

РЕЦЕНЗІЯ

доктора технічних наук, професора

Палагіна Володимира Васильовича

на дисертаційну роботу Короткого Тимофія Костянтиновича

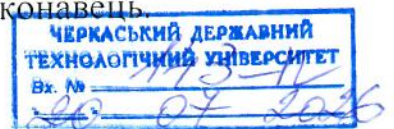
“Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокового SET-шифрування”, подану на здобуття ступеня доктора філософії за спеціальністю 126 – Інформаційні системи та технології галузі знань 12 – Інформаційні технології

1. Актуальність теми дисертації

В умовах сучасних інформаційних протистоянь питання захисту національного інформаційного простору є надзвичайно важливим. В наш час одним із ефективних шляхів захисту конфіденційної інформації в кіберпросторі є криптографія. Проте паралельно з розвитком криптографічних систем розвиваються і засоби криптоаналізу. Між даними системами існує постійна конкуренція і протиборство. Якщо створено новий криптоалгоритм, то разом з ним розвиваються та вдосконалюються засоби його злому. Тому на розробку систем криптоаналізу суттєво збільшується фінансування, яке стимулює додаткове залучення значної кількості висококваліфікованих фахівців. Це приводить до скорочення проміжку часу від створення криптосистеми до її злому. Єдиним ефективним шляхом протидії фінансовим інвестиціям в криптоаналіз є зменшення часу на створення нових, більш ефективних криптоалгоритмів. Нині існує велика кількість інформаційних систем для оцінки якості систем захисту інформації. Проте технологіям автоматизації проєктування захищених інформаційних систем не приділялося достатньої уваги. Окрім того, не повною мірою вирішено задачу моделювання генераторів груп симетричних і несиметричних криптографічних перетворень для систем потокового шифрування.

З огляду на наведені аргументи можна стверджувати, що тема дисертаційної роботи “Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокового SET-шифрування” є актуальною.

Отримані наукові результати роботи відображені в рамках науково-дослідної роботи, що проводилися за планами наукової та науково-дослідної діяльності Черкаського державного технологічного університету: «Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування» (ДР № 0121U114389); «Інформаційна технологія психолінгвістичного аналізу тексту для стеганографічних систем» (ДР № 0123U102085), в яких здобувач брав участь як виконавець.



2. Наукова новизна отриманих результатів.

Наукова новизна дисертаційного дослідження полягає в наступному:

- 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 побудови перспективних, стійких та малоресурсних алгоритмів потокового шифрування;
- удосконалено технологію побудови моделей некомутативних двохрозрядних двооперандних СЕТ-операцій за результатами обчислювального експерименту шляхом встановлення взаємозв'язків між моделями до і після перестановки операндів; це забезпечило зменшення складності процесів моделювання некомутативних СЕТ-операцій завдяки реалізації прямого переходу від базової моделі СЕТ-операції до моделі з переставленими операндами;
- удосконалено метод синтезу двооперандних двохрозрядних операцій криптографічного перетворення на основі методу синтезу симетричних операцій шляхом застосування в якості першої базової операції несиметричної операції криптоперетворення та додаткової побудови оберненої операції за результатами обчислювального експерименту, що забезпечило можливість додаткового синтезу несиметричних двооперандних двохрозрядних операцій подвійного циклу;
- удосконалено метод побудови двохрозрядних двооперандних операцій, які допускають перестановку операндів, на основі об'єднання двохрозрядних однооперандних операцій криптографічного перетворення шляхом встановлення взаємозв'язків між прямими і оберненими операціями, що дозволило змодельовати всі двохрозрядні двооперандні операції, які допускають перестановку операндів.

3. Практичне значення одержаних результатів.

