РЕЦЕНЗІЯ

офіційного рецензента

Бережної Ольги Володимирівни

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 дисертаційного дослідження. Дисертаційне дослідження Бондаренка М. О. присвячене актуальній темі розробки моделей та методів криптографічних систем на основі функцій дійсної змінної. Актуальність обраної тематики зумовлена комплексом факторів, що формують сучасні виклики у сфері інформаційної безпеки та криптографії. Сучасний стан розвитку інформаційних технологій характеризується стрімким прогресом у галузі обчислювальної техніки, що створює нові загрози для існуючих криптографічних систем. Більшість сучасних криптосистем, таких як AES та RSA, базуються на операціях з цілими числами, що призводить до необхідності постійного збільшення довжини ключів та зростання обчислювальних витрат. Крім того, розвиток квантових комп'ютерів ставить під загрозу безпеку багатьох існуючих криптографічних алгоритмів, особливо тих, що ґрунтуються на проблемах факторизації та дискретного логарифму. Ці фактори стимулюють пошук нових підходів до захисту інформації, зокрема, дослідження в області криптосистем на основі дійсних чисел та інтегральної криптографії. Використання функцій дійсної змінної в криптографії представляє перспективний напрямок, що потенційно може забезпечити більший простір ключів та вищу криптографічну стійкість. Окремим важливим аспектом є розробка спеціалізованих криптографічних рішень для захисту різних типів даних, включаючи зображення. У цьому контексті дослідження Бондаренка М. О. спрямоване на розв'язання актуального науково-

практичного завдання, яке має потенціал для створення нових криптографічних примітивів та подолання обмежень існуючих систем. Автор ставить перед собою комплексне завдання, яке включає аналіз сучасних криптографічних систем, розробку математичної моделі криптосистем на основі функцій дійсної змінної, створення методів шифрування та дешифрування даних, а також їх адаптацію для роботи із зображеннями. Особливу увагу приділено розробці алгоритму використання зображення як криптографічного ключа та створенню програмної реалізації розроблених криптосистем. Важливо відзначити, що дисертаційна робота виконана в рамках пріоритетних напрямків наукових досліджень Сумського державного університету та відповідає плану науково-дослідних робіт за держбюджетною темою «Методи, математичні моделі та інформаційні технології аналізу і синтезу інфокомунікаційних систем» (ДР № 0118U006971, 2018-2023). Таким чином, дисертаційне дослідження Бондаренка М. О. є актуальним та важливим внеском у розвиток сучасної криптографії, що має потенціал для підвищення безпеки цифрової інформації в умовах нових викликів та загроз.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій. Дисертаційна робота Бондаренка М. О. характеризується високим рівнем обґрунтованості та достовірності наукових положень, висновків і рекомендацій. Методологічною основою дослідження є комплексне застосування методів наукового пізнання, що включає принципи і методи криптографії, методи розпізнавання сигналів і функції непропорційності. Системний підхід, використаний автором, забезпечує цілісність дослідження та логічну послідовність викладення матеріалу.

Наукові тези та висновки, які викладені в дисертації, мають тверде теоретичне обґрунтування, що базується на глибокому аналізі існуючих криптографічних систем та їх обмежень. Автор успішно вирішив науково-прикладну задачу розробки моделей, методів, алгоритмів і програмних засобів створення криптосистем на основі функцій дійсних змінних, що дозволило отримати низку нових і суттєвих наукових результатів.

Особливої уваги заслуговує математична модель криптосистем на основі функцій дійсної змінної, яка розроблена автором за результатами аналізу

сучасного стану криптографії. Запропонована математична модель створює теоретичне підґрунтя для подальших практичних розробок.

Достовірність теоретичних положень підтверджується результатами експериментальних досліджень. Створене автором програмне забезпечення для реалізації розроблених криптографічних алгоритмів дозволило провести серію експериментів, результати яких підтверджують ефективність запропонованих методів. Важливо відзначити, що автор не обмежується лише теоретичними розробками, а доводить їх до конкретних інженерних методів та алгоритмів.

Практична значущість роботи підтверджується розробкою криптосистеми для захисту зображень з використанням довільно обраного зображення в якості ключа. Розроблена система демонструє потенціал практичного застосування результатів дисертаційної роботи в різних сферах, де потрібен захист візуальної інформації.

Результатами експериментальних досліджень підтверджено достатньо високий рівень крипостійкості розроблених методів, що має важливе значення для порівняльного аналізу різних підходів до шифрування, а також свідчить про наукову новизну та практичну цінність отриманих результатів.

Таким чином, аналіз дисертаційної роботи Бондаренка М. О. дозволяє зробити висновок про належну обґрунтованість наукових положень, висновків і рекомендацій. Достовірність результатів теоретичних досліджень, що ґрунтуються на сучасних методах криптографії та теорії функцій дійсної змінної, підтверджується результатами експериментальних досліджень. Це дозволяє стверджувати, що дисертаційна робота є цілісним та завершеним науковим дослідженням, результати якого мають як теоретичне, так й практичне значення для розвитку сучасної криптографії.

