ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації

Кандія Сергія Олеговича

«Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак»,

яка подається на здобуття наукового ступеня доктора філософії

з галузі знань 12 – Інформаційні технології

за спеціальністю 125 – Кібербезпека та захист інформації

1. Оцінка роботи здобувача у процесі підготовки дисертації і виконання індивідуального плану навчальної та наукової роботи.

Здобувач Кандій Сергій Олегович виконав у повному обсязі Індивідуальний план виконання освітньо-наукової програми підготовки доктора філософії. Освітня програма в обсязі 40 кредитів ECTS виконана у повному об'ємі. Він успішно склав наступні дисципліни:

- залік з навчальної дисципліни «Філософські засади та методологія наукових досліджень» (97 балів);
- іспит з навчальної дисципліни «Іноземна мова для аспірантів (англійська)» (87 балів);
- залік з навчальної дисципліни «Підготовка наукових публікацій та презентація результатів досліджень» (96 балів);
- залік з навчальної дисципліни «Реєстрація прав інтелектуальної власності» (90 балів);
- іспит з навчальної дисципліни «Математичні методи в кібербезпеці» (99 балів);
- іспит з навчальної дисципліни «Методи синтезу та аналізу захищених телекомунікацій» (95 бали);
- залік з навчальної дисципліни «Моделі і методи комп'ютерної стеганографії» (50 балів);

Всі заплановані види робіт були виконані своєчасно. Здобувач плідно співпрацював з науковим керівником протягом усього терміну навчання.

2. Обґрунтування вибору теми дослідження.

Сучасний світ важко уявити без інформаційно-телекомунікаційних мереж. Фактично, уся фінансова та економічна діяльність відбувається з використанням інформаційно-телекомунікаційних мереж. Проте, дані, що поширюються такими мережами, потребують надійного захисту. Зокрема, криптографічного захисту інформації. Сучасні криптографічні протоколи, такі як TLS, SSH та IPSec, використовують як симетричні криптографічні перетворення, так і асиметричні схеми шифрування.

Більшість сучасних асиметричних криптографічних перетворень, що використовуються для забезпечення безпеки інформації, базуються на таких складних математичних проблемах, як факторизація цілих чисел і дискретне логарифмування. Такі перетворення широко застосовуються в практичних системах захисту даних, включаючи стандарти шифрування, електронні підписи і механізми обміну ключами. Алгоритми RSA, DSA та системи на основі еліптичних кривих стали невід'ємною частиною сучасних інформаційно-телекомунікаційних технологій. Однак, ці алгоритми мають одну спільну вразливість: вони вразливі до атак, що здійснюються за допомогою квантових комп'ютерів.

Квантові комп'ютери, що наразі перебувають на стадії активної розробки, пропонують принципово новий підхід до обчислень, що суттєво відрізняється від класичних методів. Одним з найбільш революційних досягнень у цій сфері став квантовий алгоритм, запропонований американським математиком і дослідником Пітером Шором ще в 1994 році. Алгоритм Шора відкрив можливість вирішувати задачу факторизації цілих чисел за поліноміальний час на квантовому комп'ютері. У класичних обчисленнях ця задача є основою безпеки багатьох сучасних криптографічних систем, і її вирішення вимагає експоненційних ресурсів часу та пам'яті. Проте, квантові обчислення суттєво знижують цю складність, що означає потенційну загрозу для всіх систем, заснованих на факторизації.

Після оприлюднення алгоритму Шора інші дослідники також почали адаптувати його підходи для вирішення низки інших проблем, що раніше вважалися складними для класичних комп'ютерів. Зокрема, була розроблена адаптація алгоритму для розв'язання проблеми дискретного логарифмування, що також використовується в багатьох криптографічних системах. Проблема дискретного логарифмування у різних математичних структурах, включаючи мультиплікативні групи цілих чисел та групи точок еліптичних кривих, є основою безпеки таких популярних алгоритмів, як DSA (електронний підпис) та EC-DSA (електронний підпис на основі еліптичних кривих). Адаптація алгоритму Шора показала, що задача дискретного логарифмування також може бути розв'язана за поліноміальний час на квантовому комп'ютері. Це ставить під загрозу всі сучасні криптографічні системи, що базуються на дискретному логарифмуванні, оскільки їх безпека перестане відповідати необхідному рівню стійкості в умовах появи квантових обчислювальних машин.

Таким чином, виникає нагальна необхідність розробки нових криптографічних перетворень, стійких до квантових атак. Це спонукає дослідників усього світу шукати нові математичні основи для криптографічних систем, які могли б бути стійкими квантових обчислень і забезпечити надійний захист інформації у майбутньому квантовому світі.

