РЕЦЕНЗІЯ

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.

У зв'язку з великою кількістю досліджень технологій для побудови масштабованого квантового комп'ютера, а також із зростанням комплексності загроз на сучасні інформаційно-комунікаційні системи, стрімко почала розвиватись і постквантова криптографія – розділ криптографії, який займається розробкою криптографічних методів і протоколів, придатних для захисту інформації від атак з використанням можливостей квантових комп'ютерів. У 2016 році Національний інститут стандартів та технологій США (NIST) оголосив конкурс постквантових асиметричних криптопримітивів, які б реалізовували схему шифрування, механізм інкапсуляції ключів або схему цифрового підпису. Близько третини усіх криптосистем і протоколів, запропонованих міжнародними дослідницькими групами, побудовані на основі решіток (належать до NTRU-подібних). Зокрема, новітній стандарт асиметричного шифрування та інкапсуляції ключів ДСТУ 8961:2019 («Скеля») також є NTRU-подібним.

З іншого боку, сьогодні є актуальною задача створення симетричних шифросистем, стійкість яких, аналогічно асиметричним, базується на складності розв'язанні лише однієї обчислювальної задачі. Варто зауважити, що сучасні блокові чи потокові шифри не володіють такою властивістю. На сьогодні існує лише одна симетрична NTRU-подібна шифросистема – NTRUCipher, проте виникають певні питання щодо стійкості зазначеної шифросистеми відносно атак на основі підібраних відкритих текстів.

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 суто 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.

Наведені у роботі наукові основи, положення, висновки та практичні рекомендації повністю обґрунтовані, базуються на правильності застосування відомих математичних методів (методи теорії скінченних полів, теорії дискретного перетворення Фур'є на скінченних абелевих групах, лінійної алгебри, теорії ймовірностей, кореляційного криптоаналізу). Обґрунтованість і достовірність результатів дисертаційної роботи забезпечується адекватністю припущень, що лежать в основі проведених наукових досліджень та узгодженням теоретичних висновків з результатами проведених чисельних досліджень.

Наукові дослідження виконані здобувачкою в КПІ ім. Ігоря Сікорського в рамках НДР "Дорадо" (номер держреєстрації 0119U102099) та "Сарган" (номер держреєстрації 0120U101801) на замовлення Служби зовнішньої розвідки

України та відповідно до планів науково-дослідної роботи Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" під керівництвом професора Спеціальної кафедри № 1, д.т.н., доцента Олексійчука Антона Миколайовича.

Отже, в дисертаційній роботі поставлене наукове завдання, яке полягає в розробці методу побудови симетричних NTRU-подібних шифросистем, що є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів, виконано повністю, здобувачка повною мірою оволоділа методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувачки 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 здобувачки у наукові науково-технічні знання в сфері 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 здобувачки і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Найбільша кількість текстових співпадінь є посиланнями на статті Матійко Александри Андріївни, які були зазначені в анотації дисертації, а всі посилання оформлені належним чином, усі першоджерела, з яких взяті цитування присутні у списку використаних джерел.

Мова та стиль викладення результатів.

Дисертаційна робота написана українською мовою. Робота написана сучасною науковою мовою з використанням загальноприйнятої термінології. Стиль викладення матеріалів є послідовним та зрозумілим, стилістичний рівень роботи є високим. Структура роботи, подання теоретичних матеріалів та практичних результатів досліджень зроблено у логічній послідовності відповідно до поставленої мети і сформульованих задач досліджень.

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

У вступі обґрунтовано актуальність теми дисертаційного дослідження; сформульовано мету і задачу наукового дослідження; наведені об'єкт, предмет та методи дослідження; сформульована наукова новизна та практичне значення

отриманих результатів. Описано особистий внесок здобувачки та представлена інформація щодо апробації результатів дисертації та публікацій.

У першому розділі проведено огляд стану досліджень у створенні квантового комп'ютера та основних напрямів у розробці постквантових криптосистем та протоколів, які залишаться стійкими за умови існування потужних квантових комп'ютерів. Також у роботі аргументовано вибір напряму дослідження, а також описано основні обчислювально складні задачі, класифікацію та показники практичності NTRU-подібних шифросистем, проведений аналіз методів оцінювання та обґрунтування стійкості зазначених шифросистем.

Другий розділ присвячений дослідженню практичності NTRU-подібних шифросистем, а саме отриманню перших двох наукових результатів. Здобувачкою наведено аналітичні співвідношення для оцінювання ймовірності оборотності випадкових поліномів та ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах. Окрім того, дисертанткою розроблений ефективний алгоритм, який дозволяє в режимі реального часу обчислювати значення параметру Любашевського.

Третій розділ присвячений дослідженню стійкості NTRU-подібних шифросистем відносно статистичних атак, а саме отриманню третього наукового результату. У розділі наведено означення шифросистеми NTRUCipher та її природного узагальнення NTRUCipher+, отримано аналітичні оцінки складності BKW-атаки на зазначені шифросистеми та розрізнювальної атаки на шифросистему NTRUCipher+. За результатами чисельних розрахунків показано, що шифросистема NTRUCipher+ є цілком вразливою до розрізнювальної атаки, яка може бути реалізована в режимі реального часу. Звідси зроблено висновок, що для побудови симетричних NTRU-подібних шифросистем необхідно використовувати методи, відмінні від розглянутих.

У четвертому розділі представлений четвертий науковий результат, а саме метод побудови симетричних NTRU-подібних шифросистем, що є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів. Наведено 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 у 9 наукових публікаціях здобувачки, 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. Також результати дисертації були апробовані на 6 наукових фахових конференціях.

Усі публікації здобувачки мають високий науковий рівень. У жодній з публікацій не порушено принципи академічної доброчесності. Особистий внесок здобувачки до всіх наукових публікацій, опублікованих зі співавторами та зарахованих за темою дисертації, є вагомим та не викликає сумнівів.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувачки.

Недоліки та зауваження до дисертаційної роботи.

1. Висновки про співставність часу зашифрування та розшифрування повідомлень у запропонованих шифросистемах та алгоритмі NTRU Prime відповідно було б доцільно підтвердити результатами обчислювальних експериментів.

2. У четвертому розділі дисертації при викладенні алгоритму вибору параметрів запропонованих шифросистем не наводиться аргументів на користь застосування викладених методик оцінювання стійкості таких шифросистем відносно первинної та дуальної атак.

3. У дисертації трапляються орфографічні помилки, зокрема на сторінці 128 (NTRU-побідних замість NTRU-подібних), помилки перекладу (на ст. 9 не переведено на англійську мову прийменники "з" та "до"). Також на рисунках 2.1, 2.2 відсутні назви осей координат.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на 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 наукове завдання, що має істотне значення для галузі знань Інформаційні технології. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п.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.

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

Рецензент:
Заступник начальника інституту
(з наукової роботи)
Інституту спеціального зв'язку та
захисту інформації
Національного технічного
університету України
"Київський політехнічний
інститут ім. Ігоря Сікорського",
к.т.н., доцент / Сергій КОНЮШОК

М.П. «06» грудня 2023 року