Голові разової
спеціалізованої вченої ради
харківського національного
університету імені В. Н. Каразіна
професору Віталію ЄСІНУ
майдан Свободи 4, м. Харків, 61022

Рецензія

офіційного рецензента, доктора технічних наук, професора, професора кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп’ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна Олійникова Романа Васильовича на дисертаційну роботу Кандія Сергія Олеговича «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертації

Останні наукові досягнення в області квантових обчислень свідчать про потенційну можливість практичної реалізації алгоритмів криптоаналізу із використанням квантового комп’ютера, що робить криптографічні системи на основі факторизації та дискретного логарифмування потенційно небезпечними. У зв’язку з цим в Україні та в світі розпочався перехід до квантово-стійких криптографічних алгоритмів.

На міжнародному рівні існує відповідна тенденція до стандартизації криптографічних засобів, що забезпечує сумісність систем безпеки між різними країнами. Такі структури, як Міжнародна організація зі стандартизації (ISO) та Національний інститут стандартів і технологій США (NIST), ведуть активну роботу над розробкою сучасних стандартів, здатних протистояти актуальним загрозам, включаючи ризики, пов’язані з квантовими обчисленнями.

Водночас є активний розвиток криптографії на національному рівні. Зокрема, в Україні посилюються зусилля, спрямовані на розробку власних криптографічних стандартів і нормативних актів, що регулюють застосування засобів криптографічного захисту.

Аналіз квантово-стійких алгоритмів показує, що перспективні криптографічні схеми на решітках, такі як Kyber, Dilithium, Falcon, наразі домінують завдяки вдалому балансу безпеки і продуктивності, що робить актуальною задачу аналізу та розробки методів та моделей для аналізу стійкості і можливого підвищення захищеності асиметричних криптографічних систем на решітках.

Таким чином, тема дисертаційного дослідження, спрямованого на аналіз та розробку методів та моделей для підвищення захищеності асиметричних криптографічних систем на решітках, є своєчасною та важливою для вирішення актуальних науково-прикладних завдань у галузі інформаційної безпеки.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації

Аналіз анотацій, змісту дисертації та наукових публікацій Кандія С.О. свідчить про наукову обґрунтованість і достовірність отриманих результатів. Висновки, рекомендації та положення дисертаційної роботи логічно послідовні, аргументовані та спираються на чітко сформульовані теоретичні засади. Вони повністю узгоджуються з метою та завданнями дослідження, що зумовлено

коректним вибором методологічного підходу. Достовірність результатів підтверджується належною апробацією та публікацією основних положень у фахових наукових виданнях.

Найвагоміші наукові результати, що містяться в дисертації

Найвагоміші результати, які відзначаються науковою новизною, включають:

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.

- 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.

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.

Набули подальшого розвитку:

- 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.

Апробація дисертації та публікації

Основні результати дисертаційної роботи були апробовані та відповідним чином опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційної роботи було опубліковано 16 наукових праць, серед яких 7 статей у фахових виданнях України, 3 статті у зарубіжних виданнях (індексуються у Scopus, Web of Science), 4 матеріали та тези доповідей на конференціях.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пунктів 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44 (редакція від 08.05.2024).

Оцінка змісту дисертації, її завершеності в цілому і оформлення

Дисертаційна робота містить: вступ, 5 розділів, висновки, перелік посилань та додатки. Загальний обсяг дисертації складає 190 сторінки друкованого тексту, з яких: 137 сторінок основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 5 сторінках, 2 сторінки змісту, 3 сторінки переліку умовних позначень, список використаних джерел із 89 найменувань на 10 сторінках, додатки на 36 сторінках. Робота містить 24 таблиць та 37 рисунків.

У вступі обґрунтовується актуальність дослідження, поставлена мета та визначаються основні завдання, об’єкт та предмет дослідження. Також тут викладено наукову новизну, практичне значення отриманих результатів та особистий внесок здобувача. Наводяться відомості щодо апробації та опублікованих результатів досліджень.

У першому розділі дисертації показано, що розвиток квантових алгоритмів обумовлений двома техніками – квантовим пошуком та квантовою вибіркою Фур’є. Обґрунтовано, що криптографія на решітках є стійкою до застосування цих технік. Розкриті вимоги до квантово–стійкої криптографії. Розкрита сутність

доказової безпеки та моделей безпеки IND–CCA (Indistinguishability under Adaptive Chosen Chiphertext Attack) для механізмів інкапсуляції ключів та EUF–CMA (Existentially unforgeable under adaptive chosen message attacks) для електронних підписів. Наведено відомості з теорії решіток та теорії квантових обчислень.

