ВІДГУК

офіційного опонента на дисертацію Ігнатенка Сергія Михайловича «Методи розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації

Актуальність теми дисертаційного дослідження.

Можлива поява в найближчому майбутньому багатокубітних універсальних квантових комп'ютерів становить загрозу сучасним шифросистемам. У зв'язку з цим виникає потреба у так званих постквантових шифросистемах, що залишаються стійкими у моделі квантових обчислень. Останнім часом такі шифросистеми активно створюються і розвиваються, в тому числі в рамках конкурсів на стандарти постквантових алгоритмів, оголошені Національним Інститутом Стандартів та Технологій (NIST) США, Європейським Інститутом Телекомунікаційних Стандартів (ETSI) тощо.

При цьому виникає необхідність в створенні не тільки традиційних асиметричних шифросистем, які активно розвиваються. Гостро також стоїть потреба в створенні та застосуванні на практиці симетричних постквантових шифросистем, стійкість яких базується на складності розв'язання єдиної обчислювально складної задачі. Серед таких шифросистем широке розповсюдження поряд з іншими мають такі, що базуються на складності розв'язання як двійкової задачі LPN над полем з двох елементів, так і над кільцями лишків.

Разом з тим, застосування шифросистем в сучасних інформаційно-телекомунікаційних системах можливе лише після їх детального аналізу, в тому числі оцінювання їх криптографічної стійкості. Тобто залишається відкритим питання вибору параметрів постквантових шифросистем, що забезпечують їх стійкість відносно конкретних атак.

Враховуючи вищесказане, тема дисертаційного дослідження Ігнатенка С. М. є актуальною. Здобувачем вирішується актуальне наукове та практичне завдання розробки більш ефективних (в порівнянні з перебірним) методів розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем.

Зв'язок роботи з науковими програмами, планами, темами.

Дослідження, результати яких викладені в дисертації, проводились відповідно до планів науково-дослідної роботи спеціального факультету Служби безпеки України у складі військового інституту телекомунікацій та інформатизації Національного технічного університету України «Київський політехнічний інститут» та в рамках науково-дослідних робіт «Баракуда» (№ держреєстрації 0108U000007д) на замовлення Служби зовнішньої розвідки України, НДР «Самсон» на замовлення Служби безпеки України.

Зміст та структура дисертаційної роботи.

Дисертаційна робота складається з анотації, вступу, чотирьох розділів, які містять основні наукові результати роботи, загальних висновків та чотирьох додатків.

У ***вступі*** обґрунтовано актуальність напрямку дослідження, наведено зв'язок роботи із науковими програмами, сформульовані мета та задачі дослідження, відображені наукова новизна та практичне значення отриманих результатів, особистий внесок здобувача, наведені відомості про апробацію результатів дисертації та публікації. Визначено об'єкт та предмет дослідження, надана загальна характеристика роботи у відповідності з діючими вимогами до дисертацій.

Перший розділ дисертації має оглядовий характер. Наголошується на ролі постквантових криптосистем і протоколів, наведено їх класифікацію. Підкреслена актуальність задачі розробки методів побудови та оцінювання стійкості постквантових криптосистем, зокрема, симетричних. Наведено формулювання задачі LPN над скінченними кільцями, проаналізовано методи розв'язання цієї задачі. Виконано постановку задач дослідження для вирішення визначеної наукової задачі та її деталізацію. Розділ завершується формулюванням висновків щодо доцільності проведення подальших досліджень.

У ***другому розділі*** наведено аналітичні оцінки обсягу матеріалу, достатнього для розв'язання задачі LPN над скінченними кільцями методом максимальної правдоподібності із заданою достовірністю. Отримані оцінки мають важливе значення для практичного застосування, оскільки вони дають можливість отримати коректні значення часової складності методу максимуму правдоподібності та інших алгоритмів розв'язання задачі LPN над довільним скінченним кільцем. Це, в свою чергу, дозволяє оцінити стійкість симетричних постквантових шифросистем, стійкість яких базується на складності розв'язання задачі LPN над довільним скінченним кільцем.

Показана залежність обсягу матеріалу від розподілу спотворень у правих частинах системи рівнянь.

У ***третьому розділі*** наведено два методи підвищення ефективності розв'язання задачі LPN за допомогою методу максимуму правдоподібності. Перший метод є застосовним для довільного скінченного фробеніусова кільця та базується на використанні швидкого перетворення Фур'є допоміжних функцій, що визначаються на цьому кільці. Другий метод є застосовним до задачі LPN над кільцем лишків за модулем 2^N і базується на використанні числового перетворення Ферма.

