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.

Останні роки має місце бурхливий розвиток квантових комп'ютерів та систем квантових обчислень, які використовують квантово-механічні явища для розв'язання обчислювальних задач, які є практично нерозв'язними у класичних обчислювальних моделях. Створення повноцінних квантових комп'ютерів наразі виглядає лише питанням часу, і це створює ризики конфіденційності та цілісності інформації у спеціальних інформаційно-комунікаційних системах. Окрема галузь криптології, а саме, постквантово стійка криптографія, займається питаннями побудови та аналізу криптографічних алгоритмів, стійких у квантовій моделі обчислень. Серед запропонованих алгоритмів, у тому числі таких, які подано як кандидати на майбутні стандарти США, значна частина побудована на основі криптосистеми NTRU та її модифікацій. NTRU-подібним є й стандартизований в Україні постквантовий алгоритм відкритого шифрування «Скеля» (ДСТУ 8961:2019). Таким чином, тема дисертації є актуальною.

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, які є справедливими для більш загального випадку, ніж відомі аналоги. Вони базуються на застосуванні апарату перетворення Фур'є розподілів ймовірностей на скінченному полі та надають змогу оцінювати і в окремих 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,

які є справедливими для усіх видів сучасних NTRU-подібних шифросистем. Вони дозволяють оцінювати ймовірність помилкового розшифрування повідомлень в NTRU-подібних шифросистемах при фіксованому ключі, надаючи 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 криптографічних 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.

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.

Наукові дослідження були виконані здобувачем на Спеціальній кафедрі №1 ІССЗІ КПІ ім. Ігоря Сікорського під керівництвом д.т.н., доцента Олексійчука Антона Миколайовича

Отже, в дисертаційній роботі поставлене наукове завдання, а саме: 1) провести аналіз відомих методів побудови та оцінювання й обґрунтування стійкості NTRU-подібних шифросистем; 2) отримати аналітичні співвідношення для ймовірності оборотності випадкових поліномів, які використовуються в NTRU-подібних шифросистемах; 3) отримати аналітичні співвідношення для оцінювання ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах при фіксованому ключі; 4) отримати аналітичні оцінки складності статистичних атак на симетричні шифросистеми NTRUCipher та NTRUCipher+; 5) розробити метод побудови симетричних NTRU-подібних шифросистем, які мають обґрунтовану стійкість відносно атак на основі підібраних відкритих текстів; – виконано повністю, здобувач повною мірою оволодів 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 здобувача у науковий напрям асиметричної криптографії, зокрема, у дослідження постквантово стійких криптоалгоритмів.

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.

Матеріал викладено чітко, у логічній послідовності. Авторка неухильно дотримується наукового стилю представлення матеріалу. Теоретичні результати мають строге доведення або належне обґрунтування і супроводжуються ілюстративними результатами експериментальних досліджень. У роботі використовується загальноприйнята у криптології термінологія та система позначень.

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

У вступі окреслено актуальність теми дослідження, сформульовано мету, завдання, об'єкт, предмет та методи дослідження, зазначено наукову новизну та практичне значення одержаних результатів, наведено відомості про апробацію результатів та публікації здобувачки, та її особистий вклад для публікацій у співавторстві.

У першому розділі наведено огляд стану розвитку постквантово стійких криптосистем, а також відомі результати побудови та аналізу системи NTRU та її модифікацій.

У другому розділі сформульовано та доведено аналітичні співвідношення для оцінювання ймовірності оборотності полінома у кільці зрізаних поліномів при деяких припущеннях про розподіл значень його коефіцієнтів. Також у розділі сформульовано та доведено аналітичні співвідношення для оцінювання ймовірності помилкового розшифрування повідомлень при фіксованому ключі у шифросистемі NTRUEncrypt та для довільних NTRU-подібних шифросистем.

У третьому розділі присвячено дослідженню стійкості шифросистем NTRUCipher та NTRUCipher+, відносно двох статистичних атак. Сформульовано та доведено аналітичні співвідношення для ймовірності безпомилкового розшифрування шифрованих повідомлень у шифросистемі NTRUCipher+, аналітичні оцінки складності BKW-атаки на шифросистеми NTRUCipher та NTRUCipher+, а також запропоновано швидку розрізнювальну атаку на шифросистему NTRUCipher+ і отримано аналітичні оцінки складності проведення запропонованої атаки.

У четвертому розділі запропоновано метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем на основі еталонної обчислювально складної задачі Decision-Ring-LWE. Викладено наукові основи запропонованого методу, наведено алгоритм вибору параметрів для побудови 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 здобувача, 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, віднесених до другого та третього квартилів (Q2 для публікації [8], Q3 для публікації [9]) відповідно до класифікації SCImago Journal and Country Rank.

Також результати дисертації були апробовані на 6 наукових фахових конференціях та у 2 науково-дослідних роботах.

Усі наукові публікації здобувачки мають високий рівень та виконані із дотримання принципів академічної доброчесності. Для публікацій, які виконані у співавторстві (здебільшого із науковим керівником) у тексті дисертації виокремлено особистий внесок здобувачки, який відповідає результатам, які виносяться на захист.

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

Недоліки та зауваження до дисертаційної роботи.

До зауважень до дисертаційної роботи можна віднести таке.

1. Для рівності (2.19) на стор. 80 зазначено, що вона є наближеною, однак в самій формулі використовується знак рівності. Так само наближеними називаються деякі одержані нерівності (наприклад, (2.15), стор. 78). Однак у тексті дисертаційної роботи недостатньо чітко сформульовано, що саме мається на увазі під наближеністю для зазначених співвідношень, що, разом із використанням символу «=» може привести до некоректної інтерпретації результатів, одержаних здобувачкою.

2. У таблиці 3.1 (стор. 105) зірочками позначено набори параметрів криптосистем NTRUCipher та NTRUCipher+, при яких імовірність помилкового розшифрування p_{er} дорівнює нулю, – і в цій же таблиці для цієї імовірності наводиться оцінка, яка є ненульовим (хоча й дуже маленьким) значенням. На

мою думку, якщо умови, наведені у формулах (3.3) та (3.8) не є прямими наслідками з тверджень, які наводяться у розділі 3.1 та формулюють оцінку для імовірності p_{er}, треба чіткіше артикулювати відмінність між ними, щоб запобігти некоректній інтерпретації результатів.

3. Оформлення дисертаційної роботи має окремі недоліки, зокрема, деякі таблиці розбиті між сторінками, а деякі заголовки розділів стоять наприкінці сторінки окремо від подальшого тексту.

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 здобувачки 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 12 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:
В.о. завідувача кафедри
математичних методів захисту інформації
НН ФТІ КПІ ім. Ігоря Сікорського,
к.т.н. Сергій ЯКОВЛЄВ

Підпис засвідчую:
Перший заступник директора НН ФТІ Тетяна ЛИТВИНОВА

«05» грудня 2023 року