У другому розділі дисертації обґрунтовано, що фактор Ерміта відіграє важливу роль при аналізі моделей редукції решіток. Проведено серію експериментів, що направлені на визначення точності існуючих асимптотичних оцінок фактору Ерміта на криптографічно значущих розмірностях решіток. Показано, що істинне значення фактору Ерміта швидко наближається до асимптотичних оцінок і на криптографічно значущих розмірностях можливо вважати помилку апроксимації фактору Ерміта незначною. Проведено порівняльний аналіз існуючих симуляторів редукції решіток. Для порівняння симуляторів проведено ряд експериментів на решітках малої розмірності. Показано, що симулятор Альбрехта–Лі дає найменшу середньоквадратичну помилку серед усіх симуляторів. Для NTRU решіток розкрито сутність розрідженої підрешітки.

У третьому розділі дисертації наведено класифікацію існуючих атак на криптографічні перетворення на решітках. Для атак вкладення та декодування запропонована удосконалена модель оцінки складності атаки, що базується на проведеному у другому розділі аналізі. Для атак декодування запропонований метод визначення оптимальних параметрів атаки. 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 атак на їх основі.

У четвертому розділі дисертації уточнено оцінки захищеності механізмів інкапсуляції ключів ДСТУ 8961:2019 та Crystals–Kyber. Показано, що врахування структури алгебраїчних решіток, згідно до методу, що був розроблений в розділі 3,

дає більші оцінки безпеки, ніж класична модель GSA. 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.

У п’ятому розділі дисертації (Оцінка захищеності електронних підписів на алгебраїчних решітках) уточнено оцінки захищеності електронних підписів Falcon та Crystals–Dilithium. Показано, що врахування структури алгебраїчних решіток, згідно до методу, що був розроблений в розділі 3, дає більші оцінки безпеки, ніж класична модель GSA. Для електронного підпису Falcon 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.

Список використаних у роботі джерел свідчить про те, що під час роботи були проаналізовані сучасні результати наукових досліджень. Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки криптографічних перетворень на решітках. Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

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».

Практичне значення отриманих результатів

1. 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.

2. 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 США FIPS 203)
- Проводити моделювання редукції решіток (у тому числі при дослідженні безпеки стандартів ДСТУ 8961:2019, ДСТУ 9212:2023)

3. 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.

Дотримання академічної доброчесності

При аналізі дисертаційної роботи, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній Інтернет-системі strikeplagiarism.com) встановлено, що текст дисертації не містить запозичень, дисертаційна робота виконана самостійно і відповідає вимогам академічної доброчесності.

Дискусійні положення та зауваження до змісту дисертації

1. Метрика середньоквадратичної помилки, що використовується для оцінки якості роботи моделей редукції решіток, оцінює лише “середній” сценарій. У криптографії критичні саме гірші випадки. У роботі не показано, чи не приховують усереднені цифри окремі, але небезпечні для безпеки аномалії профілю базису.

2. Формула (3.9) базується на припущенні нормального розподілу таємного вектора, тоді як у гібридній атаці використовуються інші розподіли. Автор сам зауважує цю невідповідність, але пропонує лише апроксимацію, не перевіряючи похибку такої заміни на безпеку.

3. Роботі бракує порівняльного тестування з альтернативними оцінками точності роботи симуляторів редукції решіток. Хоча автор наводить власні симуляції, відсутнє пряме зіставлення з незалежними цифрами, що обмежує зовнішню валідацію висновків.

Однак, висловлені зауваження не впливають суттєво на загальну високу оцінку дисертаційного дослідження, його цілісність та результативність. Наукова

новизна та практична значущість отриманих результатів залишаються вагомими та не применшуються зазначеними дискусійними моментами.

Загальні висновки

Дисертаційна робота Кандія Сергія Олеговича «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак» є самостійним, оригінальним і завершеним науковим дослідженням, присвяченим вирішенню важливого завдання сучасної криптографії. За актуальністю, змістом та повнотою викладу результатів дисертації у наукових публікаціях, обсягом і оформленням дисертаційне дослідження цілком відповідає 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 12.01.2017 р. № 44) та наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації». Виходячи з цього, вважаю, що Кандій Сергій Олегович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний рецензент
доктор технічних наук, професор,
професор кафедри кібербезпеки інформаційних систем, мереж і технологій
Навчально-наукового інституту
комп’ютерних наук та штучного інтелекту
Харківського національного
Університету імені В. Н. Каразіна Роман ОЛІЙНИКОВ

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 17:55:42 12.05.2025

Назва файлу з підписом: Рецензія_Олійников_Кандій.pdf.asice
Розмір файлу з підписом: 59.5 КБ

Перевірені файли:
Назва файлу без підпису: Рецензія_Олійников_Кандій.pdf
Розмір файлу без підпису: 57.4 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: Олійников Роман Васильович
П.І.Б.: Олійников Роман Васильович
Країна: Україна
РНОКПП: 2796617236
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 17:55:36 12.05.2025
Сертифікат виданий: "Дія". Кваліфікований надавач електронних довірчих послуг
Серійний номер: 382367105294AF9704000000F9AA0F0060BBD402
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2025.02.05 13:00

Голові разової спеціалізованої вченої
ради Харківського національного
університету імені В. Н. Каразіна
професору Віталію ЄСІНУ
майдан Свободи 4, м. Харків, 61022

ВІДГУК

офіційного опонента, доктора технічних наук, професора, професора кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка Толюпи Сергія Васильовича на дисертаційну роботу Кандія Сергія Олеговича «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертаційної роботи

Останні наукові здобутки в галузі квантових обчислень вказують на високу ймовірність практичного застосування квантових алгоритмів у найближчі десятиліття. Це створює загрозу для криптографічних систем, що базуються на задачах факторизації та дискретного логарифмування. У зв’язку з цим в Україні та в багатьох інших країнах світу розпочато перехід до криптографічних рішень, захищених від потенційних квантових атак.

