ВІДГУК

Офіційного опонента на дисертаційну роботу Пустовіта Олександра Сергійовича «Застосування теорії екстремальних графів до сучасних проблем інформаційної безпеки », що представлена на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології

Актуальність теми дисертаційної роботи та її зв'язок з науковими програмами, планами, темами.

Однією з видатних подій в історії науки є створення у 70-х роках минулого сторіччя напрямку так званої сучасної криптографії, що вивчає алгоритми з публічним ключем та методи електронного підпису, протоколи обміну ключами та пов'язані з ними алгоритми Ель Гамаля, методи розподілу секрету.

Очікування появи реально діючого квантового комп'ютера призвело до перегляду існуючих зараз алгоритмів. Пітер Шор довів, що на квантовому комп'ютері розклад цілого числа на множники можна виконати за поліноміальний час. Це означає, що широко відомий в наш час асиметричний алгоритм RSA не можна використати в постквантову епоху. Виявилося, що й протоколи Діффі – Хелмана для обміну ключів також не мають постквантової перспективи, тому що задача відшукання дискретного логарифму для мультиплікативної групи простого скінченого поля перестає бути складною.

Криптографи, не чекаючи на появу реально діючих квантових комп'ютерів, вже розпочали побудову нових алгоритмів для яких задача постквантового криптографічного аналізу видається важкою. Зокрема Національний інститут стандартизації технологій Сполучених Штатів Америки (NIST) вже у 2017 році оголосив міжнародний тендер щодо створення алгоритмів з публічним ключем, призначених як для шифрування інформації, так і виконання цифрового підпису. Зараз проходить третій етап цього міжнародного проєкту.

У симетричній криптографії також виникає потреба модернізації алгоритмів захисту інформації. Така необхідність пов'язана з появою нових тенденцій в розвитку комп'ютерних послуг, обчислень та технологій, таких як обчислення в хмарах (Cloud Computing), символьні обчислення, паралельні обчислення та інше. Сучасні симетричні методи захисту інформації потребують подальшого розвитку також у зв'язку зі зростом обчислених можливостей сучасних комп'ютерів, успіхів криптоаналізу та вдосконалення техніки, проведення успішних хакерських атак.

Задача вирішення згаданих вище науково-технічних проблем сформульована в Стратегії кібербезпеки України, затвердженої Указом Президента України від 27.01.2016 р., в «Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» затвердженому наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 02.12.2014 р.

вх. N 161/25.10.21-2

Саме цим задачам і присвячена рецензована дисертаційна робота О. С. Пустовіта. Вона 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).

Ці проєкти мені добре відомі як одному з рецензентів звітів по їх виконанню.

У роботі було обрано напрямок поліноміальної криптографіі від багатьох змінних, що є одним з головних напрямків постквантової криптології міжнародного проєкту NIST-2017. Поза постквантовою криптографією ця галузь досліджує симетричні потокові алгоритми шифрування великих файлів та залежні від ключа функції скруту, що використовуються для виявлення кібератак на сховища електронних документів. Дисертант розглядає алгоритми, що використовують екстремальні алгебраїчні графи. Зазначимо, що методи з використанням екстремальних графів у комп'ютерних науках активно розв'язуються в останні роки. Відомі спеціалісти у цьому напрямку Ласло Ловац та Аві Вігдерсон отримали у 2020 році нагороду Абеля.

У дисертації використовуються і методи Некомутативної Криптографії, що є новим «гарячим» напрямком, який буде представлено на сателітній конференції «Математичні методи постквантової криптографії» Міжнародного конгресу математиків 2022.

Підсумовуючи, зазначимо, що дисертаційна робота Олександра Сергійовича Пустовіта присвячена дуже важливим питанням, пов'язаних із сучасними викликами теорії та практики захисту інформації, тематика дисертаційної роботи повністю відноситься до актуальних проблем напрямку 05.13.06 – Інформаційні технології.

Оцінка змісту дисертації

Дисертація складається зі вступу, переліку умовних позначень, п'яти розділів, висновків та списку використаних джерел (>200 назв).

У *вступі* добре обгрунтовано актуальність теми, сформульовано мету і завдання дослідження, відображено наукову новизну та практичне значення роботи, вказано на деякі впровадження результатів роботи.

Розділ 1 присвячено задачі створення алгоритмів шифрування з публічним ключем у термінах криптографії від багатьох змінних. Автор наводить досить повний огляд літератури по цій тематиці. Для імплементації з подальшою оптимізацією він обирає алгоритми, що використовують спеціальні групи поліноміальних перетворень афінного простору вимірності n над скінченним комутативним кільцем. Важливою властивістю груп є можливість обчислення суперпозиції n-елементів групи за поліноміальний час від змінної n. О. С. Пустовіт використовує два відомі класи таких підгруп, а саме підгрупу афінної

групи Кремони, що утворено елементами максимальна степінь яких обмежена незалежною сталою d (стабільні підгрупи) та підгрупи Ейлерівських перетворень, що складаються з відображень, що переводять кожну змінну у деякий одночлен.