Наукові результати. Наукова новизна одержаних результатів полягає у тому, що у дисертаційній роботі розв'язано важливу науково-практичну задачу створення моделей та методів криптографічних систем на основі функцій дійсної змінної. Отримані такі результати:

вперше:

– розроблено метод використання інтегральних функцій непропорційності для дешифрування даних, що дозволяє використовувати в криптосистемі дискретні функції-ключі;

– розроблено криптосистему, що поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності. Запропоновано двох-етапне шифрування, при якому результат першого етапу шифрується ще раз, що суттєво ускладнює злам криптосистеми. Експериментально підтверджено високу крипостійкість розроблених методів шифрування до атак грубої сили через необхідність підбору значень ключа з високою точністю. Також продемонстровано високу здібність до декореляції значень шифротексту;

– розроблено криптосистему для захисту зображень, в якій інше довільно обране зображення використовується в якості криптографічного ключа, шляхом використання функцій інтегральної непропорційності. Запропонований підхід значно спрощує передачу ключа порівняно з передачею функцій-ключів в аналітичному вигляді. Це зображення легше непомітно передати приймальній стороні при використанні симетричних криптосистем. Крім того, зловмиснику складніше буде виявити зображення-ключ серед багатьох зображень, до яких він отримав доступ.

удосконалено:

– моделі та методи створення криптосистем на основі функцій дійсної змінної, що призводить до збільшення крипостійкості;

– метод шифрування даних шляхом впровадження додаткового елементу перестановки функцій-ключів, що також підвищує крипостійкість системи;

Заслугою автора є обґрунтована та доведена пропозиція щодо створення моделей та методів криптосистем на основі функцій дійсної змінної.

Практичне значення отриманих результатів. Дисертаційна робота Бондаренка М. О. демонструє значний потенціал практичного застосування отриманих наукових результатів у сфері криптографії та захисту інформації.

Автор успішно трансформував теоретичні розробки у конкретні інженерні методики та алгоритми, що є важливим кроком до їх практичної реалізації.

Ключовим досягненням є розробка інформаційної технології шифрування та дешифрування даних за допомогою функцій дійсних змінних. Ця технологія лежить в основі запропонованих криптосистем, які можуть бути практично реалізовані для вирішення реальних завдань захисту інформації.

Особливу практичну цінність має розроблена криптосистема для захисту зображень, яка використовує довільно обране зображення в якості ключа. Запропонована інноваційна розробка відкриває нові можливості для експериментального захисту візуальної інформації в різних сферах, де потрібна підвищена безпека графічних даних. Такий підхід може знайти застосування в галузях, де захист візуальної інформації є критично важливим, наприклад, у медицині, військовій справі чи промисловому дизайні.

Створене автором програмне забезпечення для реалізації розроблених криптографічних алгоритмів є важливим практичним результатом дослідження. Програмне забезпечення може бути використане не лише для проведення подальших наукових досліджень та експериментів у галузі криптографії на основі функцій дійсної змінної, але й в якості основи для розробки комерційних продуктів захисту інформації.

Важливо відзначити, що автор досяг мети дисертаційного дослідження шляхом розробки нових моделей та методів криптосистем на основі функцій дійсної змінної. Розроблені моделі та методи спрямовані на підвищення стійкості та ефективності шифрування як текстових даних, так й зображень, що відповідає сучасним вимогам до систем захисту інформації та має безпосереднє практичне значення.

Таким чином, практична цінність отриманих результатів полягає у можливості їх застосування для створення нових, більш ефективних систем захисту інформації, а також у відкритті нових напрямків досліджень та розробок у галузі криптографії на основі функцій дійсної змінної.

Повнота викладу результатів роботи. Наукові положення, висновки і рекомендації, сформульовані у дисертації, викладені в десяти наукових працях, з них: чотири статті у наукових фахових виданнях України, з яких дві

включені до міжнародних наукометричних баз (у тому числі, одна стаття у виданні, що індексується міжнародною наукометричною базою Scopus), чотири публікації за матеріалами конференцій, два патенти на корисну модель.

Таким чином, дисертація Бондаренка Микити Олеговича «Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних» є самостійним завершеним дослідженням, в якому отримано нові науково обґрунтовані результати, що в сукупності вирішують конкретне наукове завдання, яке має вагоме значення для розвитку комп'ютерних наук. Дисертація відповідає вимогам «Порядку присудження ступеня доктор 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.

Академічна доброчесність. Дисертаційна робота та наукові публікації Бондаренка М. О. відповідають принципам академічної доброчесності. Порушень у цій сфері не виявлено. Здобувач самостійно отримав наукові результати, що винесені на захист, та належно висвітлив їх у своїх роботах. У публікаціях, написаних у співавторстві, використано лише особисті наукові здобутки дисертанта.

Зауваження до змісту дисертаційної роботи. При загальній позитивній оцінці дисертаційного дослідження Бондаренка М. О., яке виконане на достатньо високому науковому рівні, варто відзначити деякі зауваження.

1. В роботі не вказано кількісних метрик крипостійкості запропонованих методів. Наприклад, варто було б зазначити, який саме час і ресурси потрібні зловмиснику, щоб зламати цей шифр шляхом атаки методом грубої сили.
2. Було б доречно додати в дисертаційну роботу таблиці та графіки порівняння характеристик запропонованих методів з характеристиками інших криптосистем.
3. В запропонованих методах, розмір шифротексту перевищує розмір повідомлення, що шифрується.

4. У методі шифрування зображення не шифрується перший піксель, що потенційно може призводити до вразливостей.
5. У методі шифрування зображення не досліджено, яким чином вибір зображення-ключа впливає на крипостійкість.

Висновки. Таким чином, дисертація Бондаренка Микити Олеговича «Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних» є самостійним завершеним дослідженням, в якому отримано нові науково обґрунтовані результати, що в сукупності вирішують конкретне наукове завдання, яке має вагоме значення для розвитку комп'ютерних наук. Дисертація відповідає вимогам «Порядку присудження ступеня доктор 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, а її автор, Бондаренко Микита Олегович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки».

Рецензент:
кандидат технічних наук,
доцент кафедри електроніки
і комп'ютерної техніки
Сумського державного
університету **Ольга БЕРЕЖНА**