На міжнародній арені спостерігається виразна тенденція до уніфікації криптографічних інструментів задля забезпечення сумісності систем інформаційного захисту між різними країнами. Такі організації, як Міжнародна організація зі стандартизації (ISO) та Національний інститут стандартів і технологій США (NIST), активно займаються розробкою сучасних криптографічних стандартів, здатних ефективно протистояти актуальним загрозам, зокрема викликаним стрімким розвитком квантових технологій.

Поряд із міжнародними зусиллями, криптографія активно розвивається і на національному рівні. В Україні, зокрема, посилюються заходи зі створення власних криптографічних стандартів та нормативно-правової бази, що регулює порядок застосування засобів криптографічного захисту інформації.

Дослідження квантостійких алгоритмів показує переважання решіткових схем, зокрема Kyber, Dilithium і Falcon, завдяки їх високій безпеці та продуктивності. Це підкреслює актуальність розробки ефективних методів і моделей для зміцнення захисту асиметричних криптосистем на основі решіток.

Таким чином, тема дисертаційного дослідження, що зосереджена на аналізі та розробці методів і моделей для підвищення захищеності асиметричних криптографічних систем, побудованих на решіткових конструкціях, є вкрай актуальною та науково значущою. Вона відповідає сучасним викликам інформаційної безпеки та спрямована на вирішення важливих прикладних завдань у цій галузі.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій

Проведений аналіз анотацій, змісту дисертації та наукових публікацій Кандія С.О. дозволяє констатувати, що результати виконаного дослідження є науково обґрунтованими й достовірними. Усі висновки, рекомендації та наукові положення належно аргументовані та базуються на чітких теоретичних засадах. Вони повністю відповідають заявленій меті та завданням дисертації, що стало можливим завдяки адекватному вибору методів дослідження. Достовірність отриманих результатів і висновків підтверджена достатнім рівнем їх апробації, а також опублікуванням матеріалів дисертації у виданнях високого наукового рівня.

Наукова новизна одержаних результатів, що містяться в дисертаційній роботі

Основними науковими результатами, одержаними в дисертації, є наступні:

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.

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.

Апробація дисертації та публікації

Основні результати дисертаційної роботи були апробовані та відповідним чином опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційної роботи було опубліковано 16 наукових праць, серед яких 7 статей у фахових виданнях України, 3 статті у зарубіжних виданнях (індексуються у Scopus, Web of Science), 4 матеріали та тези доповідей на конференціях.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пунктів 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44 (редакція від 08.05.2024).

Оцінка змісту дисертації, її завершеності в цілому і оформлення

Дисертаційна робота містить: вступ, 5 розділів, висновки, перелік посилань та додатки. Загальний обсяг дисертації складає 190 сторінки друкованого тексту, з яких: 137 сторінок основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 5 сторінках, 2 сторінки змісту, 3 сторінки переліку умовних позначень, список використаних джерел із 89 найменувань на 10 сторінках, додатки на 36 сторінках. Робота містить 24 таблиць та 37 рисунків.

У вступі обґрунтовується актуальність дослідження, поставлена мета та визначаються основні завдання, об’єкт та предмет дослідження. Також тут викладено наукову новизну, практичне значення отриманих результатів та особистий внесок здобувача. Наводяться відомості щодо апробації та опублікованих результатів досліджень.

У першому розділі дисертації показано, що розвиток квантових алгоритмів обумовлений двома техніками – квантовим пошуком та квантовою вибіркою Фур’є. Обґрунтовано, що криптографія на решітках є стійкою до застосування цих технік. Розкриті вимоги до квантово–стійкої криптографії. Розкрита сутність доказової безпеки та моделей безпеки IND–CCA (Indistinguishability under Adaptive Chosen Chiphertext Attack) для механізмів інкапсуляції ключів та EUF–CMA (Existentially

unforgeable under adaptive chosen message attacks) для електронних підписів. Наведено відомості з теорії решіток та теорії квантових обчислень.