Протягом тривалого часу квантові комп'ютери залишалися більше теоретичною концепцією, яка існувала лише у вигляді математичних моделей та абстракцій. Загроза для класичних криптографічних систем, пов'язана з потенційними можливостями квантових комп'ютерів, здавалася далекою і суто гіпотетичною. Проте, за останнє десятиріччя в галузі квантових обчислень було досягнуто вражаючого прогресу, який призвів до змін у сприйнятті цієї загрози. Квантові обчислювальні технології почали активно розвиватися, і сьогодні існують реальні прототипи квантових комп'ютерів, здатні виконувати обчислення на невеликій кількості кубітів.

Зокрема, кілька провідних технологічних компаній зробили значні інвестиції в дослідження та розробку квантових обчислень, серед яких особливо варто відзначити компанію IBM. Вона виділяється своєю комплексною та

системною стратегією розробки квантових чіпів. IBM є однією з компаній, яка не тільки активно займається теоретичними дослідженнями в цій галузі, але й робить значні кроки в напрямку створення практичних рішень для квантових обчислень. Вони поступово покращують свої квантові процесори, і кожен новий прототип відрізняється підвищеною кількістю кубітів, кращою стабільністю та продуктивністю.

Згідно з їх офіційними планами та звітами, зокрема зі звітом, оприлюдненим у 2023 році, компанія IBM має амбітну мету досягти значного прориву в розробці квантових процесорів. Їх стратегія спрямована на створення робочих квантових чіпів, що містять не менше 5000 кубітів, до 2030 року. Якщо ці плани втіляться в життя, квантові комп'ютери такого масштабу зможуть вирішувати задачі, які знаходяться далеко за межами можливостей сучасних класичних комп'ютерів. Це означає, що загроза для сучасних криптографічних систем стане не лише гіпотетичною, але й цілком реальною.

Така перспектива спричиняє велике занепокоєння в сфері інформаційної безпеки. Адже традиційні криптографічні алгоритми, що ґрунтуються на складності таких задач, як факторизація цілих чисел чи дискретне логарифмування, можуть бути легко зламані квантовими комп'ютерами, здатними працювати з великою кількістю кубітів. Саме тому криптографічні дослідження сьогодні фокусуються на пошуку нових методів захисту інформації, які зможуть забезпечити безпеку навіть у епоху квантових обчислень.

Зважаючи на такий стрімкий розвиток, NIST США провели відкритий конкурс для створення нових квантово-стійких стандартів електронного підпису та механізмів інкапсуляції ключів. За результатами цього конкурсу було обрано чотири кандидати на стандартизацію. При чому, три з них ґрунтуються на складних проблемах з теорії решіток.

У той же час, в Україні паралельно відбувалася розробка власних квантово-стійких стандартів інкапсуляції ключів та електронного підпису. За результатами досліджень були створені стандарти ДСТУ 8961:2019 та ДСТУ 9212:2023, які також ґрунтуються на проблемах з теорії решіток. Особливістю українських стандартів, у порівнянні з стандартами NIST, є наявність додаткових рівнів

безпеки для 384 та 512 біт безпеки. Використання таких нестандартних для світової практики рівнів безпеки вимагає більш детальних досліджень та обережності при виборі загальносистемних параметрів.

Розвиток криптографії на решітках призвів до кращого розуміння складності проблем в теорії решіток. Проте, багато моделей, що застосовується на практиці, досі використовують спрощені представлення про решітки, що призводить до деякого зміщення у оцінках безпеки. Тож, розробка моделей оцінки безпеки електронних підписів та механізмів інкапсуляції ключів на решітках є важливим та актуальним напрямком досліджень.

Мета і завдання дослідження. Метою дисертаційної роботи є аналіз та розробка методів та засобів для підвищення захищеності асиметричних криптографічних систем на решітках для постквантового періоду від існуючих та потенційних атак.

Основні завдання дисертаційного дослідження:

1. Вибір та обґрунтування моделей редукції решіток, які враховують існуючі відомості щодо поведінки базисів під час процесу редукції решіток та оцінка точності існуючих моделей редукції решіток.

2. Дослідження впливу моделей редукції решіток на складність атак на криптографічні перетворення на решітках та удосконалення методики оцінювання криптографічних перетворень на решітках.

3. Аналіз криптографічних перетворень на основі решіток у формальних моделях безпеки, які враховують потенціал класичних та квантових атак.

4. Дослідження впливу обчислень з плаваючою точкою на безпеку алгоритмів електронного підпису на решітках.

Об'єкт та предмет дослідження.

Об'єкт дослідження – процеси оцінки захищеності існуючих та перспективних асиметричних криптографічних перетворень від класичних та квантових атак.

Предмет дослідження – методи та моделі забезпечення захищеності асиметричних криптографічних систем на решітках від існуючих та потенційних квантових атак.

