ВІДГУК

офіційного опонента
Котуха Євгена Володимировича
на дисертаційну роботу Бондаренка Микити Олеговича
«Моделі та методи інформаційної технології створення
криптосистем на основі функцій дійсних змінних»,
представлену на здобуття наукового ступеня доктора філософії
в галузі знань 12 Інформаційні технології
за спеціальністю 122 – Комп'ютерні науки

Актуальність теми. У дисертаційній роботі розв'язано науково-практичне завдання розробки моделей та методів криптографічних систем на основі функцій дійсної змінної. Тема дослідження обумовлена розвитком технологій квантових обчислень та зростанням ролі методів штучного інтелекту. Тандем цих технологій дозволяють значно прискорити розв'язання задач прямого перебору (brute-force) в практичних реалізаціях алгоритмів, в тому числі алгоритмів криптографічним примітивів. Це зумовлює появу нових напрямів, що визначатимуть розвиток криптоаналізу та зумовлюють актуальність роботи Бондаренко М.О.

Тема відповідає пріоритетним напрямкам наукових досліджень Сумського державного університету. Дослідження виконано відповідно до плану науково-дослідних робіт за держбюджетною темою «Методи, математичні моделі та інформаційні технології аналізу і синтезу інфокомунікаційних систем» (ДР № 0118U006971, 2018-2023). Бондаренко М.О. розробив моделі та методи шифрування і дешифрування даних на основі функцій дійсної змінної для застосування в інформаційно-телекомунікаційних системах.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій. Аналіз змісту дисертаційної роботи демонструє належну обґрунтованість наукових положень роботи. Достовірність отриманих наукових результатів має теоретичне підґрунтя та підтверджується результатами експериментальних досліджень. Бондаренко М.О. розв'язав науково-прикладне завдання з розробки методів та алгоритмів криптосистем на основі функцій дійсних змінних, а також впровадив програмного забезпечення, що в продемонструвало застосовність отриманих теоретичних результатів у практичній

роботі. Результатами роботи стали нові наукові результати.

Основні наукові результати отримані за результатами дисертаційного дослідження:

- уперше розроблено комбіновану криптосистему, яка поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності;
- уперше розроблено криптосистему для захисту зображень на основі функцій дійсної змінної шляхом використання функцій інтегральної непропорційності, де інше довільне зображення використовується в якості криптографічного ключа;
- уперше впроваджено метод дешифрування шляхом використання інтегральних функцій непропорційності, що дозволяє визначати невідомі коефіцієнтів в сумі функцій дійсної змінної;
- удосконалено моделі та методи створення криптосистем на основі функцій дійсної змінної;
- удосконалено метод шифрування даних шляхом впровадження додаткового елементу перестановки функцій-ключів;

Практична значення отриманих результатів.

Отримані результати забезпечують можливість практичної реалізації інженерних бібліотек запропонованих криптосистем, що дозволяє створення програмного коду для будь-яких прикладних застосувань (web рішення, вбудоване програмне забезпечення, шифрування баз даних). Запропонована криптосистема для захисту зображень може знайти експериментальне застосування в сучасних системах автентифікації з використанням довільного зображення в якості автентифікатора. Результати експериментів щодо криптостійкості запропонованих методів можуть бути використані для порівняльного аналізу різних підходів до шифрування.

Повнота викладу результатів роботи в опублікованих працях. Наукове завдання дисертаційній роботі було виконано в повному обсязі. Здобувач осягнув методологію наукових досліджень та опублікував за темою дисертаційної роботи 10 наукових праць, з них: 4 статті у наукових фахових виданнях України, з яких 2

включені до міжнародних наукометричних баз з них 1 стаття у виданні, що індексується міжнародною наукометричною базою Scopus, 4 публікації за матеріалами конференцій, 2 патенти на корисну модель.

Участь здобувача у роботах, що опубліковані у співавторстві, зазначена у дисертаційній роботі. Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пункту 8 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44 зі змінами від 03.05 2024 р. (Постанова КМУ від №507).

Оцінка змісту дисертації. Дисертація складається зі анотації, вступу, чотирьох розділів, висновків, списку використаних джерел і одного додатку. Загальний обсяг дисертації складає 170 сторінок, з яких анотація на 5 сторінках, основна частина на 182 сторінках, список використаних джерел із 182 найменувань на 20 сторінках і додаток на 3 сторінках. Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації» та за структурою, мовою та стилем викладення відповідає вимогам МОН України.

У вступі обґрунтовано актуальність дослідження, сформульовано мету і завдання роботи, визначено об'єкт, предмет і методи дослідження, а також розкрито наукову новизну та практичну значущість отриманих результатів.