У другому розділі дисертації обґрунтовано, що фактор Ерміта відіграє важливу роль при аналізі моделей редукції решіток. Проведено серію експериментів, що направлені на визначення точності існуючих асимптотичних оцінок фактору Ерміта на криптографічно значущих розмірностях решіток. Показано, що істинне значення фактору Ерміта швидко наближається до асимптотичних оцінок і на криптографічно значущих розмірностях можливо вважати помилку апроксимації фактору Ерміта незначною. Проведено порівняльний аналіз існуючих симуляторів редукції решіток. Для порівняння симуляторів проведено ряд експериментів на решітках малої розмірності. Показано, що симулятор Альбрехта–Лі дає найменшу середньоквадратичну помилку серед усіх симуляторів. Для NTRU решіток розкрито сутність розрідженої підрешітки.

У третьому розділі дисертації наведено класифікацію існуючих атак на криптографічні перетворення на решітках. Для атак вкладення та декодування запропонована удосконалена модель оцінки складності атаки, що базується на проведеному у другому розділі аналізі. Для атак декодування запропонований метод визначення оптимальних параметрів атаки. 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 атак на їх основі.

У четвертому розділі дисертації уточнено оцінки захищеності механізмів інкапсуляції ключів ДСТУ 8961:2019 та Crystals–Kyber. Показано, що врахування структури алгебраїчних решіток, згідно до методу, що був розроблений в розділі 3, дає більші оцінки безпеки, ніж класична модель GSA. 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.

У п’ятому розділі дисертації (Оцінка захищеності електронних підписів на алгебраїчних решітках) уточнено оцінки захищеності електронних підписів Falcon та Crystals–Dilithium. Показано, що врахування структури алгебраїчних решіток, згідно до методу, що був розроблений в розділі 3, дає більші оцінки безпеки, ніж класична модель GSA. Для електронного підпису Falcon 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.

Список використаних у роботі джерел свідчить про те, що під час роботи були проаналізовані сучасні результати наукових досліджень.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки криптографічних перетворень на решітках.

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Оформлення дисертації

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Дотримання академічної доброчесності

При аналізі дисертаційної роботи, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній Інтернет-системі strikeplagiarism.com) встановлено, що текст дисертації не містить запозичень, дисертаційна робота виконана самостійно і відповідає вимогам академічної доброчесності.

Недоліки та зауваження до змісту дисертаційної роботи

1. У роботі наведено ґрунтовний теоретичний аналіз криптографічних схем, проте не показано, як отримані наукові результати трансформуються у практичні рекомендації чи безпосереднє вдосконалення реальних протоколів і стандартів.

2. Оцінка складності атак вкладення значною мірою спирається на евристику (критерій (3.2) та ймовірність відновлення (3.3)). Хоча ці евристики добре зарекомендували себе на практиці, відсутність строгих доведень є слабким місцем. Варто було б зазначити цю обмеженість.

3. Відсутні приклади інтеграції запропонованих моделей у прикладні системи та оцінка їх впливу на продуктивність і безпеку в реальних умовах.

4. Запропонована апроксимація ненормальних розподілів нормальним за допомогою мінімізації відстані Колмогорова-Смірнова є цікавим підходом, але його обґрунтування є дещо стислим. Варто було б більш детально пояснити, чому саме цей метод є прийнятним і які можуть бути його обмеження.

5. Результати моделювання атак вкладення та декодування представлені лише для обмеженого набору параметрів (розмірності n та дисперсії σ). Для більшої

переконливості варто було б навести результати для ширшого діапазону параметрів та, можливо, для різних значень модуля q.

Однак, висловлені зауваження не впливають суттєво на загальну високу оцінку дисертаційного дослідження, його цілісність та результативність. Наукова новизна та практична значущість отриманих результатів залишаються вагомими та не применшуються зазначеними дискусійними моментами.

Висновок про дисертаційне дослідження

Дисертаційна робота Кандія Сергія Олеговича «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак» є завершеною, цілісною науковою кваліфікаційною роботою, яка має наукову новизну, теоретичне і практичне значення, відповідає чинним вимогам, зокрема, відповідає 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 12.01.2017 р. № 44) та наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Виходячи з цього, вважаю, що Кандій Сергій Олегович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

ОФІЦІЙНИЙ ОПОНЕНТ
доктор технічних наук, професор, професор
кафедри кібербезпеки та захисту інформації
Київського національного університету
Імені Тараса Шевченка Сергій ТОЛЮПА

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 16:51:48 13.05.2025

Назва файлу з підписом: Відгук Кандій.pdf.asice
Розмір файлу з підписом: 309.5 КБ

Перевірені файли:
Назва файлу без підпису: Відгук Кандій.pdf
Розмір файлу без підпису: 315.2 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: ТОЛЮПА СЕРГІЙ ВАСИЛЬОВИЧ
П.І.Б.: ТОЛЮПА СЕРГІЙ ВАСИЛЬОВИЧ
Країна: Україна
РНОКПП: 2231818791
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 16:51:51 13.05.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F04000000FEFFC100BF690006
Алгоритм підпису: ДСТУ 4145
Тип підпису: Удосконалений
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними для перевірки (XAdES-B-LT)
Сертифікат: Кваліфікований