Методи дослідження.

Методи досліджень визначені сутністю розв'язуваних задач і включають методи комп'ютерного моделювання, теорії ймовірностей та математичної статистики. Експериментальні дослідження та чисельні розрахунки виконувалися на мовах програмування C++ та Python.

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

Дисертаційні дослідження проводились в рамках науково-дослідницьких робіт: № 28-20 «Механізми та засоби асиметричних криптоперетворень у постквантовий період» (Шифр «Квант-2021»), № 34-21 «Методи та алгоритми постквантових криптоперетворень, їх стандартизація та впровадження» (Шифр «Квант-2022»), № 09-22 «Методи та засоби генерування псевдовипадкових та випадкових послідовностей на основі класичних та квантових ефектів» (Шифр «Квант-2023»). № 10-23 «Методи та алгоритми постквантових перетворень типу електронний підпис, їх стандартизація та впровадження» (Шифр «Квант-2024»).

Результати дисертаційних досліджень були використані при підготовці та проведенні лабораторних робіт по дисципліні «Прикладна Криптологія» для спеціальності «Кібербезпека та захист інформації».

4. Особистий внесок дисертанта в отриманні наукових результатів та їх новизна.

Особистий внесок дисертанта в отриманні наукових результатів та їх новизна полягає у наступному:

1. Вперше виконано кількісне порівняння точності моделей редукції решіток із застосуванням метрики середньоквадратичної помилки для моделі GSA (Geometric Series Assumption) та симуляторів редукції решіток. Попередні дослідження фокусувалися на якісних або суто теоретичних оцінках якості роботи моделей. Отримані оцінки дозволяють кількісно оцінювати якість роботи симуляторів в залежності від параметрів решіток для оцінки захищеності від класичних та квантових атак.

2. Вперше було отримано узагальнений доказ IND-CCA безпеки перетворень, що використовуються в стандарті ДСТУ 8961:2019, у моделі

квантового випадкового оракула. Попередні дослідження не вивчали IND-CCA безпеку перетворень ДСТУ 8961:2019 у моделі квантового випадкового оракула.

3. Удосконалено методику оцінювання складності криптографічної задачі SIS (Shortest Integer Solution), що відрізняється від існуючих тим, що у даній методиці враховується алгебраїчна структура решіток під час аналізу процесів редукції для оцінки параметрів та характеристик на їх основі атак.

4. Отримали подальший розвиток обґрунтування оцінки атаки відновлення ключів, що використовує обчислення з плаваючою крапкою, для алгоритмів електронного підпису на основі решіток, що дало змогу підвищити безпеку електронних підписів на решітках.

5. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій, які захищаються.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертаційній роботі, забезпечується: адекватністю припущень, які лежать в основі проведених наукових досліджень, а також коректним застосуванням відомих математичних методів. Результати проведених чисельних розрахунків узгоджуються з отриманими теоретичними висновками.

Основні результати дисертаційного дослідження опубліковані в індексованих наукових журналах та доповідалися на міжнародних наукових конференціях. Висновки дисертаційної роботи є обґрунтованими.

6. Наукове, теоретичне та практичне значення результатів дисертації.

У наукових статтях, опублікованих у співавторстві, здобувачу належать наступні результати:

- Обґрунтування точності асимптотичних оцінок фактора Ерміта при аналізі редукції решіток з криптографічно значущими розмірностями.

- Порівняння якості роботи симуляторів редукції решіток на експериментальних даних.

- Уточнено оцінки атак вкладення та декодування для проблем NTRU та LWE.

- Удосконалено метод оцінки атак на проблему SIS.

- Отримано доказ безпеки ДСТУ 8961:2019 у моделі квантового випадкового оракула.

- Для атаки відновлення ключів на Falcon знайдена оптимальна кількість підписів.

- Удосконалено існуючі аналітичні оцінки безпеки для електронних підписів Falcon та Crystals-Dilithium та механізмів інкапсуляції ключів ДСТУ 8961:2019 та Crystals-Kyber.

- Уточнено оцінки безпеки криптографічних перетворень на решітках, які підтверджують рівні стійкості квантово-стійких стандартів електронного підпису (ДСТУ 9212:2023) та механізмів інкапсуляції ключів (ДСТУ 8961:2019), що обґрунтовує їх застосування як національних стандартів.

- Розроблено програмне забезпечення, яке дозволяє:

  - Оцінювати складність атак вкладення та декодування для проблем LWE та NTRU при процесі практичного оцінювання безпеки криптографічних перетворень на решітках (у тому числі для стандартів ДСТУ 8961:2019, ДСТУ 9212:2023).