Перший розділ присвячений аналізу сучасного стану та перспектив розвитку криптографічних систем. Автор провів ґрунтовний огляд існуючих підходів до побудови криптосистем і методів їх реалізації, виявив їхні недоліки і визначив напрямки для подальших досліджень.

У другому розділі запропонована математична модель повідомлення, зашифрованого за допомогою суми функцій дійсної змінної, представлених у вигляді одновимірних масивів. Збільшення криптостійкості забезпечується за рахунок використання генераторів псевдовипадкових чисел. Запропонований метод дешифрування, заснований на функціях інтегральної непропорційності,

дозволяє обчислювати невідомі коефіцієнти при відомих функціях у їхній сумі.

У третьому розділі проведено дослідження криптосистеми, побудованої на основі функцій дійсної змінної. Проаналізовано метод дешифрування повідомлень, зашифрованих сумою таких функцій, з використанням властивостей функцій інтегральної непропорційності для визначення невідомих коефіцієнтів. Окреслено та описано обмеження, які накладаються на ключові функції для забезпечення коректності шифрування. Запропоновано модифікації існуючих алгоритмів з метою підвищення криптостійкості системи.

У четвертому розділі розглянуто можливості створення спеціалізованих криптосистем для захисту зображень, де в якості ключа використовується інше зображення. Запропонована криптосистема базується на застосуванні дійсних чисел, а також розроблено алгоритми шифрування та дешифрування, що використовують властивості інтегральної непропорційності. Експериментально перевірено роботу алгоритму, виявлено високу чутливість до змін ключа, складність зламу системи методом перебору (брутфорсу) та здатність алгоритму до декореляції шифротексту, що підвищує рівень захисту інформації.

Академічна доброчесність. Порушень академічної доброчесності в дисертації та наукових публікаціях, що містять основні наукові результати роботи, не виявлено. Наукові результати, представлені здобувачем для захисту, отримані ним самостійно і відображені у відповідних публікаціях. У спільних роботах використані лише ті ідеї, положення та розрахунки, які є результатом власних наукових пошуків автора.

До зауважень щодо змісту дисертаційної роботи можна віднести наступні:

1. У роботі відсутні оцінки швидкодії пропонованих алгоритмів для шифрування/розшифрування візуальної інформації. Не наведені чисельні оцінки криптостійкості, які використовуються у випадку шифрування зображень (ентропія, UACI, NPCR, кореляція сусідніх пікселів). Відсутнє порівняння цих показників з наявними системами, особливо в контексті розвитку постквантової криптографії.

2. У методі шифрування зображення шифрується лише візуальна складова зображення без метаданих. Розшифроване зображення є ідентичним до оригінального лише по-піксельно, а не по-байтово, що може породжувати додаткові виклики - наприклад, хеш-сума оригінального та розшифрованого файлів буде різною. Також, байтовий розмір розшифрованого зображення може перевищувати розмір оригінального зображення.

3. У методі шифрування зображення не шифрується перший піксель, що потенційно може призводити до вразливості.

4. У методі шифрування сумою функцій-ключів недостатньо формалізований підхід до створення функцій-ключів.

5. Внаслідок появи помилок округлення даний метод вимагає узгодження числа, наближеного до нуля ε при дешифруванні повідомлення.

6. Оформлення деяких зображень (наприклад, Рис. 4.9-4.11) не відповідають вимогам оформлення ДСТУ 3008:2015.

Висновки. Дисертаційна робота Бондаренка Микити Олеговича є завершеною науково-дослідною роботою, що містить науково обґрунтовані результати, демонструє наукову новизну та відкриває перспективи для подальших досліджень. Тематика досліджень повністю відповідає галузі знань 12 «Інформаційні технології» та спеціальності 122 «Комп'ютерні науки».

З огляду на актуальність теми, отримані результати та їх практичну значущість, вважаю, що дисертація Бондаренка Микити Олеговича на тему «Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних» відповідає вимогам чинного законодавства України, визначеним у п. 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», від 12 січня 2022 року № 44 зі змінами від 03.05.2024 р. (Постанова КМУ № 507), а також вимогам до оформлення дисертації, затвердженим МОН України від 12.01.2017 № 40. Сам автор, Бондаренко Микита Олегович, заслуговує на присудження наукового ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки».

Офіційний опонент:

професор кафедри
безпеки інформації та телекомунікацій
Національного Технічного Університету
«Дніпровська Політехніка»
доктор наук з державного управління,
кандидат технічних наук, доцент Євген Котух

«24» жовтня 2024 року

Підпис Євгена КОТУХА засвідчую:
Учений секретар Національного Технічного Університету
«Дніпровська Політехніка» Таїсія КАЛОЖНА