Версія від: 2025.02.05 13:00

Голові разової
спеціалізованої вченої ради
харківського національного
університету імені В. Н. Каразіна
професору Віталію ЄСІНУ
майдан Свободи 4, м. Харків, 61022

Відгук

офіційного опонента, доктора технічних наук, професора, начальника кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імені Героїв Крут Чевардіна Владислава Євгенійовича на дисертаційну роботу Кандія Сергія Олеговича "Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак", подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертаційної роботи

Новітні досягнення у сфері квантових обчислень свідчать про реальну перспективу впровадження квантових алгоритмів у практику вже в найближчі десятиліття. Це становить серйозну загрозу для криптографічних систем, заснованих на складності задач факторизації та дискретного логарифмування. У зв'язку з цим в Україні, як і в багатьох інших країнах світу, розпочато перехід до криптографічних технологій, стійких до можливих квантових атак.

На міжнародному рівні чітко простежується тенденція до уніфікації криптографічних засобів з метою забезпечення взаємної сумісності систем захисту інформації між різними державами. Провідні організації, такі як Міжнародна організація зі стандартизації (ISO) та Національний інститут стандартів і

технологій США (NIST), активно працюють над створенням сучасних криптографічних стандартів стійких до сучасних загроз пов'язаних з швидким розвитком квантових технологій.

Паралельно з міжнародними ініціативами, криптографія динамічно розвивається й на національному рівні. В Україні, зокрема, активізуються заходи щодо формування власних криптографічних стандартів, а також удосконалення нормативно-правової бази, яка регламентує використання засобів криптографічного захисту інформації.

Дослідження у сфері квантостійких алгоритмів показують перевагу решіткових схем, таких як Kyber, Dilithium і Falcon, що дає підстави для розробки дієвих методів і моделей посилення захисту асиметричних криптосистем з використанням структур на решітках.

Отже, тема дисертаційного дослідження, присвячена аналізу та розробці методів і моделей підвищення захищеності асиметричних криптографічних систем на основі решіткових конструкцій, є актуальною та спрямована на розв’язання важливих прикладних задач у галузі криптографічного захисту інформації.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій

Проведений аналіз анотацій, змісту дисертації та наукових публікацій Кандія С.О. дозволяє констатувати, що результати виконаного дослідження є науково обґрунтованими й достовірними. Усі висновки, рекомендації та наукові положення належно аргументовані та базуються на чітких теоретичних засадах. Вони повністю відповідають заявленій меті та завданням дисертації, що стало можливим завдяки адекватному вибору методів дослідження. Достовірність отриманих результатів і висновків підтверджена співпадінням теоретичних та практичних результатів дослідження, достатнім рівнем їх апробації в міжнародних та фахових виданнях.

Наукова новизна одержаних результатів, що містяться в дисертаційній роботі

Основними науковими результатами, одержаними в дисертації, є наступні:

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.

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.

Апробація дисертації та публікації

Основні результати дисертаційної роботи були апробовані та відповідним чином опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційної роботи було опубліковано 16 наукових праць, серед яких 7 статей у фахових виданнях України, 3 статті у зарубіжних виданнях (індексуються у Scopus, Web of Science), 4 матеріали та тези доповідей на конференціях.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пунктів 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44 (редакція від 08.05.2024).

Оцінка змісту дисертаційної роботи, її завершеності в цілому

Дисертаційна робота містить: вступ, 5 розділів, висновки, перелік посилань та додатки. Загальний обсяг дисертації складає 190 сторінки друкованого тексту, з яких: 137 сторінок основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 5 сторінках, 2 сторінки змісту, 3 сторінки переліку умовних позначень, список використаних джерел із 89 найменувань на 10 сторінках, додатки на 36 сторінках. Робота містить 24 таблиць та 37 рисунків.

У вступі обґрунтовується актуальність дослідження, поставлена мета та визначаються основні завдання, об’єкт та предмет дослідження. Також тут викладено наукову новизну, практичне значення отриманих результатів та особистий внесок здобувача. Наводяться відомості щодо апробації та опублікованих результатів досліджень.

У першому розділі дисертації показано, що розвиток квантових алгоритмів обумовлений двома техніками – квантовим пошуком та квантовою вибіркою Фур’є. Обґрунтовано, що криптографія на решітках є стійкою до застосування цих технік. Розкриті вимоги до квантово–стійкої криптографії. Розкрита сутність доказової безпеки та моделей безпеки IND–CCA (Indistinguishability under Adaptive Chosen Chiphertext Attack) для механізмів інкапсуляції ключів та EUF–CMA (Existentially unforgeable under adaptive chosen message attacks) для електронних підписів. Наведено відомості з теорії решіток та теорії квантових обчислень.

