми створення дайджестів великих документів за допомогою залежних від ключа функій хешування.

В ***четвертому розділі*** розглянуті питання побудови криптосистем з публічним ключем шифрування для випадку бієктивних відображень.

Наведено результати імітаційного моделювання розробленої інформаційної технології, показано методичну оцінку ефективності функціонування запропонованих алгоритмів.

В ***п'ятому розділі*** розглянуті питання побудови систем цифрового підпису з використанням модифікованих алгоритмів електронного цифрового підпису.

Наведено результати дослідження модифікованих алгоритмів електронного цифрового підпису. Досліджено питання постквантового статусу модифікованого алгоритму електронного цифрового підпису.

Висновки до роботи є логічними, обґрунтованими та чітко описують отримані здобувачем результати.

Обґрунтованість висновків і одержаних результатів дисертаційної роботи переконливо окреслена використанням сучасних методів і механізмів некомутативної криптографії, що базується на алгебраїчних об'єктах, таких як групи, напівгрупи, некомутативні кільця та алгебри, методи поліноміальної криптографії від багатьох змінних, прикладної комп'ютерної алгебри та прикладної теорії символьних обчислень..

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, які сформульовані в дисертаційній роботі, забезпечуються широким розкриттям теми досліджень, постановкою чітких та конкретних задач, адекватним математичним та алгоритмічним описанням проблеми та методів її розв'язання. В дисертації достатньо повно викладений огляд досліджень,

теоретичні та експериментальні результати комп'ютерного моделювання. Результати моделювання не викликають сумнівів щодо отриманих результатів.

Отримані автором наукові результати відповідають поставленим задачам досліджень, є логічними, не суперечать фундаментальним фізичним і математичним закономірностям та підтверджуються достатньою апробацією основних положень і висновків на міжнародних форумах, науково-технічних конференціях та семінарах.

Достовірність результатів дисертаційної роботи підтверджується результатами проведених досліджень, коректністю застосування математичного апарату, можливих припущень та формулюванням умов досліджень, а також математичному і імітаційному моделюванні процесів і методів некомутативної криптографії, що базується на алгебраїчних об'єктах, таких як групи, напівгрупи, некомутативні кільця та алгебри, методи поліноміальної криптографії від багатьох змінних, прикладної комп'ютерної алгебри та прикладної теорії символьних обчислень..

Найбільш вагомими науковими результатами, отриманими в дисертації є:

1. 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. Розроблені алгоритми створення чутливих дайджестів електронних файлів для виявлення кібератак на віртуальні організації з покращеним на 45% показником аваланч ефекту;

3. 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. 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. Теорію скінченних геометрій використано для створення алгоритмів електронного підпису криптографії від багатьох змінних, які замість публічних ключів використовують протоколи некомутативної криптографії.

Теоретичне, наукове і практичне значення результатів полягає в

подальшому розвитку теоретичних та практичних методів і моделей некомутативної криптографії, що базуються на алгебраїчних об'єктах, таких як групи, напівгрупи, некомутативні кільця та алгебри, методи поліноміальної криптографії від багатьох змінних, прикладної комп'ютерної алгебри та прикладної теорії символьних обчислень.

Практичне значення одержаних результатів полягає в наступному:

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. Використані 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 икористовують небієктивне відображення необмеженої степені. Параметри (степінь, густина, період) підібрані так, що відомі методи криптоаналітичних 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).

Рекомендації щодо використання наукових результатів

Теоретичні положення, що отримані в дисертаційній роботі, можуть бути розповсюджені на задачі з застосуванням теорії екстремальних графів, проблем постквантової криптографії, проблем безпечного процесування великих файлів, створення новітніх систем захисту інформації та кібернетичної безпеки.

Додаткового дослідження вимагають задачі створення альтернативних публічному ключу алгоритмів, що мають постквантову перспективу, а також опрацювання задач, що пов'язані з напрямком Некомутативної Криптографії, яка базується на алгебраїчних об'єктах (групи, напівгрупи, некомутативні кільця та алгебри). Також інтерес представляють дослідження в напрямку поліноміальної криптографії від багатьох змінних й іншими напрямками прикладної комп'ютерної алгебри та прикладної теорії символьних обчислень..

Завершеність, стиль викладання, публікації

Дисертація та автореферат написані грамотно, а стиль викладення в них матеріалів досліджень, наукових положень, висновків і рекомендацій відповідає вимогам стандарту ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки» й у цілому забезпечує доступність їх сприйняття.

Зміст автореферату відображає основні результати роботи, які приведені в дисертації. Дисертація по тематиці і результатам відповідає паспорту спеціальності 05.13.06 – інформаційні технології.

Основні положення та висновки дисертаційної роботи представлені в 19 наукових працях, 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. В дисертації та авторефераті досить чітко вказано особистий вклад дисертанта при отриманні нових наукових результатів.

Зазначені публікації повною мірою висвітлюють основні наукові положення дисертації. Стиль викладення автореферату в цілому забезпечує його доступність та сприйняття. В ньому чітко і лаконічно викладені наукові завдання дисертаційного дослідження та шляхи їх вирішення. З тексту зрозуміла наукова і практична значимість дисертаційної роботи, особистий внесок здобувача.

Недоліки та зауваження

1) В дисертаціюній роботі недостатньо висвітлені концептуальні зв'язки між теорією алгебр Лі та побудовами алгебраїчних графів, що використовують системи коренів у Евклідових просторах.

2) В дисертаціюній роботі нові модифіковані алгоритми криптографії від багатьох змінних порівнюються тільки з класичними алгоритмами цієї галузі, яка є одним з п'яти напрямків пост квантової криптографії. Було б доцільно навести порівняння нових модифікованих алгоритмів криптографії від багатьох змінних з криптосистемами з інших чотирьох галузей.

3) Модернізований алгоритм потокового шифрування природно було порівняти з RC4 або іншим алгоритмом з цього класу. При порівнянні дайджестів важливий не тільки аваланч ефект, але й швидкодія. Можна було б порівняти ефективність дайджестів з дисертації зі швидкодією алгоритму Кренделева та Сазонової.

4) В тексті роботи та в авторефераті мають місце окремі описки та інколи використовуються терміни і позначення, які не є загальновідомими або загальноприйнятими.

Зазначені недоліки суттєво не впливають на загальне позитивне враження від роботи, не зменшують її наукової цінності та практичної значимості.

Висновки

1. Дисертаційна робота Пустовіта Олександра Сергійовича за темою «Застосування теорії екстремальних графів до сучасних проблем інформаційної безпеки» є кваліфікаційною науковою працею, виконаною особисто здобувачем у вигляді спеціально підготовленого рукопису, яка в цілому відповідає вимогам паспорту спеціальності 05.13.06 – інформаційні технології.

2. Сукупність наукових положень, які сформульовані та обґрунтовані в дисертаційній роботі, має практичну цінність, що підтверджується актами про впровадження результатів.

Дисертаційна робота виконана на високому науковому рівні, відповідає вимогам п.п. 9, 11, 12, 13 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України №567 від 24 липня 2013 р. (зі змінами), а її автор - Пустовіт Олександр Сергійович заслуговує присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології.

Офіційний опонент
доктор технічних наук, доцент,
професор кафедри комп'ютеризованих
систем управління факультету кібербезпеки,
комп'ютерної та програмної інженерії
Національного авіаційного університету В.В. Семко

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ * 01132 * МІСТО КИЇВ *

Семука В.В.
с ф і д ч у ю
Вчений секретар
Національного авіаційного університету
М.Ленковська