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.

Можливість виконання алгоритмів Шора та Гровера на повноцінному квантовому комп'ютері створює потенційну загрозу стійкості сучасних традиційних асиметричних та симетричних криптоалгоритмів відповідно. Зазначене стимулює до розробки шифросистем нового типу (постквантових), стійкість яких, по-перше, здатна протистояти атакам з використанням квантового комп'ютера, а по-друге, буде залежати від здатності обчислювальної техніки розв'язувати одну єдину складну математичну задачу.

Однією з таких задач є LPN (learning parity with noise), яка фактично полягає в розв'язуванні системи лінійних рівнянь зі спотвореними правими частинами. Як правило, такі системи рівнянь розглядаються над полем із двох елементів, проте останнім часом набувають поширення шифросистеми, побудовані над більш складними алгебраїчними структурами, взагалі кажучи, над будь-яким скінченним кільцем. Такі шифросистеми мають вищу швидкість шифрування (розшифрування) даних у порівнянні з традиційними. Крім того, потенційно від них можна очікувати приросту стійкості, проте це питання на сьогодні залишається відкритим, оскільки у відкритих джерелах відсутні методи оцінювання стійкості шифросистем, що будуються на складності розв'язання задачі LPN над скінченними кільцями загального вигляду.

Тому, робота Ігнатенка Сергія Михайловича, що пов'язана з отриманням науково обґрунтованих оцінок стійкості симетричних шифросистем, які базуються на складності розв'язання задачі LPN над скінченними кільцями для їх подальшого практичного використання, безумовно є актуальною.

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

Дослідження, результати яких викладені в дисертації, проводились в рамках науково-дослідних робіт "Баракуда" (№ держреєстрації 0108U000007д) на замовлення Служби зовнішньої розвідки України та НДР "Самсон" (держреєстрації не підлягає) на замовлення Служби безпеки України.

Структура дисертаційної роботи.

Дисертаційна робота складається з анотації, вступу, чотирьох розділів, які містять основні наукові результати, 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 практична цінність роботи, особистий внесок здобувача, наведені відомості про апробацію результатів дисертації та публікації. Визначено об'єкт та предмет дослідження та надана загальна характеристика роботи у відповідності з діючими вимогами до дисертацій.

Перший розділ дисертації має оглядовий характер. Проводиться аналіз основних видів постквантових криптосистем і протоколів. Аналізуються методи побудови та оцінювання стійкості симетричних постквантових шифросистем, стійкість яких базується на складності розв'язання задачі LPN. Значну увагу приділено існуючим методам розв'язання зазначеної задачі над полем з двох елементів, викладено методи зменшення трудомісткості таких методів. Наведено асимптотичні оцінки часової складності методів розв'язання систем лінійних рівнянь зі спотвореними правими частинами в залежності від наявного числа рівнянь.

У ***другому розділі*** показано як по заданим параметрам системи лінійних рівнянь зі спотвореними правими частинами над довільним скінченним кільцем (число невідомих, розподіл ймовірносте спотворень) обчислювати обсяг числа рівнянь, достатнього для розв'язання такої системи із заданою надійністю. Наведено порівняння отриманих оцінок з відомою нижньою межею обсягу матеріалу.

Показано, як скористатися отриманими оцінками для визначення часової складності та оптимізації узагальненого алгоритму BKW, відомий прототип якого є на сьогодні одним з найефективніших алгоритмів розв'язання класичної задачі LPN. На прикладах продемонстрована значна перевага в трудомісткості узагальненого алгоритму BKW в порівнянні з методом максимуму правдоподібності.

У ***третьому розділі*** викладені дві модифікації методу максимуму правдоподібності розв'язання задачі LPN над скінченними кільцями - на основі використання швидкого перетворення Фур'є та числового перетворення Ферма відповідно. Показано, що зазначені модифікації дозволяють в окремих випадках розв'язувати системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями набагато швидше при тій самій надійності.

Значно розширено клас алгебраїчних структур, для яких можна застосовувати швидке перетворення Фур'є з метою зменшення трудомісткості. Встановлено, що таким є дуже широкий клас фробеніусових кілець. Модифікація методу максимуму правдоподібності може бути застосована у випадку розв'язання задачі LPN над кільцем $\mathbf{Z}/(2^N)$. При цьому обчислення проводяться в кільці лишків за модулем числа Ферма.

У ***четвертому розділі*** запропоновано послідовний метод побудови нових алгоритмів розв'язання задачі LPN над кільцем лишків за модулем 2^N за довільною скінченною сукупністю вхідних таких алгоритмів. Зазначений метод дозволяє за умови достатньої множини вхідних алгоритмів будувати такий алгоритм розв'язання загальної задачі, значення трудомісткості та надійності якого найбільше задовольняють вимогам конкретної практичної необхідності.

Отримано чисельні оцінки стійкості частково гомоморфної шифросистеми типу Ring-LWE. На цьому прикладі продемонстровано потужність узагальненого алгоритму BKW у порівнянні з методом максимуму правдоподібності, що виявляється в значному зменшенні часової складності.

Виграш у трудомісткості запропонованих модифікацій методу максимуму правдоподібності показано на прикладі обчислення оцінок стійкості SNOW 2.0-подібного шифру над кільцем $\mathbf{Z}/(2^N)$ відносно кореляційних атак.

В якості прикладу практичного застосування послідовного методу запропоновано ефективну атаку на симетричну шифросистему типу LPN-C над кільцем лишків за модулем 2^N відносно атаки на основі підібраного відкритого тексту. Оцінено часову складність та обсяг матеріалу, потрібного для розв'язання систем лінійних рівнянь за допомогою узагальненого алгоритму BKW та послідовного методу відповідно. Показано, що в окремих випадках послідовний метод дозволяє більш ефективно розв'язувати задачу LPN над кільцями лишків за модулем 2^N, що свідчить про недоцільність використання таких кілець для побудови шифросистем зазначеного типу.