У другому розділі дисертації обґрунтовано, що фактор Ерміта відіграє важливу роль при аналізі моделей редукції решіток. Проведено серію експериментів, що направлені на визначення точності існуючих асимптотичних

оцінок фактору Ерміта на криптографічно значущих розмірностях решіток. Показано, що істинне значення фактору Ерміта швидко наближається до асимптотичних оцінок і на криптографічно значущих розмірностях можливо вважати помилку апроксимації фактору Ерміта незначною. Проведено порівняльний аналіз існуючих симуляторів редукції решіток. Для порівняння симуляторів проведено ряд експериментів на решітках малої розмірності. Показано, що симулятор Альбрехта–Лі дає найменшу середньоквадратичну помилку серед усіх симуляторів. Для NTRU решіток розкрито сутність розрідженої підрешітки.

У третьому розділі дисертації наведено класифікацію існуючих атак на криптографічні перетворення на решітках. Для атак вкладення та декодування запропонована удосконалена модель оцінки складності атаки, що базується на проведеному у другому розділі аналізі. Для атак декодування запропонований метод визначення оптимальних параметрів атаки. 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 атак на їх основі.

У четвертому розділі дисертації уточнено оцінки захищеності механізмів інкапсуляції ключів ДСТУ 8961:2019 та Crystals–Kyber. Показано, що врахування структури алгебраїчних решіток, згідно до методу, що був розроблений в розділі 3, дає більші оцінки безпеки, ніж класична модель GSA. 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.

У п’ятому розділі дисертації (Оцінка захищеності електронних підписів на алгебраїчних решітках) уточнено оцінки захищеності електронних підписів Falcon та Crystals–Dilithium. Показано, що врахування структури алгебраїчних решіток,

згідно до методу, що був розроблений в розділі 3, дає більші оцінки безпеки, ніж класична модель GSA. Для електронного підпису Falcon 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.

Список використаних у роботі джерел свідчить про те, що під час роботи були проаналізовані сучасні результати наукових досліджень.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки криптографічних перетворень на решітках.

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Оформлення дисертації

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Дотримання академічної доброчесності

При аналізі дисертаційної роботи, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній Інтернет-системі strikeplagiarism.com) встановлено, що текст дисертації не містить запозичень, дисертаційна робота виконана самостійно і відповідає вимогам академічної доброчесності.

Недоліки та зауваження до змісту дисертаційної роботи

1. У роботі дуальні атаки згадані лише побіжно. Відсутній їхній детальний математичний аналіз, кількісні оцінки складності та порівняння з атаками вкладення чи декодування; не розглянуто також вибір параметрів, що мінімізують ризик саме дуальних методів. Через це лишається неясним, наскільки

запропоновані рекомендації забезпечують стійкість проти найсучасніших дуальних підходів до криптоаналізу схем на решітках.

2. Оцінки стійкості подані розрізнено: параметри та результати для DSTU 8961/CRYSTALS-Kyber наведені в розділі 4, тоді як для Falcon і CRYSTALS-Dilithium — у розділі 5. Проте зведеної порівняльної таблиці, яка б концентровано демонструвала всі отримані оцінки (рівні безпеки, час атак, параметри редукції тощо) для всіх розглянутих схем, у роботі немає; це ускладнює швидке співставлення результатів і формування практичних рекомендацій.

3. У таблиці 1.1 наведено оцінки часу роботи алгоритмів просіювання на класичному комп'ютері, однак не вказано, яка з них є теоретичною оцінкою, а яка - експериментальною (практичною), отриманою на основі емпіричних досліджень. Відсутність такого розмежування ускладнює аналіз точності оцінок і їх прикладну інтерпретацію, особливо з урахуванням того, що значення констант та доданків виду o(β) можуть суттєво впливати на реальну складність атаки.

4. У джерелі [47], на яке посилається автор, важливу роль відіграє метод Карацуби, який використовується як один з основних способів оптимізації реалізації криптосистеми NTRU Prime. Однак у дисертації не розглянуто це питання, не надано аналізу або згадки про вибір методу множення поліномів. Урахування цих аспектів могло б підсилити практичну цінність роботи, а також дати ширше уявлення про ефективність реалізації.

Однак, висловлені зауваження не впливають суттєво на загальну позитивну оцінку дисертаційного дослідження, його цілісність та результативність. Наукова новизна та практична значущість отриманих результатів залишаються вагомими та не применшуються зазначеними дискусійними моментами.

Висновок про дисертаційне дослідження

Дисертаційна робота Кандія Сергія Олеговича «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак» є завершеним науковим дослідженням, що має

наукову новизну і практичну значущість. Дана дисертаційна робота за актуальністю, змістом та повнотою викладу її результатів у наукових публікаціях, обсягом і оформленням цілком відповідає 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 12.01.2017 р. № 44) та наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Виходячи з цього, вважаю, що Кандій Сергій Олегович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Протокол засідання кафедри кібербезпеки від 10.05.2025 №17.