Дисертант розробив комп'ютерні програми, що генерують стабільне перетворення S афінної групи Кремони разом з Ейлерівським відображенням E. Власник публічного ключа має обидва перетворення разом з оберненими до них у многовидах K^n та $(K^*)^n$, де K обране комутативне кільце з мультиплікативною групою K^*. Публічний користувач має лише перетворення ES, записане у його стандартній формі визначеної списком впорядкованих одночленів. Цей алгоритм з публічним ключем вперше імплементовано для скінченних полів характеристики 2 та кілець лишків за модулем 2^m.

У дисертації наводяться оцінки складності, показано, що при $d=3$ кодуюче перетворення складається з $O(n^4)$ мономів та має лінійну степінь $O(n)$. Відзначимо, що класична криптосистема шифрування з публічним ключем від багатьох змінних використовує кодуючи бієктивні відображення степені 2 або 3. Безпека алгоритму грунтується на складності загальної задачі розв'язку системи n поліноміальних рівнянь лінійної степені >n.

Атаки опонента, що використовують методи лінеаризації неможливо виконати за недоліком необхідних ресурсів. Зазначимо, що дисертант успішно використав застосування теорії алгебр Лі типу Каца-Муді, знайшов цікаві розв'язання для генерування алгебраїчних об'єктів у пам'яті комп'ютера, використав теорію символьних перетворень, пов'язану з алгебраїчними графами.

Розділ 4 присвячено криптосистемам шифрування з публічним ключем, що спирається на бієктивні відображення криптографії від багатьох змінних, Ейлерівські та стабільні перетворення використовуються окремо. Відзначимо випадок відображень, що спираються на перетворення, що будуються за подвійними графами Шуберта. У цьому випадку публічний ключ задається перетворенням степені n та густини $O(n^2)$.

Розділи 2 та 3 присвячені задачам симетричної криптографії. У другому розділі детально описано імплементацію потокового алгоритму шифрування перетвореннями, що будуються за екстремальними графами великого обгорту. Дисертант використовує відому групу $GA(n, K)$ та $DA(n,k)$ кубічних перетворень, що будуються за графами $A(n, K)$ та $D(n,K)$. У випадку, коли K є скінченним полем порядку q проективна границя графів $A(n, K)$ при зростаючому n буде нескінченним регулярним деревом, а границя графів $D(n, K)$ буде нескінченним лісом з нескінченними регулярними деревами.

У цьому випадку можна вважати, що перетворення групи $GA(n,K)$ визначається прогулянкою у дереві або ж лісі. При достатньо великому n різним прогулянкам з початкової вершини графу відповідають різні кінцеві вершини. Дисертант побудував нові потокові алгоритми шифрування за допомогою елементів TGT^{-1} де $G=A(n,K)$ та T спеціальне лінійне перетворення. Йому вдалося так підібрати матрицю перетворення T, що зміна одного символу у відкритому тексті призводить до зміни 98% символів шифрограми.

Отже побудовано новий потоковий алгоритм шифрування кубічними поліноміальними перетвореннями. Відомо, що у випадку стабільного кубічного перетворення атака лінеаризації потребує $O(n^3)$ перехоплень пар типу відкритий текст разом з відповідною йому шифрограмою. Це означає, що при роботі з великими файлами атаки лінеаризації неможливий за браком ресурсів.

Зазначимо, що теоретична швидкість шифрування становить $O(n)$, тобто вона пропорційна швидкості читання файлу комп'ютером. Матеріал цього розділу ілюстровано результатами комп'ютерної симуляції, що відображені у таблицях і графіках. Крім швидкодії досліджувалася густина кубічного перетворення через кількість його одночленів. Цей параметр можна вжити для уточнення оцінки складності атаки лінеаризації. Вважаю, що представлені вдосконалені потокові алгоритми шифрування безумовно будуть використані при процесуванні великих файлів у бінарному алфавіті.

У третьому розділі описано нові алгоритми створення дайджестів великих документів за допомогою залежних від ключа функій хешування. Автор використовує взаємно однозначну відповідність між текстами в алфавіті K та елементами напівгрупи шляхів у кореневому дереві $A(K)$, визначеному у першому розділі. Образ побудованого гомоморфізму цієї напівгрупи у групу кубічних перетворень, визначеним графом $A(n, K)$ та його спряження з лінійними перетвореннями використані для побудови чутливих дайджестів електронних документів. Побудовані хеш функції характеризують високий показник лавинного ефекту. Поєдина зміна символу в тексті змінює більш ніж 98% символів дайджесту. Вважаю, що такі чутливі інструменти детекції атак на електронні сховища можуть успішно використовуватися у системах кібербезпеки.

Останній п'ятий розділ присвячено постквантовим протоколам захисту ключів та їх розширенням до криптосистем типу Ель Гамаля. Автор використовує відомі платформи, що є родинами піднапівгрупами афінних груп Кремони вимірності n. Обрані платформи мають важливу властивість можливості обчислення добутку n–елементів за поліноміальний час від n. Вони підрозділяються на два різні класи – напівгрупу Ейлерівських перетворень та стабільні групи Кремони, визначені за алгебраїчними графами.