У ***висновках*** викладено найважливіші наукові та практичні результати, які одержані в дисертації.

Додатки містять: опис додаткових матеріалів, на які спираються дослідження, виконані в роботі; отримання деяких формул, які мають значний обсяг; програмні коди реалізації модифікації методу максимуму правдоподібності з використанням швидкого перетворення Фур'є та послідовного методу розв'язання системи лінійних рівнянь над кільцем $\mathbf{Z}/(2^N)$; акти реалізації використання (акти впровадження результатів дисертаційної роботи).

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

Положення та висновки, що викладені в дисертаційній роботі, обґрунтовано із залученням значного обсягу сучасних теоретичних та експериментальних методів дослідження, а також співставленням одержаних результатів з літературними даними, співпадінням результатів, що отримані аналітичними методами, із даними імітаційно-математичних моделей. Достовірність одержаних результатів досліджень, положень та висновків забезпечено адекватним застосуванням сучасних методів обробки експериментальних даних, детальним аналізом одержаних результатів, несуперечливістю відомим положенням теорії криптології, абстрактної алгебри, відомим теоретичним та практичним результатам, та співпадінням результатів статистичних випробувань та досліджень з теоретичними оцінками.

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

1. Вперше отримано 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. Удосконалено метод максимуму правдоподібності розв'язання задачі LPN над скінченними фробеніусовими кільцями на основі використання швидкого перетворення Фур'є, що дозволяє помітно 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. Удосконалено 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 розроблено 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.

Повнота викладених результатів дисертаційних досліджень в опублікованих працях здобувача.

Основні результати роботи викладено у 10 наукових статтях, з них 7 статей у наукових фахових виданнях України, 1 стаття у виданні України, що входить до міжнародної наукометричної бази SCOPUS та 7 публікаціях, які засвідчують апробацію матеріалів дисертації (загальний обсяг публікацій 5,82 д.а.). Публікації повністю відображають зміст дисертаційної роботи.

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.

Дисертаційна робота написана грамотною мовою, стиль викладення матеріалів теоретичних та практичних досліджень, наукових положень і висновків забезпечує доступність їх сприйняття і використання. Науковий рівень дисертації відповідає існуючим вимогам до кандидатських дисертацій.

Зміст автореферату достатньо повно відображає основні положення, що викладені у дисертаційній роботі. Оформлення дисертаційної роботи і автореферату відповідає встановленим вимогам.

Практичне значення роботи полягає в появі можливості оцінювати стійкість симетричних постквантових шифросистем шляхом більш ефективного розв'язання задачі LPN над скінченними кільцями та, як наслідок, суттєвому підвищенні криптографічної стійкості симетричних постквантових шифросистем.

Зауваження до дисертації.

Відзначаючи наукову новизну, практичну значимість, якість та повноту одержаних теоретичних та практичних результатів, слід навести зауваження до дисертації, до яких, на мій погляд, належать такі:

1. Не зовсім коректним на сторінці 29 є співставлення за стійкістю до криптоаналізу (нехай і в моделі квантових обчислень) таких різних за стійкістю криптоалгоритмів як RSA та ECDSA.
2. Твердження автора про те, що «беззаперечною перевагою симетричних постквантових шифросистем є обґрунтована залежність їх стійкості від складності розв'язання лише однієї математичної задачі» (стор. 34) є некоректним з точки зору відсутності доведення для цього класу криптосистем еквівалентності задачі їх криптоаналізу лише обраній задачі в рамках теоретико-складностного підходу до оцінки стійкості.

3. Окремі твердження в главі 1 про віднесення математичних задач до тих, які не мають ефективних алгоритмів в квантовій моделі обчислень, не є загальноприйнятими.

4. При розгляді методів зменшення трудомісткості ММП в главі 3 за рахунок використання алгоритмів швидкого перетворення Фур'є (у випадку, коли R є полем порядку 2^N), не розглядається можливість застосування інших теоретико-числових перетворень (Мерсена, Уолша-Адамара, Хаара, тощо), які потенційно дозволили би розширити сферу застосування запропонованого підходу.

5. Наведений в додатку Б вихідний код програмного забезпечення (стор. 178) не відповідає вимогам «best practices» оформлення вихідного коду програм на мові програмування C++ (наприклад, Google C++ Style Guide).

Проте, відзначені недоліки не зменшують позитивного ставлення до роботи в цілому.

Відповідність дисертації встановленим вимогам і загальні висновки.

Дисертаційна робота Ігнатенка Сергія Михайловича "Методи розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем" відповідає паспорту спеціальності 05.13.21 – системи захисту інформації та профілю спеціалізованої вченої ради Д64.051.29.

Викладене дозволяє зробити загальний висновок, що дисертаційна робота Ігнатенка С. М. є завершеною науковою кваліфікаційною працею, що виконана автором особисто на належному рівні, яка вирішує актуальну наукову задачу та 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 п.п. 9, 11-14 «Порядку присудження наукових ступенів» (затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 року № 567 зі змінами), 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
професор кафедри математичних методів
захисту інформації Фізико-технічного інституту
Національного технічного університету "Київський політехнічний
інститут імені Ігоря Сікорського",
лауреат Державної премії України в галузі науки і техніки,
доктор технічних наук, старший науковий співробітник

А. М. Кудін

ЗАСВІДЧУЮ