Офіційний опонент
доктор технічних наук, професор,
начальник кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імен Героїв Крут

Владислав ЧЕВАРДІН

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 10:24:32 14.05.2025

Назва файлу з підписом: Відгук Кандій ХНУ Каразіна.pdf.asice
Розмір файлу з підписом: 144.9 КБ

Перевірені файли:
Назва файлу без підпису: Відгук Кандій ХНУ Каразіна.pdf
Розмір файлу без підпису: 150.4 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: ЧЕВАРДІН ВЛАДИСЛАВ ЄВГЕНІЙОВИЧ
П.І.Б.: ЧЕВАРДІН ВЛАДИСЛАВ ЄВГЕНІЙОВИЧ
Країна: Україна
РНОКПП: 2883718934
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 10:24:28 14.05.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F04000000AD86CA015D684E06
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Серійний номер носія особистого ключа: 021
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2025.02.05 13:00

Голові разової
спеціалізованої вченої ради
харківського національного
університету імені В. Н. Каразіна
професору Віталію ЄСІНУ
майдан Свободи 4, м. Харків, 61022

Відгук

офіційного опонента, доктора технічних наук, професора, першого проректора державного університету інформаційно-комунікаційних технологій Корченко Олександра Григоровича на дисертаційну роботу Кандія Сергія Олеговича «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертаційної роботи

Новітні наукові досягнення у сфері квантових обчислень свідчать про ймовірність впровадження квантових алгоритмів у найближчі десятиліття. Це ставить під загрозу безпеку криптографічних систем, заснованих на факторизації та дискретному логарифмуванні. У зв’язку з цим як в Україні, так і в інших країнах світу розпочато перехід до криптографічних алгоритмів, стійких до квантових атак.

На міжнародному рівні спостерігається активна тенденція до уніфікації криптографічних засобів з метою забезпечення взаємної сумісності систем захисту між країнами. Організації на кшталт Міжнародної організації зі стандартизації (ISO) та Національного інституту стандартів і технологій США (NIST) активно працюють над створенням сучасних стандартів, здатних ефективно протидіяти сучасним загрозам, зокрема тим, що пов’язані з розвитком квантових технологій.

Паралельно відбувається активний розвиток криптографії і на національному рівні. В Україні, зокрема, посилюються ініціативи щодо створення власних криптографічних стандартів та нормативно-правових документів, які визначають порядок використання засобів криптографічного захисту.

Дослідження квантово-стійких алгоритмів свідчить про домінування решіткових схем, таких як Kyber, Dilithium і Falcon, завдяки їх оптимальному поєднанню високого рівня безпеки та продуктивності. У зв'язку з цим актуалізується необхідність аналізу та розробки ефективних методів і моделей для підвищення захищеності асиметричних криптографічних систем, побудованих на основі решіток.

Отже, тема дисертаційного дослідження, присвяченого аналізу та розробці методів і моделей для зміцнення захисту асиметричних криптографічних систем на основі решіток, є актуальною та значущою. Вона відповідає сучасним викликам і спрямована на розв'язання важливих науково-прикладних задач у сфері інформаційної безпеки.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій

Аналіз анотацій, змісту дисертації та наукових публікацій Кандія С.О. свідчить про наукову обґрунтованість і достовірність отриманих результатів. Сформульовані у роботі висновки, рекомендації та наукові положення є логічно аргументованими, спираються на чітко визначені теоретичні основи та повністю узгоджуються з поставленою метою і завданнями дослідження. Це стало можливим завдяки виваженому й коректному вибору методологічного інструментарію. Достовірність результатів підтверджується належною апробацією положень дисертації, а також публікацією основних матеріалів у наукових виданнях, що відповідають вимогам фахового рівня.

Наукова новизна одержаних результатів, що містяться в дисертаційній роботі

Основними науковими результатами, одержаними в дисертації, є наступні:

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.

Апробація дисертації та публікації

Основні результати дисертаційної роботи були апробовані та відповідним чином опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційної роботи було опубліковано 16 наукових праць, серед яких 7 статей у фахових виданнях України, 3 статті у зарубіжних виданнях (індексуються у Scopus, Web of Science), 4 матеріали та тези доповідей на конференціях.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пунктів 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44 (редакція від 08.05.2024).

Оцінка змісту дисертації, її завершеності в цілому і оформлення

Дисертаційна робота містить: вступ, 5 розділів, висновки, перелік посилань та додатки. Загальний обсяг дисертації складає 190 сторінки друкованого тексту, з яких: 137 сторінок основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 5 сторінках, 2 сторінки змісту, 3 сторінки переліку умовних позначень, список використаних джерел із 89 найменувань на 10 сторінках, додатки на 36 сторінках. Робота містить 24 таблиць та 37 рисунків.

У вступі обґрунтовано актуальність теми, сформульовано мету, визначено завдання, об’єкт і предмет дослідження. Наведено наукову новизну, практичне значення одержаних результатів, особистий внесок здобувача, а також відомості про апробацію та публікації.

Перший розділ присвячено теоретичним засадам квантово-стійкої криптографії. Розглянуто моделі доказової безпеки IND–CCA та EUF–CMA, а також подано базові положення теорії решіток і квантових обчислень.

