

РЕЦЕНЗІЯ

кандидата технічних наук, доцента

Розломій Інни Олександрівни

на дисертаційну роботу Підласого Дмитра Андрійовича

«Метод синтезу СЕТ-операцій на основі елементарних функцій операцій,

керованих інформацією»,

подану на здобуття ступеня доктора філософії

за спеціальністю 123 Комп'ютерна інженерія

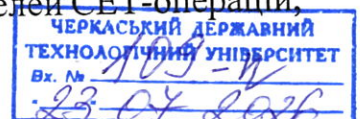
галузі знань 12 Інформаційні технології

1. Актуальність теми дисертаційної роботи.

Сучасний розвиток інформаційно-комунікаційних технологій, систем Інтернету речей, вбудованих платформ та бездротових мереж супроводжується стрімким зростанням кількості пристроїв, для яких необхідно забезпечити криптографічний захист за умов жорстких обмежень щодо обчислювальної потужності, обсягу пам'яті та енергоспоживання. Використання традиційних криптографічних алгоритмів у таких середовищах не завжди є ефективним через їх високу ресурсоемність, що обумовлює необхідність розвитку спеціалізованих методів малоресурсної криптографії.

Одним із перспективних напрямів розвитку потокового шифрування є використання криптографічних перетворень, побудованих на основі таблиць випадкових підстановок та СЕТ-операцій. Разом із тим, існуючі підходи переважно ґрунтуються на вже відомих моделях СЕТ-перетворень і не забезпечують достатньої варіативності криптографічних операцій без суттєвого ускладнення реалізації. Особливо актуальною залишається проблема побудови нових моделей СЕТ-операцій, здатних забезпечити підвищення кількості можливих криптографічних перетворень при збереженні низької обчислювальної складності.

У цьому контексті особливий інтерес становить використання операцій, керованих інформацією, коли процес криптографічного перетворення визначається не лише ключовою інформацією, а й самими вхідними даними. Такий підхід потенційно дозволяє суттєво розширити множину можливих підстановок, підвищити варіативність потокових шифрів та ускладнити криптоаналіз без істотного збільшення ресурсних витрат. Разом із тим, побудова подібних криптографічних механізмів потребує створення відповідного математичного апарату синтезу елементарних функцій та моделей СЕТ-операцій.



що робить даний напрям наукових досліджень достатньо складним і водночас актуальним.

Актуальність дисертаційної роботи Підласого Дмитра Андрійовича полягає у розв'язанні саме цієї науково-прикладної проблеми шляхом розроблення методу синтезу SET-операцій на основі елементарних функцій операцій, керованих інформацією, що забезпечує можливість подвійного керування процесом криптографічного перетворення, розширює множину використовуваних таблиць підстановки та підвищує варіативність малоресурсних потокових криптографічних систем. Запропонований підхід орієнтований на практичне застосування у комп'ютерних системах із обмеженими ресурсами та відповідає сучасним тенденціям розвитку малоресурсної криптографії.

Отже, тема дисертаційного дослідження є актуальною, оскільки спрямована на розвиток математичного та алгоритмічного забезпечення малоресурсних криптографічних систем, розширення можливостей потокового шифрування на основі SET-операцій та підвищення ефективності захисту інформації в сучасних комп'ютерних системах і мережах.

2. Наукова новизна результатів роботи.

Наукова новизна дисертаційної роботи:

- *вперше* запропоновано метод синтезу елементарних функцій операцій, керованих інформацією, на основі відомих дискретних моделей елементарних функцій, отриманих за результатами обчислювального експерименту, за допомогою встановлення і формалізації взаємозв'язків між дискретними змінними, що забезпечило можливість побудови повних множин дискретно-алгебраїчних і дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією для спрощення подальшого дослідження синтезу SET-операцій на основі елементарних функцій операцій, керованих інформацією;
- *вперше* побудовано метод синтезу 3Сі-квантових SET-операцій на основі елементарних функцій операцій, керованих інформацією шляхом синтезу базових груп симетричних однооперандних SET-операцій за критерієм простоти їх побудови та критерієм відмінності відповідних елементарних функцій, багатоваріантного представлення SET-операцій дискретно-казуальними моделями, мінімізації взаємозв'язків в кортежі однооперандних SET-операцій при побудові двооперандної SET-

операції, що забезпечило можливість подвійного управління процесом криптографічного перетворення при зменшенні складності реалізації SET-операцій.