Практична цінність роботи полягає в наступному:

- отримані наукові результати здобувачем доведені до алгоритмів реалізації моделей та варіантів застосування моделей генераторів псевдовипадкових послідовностей СЕТ-операцій;

- створено програмний макет ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування. Дана інформаційна система забезпечує синтез і аналіз 576 двохоперандних 2Сі-квантових СЕТ-операцій, які допускають перестановку операндів. Забезпечує можливість побудови і дослідження генераторів послідовностей криптоперетворень, які можуть використовувати до 10623 2Сі-квантових і до $65 \cdot 10^{35}$ 3Сі-квантових несиметричних двохоперандних СЕТ-операцій;
- практична цінність роботи підтверджена актами впровадження в навчальний процес Черкаського державного технологічного університету.

4. Структура роботи, оцінка змісту дисертації та її завершеність

Дисертаційна робота складається зі вступу, п'яти розділів, висновків, списку використаних джерел і трьох додатків. Загальний обсяг дисертації – 190 сторінок, з яких 158 сторінок основного тексту, списку використаних джерел, який включає 103 найменування та трьох додатків.

У вступі обґрунтовано актуальність теми дослідження, визначено мету, предмет і об'єкт дослідження. Сформульовано наукову новизну і практичне значення отриманих результатів, наведено методи дослідження, які використовувалися для вирішення кожної наукової задачі, подано відомості про публікації за результатами дослідження, особистий внесок здобувача в наведених публікаціях та апробацію отриманих результатів.

У першому розділі проведено аналіз сучасного стану та перспектив розвитку інформаційних систем і технологій проєктування малоресурсних криптографічних систем. За результатами аналізу встановлено, що системи потокового СЕТ-шифрування недостатньо досліджені, а для їх подальшого розвитку необхідно будувати інформаційні технології проєктування систем захисту інформації.

В другому розділі удосконалено технологію побудови моделей некомутативних двохранрядних двооперандних СЕТ-операцій. Результати даного розділу забезпечують зменшення складності процесів моделювання некомутативних СЕТ-операцій. Даний ефект досягнуто за рахунок прямого переходу від побудованої моделі СЕТ-операції до моделі СЕТ-операції з переставленими операндами.

У третьому розділі удосконалено метод синтезу двохоперандних двохранрядних СЕТ-операцій. Удосконалений метод забезпечив можливість додаткового синтезу несиметричних двохоперандних двохранрядних операцій подвійного циклу.

В четвертому розділі удосконалюється метод побудови двохранрядних двооперандних операцій, які допускають перестановку операндів, на основі

об'єднання двохрозрядних однооперандних операцій криптографічного перетворення. Отриманий результат дозволяє синтезувати двохоперандні SET-операції, які допускають перестановку операндів без обмеження на розрядність операндів.

В п'ятому розділі досліджуються моделі генераторів псевдовипадкових послідовностей SET-операцій для побудови систем потокового шифрування. Будується модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних SET-операцій.

У висновках дисертації відображаються основні наукові і практичні результати, які отримав здобувач. Зміст і наповнення розділів узгоджується з метою та завданнями дисертаційного дослідження. Дисертаційна робота є завершеною науковою працею, в якій отримані наукові результати, змістовний аспект яких не був відомий раніше. Дана робота має теоретичне і практичне значення для створення інформаційних систем для дослідження і проектування перспективних малоресурсних систем захисту інформації.

5. Відсутність (наявність) порушень принципів академічної доброчесності

Ознайомившись із змістом дисертаційної роботи, можна зробити висновок, що робота виконана з дотриманням принципів академічної доброчесності. Результати наукових досліджень інших авторів супроводжуються посиланнями на їхні публікації і відокремлені від результатів здобувача. Наукові положення дисертації і висновки мають авторське обґрунтування. Ознак порушення академічної доброчесності не встановлено.

6. Повнота викладення дисертації в опублікованих працях

Основні результати дисертаційної роботи опубліковано у 16 друкованих працях, серед яких 7 статей у фахових виданнях України із них 2 статті в фахових журналах категорії А (проіндексовані в науково-метричній базі SCOPUS), 3 статті опублікованих за кордоном, із них одна включена до науково-метричної бази SCOPUS і належить до квартиля Q1, одноосібному розділі колективної монографії. Результати роботи доповідались та обговорювались на двох міжнародних науково-технічних конференціях, одній міжнародній науково-практичній конференції, одній науково-практичній конференції та міжнародному академічному форумі.

