

РЕЦЕНЗІЯ

кандидата технічних наук, доцента

Розломій Інни Олександрівни

на дисертаційну роботу Короткого Тимофія Константиновича

«Ієрархічна інформаційна система моделювання і дослідження алгоритмів

потокowego SET-шифрування»,

подану на здобуття ступеня доктора філософії

за спеціальністю 126 Інформаційні системи та технології

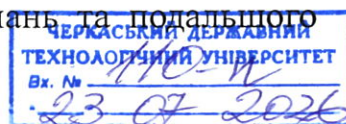
галузі знань 12 Інформаційні технології

1. Актуальність теми дисертаційної роботи.

Сучасний розвиток інформаційних систем характеризується переходом від засобів накопичення та оброблення даних до інтелектуальних систем, здатних підтримувати процеси наукових досліджень, моделювання складних об'єктів, автоматизованого проектування та аналізу отриманих результатів. Особливо актуальним такий підхід є у предметних областях, де кількість можливих варіантів дослідження надзвичайно велика, а отримання нових наукових результатів потребує значних обчислювальних експериментів і багаторазового використання накопичених знань.

Однією з таких предметних областей є побудова сучасних алгоритмів потокowego SET-шифрування. Дослідження математичних моделей SET-операцій, їх класифікація, синтез нових операцій, аналіз криптографічних властивостей та формування генераторів псевдовипадкових послідовностей пов'язані з обробленням значних обсягів взаємопов'язаної інформації. За відсутності спеціалізованих інформаційних систем виконання таких досліджень значною мірою здійснюється вручну або за допомогою окремих програмних засобів, що істотно ускладнює накопичення результатів, їх повторне використання та подальший розвиток предметної області.

Разом із тим існуючі інформаційні системи переважно орієнтовані на розв'язання окремих задач моделювання або підтримують лише окремі класи SET-операцій. Недостатньо дослідженими залишаються питання побудови ієрархічних інформаційних систем, у яких математичні моделі, методи синтезу, результати обчислювальних експериментів, бази даних та бази знань об'єднані єдиною структурою із встановленими взаємозв'язками між різними рівнями ієрархії. Саме така організація інформаційної системи забезпечує можливість автоматизованого синтезу нових моделей, накопичення знань та подальшого



розширення функціональних можливостей системи без зміни її концептуальної структури.

Актуальність дисертаційної роботи Короткого Тимофія Константиновича полягає у розв'язанні саме цієї науково-прикладної проблеми шляхом розроблення моделі ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування, яка ґрунтується на встановленні нових та уточненні існуючих взаємозв'язків між моделями різних ієрархічних рівнів, забезпечує автоматизований синтез і дослідження симетричних та несиметричних СЕТ-операцій, генераторів їх псевдовипадкових послідовностей, а також створює основу для подальшого розвитку інформаційних технологій підтримки криптографічних досліджень.

Отже, тема дисертаційного дослідження є актуальною, оскільки спрямована на розвиток інформаційних систем підтримки наукових досліджень, удосконалення методів автоматизованого моделювання та синтезу СЕТ-операцій і підвищення ефективності дослідження алгоритмів потокового СЕТ-шифрування, що має важливе значення для розвитку сучасних інформаційних систем і технологій.

2. Наукова новизна результатів роботи.

Наукова новизна дисертаційної роботи:

- *вперше* побудована модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій, на основі методів синтезу СЕТ-операцій і груп СЕТ-операцій, шляхом вдосконалення моделей, методів і технології побудови комутативних і некомутативних СЕТ-операцій, а також генераторів псевдовипадкових наборів СЕТ-операцій, що дозволило встановлювати нові залежності між моделями синтезу симетричних і несиметричних операцій, які приводять до розширення взаємозв'язків між моделями ієрархічних рівнів інформаційної системи, реалізація якої забезпечить експериментальну підтримку для побудову перспективних стійких малoresурсних алгоритмів потокового шифрування;
- *удосконалено* технологію побудови удосконалених моделей некомутативних двохранрядних двохрандних СЕТ-операцій за результатами експерименту, на основі побудови удосконалених моделей

СЕТ-операцій за результатами експерименту, шляхом встановлення взаємозв'язків між моделями до і після перестановки операндів, що забезпечило зменшення складності моделювання некомутативних СЕТ-операцій на основі реалізації прямого переходу від побудованої моделі СЕТ-операції до моделі СЕТ-операції з переставленими операндами;