Ці платформи використано для створення нових протоколів, безпека яких спирається на складність задачі знаходження розкладу елементу напівгрупи у добуток відомих породжуючих твірних. На сьогоднішній день розв'язки цієї задачі за поліноміальний час при використанні як машини Тюрінга, так і теоретичного квантового комп'ютера не знайдено.

Тому представлені протоколи та криптосистеми мають постквантовий статус. При їх побудові використані методи криптографії від багатьох змінних так і некомутативної криптографії. Варто відзначити такі дві особливості: протоколи використовують гомоморфізми, що швидко обчислюються, колізійний елемент та генератори платформи представляються у стандартній формі криптографії від багатьох змінних.

Створені асиметричні криптосистеми цього розділу принципово відмінні від публічних ключів, тому що перетворення шифрування не надається публічно, воно виробляється кореспондентами під час протоколу.

Вважаю, що такі постквантові криптосистеми є більш гнучкими у порівнянні з публічними ключами і можуть знайти широкі застосування. О. С. Пустовіт наводить приклади застосування таких протоколів для вирішення задачі електронного підпису. Зокрема наводиться модифікація відомого алгоритму ''Uubalanced Rainbow like Oil and Vinegar system'', в якому користувачі переводять публічне відображення у прийнятий ключ, відомий кожній зі сторін.

Рекомендації щодо використання результатів дисертації.

Підсумовуючи вище сказане вважаю, що дисертаційна робота Олександра Сергійовича Пустовіта, що розв'язує кілька важливих технічних проблем, захисту інформації містить кілька добре описаних нових алгоритмів криптографії від багатьох змінних, що мають певну постквантову перспективу.

Вважаю, що результати дисертаційної роботи будуть використатися дослідниками Київського національного університету імені Тараса Шевченка, Інституту Кібернетикі ім. В. М. Глушкова НАН України, Інституту телекомунікацій та глобального інформаційного простору НАН України,. Київського Політехнічного Університету та інших установ, де створюються комп'ютерні системи кібербезпеки.

Зауваження щодо змісту дисертаційної роботи.

Опис деяких алгоритмів у роботі потребує доповнення у вигляді графічних схем або презентації у псевдокоді. Однак такі доповнення значно б збільшили і без того великий обсяг роботи.

Треба було б перелічити переваги екстремальних графів перед загальними алгебраїчними при їх застосуванні у криптографії. Зазначити, що у випадках графів великого обгорту, саме обгорт гарантує властивість – різні ключі – різні шифрограми. Звязність графу гарантує транзитивність дії групи кодуючих перетворень, вказати переваги так званих графів малого світу.

Згадані недоліки невпливають суттєво на мою високу оцінку змісту дисертації.

Оцінка мови, стилю та оформлення дисертації та автореферату.

Оформлення дисертаційної роботи й автореферату цілком відповідає встановленим вимогам. На мій погляд розділ 4 треба було б розмістити безпосередньо за першим розділом, ці розділи об'єднує спільна задача – створення публічних ключів.

Робота й автореферат написано на досить високому стилістичному рівні та з використанням загальновизначеної сучасної наукової термінології, що забезпечує доступність їх сприйняття та використання. Дисертація в цілому досить добре написана, незважаючи на певну кількість описок та опечаток, неминучих у роботі такого значного обсягу (> 160 сторінок). Звичайно, такі зауваження не впливають на високу оцінку роботи.

Основні результати своєчасно опубліковані у фахових журналах із політехнічних та фізико-математичних наук, що відповідають вимогам МОН України; зокрема, дві статті опубліковано в журналах що індексуються в SCOPUS.

Загальний висновок.

Таким чином, дисертаційна робота є вагомим внеском у теорію постквантової криптографії, у ній, зокрема, в явному вигляді описано нові алгоритми, що використовують разом криптографію від багатьох змінних та елементи некомутативної криптографії.

Дисертаційна робота Пустовіта О. С. виконана на актуальну тему, на високому науковому рівні, висунуті на захист результати та обґрунтовані положення, мають наукову новизну та практичну цінність, дисертаційна робота задовольняє п.п 9, 11, 12, 13 «Порядку присудження наукових ступенів», затвердженого постановою КМУ №567 від 24.07.2013 р. (зі змінами, внесеними згідно з Постановами КМУ №656 від 19.08.2015 р., №1159 від 30.12.2015 р. та №567 від 27.07.2016 р.), а її автор, Пустовіт Олександр Сергійович, заслуговує на присудження наукового ступеня кандидата технічних наук зі спеціальності 05.13.06 – Інформаційні технології.

Офіційний опонент:
завідувач кафедри алгебри і комп'ютерної математики
Київського національного університету
імені Тараса Шевченка
доктор фізико-математичних наук, професор А. П. Петравчук

Підпис [illegible]
Вчений секретар НДЧ
Карабульна Н. В.
19.11.2021 р.

Україна * Київський національний університет імені Тараса Шевченка * Ідентифікаційний код 02070944