

ВІДГУК

офіційного опонента

на дисертаційну роботу Підласого Дмитра Андрійовича на тему «Метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією», подану на здобуття наукового ступеня доктора філософії за спеціальністю 123 – комп'ютерна інженерія галузі знань 12 – Інформаційні технології

1. Актуальність теми дослідження та зв'язок з науковими програмами, планами та темами.

В результаті розвитку інформаційно-комунікаційних технологій та зростання обсягів інформації в кіберпросторі проблема забезпечення криптографічного захисту інформації набуває особливої ваги. Традиційні криптографічні методи, що ґрунтуються на арифметиці з багаторозрядними числами, стикаються з обмеженнями щодо продуктивності, енергоефективності та необхідності паралельної обробки даних, особливо в умовах обмежених ресурсів. Крім того розвиток квантових обчислювальних засобів актуалізують пошук альтернативних підходів до побудови криптографічних перетворень. У цьому контексті наукові дослідження, спрямовані на розробку методів криптографічного захисту інформації на основі СЕТ-операцій, є своєчасними та науково обґрунтованими. Запропоновані в дисертаційній роботі рішення мають потенціал підвищення рівня криптостійкості та ефективності захисту інформації, що зумовлює їх практичну значущість для сучасних інформаційних та телекомунікаційних систем. Таким чином, тема дисертаційної роботи «Метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією» є актуальною.

Крім того, актуальність і практичне значення даної наукової роботи підтверджується виконанням двох науково-дослідних робіт: «Методи та засоби синтезу груп симетричних двухоперандних операцій криптографічного кодування для малоресурсних криптоалгоритмів» (ДР № 0121U114390); «Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування» (ДР № 0121U114389) у яких автор брав участь як виконавець.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій.

Наукові положення, висновки і рекомендації дисертаційної роботи Підласого Дмитра Андрійовича є обґрунтовані, підтверджені коректним використанням основ теорії СЕТ-шифрування, дискретної математики, теорії алгоритмів, методів комп'ютерного моделювання та математичної статистики.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій забезпечено комплексним характером досліджень, публікаціями у фахових виданнях категорії Б, обговоренням висунутих наукових положень та отриманих висновків на міжнародних та національних науково-технічних конференціях. Отримані результати відповідають висунутих теоретичним положенням.

3. Наукова новизна результатів роботи.

На основі аналізу результатів дисертаційної роботи Підласого Д.А. можна зробити висновок, що найбільш суттєвими науковими результатами, які одержані в дисертації, є такі:

1) 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 СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією;

2) вперше побудовано метод синтезу 3Сі-квантових СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, шляхом синтезу базових груп симетричних однооперандних СЕТ-операцій за критерієм простоти їх побудови та критерієм відмінності відповідних елементарних функцій, багатоваріантного представлення СЕТ-операцій дискретно-казуальними моделями, мінімізації взаємозв'язків в кортежі однооперандних СЕТ-операцій при побудові двооперандної СЕТ-операції, що забезпечило можливість подвійного управління процесом криптографічного перетворення при зменшенні складності реалізації СЕТ-операцій;

3) удосконалено системи потокового шифрування на основі випадкових підстановок шляхом застосування двохоперандних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, і генераторів модифікованих СЕТ-операцій, що забезпечило можливість подвійного управління процесом криптографічного перетворення від ключової послідовності і від вхідної інформації, збільшило кількість таблиць підстановки до 192 (кількість СЕТ-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

4. Зміст дисертації та відповідність встановленим вимогам

Дисертаційна робота є завершеною науковою працею, яка містить вступ, чотири розділи, висновки, список використаних джерел із 103 найменувань та 4 додатків на 14 сторінках. Дисертація має 203 сторінки, з яких 145 містять основний текст. У роботі є 7 рисунків і 17 таблиць. Побудова дисертації відповідає прийнятим для наукового дослідження вимогам.

У **вступі** обґрунтовано актуальність теми досліджень; показано зв'язок роботи з науковими програмами, планами, темами; сформульовано мету та основні задачі досліджень; подано наукову новизну і практичне значення отриманих результатів; визначено особистий внесок здобувача; наведено дані про апробацію, публікації та використання результатів дослідження.

У **першому розділі** проаналізовано основні області застосування малоресурсного захисту та методи і засоби його реалізації. Детально проаналізовано відомі методи і засоби мало ресурсного СЕТ-шифрування. На основі проведеного аналізу та встановлених недоліків сформульована мета і завдання дослідження.

У **другому розділі** досліджуються елементарні функції операцій, керованих інформацією. Розробляється метод синтезу елементарних функцій операцій, керованих інформацією представлених дискретно-алгебраїчними і дискретно-казуальними моделями.

Третій розділ присвячено побудові і дослідженню моделей СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. Розробляється метод синтезу 3Сі-квантових СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

Четвертий розділ присвячено синтезу двохоперандних СЕТ-операцій, керованих інформацією та побудові і дослідженню криптографічних систем на їх основі. Удосконалюються системи потокового шифрування на основі випадкових підстановок шляхом застосування двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, і генераторів модифікованих СЕТ-операцій.

У **висновках** стисло сформульовано основні наукові та практичні результати дисертаційної роботи.