Показано, що застосування швидкого перетворення Фур'є або числового перетворення Ферма на другому етапі узагальненого алгоритму BKW значно зменшує складність останнього.

У ***четвертому розділі*** викладено послідовний метод розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем лишків за модулем 2^N. Базується він на ідеї розбиття заданої системи рівнянь на системи рівнянь над кільцями меншого порядку та послідовного їх розв'язання тими алгоритмами із заданої множини таких алгоритмів, які найбільше підходять, виходячи з характеристик їх ефективності.

В якості прикладів ефективного застосування розроблених методів розв'язання задачі LPN над кільцем лишків за модулем 2^N, обчислено оцінки стійкості шифросистем типу RING-LWE та LPN-C відносно атак на основі підібраних відкритих повідомлень та SNOW 2.0-подібного потокового шифру відносно кореляційних атак. Отримані оцінки дозволяють при проектуванні шифру обирати конкретні значення його параметрів в залежності від необхідної стійкості. Результати застосування отриманих результатів демонструють перевагу в ефективності запропонованих методів розв'язання задачі LPN над скінченними кільцями, що дозволяє в свою чергу уточнювати оцінки стійкості шифросистем, стійкість яких базується на цій задачі.

У ***висновках*** викладено найважливіші наукові та практичні результати, які отримані в дисертаційній роботі, що дають розв'язок сформульованих наукових задач дисертаційного дослідження.

Додатки містять: доведення окремих лем та тверджень, опис швидкого алгоритму множення вектора на тензорний степінь матриці над комутативним кільцем, програмний код реалізації окремих методів розв'язання задачі LPN над скінченними кільцями, акти впровадження результатів дисертаційної роботи.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації.

Висновки та результати дисертації викладені змістовно, в логічній послідовності, у відповідності зі структурою задач, поставлених і вирішених у дисертаційній роботі.

Обґрунтованість отриманих результатів дисертаційного дослідження підтверджується збігом результатів, що отримані аналітичними методами, з результатами імітаційного моделювання. Достовірність одержаних результатів досліджень, висновків та рекомендацій підтверджується їх несуперечливістю відомим положенням теорії криптології, абстрактної алгебри, відомим теоретичним та практичним результатам, та збігом результатів статистичних випробувань та досліджень з теоретичними оцінками, а також опублікованими науковими працями та актами впровадження результатів дисертаційної роботи.

До основних наукових результатів, які одержані в дисертаційній роботі, можна віднести:

1. Вперше отримані аналітичні оцінки обсягу матеріалу, достатнього для розв'язання із заданою достовірністю задачі LPN над довільним скінченним кільцем, які узагальнюють аналогічну оцінку, відому для випадку класичної задачі LPN та дозволяють визначити часову складність узагальненого алгоритму BKW, відомий прототип якого є на сьогодні одним з найефективніших алгоритмів розв'язання класичної задачі LPN.

2. Удосконалений метод максимуму правдоподібності (ММП) розв'язання задачі LPN над скінченними фробеніусовими кільцями на основі використання швидкого перетворення Фур'є, що дозволяє суттєво зменшити часову складність розв'язання задачі LPN над фробеніусовими кільцями як за допомогою самого ММП, так і інших алгоритмів, що використовують ММП як допоміжну процедуру.

3. Удосконалений метод максимуму правдоподібності розв'язання задачі LPN над кільцем лишків за модулем 2^N на основі використання числового перетворення Ферма, що надає можливість суттєво зменшити часову складність розв'язання задачі LPN за допомогою узагальненого алгоритму BKW.

4. Вперше розроблений метод побудови нових алгоритмів розв'язання задачі LPN над кільцем лишків за модулем 2^N за довільною скінченною сукупністю вхідних таких алгоритмів, що надає можливість підвищити ефективність розв'язання цієї задачі шляхом належного вибору композиції числа N.

Вважаю, що новизна наукових положень, висновків і рекомендацій дисертаційної роботи відповідає сучасному стану розвитку систем захисту інформації та в достатньому обсязі відображена в дисертаційній роботі та авторефераті.

Практичне значення дисертаційної роботи полягає у розробленні нових методів більш точної оцінки стійкості симетричних постквантових шифросистем, що базуються на задачі LPN над скінченними кільцями, можливості при проектуванні таких шифрів обирати конкретні значення параметрів в залежності від стійкості, яку необхідно забезпечити на практиці. Практичне значення розроблених нових та удосконалених існуючих методів розв'язання задачі LPN над скінченними кільцями також доводиться актами впровадження результатів дисертаційного дослідження.