- **удосконалено** системи потокового шифрування на основі випадкових підстановок шляхом застосування двохоперандних SET-операції на основі елементарних функцій операцій, керованих інформацією і генераторів модифікованих SET-операцій, що забезпечило можливість подвійного управління процесом криптографічного перетворення від ключової послідовності і від вхідної інформації, збільшило кількість таблиць підстановки до 192 (кількість SET-операцій в групі операцій на основі елементарних функцій операцій, керованих інформацією) для перетворення 3 Сі-квантів інформації (3 біт інформації). Стійкість результатів шифрування до статистичного криптоаналізу відповідає вимогам методики NIST STS.

3. Практичне значення одержаних результатів.

Практична цінність результатів дисертаційного дослідження полягає у наступному:

1. Розроблено методичне та алгоритмічне забезпечення синтезу SET-операцій на основі елементарних функцій операцій, керованих інформацією, що може бути використане при створенні малоресурсних криптографічних систем для захисту інформації у комп'ютерних системах, мережах та вбудованих пристроях.

2. Запропоновані моделі криптографічних перетворень забезпечують реалізацію подвійного керування процесом шифрування як від ключової послідовності, так і від вхідної інформації, що дозволяє підвищити варіативність криптографічних алгоритмів за рахунок використання до 192 таблиць підстановки та формування 4096 варіантів базових груп симетричних двохоперандних SET-операцій.

3. Практична реалізація запропонованих рішень забезпечує підвищення стійкості потокового шифрування до статистичного криптоаналізу, що підтверджено відповідністю результатів тестування вимогам методики NIST STS.

4. Практичну значущість отриманих результатів підтверджено впровадженням удосконаленої системи потокового шифрування на основі операцій, керованих інформацією, у програмному модулі захищеної системи

дистанційного керування наземним роботизованим комплексом «MOROZ-02L», що свідчить про можливість використання запропонованих рішень у спеціалізованих комп'ютерних системах.

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

Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 203 сторінки, 7 рисунків, 17 таблиць, список використаних джерел із 126 найменувань.

У першому розділі проаналізовано сучасний стан розвитку малоресурсної криптографії, розглянуто області її застосування, існуючі методи та засоби захисту інформації, особливості СЕТ-шифрування, а також обґрунтовано актуальність теми, сформульовано мету та основні завдання дисертаційного дослідження.

У другому розділі досліджено елементарні функції операцій, керованих інформацією, розроблено метод синтезу їх дискретно-алгебраїчних моделей та побудовано дискретно-казуальні моделі, що створюють математичну основу для подальшого синтезу СЕТ-операцій.

У третьому розділі розроблено метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. Досліджено результати моделювання, запропоновано підходи до формування базових груп симетричних СЕТ-операцій за різними критеріями та розроблено моделі синтезу груп СЕТ-операцій для використання у потоковому шифруванні.

У четвертому розділі розглянуто питання синтезу двохоперандних СЕТ-операцій та побудови криптографічних систем на їх основі. Запропоновано моделі дискретно-казуального подання двохоперандних СЕТ-операцій, наведено реалізацію криптографічних систем із подвійним керуванням процесом шифрування та виконано оцінювання їх криптографічних властивостей відповідно до вимог методики NIST STS.