У **додатках** містяться перелік тестів для переварки криптографічних систем та результати тестування, акти впровадження результатів дисертаційної роботи та список публікацій, в яких опубліковані основні наукові результати дисертації.

Зміст дисертаційної роботи відповідає її назві. Дисертація написана науковою мовою та оформлена відповідно до існуючих нормативних документів. Таким чином, усі положення винесені на захист, висвітлені в тексті дисертації.

5. Оформлення дисертації.

Дисертація має завершену обґрунтовану структуру та форму представлення, що повною мірою розкриває досягнуту мету та виконані завдання дослідження. Дисертаційна робота оформлена у відповідності з чинними вимогами, що ставляться до такого виду робіт.

6. Практичне значення результатів дисертаційної роботи.

Практичне значення результатів дисертаційної роботи полягає у доведенні розроблених методів і моделей до побудови криптографічних систем з подвійним управлінням процесом криптографічного перетворення, які забезпечують псевдовипадкове використання 192 таблиць підстановки для перетворення 3 Сі-квантів інформації.

Практична цінність роботи підтверджується впровадженням її результатів в модулі потокового шифрування системи управління роботизованим комплексом "MOROZ-02L"

7. Повнота викладу результатів в опублікованих працях, апробація роботи.

Основні результати дисертації достатньо повно **відображені** в 15 друкованій праці, з них, 4 статтях у фахових виданнях України, 1 статті яка проіндексована в науково-метричній базі SCOPUS, 2 колективних монографіях, в одній з яких опубліковано одноосібний розділ, 4 статтях опублікованих за кордоном, 3 тезах доповідей на міжнародних і вітчизняних конференціях.

Опубліковані роботи в повній мірі охоплюють основні результати дисертаційних досліджень. Дисертація є завершеною кваліфікаційною роботою з науковими положеннями, які характеризуються внутрішньою єдністю. Аналіз сукупності наукових результатів, поданих у роботі Підласого Д.А., дає змогу зробити висновок про їх цілісність і засвідчує особистий внесок автора в науку щодо розроблення методу синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

8 Відсутність (наявність) порушень принципів академічної доброчесності.

Ознайомившись із змістом дисертаційної роботи можна зробити висновок, що наукові положення дисертації і висновки мають авторське обґрунтування. Ознак порушення академічної доброчесності не встановлено.

9. Зауваження до дисертації та реферату.

Незважаючи на належний рівень виконаних наукових досліджень, до дисертаційної роботи виносяться такі зауваження:

1. Розділ 1 дисертації доцільно було б доповнити описом сучасних методів криптоанализу, а не константувати використання пакету NIST_STS, для оцінки результатів дисертаційного дослідження в розділі 4, без обґрунтування його вибору.

2. Наведені в підрозділі 1.1 класифікації які є відомими і не несуть інформаційного навантаження при викладенні автором отриманих результатів, тому їх можна було б не наводити.

3. В тексті дисертації відсутнє пояснення базових СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, та не сконцентровано увагу на відмінностях даних операцій.

4. В розділі 2, при побудові функціональних схем позначення елементарних функцій не зовсім коректне ($f_{23}, f_{43}, \dots$), і вони відрізняються від позначених елементарних функцій в розділах 3 і 4 ($f_{23}(x), f_{43}(x), \dots$).

5. Результати моделювання і аналізу багатоваріантного представлення СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією (ст. 83-86) в подальших дослідженнях не використовуються, тому доцільно було б обмежитися наведенням виявленої властивості даних операцій, а табл. 3.1 винести в додатки.

6. Зведені результати тестування криптографічних систем реалізованих з застосуванням двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією наведені на (ст. 166) без додаткового пояснення.

7. На мою думку, було б доцільно помимо стійкості запропонованих систем до лінійного криптоаналізу оцінити також швидкість шифрування-розшифрування інформації. Дана оцінка була б одним із показників якості отриманих наукових і практичних результатів дисертаційного дослідження.

8. У дисертаційній роботі є стилістичні і граматичні неточності.

Вказані зауваження і недоліки не впливають на загальну позитивну оцінку дисертаційного дослідження, а також не зменшують наукову новизну та практичну цінність представленої роботи.

10. Загальна оцінка роботи, її відповідність встановленим вимогам.

Дисертаційна робота Підласого Дмитра Андрійовича на тему «Метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією» є завершеною кваліфікаційною науковою роботою, яка містить нові науково обґрунтовані положення, які в сукупності вирішують актуальну науково-прикладну задачу підвищення варіативності малоресурсних поточкових шифрів випадкової підстановки за рахунок розробки і впровадження методу синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, які забезпечують можливість подвійного управління процесом криптографічного перетворення, як від ключової послідовності, так і від вхідної інформації, при збільшенні кількості таблиць підстановки, що реалізуються в криптоалгоритмі.

Вважаю, що за актуальністю теми, повнотою проведеного дослідження, науковою новизною і практичною цінністю одержаних результатів робота відповідає вимогам 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, та вимогам до оформлення дисертації, затвердженим наказом МОНУ від 12.01.2017 р. № 40, а її автор, Підласий Дмитро Андрійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 123 – комп'ютерна інженерія галузі знань 12 – Інформаційні технології

Офіційний опонент

декан факультету комп'ютерних інформаційних технологій

Західноукраїнського національного університету,

доктор технічних наук, доцент

Ігор ЯКИМЕНКО

