РЕЦЕНЗІЯ

офіційного рецензента

Москаленко В’ячеслава Васильовича

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. Дисертаційна робота Бондаренка М. О. присвячена розв'язанню актуального науково-практичного завдання 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.

Ключові аспекти, що визначають актуальність дослідження, включають:

1. Обмеження існуючих криптосистем: сучасні криптографічні системи, такі як AES та RSA, базуються на операціях з цілими числами, що призводить до необхідності постійного збільшення довжини ключів та зростання обчислювальних витрат зі збільшенням обчислювальної потужності. Крім того, кінцевий набір цілих чисел потенційно обмежує довгострокову стійкість цих систем.
2. Загроза квантових обчислень: розвиток квантових комп'ютерів ставить під загрозу безпеку багатьох існуючих криптографічних алгоритмів, особливо тих, що базуються на проблемах факторизації та дискретного логарифму.
3. Потреба в нових підходах: аналіз сучасного стану криптографії демонструє необхідність розробки інноваційних способів захисту даних на альтернативних засадах.

4. Специфіка захисту зображень: існує потреба в спеціалізованих криптографічних рішеннях для різних типів даних, зокрема для шифрування зображень.
5. Потенціал систем на основі дійсних чисел: використання криптосистем на основі дійсних чисел представляє перспективний напрямок досліджень, що потенційно може забезпечити більший простір ключів та вищу криптографічну стійкість.
6. Інтегральна криптографія: дослідження в області інтегральної криптографії відкривають нові можливості для створення криптосистем з теоретично гарантованою стійкістю.

У рамках дисертаційного дослідження автор ставить і послідовно вирішує наступні завдання:

1. Проведення аналізу сучасних криптографічних систем, їх переваг та недоліків.
2. Розробка математичної моделі криптосистем на основі функцій дійсної змінної.
3. Створення методу шифрування даних з використанням суми функцій дійсної змінної як симетричних ключів.
4. Розробка методу дешифрування даних, які зашифровані за допомогою обчислення невідомих коефіцієнтів ключових функцій.
5. Адаптація розроблених методів для шифрування та дешифрування зображень.
6. Розробка алгоритму використання зображення як криптографічного ключа для шифрування інших зображень.
7. Створення програмної реалізації розроблених криптосистем та проведення експериментальних досліджень їх ефективності.

Важливо відзначити, що дисертаційна робота відповідає пріоритетним напрямкам наукових досліджень Сумського державного університету та виконана відповідно до плану науково-дослідних робіт за держбюджетною темою «Методи, математичні моделі та інформаційні технології аналізу і синтезу інфокомунікаційних систем» (ДР № 0118U006971, 2018-2023).

Таким чином, дослідження нових методів криптографічного захисту на основі функцій дійсної змінної та інтегральної непропорційності є актуальним та важливим завданням. Воно має потенціал для створення нових криптографічних примітивів, які могли б подолати обмеження існуючих систем, та запропонувати ефективні рішення для захисту різних типів даних, включаючи зображення. Тема відповідає сучасним тенденціям розвитку криптографії та має потенціал для внеску у підвищення безпеки цифрової інформації в сучасному світі.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій. Дисертаційна робота Бондаренка М. О. містить нові науково обґрунтовані результати в галузі криптографії. Автор успішно вирішив науково-прикладну задачу розробки моделей, методів, алгоритмів і програмних засобів створення криптосистем на основі функцій дійсних змінних. Методологічною основою дослідження є сукупність методів і прийомів наукового пізнання, що включає принципи і методи криптографії, методи розпізнавання сигналів і функції непропорційності. Їх застосування обумовлюється системним підходом, що забезпечує цілісність та послідовність дослідження.

Достовірність результатів теоретичних досліджень ґрунтується на основі функцій дійсної змінної та теорії інтегральної непропорційності. Важливо відзначити, що всі теоретичні розробки дисертації автором доведено до конкретних інженерних методик та алгоритмів, з використанням запропонованої інформаційної технології шифрування та дешифрування даних за допомогою суми функцій дійсних змінних. Це дозволило отримати низку нових і суттєвих наукових результатів, які мають як теоретичне, так і практичне значення.

Особливої уваги заслуговує обґрунтована та доведена пропозиція автора щодо створення моделей та методів криптосистем на основі функцій дійсної змінної. Ця пропозиція логічно випливає з аналізу існуючих криптографічних систем та їх обмежень, що створює міцне підґрунтя для подальших розробок у цьому напрямку.

Достовірність отриманих результатів підтверджується експериментальними дослідженнями, проведеними автором. Зокрема, створене програмне забезпечення для реалізації розроблених криптографічних алгоритмів дозволило провести ґрунтовні експерименти та отримати практичні результати, які підтверджують теоретичні положення дисертації. Результати експериментальних досліджень криптостійкості розроблених методів можуть бути використані для порівняльного аналізу різних підходів до шифрування, що підкреслює їх наукову та практичну цінність.

Запропонована криптосистема для захисту зображень з використанням довільного зображення як ключа демонструє практичну спрямованість дослідження та може бути застосована для експериментального захисту візуальної інформації в різних сферах. Це свідчить про потенціал практичного застосування результатів дисертаційної роботи.

Таким чином, наукові положення, висновки і рекомендації, викладені в дисертації, мають тверде теоретичне обґрунтування та підтверджуються результатами експериментальних досліджень. Це дозволяє зробити висновок про належну обґрунтованість та достовірність наукових результатів дисертаційної роботи Бондаренка М. О.

Наукова новизна. Дисертаційна робота Бондаренка М. О. містить ряд важливих наукових результатів у галузі криптографії, які характеризуються новизною, достовірністю та належним обґрунтуванням. Основні досягнення дослідження можна узагальнити наступним чином:

Автором удосконалено моделі та методи створення криптосистем на основі функцій дійсної змінної. Це вдосконалення базується на глибокому аналізі існуючих підходів та відкриває нові можливості для розвитку криптографічних систем.