Повнота викладених результатів дисертаційного дослідження в опублікованих працях здобувача.

Основні результати дисертаційної роботи викладені у 17 наукових працях (10 статей, 7 тез доповідей). Серед статей 7 робіт у фахових виданнях України, одна робота опублікована в міжнародному журналі, включеному до міжнародних наукометричних баз, в тому числі Scopus.

Таким чином, кількість та якість наукових робіт здобувача з теми дисертації відповідають вимогам МОН України до дисертацій на здобуття наукового ступеня кандидата технічних наук.

Оцінка мови та стилю викладення дисертації та автореферату.

Дисертація Ігнатенка С. М. написана з дотриманням прийнятої термінології, стиль викладення матеріалу забезпечує доступність його сприйняття спеціалістом, а науковий рівень дисертації відповідає існуючим вимогам до кандидатських дисертацій.

Зміст автореферату достатньо повно відображає основні положення, що викладені у дисертаційній роботі Ігнатенка С.М.

Відповідність дисертаційної роботи спеціальності.

Дисертаційна робота Ігнатенка С.М. за змістом і отриманими результатами повністю відповідає паспорту спеціальності 05.13.21 – Системи захисту інформації.

Все вищевикладене дає змогу позитивно оцінити дисертаційне дослідження Ігнатенка С.М., відзначити його наукову новизну та практичне значення, а також високий рівень виконаних теоретичних та експериментальних досліджень. У цілому позитивно оцінюючи дисертаційне дослідження, необхідно зазначити наявність у ньому деяких дискусійних моментів та висловити наступні **зауваження**:

1. В дисертаційній роботі не зазначено, з яких причин для узагальнення алгоритму на випадок довільного кільця з сімейства BKW обрано саме алгоритм, описаний в роботі Zhang B., Xu C., Meier W. "Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0", а не будь-який інший з алгоритмів сімейства BKW, що існують для поля GF(2).
2. Різні параметри в роботі мають однакові позначення. Зокрема, символом ε в роботі одночасно позначено і параметр в розподілі спотворень у правих частинах рівнянь (формула 2.23, с. 74), і числа в задачі про адитивне представлення (с. 79), і параметр, який визначає близькість розподілу спотворень у правій частині систем рівнянь до рівномірного розподілу ймовірностей на кільці R. Крім того, $\varepsilon(x)$ також позначено вектор b-Ax при розв'язанні системи лінійних рівнянь зі спотвореними правими частинами (с. 67).
3. Шифросистема LPN-C (пункт 4.2.2) використовує секретний ключ, який є матрицею з великою кількістю елементів: десятки та сотні тисяч (табл. 4.3). Проте питання розподілення ключів такого значного розміру у роботі не розглядається.
4. Текст роботи перевантажений математичними доведеннями тверджень, тільки частина доведень винесена в додаток А. На наш погляд, слід було б винести всі доведення тверджень в додатки, що спростило би сприйняття тексту дисертації.
5. Текст дисертаційної роботи перевантажений абревіатурами, далеко не всі з яких зазначені у переліку умовних позначень (с. 20). Зокрема, назви більшості постквантових криптосистем і протоколів на схемі (рис. 1.1, с. 31) представлені абревіатурами без їх розкриття. Це дещо ускладнює процес оцінювання роботи при її читанні.
6. Програмні коди реалізації методів розв'язання задачі LPN над скінченними кільцями (додатки Б, В) оформлені не за правилами. Зокрема, відсутні будь-які коментарі, що ускладнює аналіз програмного коду.

Відповідність дисертації встановленим вимогам і загальні висновки.

Викладене дозволяє зробити загальний висновок, що дисертаційна робота Ігнатенка Сергія Михайловича «Методи розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем» є завершеною науковою кваліфікаційною працею, що виконана автором на високому рівні, вирішує актуальну наукову задачу розроблення ефективних методів розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем, має наукову й практичну цінність.

Таким чином, дисертаційна робота «Методи розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем» відповідає вимогам до кандидатських дисертацій «Порядку присудження наукових ступенів», а її автор, Ігнатенко Сергій Михайлович заслуговує на присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

ОФІЦІЙНИЙ ОПОНЕНТ
декан факультету Кібербезпеки, комп'ютерних і радіо технологій,
професор кафедри Кібербезпеки та технічного захисту інформації
Державного університету інтелектуальних технологій і зв'язку

доктор технічних наук, професор Є. В. Васіліу

Підпис завіряю:
Учений секретар
Руда Г.В.