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 дисертаційної роботи опубліковано в 15 наукових працях, серед яких 1 публікація з індексацією в наукометричній базі Scopus, 4 статтях у фахових виданнях України, 2 колективних монографіях, а також 3 публікації у матеріалах міжнародних науково-практичних конференцій. Наведений перелік публікацій свідчить про достатню апробацію основних результатів дисертаційного дослідження та їх оприлюднення в науковому середовищі.

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

Зауваження до роботи:

1. У дисертаційній роботі наведено значну кількість дискретно-алгебраїчних та дискретно-казуальних моделей елементарних функцій і SET-операцій. Для покращення сприйняття матеріалу доцільно було б доповнити роботу узагальнювальною схемою, яка відображала б взаємозв'язок між окремими етапами синтезу моделей та їх використанням при побудові криптографічної системи.

2. У четвертому розділі наведено результати статистичного тестування запропонованих криптографічних систем відповідно до методики NIST STS. Разом із тим, доцільно було б доповнити дослідження порівнянням запропонованого підходу з відомими сучасними малоресурсними потоковими алгоритмами за такими показниками, як швидкодія, обсяг пам'яті та обчислювальна складність.

3. Практична реалізація запропонованих методів продемонстрована на прикладі програмної реалізації системи потокового шифрування. Водночас більш повне уявлення про можливості практичного використання результатів надали б експериментальні дослідження на сучасних мікроконтролерах або інших апаратних платформах, орієнтованих на малоресурсні обчислення.

4. У роботі детально досліджено статистичні властивості сформованих шифрограм, однак питання криптостійкості до окремих видів сучасного

криптоаналізу (зокрема диференціального та лінійного) висвітлено меншою мірою. Включення такого аналізу дозволило б більш повно охарактеризувати безпекові властивості запропонованого методу.

5. У роботі використано значний математичний апарат, що забезпечує строгість викладу матеріалу. Разом із тим, окремі розділи містять велику кількість формальних моделей і позначень без їх попереднього узагальнення, тому введення коротких підсумкових схем або таблиць після ключових підрозділів покращило б сприйняття отриманих результатів.

6. У дисертації показано можливість використання запропонованих СЕТ-операцій у потоковому шифруванні, однак перспективним було б більш детально розглянути можливості їх інтеграції до інших криптографічних примітивів або протоколів захисту інформації, що окреслило б ширші напрями практичного застосування запропонованих результатів.

Зазначені зауваження не знижують наукової новизни, теоретичної цінності та практичного значення дисертаційної роботи. Вони мають переважно рекомендаційний характер і можуть бути враховані автором у подальших наукових дослідженнях та розвитку запропонованих методів.

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

Дисертаційна робота Підласого Дмитра Андрійовича на тему «Метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією» є завершеним науковим дослідженням, у якому розв'язано актуальне науково-прикладне завдання, пов'язане з розробленням методу синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, для підвищення варіативності малоресурсних поточкових шифрів та вдосконалення криптографічних систем із подвійним керуванням процесом шифрування.

За актуальністю, науковою новизною, практичним значенням, повнотою опублікування основних результатів і рівнем обґрунтованості висновків дисертація відповідає вимогам до дисертаційного дослідження на здобуття ступеня доктора філософії, визначеним чинним порядком присудження ступеня доктора філософії.

Дисертація може бути представлена для офіційного захисту в разовій спеціалізованій вченій раді, а її автор – Підласий Дмитро Андрійович –

заслуговує на присудження ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія галузі знань 12 Інформаційні технології.

Рецензент:

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

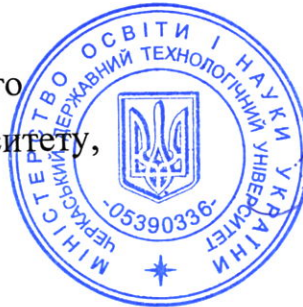


Інна РОЗЛОМІЙ

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

Учений секретар

Черкаського державного
технологічного університету,
к.т.н., доцент



Ірина МИРОНЕЦЬ