  - Оцінювати складність проблеми SIS з врахуванням структури решіток (у тому числі для міжнародного проекту стандарту Crystlas-Kyber та федерального стандарту FIPS 203).

  - Проводити моделювання редукції решіток (у тому числі при дослідженні безпеки стандартів ДСТУ 8961:2019, ДСТУ 9212:2023).

Результати дисертаційних досліджень впровадженні у Приватному акціонерному товаристві «Інститут інформаційних технологій», м. Харків та були використані при обчисленні вхідних та вихідних тестових векторів стандартів ДСТУ 8961:2019, ДСТУ 9212:2023. Математичні моделі та аналітичні співвідношення знайшли практичне застосування в ХНУ імені В. Н. Каразіна на кафедрі БІСТ в дисциплінах першого рівня вищої освіти «Прикладна криптологія», другого рівня освіти «Криптографічні методи в кібербезпеці» та третього рівня освіти «Математичні методи в кібербезпеці» при проведенні лабораторних робіт.

7. Повнота викладення матеріалів дисертації в роботах, опублікованих автором.

Основні результати дисертаційних досліджень опубліковано у **10** наукових працях, серед яких: **7** статей у фахових виданнях України, **3** статті у зарубіжних виданнях (індексується у Scopus, Web of Science), **4** матеріали та тези доповідей на конференціях.

8. Дотримання академічної доброчесності.

На підставі вивчення тексту дисертації здобувача, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній інтернет-системі Strikeplagiarism.com) встановлено, що дисертаційна робота виконана самостійно, текст дисертації не містить плагіату, а дисертація відповідає вимогам академічної доброчесності.

9. Апробація матеріалів дисертації.

Результати проведених досліджень представлялись на міжнародних та вітчизняних наукових конференціях у формі доповідей, за результатами яких були опубліковані матеріали конференцій:

1. Кандій С.О. Острянська Є.В. Генерація загальносистемних параметрів для схеми електронного підпису Rainbow. І міжнародна науково-технічна коференція «Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку». 2021. С. 226-227.
2. Кандій С.О. Порівняння аргументів безпеки перспективних механізмів інкапсуляції ключів. Праці 8-ої Міжнародній конференції «Комп'ютерне моделювання в наукоємних технологіях» (КМНТ-2022). 2022. С. 97-100.
3. Горбенко Ю.І., Острянська Є.В., Кандій С.О. Експериментальна оцінка точності фактора ерміта. IV Міжнародна науково-технічна конференція «Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку». 2024. С. 48-49.
4. Потій О.В., Качко О.Г., Кандій С.О., Каптьол Є.Ю. Дослідження впливу плаваючої точки на безпеку алгоритму електронного підпису Falcon. II Міжнародна науково-практична конференція "Кіберборотьба: розвідка, захист та протидія". 2024. С. 28-30.

10. Оцінка структури, мови та стилю дисертації.

Матеріал дисертації викладено в логічній послідовності та доступно для сприйняття. Дисертація написана науковим стилем мовлення, структура дисертації відповідає алгоритму здійсненого автором дослідження. Зміст, структура, оформлення дисертації та кількість публікацій відповідають вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (постанова Кабінету Міністрів України від 12.01.2022 р. № 44), наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

11. Відповідність змісту дисертації спеціальності, за якою вона подається до захисту.

За своїм фаховим спрямуванням, науковою новизною і практичною значимістю дисертаційна робота Кандія С. О. «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак» повністю відповідає спеціальності 125 – Кібербезпека та захист інформації. Здобувачем повністю виконано освітню та наукову складову третього (освітньо-наукового) рівня вищої освіти.

12. Результати обговорення та проведення презентації. Рекомендація дисертації до захисту.

Здобувач представив основні результати своєї дисертаційної роботи на розширеному засіданні кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна щодо попередньої експертизи дисертації (Витяг з протоколу № 8 розширеного засідання кафедри кібербезпеки інформаційних систем, мереж і технологій від 10 березня 2025 р.) у формі презентації та наукової дискусії після її завершення. На даному засіданні були присутні 16 співробітників Харківського національного університету імені В. Н. Каразіна, із яких 4 докторів наук та 9 кандидатів наук. Дисертанту було задано 6 запитань, на які він надав вичерпні відповіді. Також

виступили 4 науковця, які позитивно відізвались про дисертаційне дослідження Кандія С. О.

У рамках цього розширеного засідання було ухвалено одноголосно (16 голосів) рекомендувати дисертаційну роботу здобувача Кандія Сергія Олеговича «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак» до захисту на здобуття наукового ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека та захист інформації.

Кандидат технічних наук, доцент,
в.о. завідувача кафедри кібербезпеки
інформаційних систем, мереж і технологій
Харківського національного
університету імені В. Н. Каразіна Марина ЄСІНА