ВІДГУК

офіційного опонента на дисертаційну роботу
Матійко Александри Андріївни
на тему «Метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем»,
представлену на здобуття ступеня доктора філософії
в галузі знань 12 Інформаційні технології
за спеціальністю 125 Кібербезпека

Актуальність теми дисертації

Сьогодні забезпечення інформаційної безпеки держави є однією із найважливіших задач в умовах великої кількості внутрішніх та зовнішніх загроз. Таким чином, першочерговими задачами у сфері інформаційної безпеки держави є розробка нових та вдосконалення існуючих криптографічних систем. У той же час, через активні дослідження в галузі квантових комп'ютерів, безпека більшості сучасних криптографічних систем знаходиться під загрозою, адже квантові комп'ютери можуть надати необхідне зростання продуктивності та швидкості для виконання важкорозв'язних на сьогодні задач. У зв'язку із зазначеним, виникає необхідність у створенні нових постквантових криптографічних систем, які залишаться стійкими за умови існування потужних квантових комп'ютерів.

Важливим видом постквантових криптосистем є решіткові (NTRU-подібні) криптосистеми, до яких відноситься, зокрема, приблизно третина всіх криптосистем і протоколів, поданих до конкурсу NIST з розробки нових стандартів постквантових криптосистем та протоколів. Окрім того, новітній національний стандарт асиметричного шифрування ДСТУ 8961:2019 «Скеля» також є NTRU-подібним.

Значний розвиток решіткової криптографії стимулює створення симетричних постквантових шифросистем, стійкість яких базується на складності розв'язанні лише однієї обчислювальної задачі. Проте слід відзначити, що єдина відома на сьогодні симетрична NTRU-подібна шифросистема (NTRUCipher) виявляється уразливою відносно певних атак.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

1. Вперше отримано аналітичні співвідношення для оцінювання ймовірності оборотності випадкових поліномів, які використовуються в NTRU-подібних шифросистемах. На відміну від відомого співвідношення для ймовірності оборотності випадкового рівноймовірного елементу кільця зрізаних поліномів, отримані співвідношення є справедливими для більш загальної схеми формування

випадкових поліномів. Вони базуються на застосуванні апарату перетворення Фур'є розподілів ймовірностей на скінченному полі та надають змогу оцінювати (а в окремих практично важливих випадках – обчислювати) значення ймовірності оборотності випадкових поліномів, що використовуються в ролі компонентів секретних ключів NTRU-подібних шифросистем.

2. Удосконалено аналітичні співвідношення для оцінювання ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах. На відміну від раніше відомих, отримані співвідношення є справедливими для усіх видів сучасних NTRU-подібних шифросистем (як асиметричних, так і симетричних). Окрім того, вони дозволяють оцінювати ймовірність помилкового розшифрування повідомлень в NTRU-подібних шифросистемах при фіксованому ключі, надаючи, таким чином, більш адекватну інформацію про частоту виникнення помилок при розшифруванні.

3. Дістав подальший розвиток метод оцінювання стійкості симетричних шифросистем NTRUCipher та NTRUCipher+ за рахунок дослідження трьох додаткових атак на ці шифросистеми. Для зазначених атак отримано аналітичні оцінки складності та показано, що, принаймні, одна з них може бути реалізована в режимі реального часу (хоча й не дозволяє відновлювати ключі шифросистем, а тільки відрізняти послідовності їхніх шифрованих повідомлень від істино випадкової послідовності).

4. Вперше запропоновано метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем. Показано, що на відміну від відомих симетричних NTRU-подібних шифросистем, запропоновані шифросистеми мають обґрунтовану стійкість відносно атак на основі підібраних відкритих повідомлень, яка базується на складності еталонної обчислювально складної задачі Decision-Ring-LWE.

Обґрунтованість і достовірність результатів дисертаційної роботи забезпечується адекватністю припущень (гіпотез), які лежать в основі проведених наукових досліджень, а також коректним застосуванням відомих математичних методів. Результати проведених чисельних розрахунків узгоджуються з отриманими теоретичними висновками.

У ході дисертаційного дослідження було проаналізовано актуальну літературу, яка стосується тематики постквантових, а саме решіткових (NTRU-подібних) криптографічних систем. Системний огляд наукових джерел допоміг поглибити розуміння сучасних тенденцій і підходів у цій галузі. Були виявлені перспективні напрями досліджень, а також розкриті питання, які є необхідними для подальшого розвитку методів побудови, оцінювання та обґрунтування стійкості NTRU-подібних шифросистем.

Одним із ключових елементів дисертації є запропонований метод побудови симетричних NTRU-подібних шифросистем, що є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів. Зазначений метод

запропоновано вперше, а також наведено алгоритм вибору параметрів, які забезпечують стійкість запропонованих шифросистем на заздалегідь визначеному (необхідному) рівні.

Отже, в дисертаційній роботі поставлене наукове завдання виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності

За своїм змістом дисертаційна робота здобувача Матійко А.А. повністю відповідає напрямкам досліджень відповідно до освітньо-наукової програми «Безпека державних інформаційних ресурсів».

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям «Кібербезпека».

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Матійко Александри Андріївни є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів

Дисертаційна робота написана українською мовою.

Робота характеризується високим рівнем системності і логічною структурою викладення, що дозволяє з легкістю розуміти розвиток дослідження та логічні зв'язки між розділами. Представлення інформації чітке та зрозуміле, що сприяє засвоєнню основних понять та методів, які використовуються в дослідженні.