- *удосконалено* метод синтезу двохоперандних двохранрядних операцій криптографічного перетворення на основі метод синтезу симетричних операцій, шляхом застосування в якості першої базової операції несиметричної операції криптоперетворення та додаткової побудови оберненої операції за результатами обчислювального експерименту, що забезпечили можливість додаткового синтезу несиметричних двохоперандних двохранрядних операцій подвійного циклу;
- *удосконалено* метод побудови двохранрядних двохоперандних операцій, які допускають перестановку операндів на основі об'єднання двохранрядних однооперандних операцій криптографічного перетворення, шляхом встановлення взаємозв'язків між прямими і оберненими операціями, що дозволило змоделювати всі двохранрядні двохоперандні операції, які допускають перестановку операндів.

3. Практичне значення одержаних результатів.

Практична цінність результатів дисертаційного дослідження полягає у наступному:

- розроблено модель та програмний макет ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування, що забезпечує автоматизацію процесів синтезу, аналізу та дослідження симетричних і несиметричних СЕТ-операцій;
- запропоновано інформаційну технологію, яка об'єднує базу даних, базу знань, моделі синтезу СЕТ-операцій та генератори псевдовипадкових послідовностей, що створює основу для подальшого розширення функціональних можливостей системи та накопичення результатів наукових досліджень;
- реалізована інформаційна система суттєво розширює спектр СЕТ-операцій, доступних для автоматизованого дослідження, збільшуючи

кількість аналізованих 2Сі-квантових операцій, які допускають перестановку операндів, із 96 до 576, а також забезпечує моделювання понад 10623 двохоперандних СЕТ-операцій, що не допускають перестановку операндів;

- створено інструментальне середовище для дослідження алгоритмів потокового СЕТ-шифрування, яке забезпечує моделювання систем із використанням надзвичайно великої кількості несиметричних двохоперандних СЕТ-операцій та генераторів їх псевдовипадкових послідовностей, що істотно розширює можливості проведення обчислювальних експериментів.

4. Структура роботи, оцінка змісту дисертації та її завершеність.

Дисертаційна робота складається зі вступу, п'яти розділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації – 190 сторінок. Основний зміст викладений на 158 сторінках, у тому числі – 15 таблиць, 13 рисунків. Список використаних джерел містить 103 найменування.

У першому розділі проаналізовано сучасний стан розвитку інформаційних систем проектування малоресурсних криптографічних алгоритмів, розглянуто сучасні підходи до побудови систем потокового СЕТ-шифрування, досліджено існуючі інформаційні системи моделювання СЕТ-операцій, визначено їх переваги та недоліки, а також сформульовано мету і завдання дисертаційного дослідження.

У другому розділі досліджено особливості застосування несиметричних двохоперандних СЕТ-операцій, що допускають перестановку операндів, запропоновано моделі некомутативних двохоперандних СЕТ-операцій подвійного циклу та удосконалено технологію їх побудови на основі встановлення взаємозв'язків між моделями до і після перестановки операндів.

У третьому розділі запропоновано удосконалений метод синтезу несиметричних двохоперандних операцій криптографічного перетворення, досліджено можливості побудови груп несиметричних операцій подвійного та потрійного циклів, а також виконано експериментальну перевірку коректності запропонованих моделей синтезу.

У четвертому розділі розглянуто моделювання та синтез множин двохоперандних СЕТ-операцій шляхом поєднання однооперандних операцій криптографічного перетворення. Досліджено особливості побудови симетричних і несиметричних операцій, що допускають перестановку операндів,

а також встановлено закономірності та обмеження їх синтезу залежно від моделей перетворення першого операнда.

У п'ятому розділі розроблено модель ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування. Запропоновано структуру системи, що базується на використанні бази даних та бази знань, визначено взаємозв'язки між ієрархічними рівнями моделювання, реалізовано генератори псевдовипадкових послідовностей СЕТ-операцій та показано можливість розширення функціональних можливостей інформаційної системи шляхом накопичення результатів нових досліджень.

У висновках узагальнено основні результати проведених досліджень, сформульовано наукові та практичні результати, отримані під час виконання дисертаційної роботи. Структура дисертації є логічною та послідовною, матеріал викладено системно, а окремі розділи взаємопов'язані між собою та спрямовані на досягнення поставленої мети.