У другому розділі проаналізовано значення фактора Ерміта у контексті редукції решіток. Проведено експериментальні дослідження точності асимптотичних оцінок фактора Ерміта, а також порівняльний аналіз симуляторів редукції. Встановлено переваги симулятора Альбрехта–Лі за точністю моделювання. Розкрито структуру розріджених підрешіток у NTRU-решітках.

Третій розділ присвячено класифікації атак на криптографію на решітках. Запропоновано вдосконалені моделі оцінки складності атак вкладення та декодування з урахуванням алгебраїчної структури решіток. Удосконалено підхід до оцінки задачі SIS, що враховує процеси редукції у структурованих решітках.

У четвертому розділі уточнено оцінки стійкості механізмів інкапсуляції ключів (зокрема ДСТУ 8961:2019 і Crystals–Kyber). Показано, що застосування структурного аналізу дає вищі оцінки безпеки порівняно з класичною моделлю GSA. Вперше обґрунтовано IND–CCA безпеку перетворень ДСТУ 8961:2019 у моделі квантового випадкового оракула.

У п’ятому розділі уточнено оцінки захищеності електронних підписів Falcon і Crystals–Dilithium. Розроблена методика, що враховує алгебраїчну структуру решіток, дозволила підвищити оцінки стійкості. Удосконалено обґрунтування складності атаки відновлення ключа у схемі Falcon, зокрема при використанні обчислень з плаваючою крапкою.

Список використаних у роботі джерел свідчить про те, що під час роботи були проаналізовані сучасні результати наукових досліджень.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки криптографічних перетворень на решітках.

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Оформлення дисертації

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Дотримання академічної доброчесності

За результатами аналізу дисертаційної роботи, наукових публікацій здобувача, а також Протоколу перевірки оригінальності (проведеної із використанням антиплагіатної Інтернет-системи strikeplagiarism.com) встановлено, що дисертація

не містить текстових запозичень, є результатом самостійного наукового дослідження та відповідає встановленим вимогам академічної доброчесності.

Дискусійні положення та зауваження до змісту дисертації

1. Оцінка атак на Falcon, що використовують похибки з плаваючою точкою, не зіставлена з контр-заходами. В роботі докладно змодельовано атаку, та не подано цифр, які показали б, наскільки відомі методи захисту зменшують успішність зламу.

2. Експериментальна перевірка точності моделей редукції ґрунтується на решітках розмірності до 256, тоді як сучасні стандарти (Kyber, Dilithium, Falcon) працюють з більшими розмірностями; екстраполяція результатів на великі розмірності потребує окремого обґрунтування.

3. Оцінювання впливу квантових комп'ютерів для прискорення класичних атак в роботі зводиться до застосування консервативних моделей безпеки. Сучасні моделі, що враховують квантові гейти та особливості їх реалізації для квантових атак, в роботі не розглядаються, що зменшує практичну цінність отриманих оцінок.

4. В роботі проаналізована атака на реалізацію Falcon, проте для інших криптографічних перетворень така атака не розглядається.

Вказані побажання не впливають на загальну позитивну оцінку рецензованої дисертації, не знижують наукову цінність проведених дисертантом досліджень і отриманих результатів, достовірністю та науковою новизною яких повністю погоджуюсь.

Загальні висновки

Аналіз дисертаційної роботи Кандія Сергія Олеговича дозволяє зробити висновок, що за своїм змістом, теоретичним рівнем і практичною значущістю дисертація є завершеним науковим дослідженням. Дисертація здобувача на тему «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак» виконана на високому

науковому рівні, дотримується принципів академічної доброчесності та містить наукову новизну і практичну значущість. Дана дисертаційна робота за актуальністю, змістом та повнотою викладу її результатів у наукових публікаціях, обсягом і оформленням цілком відповідає 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 12.01.2017 р. № 44) та наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації». Зважуючи на викладене, вважаю, що Кандій Сергій Олегович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний опонент
Перший проректор Державного університету
інформаційно-комунікаційних технологій,
член-кореспондент НАН України,
лауреат Державної премії України
в галузі науки і техніки,
Заслужений діяч
науки і техніки України,
доктор технічних наук, професор Олександр КОРЧЕНКО

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 14:26:42 14.05.2025

Назва файлу з підписом: Кандій PDF.pdf.asice
Розмір файлу з підписом: 248.5 КБ

Перевірені файли:
Назва файлу без підпису: Кандій PDF.pdf
Розмір файлу без підпису: 274.3 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: КОРЧЕНКО ОЛЕКСАНДР ГРИГОРОВИЧ
П.І.Б.: КОРЧЕНКО ОЛЕКСАНДР ГРИГОРОВИЧ
Країна: Україна
РНОКПП: 2242506733
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 14:26:39 14.05.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F040000001C75FA002DAF1806
Алгоритм підпису: ДСТУ 4145
Тип підпису: Удосконалений
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними для перевірки (XAdES-B-LT)
Сертифікат: Кваліфікований

Версія від: 2025.02.05 13:00