У дисертаційній роботі здобувач демонструє володіння загальноприйнятою термінологією у цій науковій галузі, вміло використовує терміни та поняття, що дозволяє роботі бути актуальною та зрозумілою для наукової спільноти. Також, варто зазначити стиль мовлення, який характеризується виразністю та чіткістю. Дисертаційна робота включає чітко сформульовані мету та завдання, а також змістовні розділи, які підкреслюють актуальність та наукову цінність дослідження.

Дисертація складається із вступу, 4 розділів, висновків, списку літератури та додатків. Загальний обсяг дисертації 178 сторінок.

У вступі обґрунтовується актуальність дослідження, зазначаються мета, задачі, методи дослідження. Також, висвітлюється наукова новизна та практичне значення отриманих результатів. Здобувач вказує на власний внесок у дослідження, надає інформацію про наукові публікації за темою дослідження та апробацію матеріалів дисертації.

У першому розділі викладено аналіз стану та напрямів розвитку методів побудови NTRU-подібних шифросистем. Висвітлено причини необхідності створення нових постквантових криптосистем, основні їх види та переваги решіткових (NTRU-подібних) криптосистем. Досліджено обчислювально складні задачі, на яких базується стійкість NTRU-подібних шифросистем, створена класифікація NTRU-подібних шифросистем для розуміння будови таких шифросистем. Окрім того, здійснено аналіз методів побудови, оцінювання та обґрунтування стійкості NTRU-подібних шифросистем.

У другому розділі дисертації висвітлено означення NTRU-подібних шифросистем, а також здобувачем отримано аналітичні співвідношення для параметрів шифросистем, які характеризують їх практичність, а саме ймовірність оборотності випадкових поліномів та ймовірність помилкового розшифрування повідомлень при фіксованому ключі.

Третій розділ присвячено дослідженню стійкості шифросистем NTRUCipher та NTRUCipher+ відносно двох статистичних атак: BKW-атаки та певної розрізнювальної атаки. Такі атаки раніше не досліджувалися, а отримані здобувачем аналітичні оцінки складності зазначених атак дозволяють порівняти шифросистеми за стійкістю та практичністю. Важливо відмітити, що шифросистема NTRUCipher+ виявилася вразливою відносно так званої розрізнювальної атаки, і може бути реалізована в режимі реального часу. Тому для побудови симетричного аналога криптосистеми NTRU слід використовувати інші методи побудови шифросистем, що базуються на решітках.

Четвертий розділ присвячено методу побудови симетричних NTRU-подібних шифросистем, що є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів. Цей метод запропоновано вперше, а також наведений алгоритм вибору параметрів запропонованих шифросистем, які забезпечують їхню стійкість на заздалегідь визначеному рівні.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи

Наукові результати дисертації висвітлені здобувачем у 9 наукових публікаціях, серед яких: 7 статей у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 2 статті у періодичних наукових виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus, з яких 2 статті у виданнях, віднесених до першого - третього квартилів (Q1-Q3) відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports.

Результати дисертації були апробовані на 6 наукових фахових конференціях. Також наукові та практичні результати дисертаційної роботи реалізовані в Службі

зовнішньої розвідки України – в результаті виконання НДР «Дорадо» (акт від 27.09.2022) та НДР «Сарган» (акт від 27.09.2022) та в науково-технічних розробках АТ «Інститут інформаційних технологій» (акт від 24.11.2022).

Усі публікації здобувача демонструють високий науковий рівень, і в них висвітлюються основні наукові результати досліджень. Дисертант зробила значний особистий внесок у публікації. Слід зазначити, що в усіх наукових публікаціях збережено принципи академічної доброчесності.

Наукові результати, описані в дисертаційній роботі, у повній мірі висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

1. У підрозділі 1.3 дисертації наведена класифікація NTRU-подібних шифросистем, але деякі з класів описані недостатньо повно, наприклад, NTRU-подібні шифросистеми, побудовані над кільцями цілих гаусових чисел чи цілочисельних кватерніонів тощо.

2. У підрозділі 2.1 дисертаційної роботи у рисунках 2.1, 2.2 відсутні назви координатних осей.

3. У тексті дисертації зустрічається велика кількість скорочень та абревіатур, проте далеко не всі вони є відображеними у відповідному переліку на стор. 15. Зазначене дещо ускладнює розуміння роботи і отриманих результатів при її читанні.

4. Для більш кращого розуміння нових і удосконалених наукових результатів було б добре, щоб здобувач їх відобразив не лише математичними виразами, а й певними структурно-аналітичними моделями чи послідовними етапами (зокрема, це стосується четвертого пункту наукової новизни).

5. Наукова новизна, на мою думку, сформульована не у повній мірі відповідно до вимог та рекомендованої практики (ступінь новизни, об'єкт наукової новизни, відмінність від існуючих підходів, досягнутий ефект), що дещо ускладнює розуміння сутності результатів та шляхів їх досягнення.

6. На мою думку, було б добре, щоб здобувач вкінці роботи навів порівняння з аналогічними підходами до вирішення поставленого завдання (дослідженими у першому розділі дисертації), що дало б змогу більш чітко виявити переваги отриманих автором результатів над відомими.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на загальну позитивну оцінку дисертаційної роботи.

Висновок про дисертаційну роботу

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Матійко Александри Андріївни на тему «Метод побудови обґрунтовано стійких

симетричних NTRU-подібних шифросистем» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує актуальне і важливе наукове завдання, що має істотне значення для галузі знань 12 Інформаційні технології. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в пп. 6-9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувач Матійко Александра Андріївна заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Офіційний опонент:

Декан факультету комп'ютерних наук та технологій
Національного авіаційного університету,
доктор технічних наук, професор Сергій ГНАТЮК

М.П.

«08» грудня 2023 року

Підпис гр. Гнатюка С.
засвідчую
Вчений секретар
Національного авіаційного університету
М. Ченевський