Вперше в роботі впроваджено метод захисту даних з використанням інтегральних функцій непропорційності, що дозволяє використовувати в криптосистемі дискретні функції-ключі. Цей метод дозволяє визначати невідомі коефіцієнти в сумі функцій дійсної змінної, що є суттєвим внеском у

теорію криптографії. Автор детально обґрунтовує цей метод, демонструючи його математичну коректність та практичну застосовність.

Особливої уваги заслуговує вперше розроблена автором комбінована криптосистема, яка поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності. Ця розробка демонструє здатність до синтезу різних підходів та створення нових, більш ефективних методів захисту інформації.

Автор також удосконалив метод шифрування даних шляхом впровадження додаткового елементу перестановки функцій-ключів. Це вдосконалення підвищує криптостійкість системи та розширює спектр її можливих застосувань.

Нарешті, вперше розроблено криптосистему для захисту зображень на основі функцій інтегральної непропорційності. Інноваційним аспектом цієї системи є використання довільного зображення в якості криптографічного ключа, що відкриває нові перспективи у сфері захисту візуальної інформації. Це зображення легше непомітно передати приймальній стороні при використанні симетричних криптосистем. Крім того, зловмиснику складніше 6 виявити зображення-ключ серед багатьох зображень, до яких він отримав доступ.

Практичне значення отриманих результатів. Дисертаційне дослідження Бондаренка М. О. має вагоме практичне значення для галузі криптографії та захисту інформації. Отримані результати дозволяють здійснити практичну реалізацію запропонованих криптосистем, що є важливим кроком у розвитку сучасних методів шифрування. Автор успішно довів усі теоретичні розробки до рівня конкретних інженерних методик та алгоритмів, використовуючи запропоновану інформаційну технологію шифрування та дешифрування даних за допомогою функцій дійсних змінних.

Особливої уваги заслуговує розроблена криптосистема для захисту зображень, яка використовує довільне зображення як ключ. Ця інноваційна розробка відкриває широкі можливості для експериментального захисту

візуальної інформації в різноманітних сферах, де потрібна підвищена безпека графічних даних.

Створене автором програмне забезпечення для реалізації розроблених криптографічних алгоритмів має значний потенціал для подальшого використання. Воно може стати цінним інструментом для проведення додаткових досліджень та експериментів у галузі криптографії на основі функцій дійсної змінної, що сприятиме подальшому розвитку цього перспективного напрямку.

Варто зазначити, що автор досяг мети дисертаційного дослідження, розробивши нові моделі та методи криптосистем на основі функцій дійсної змінної. Ці розробки спрямовані на підвищення стійкості та ефективності шифрування як текстових даних, так і зображень, що відповідає сучасним вимогам до систем захисту інформації.

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

Повнота викладу результатів роботи. Дисертаційне дослідження Бондаренка М. О. знайшло належне відображення в наукових публікаціях. За темою дисертації опубліковано 10 наукових праць, що всебічно висвітлюють основні результати дослідження. Серед них 4 статті у наукових фахових виданнях України, 2 з них включені до міжнародних наукометричних баз. З них одна стаття опублікована у виданні, яке індексується міжнародною наукометричною базою Scopus.

Крім того, результати дослідження були представлені на наукових конференціях, про що свідчать 4 публікації за матеріалами конференцій.

Практична значущість роботи підтверджується отриманням 2 патентів на корисну модель, що вказує на потенціал комерціалізації результатів дослідження.

У роботах, опублікованих у співавторстві, внесок здобувача чітко зазначений у дисертаційній роботі, що свідчить про прозорість та етичність

проведеного дослідження. 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 Кабінету Міністрів України від 12.01.2022 р. №44 зі змінами від 03.05.2024 р. (Постанова КМУ №507).

Таким чином, можна зробити висновок, що результати дисертаційної роботи Бондаренка М. О. повно та всебічно викладені в опублікованих наукових працях.

Академічна доброчесність. У дисертації та наукових публікаціях Бондаренка М. О. порушень академічної доброчесності не виявлено. Наукові результати, винесені на захист, отримано автором самостійно та належно висвітлено в опублікованих роботах. У співавторських публікаціях використано лише ідеї, положення та розрахунки, що є результатом особистих наукових пошуків здобувача.

Зауваження до змісту дисертаційної роботи. Хоча дисертаційне дослідження загалом виконане на достатньо високому рівні, можна вказати декілька зауважень:

1. В роботі не вказані показники швидкодії запропонованих методів – час шифрування та дешифрування.
2. В роботі відсутнє порівняння чисельних метрик криптостійкості з існуючими криптосистемами.
3. У методі шифрування сумою функцій, через вимоги до функцій-ключів, існує необхідність попередньо перевіряти коректність шифрування і дешифрування на всьому алфавіті повідомлення перед узгодженням нового ключа, що підвищує складність процесу.
4. У методі шифрування сумою функцій не розглянуто випадок, коли передається символ, в якому всі біти нульові – в такому разі, шифротекст відповідного символу теж буде нульовим.
5. У запропонованих методах, збільшення розміру шифротексту відносно розміру повідомлення може потребувати підвищених вимог до пропускної здатності каналу зв’язку.

6. В тексті дисертації присутні описки, інколи є неточності в позначеннях змінних (наприклад, xmin замість x_{min}).

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 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 зі спеціальності 122-Комп'ютерні науки.

Рецензент:
кандидат технічних наук,
доцент кафедри
електроніки і комп'ютерної техніки
Сумського державного
університету **В'ячеслав Москаленко**