Дисертаційна робота є завершеною науковою працею. Поставлену мету дослідження досягнуто, а сформульовані завдання повною мірою вирішено.

5. Відсутність (наявність) порушень принципів академічної доброчесності.

Ознак порушень здобувачем принципів академічної доброчесності не встановлено. У роботі наведено посилання на використані праці, а результати, що становлять наукову новизну, сформульовано як авторський внесок здобувача.

6. Повнота викладення дисертації в опублікованих працях.

Основні положення дисертації опубліковано у 16 друкованих працях, зокрема: у 7 статтях у фахових виданнях України, із яких 2 статті в фахових журналах категорії А з індексацією в науково-метричній базі Scopus, 3 статтях опублікованих за кордоном, із яких 1 стаття включена до науково-метричної бази Scopus та WoS, одноосібному розділі колективної монографії, а також в матеріалах 4 міжнародних конференцій.

7. Зауваження та недоліки дисертації щодо її оформлення і змісту.

Зауваження до роботи:

1. У дисертаційній роботі запропоновано модель ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-

шифрування. Разом із тим, для кращого сприйняття архітектури системи доцільно було б доповнити роботу узагальнювальною схемою інформаційних потоків між окремими ієрархічними рівнями, базою даних, базою знань та програмними модулями.

2. Значну увагу приділено математичному моделюванню СЕТ-операцій та алгоритмам їх синтезу. Водночас було б доцільно більш детально розкрити питання програмної реалізації інформаційної системи, зокрема описати її програмну архітектуру, використані програмні засоби та принципи взаємодії окремих модулів.

3. Практичні результати роботи підтверджено створенням програмного макета інформаційної системи. Разом із тим, більш повну оцінку ефективності запропонованого підходу забезпечило б експериментальне порівняння продуктивності розробленої системи з існуючими засобами моделювання криптографічних алгоритмів або аналіз часових витрат на виконання основних операцій синтезу та моделювання.

4. У роботі показано можливість суттєвого розширення множини досліджуваних СЕТ-операцій, однак перспективним було б більш детально розглянути питання масштабованості запропонованої інформаційної системи при подальшому збільшенні розрядності операцій та обсягів накопичених у базі знань моделей.

5. У дисертації наведено значний обсяг математичних моделей, результатів моделювання та експериментальних досліджень. Для покращення сприйняття матеріалу доцільно було б після окремих ключових підрозділів навести узагальнювальні таблиці або схеми, які відображали б взаємозв'язки між розробленими моделями, методами синтезу та компонентами ієрархічної інформаційної системи.

Зазначені зауваження не знижують наукової новизни, теоретичної цінності та практичного значення дисертаційної роботи. Вони мають переважно рекомендаційний характер і можуть бути враховані автором у подальшому розвитку запропонованої ієрархічної інформаційної системи та розширенні її функціональних можливостей.

8. Висновок щодо відповідності дисертації вимогам, які висуваються до ступеня доктора філософії.

Дисертаційна робота Короткого Тимофія Константиновича на тему «Ієрархічна інформаційна система моделювання і дослідження алгоритмів

потокowego SET-шифрування» є завершеним науковим дослідженням, у якому розв'язано актуальне науково-прикладне завдання, пов'язане з розробленням моделі ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокowego SET-шифрування, що забезпечує автоматизований синтез, аналіз і дослідження симетричних та несиметричних SET-операцій, розширює взаємозв'язки між моделями різних ієрархічних рівнів та підвищує ефективність проведення досліджень у галузі малоресурсної криптографії.

За актуальністю теми, науковою новизною, теоретичною та практичною значущістю отриманих результатів, ступенем їх обґрунтованості, повнотою апробації та опублікування основних положень дисертаційна робота відповідає вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії.

Дисертація може бути представлена для офіційного захисту в разовій спеціалізованій вченій раді, а її автор – Короткий Тимофій Константинович – заслуговує на присудження ступеня доктора філософії за спеціальністю 126 Інформаційні системи та технології галузі знань 12 Інформаційні технології.

Рецензент:

кандидат технічних наук, доцент,
доцент кафедри інформаційної безпеки
та комп'ютерної інженерії
Черкаського державного
технологічного університету



Інна РОЗЛОМІЙ

Підпис к.т.н., доцента Інни РОЗЛОМІЙ засвідчую:

Учений секретар

Черкаського державного
технологічного університету,

к.т.н., доцент



Ірина МИРОНЕЦЬ