7. Зауваження та недоліки дисертації щодо її вмісту й оформлення

Доцільно відзначити деякі недоліки дисертаційної роботи.

1. Надмірна формалізація вхідних і вихідних даних в наведених алгоритмах (стор. 62, стор. 154 – 156) ускладнюють їх сприйняття і вимагають додаткового ознайомлення з специфічним описом моделей СЕТ-операцій, їх класифікацією, варіантами поєднання в процесі синтезу.

2. В наведеній ієрархічній архітектурі інформаційної системи вимоги до процесів (режимів) функціонування недостатньо формалізовані, що ускладнює сприйняття задекларованих можливостей щодо моделювання і дослідження на сьогоднішній день невідомих поточкових шифрів (рис.5.2, на стор. 149).

3. Не всі з розроблених автором моделей синтезу двохоперандних СЕТ-операцій використані автором при побудові макету інформаційної системи моделювання і дослідження двохоперандних операцій криптоперетворення інформації. Наприклад, моделі 5.40 – 5.42 на стор.139.

4. Для підвищення практичної цінності результатів дослідження доцільно було б передбачити можливість поєднання автоматизації процесу синтезу поточкових шифрів з автоматизацією оцінки результатів тестування з використанням відомих методик, наприклад NIST-STS.

5. Дисертаційна робота перевантажена математичними моделями, математичними перетвореннями над моделями і т.п., що ускладнює її сприйняття.

6. Основний недолік розробленої інформаційної системи – орієнтація на дуже вузьке коло потенційних користувачів. Адже користувач даної системи повинен бути фахівцем в інформаційних системах, програмуванні, криптографії, а також мати глибокі знання в прикладній дискретній математиці.

7. В роботі наявні стилістичні і орфографічні неточності.

Не зважаючи на вказані недоліки дисертаційна робота містить суттєві наукові результати, які є важливими для розвитку інформаційних систем і технологій, та заслуговує позитивної оцінки.

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

Дисертаційна робота Короткого Тимофія Костянтиновича “Ієрархічна інформаційна система моделювання і дослідження алгоритмів поточкового СЕТ-шифрування” є завершеним науковим дослідженням, в якому розв’язано науково-прикладне завдання підвищення продуктивності дослідження СЕТ-операцій при побудові перспективних стійких алгоритмів поточкового шифрування на основі розширення можливостей ієрархічної інформаційної системи моделювання і дослідження СЕТ-операцій за рахунок встановлення

нових і уточнення існуючих взаємозв'язків між моделями ієрархічних рівнів, які в сукупності забезпечать автоматизований синтез і аналіз симетричних та несиметричних однооперандних і багатооперандних СЕТ-операцій, а також генераторів їх псевдовипадкових послідовностей для потокового СЕТ-шифрування.

За актуальністю теми, науковою новизною і практичним значенням отриманих результатів, теоретичною обґрунтованістю, повнотою їх опублікування і апробації, та відповідністю спеціальності 126 – Інформаційні системи та технології дисертаційна робота відповідає вимогам до дисертацій на здобуття ступеня доктора філософії, встановленим “Порядком 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 січня 2022 р. № 44 зі змінами, та “Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради в Черкаському державному технологічному університеті” затвердженим вченою радою Черкаського державного технологічного університету 18 квітня 2022 р. (протокол № 14) зі змінами та доповненнями.

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

Рецензент:

завідувач кафедри
робототехнічних і телекомунікаційних
систем та кібербезпеки
Черкаського державного
технологічного університету,
доктор технічних наук, професор



Володимир ПАЛАГІН

Підпис Палагіна В.В. засвідчую:

Вчений секретар
Черкаського державного
технологічного університету,
кандидат технічних наук, доцент



Ірина МИРОНЕЦЬ