

РЕЦЕНЗІЯ

кандидата технічних наук, доцента

Миронюк Тетяни Василівни

на дисертаційну роботу Підласого Дмитра Андрійовича

«Метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією», подану на здобуття ступеня доктора філософії

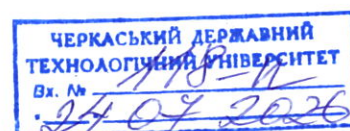
за спеціальністю 123 – Комп'ютерна інженерія

галузі знань 12 – Інформаційні технології

1. Актуальність теми дисертації

В нашій державі системи накопичення, обробки інформації та реалізація доступу до них з використанням мережних технологій швидко розвиваються і комерціалізуються. Інформацію сьогодні, взагалі, слід розглядати як стратегічний продукт широкого попиту. Тривалий час розвиток засобів захисту інформації був орієнтований на державні структури, особливо на військову сферу і дипломатію. Однак інформаційний вибух останніх років висунув на одне з перших місць проблему захисту величезної кількості конфіденційної інформації, що обробляється і передається в корпоративних комп'ютерних системах і мережах, а також глобальній мережі Internet. Особливо гостро питання вискоєфективного захисту інформаційних ресурсів стало після введення військового стану. Не дивлячись на зусилля великої кількості вітчизняних і зарубіжних науковців, залишається цілий ряд невирішених задач, що відіграють важливу роль у розвитку криптології та захисту інформації. Однією з таких задач є підвищення якості систем захисту інформації в комп'ютерних системах на основі використання операцій, керованих інформацією. Виходячи з цього можна стверджувати, що тема дисертаційної роботи «Метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією» є актуальною.

Результати дисертаційної роботи використані при виконанні науково-дослідних робіт, 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 в якості виконавця.



2. Наукова новизна отриманих результатів.

Наукова новизна дисертаційного дослідження полягає в наступному:

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 двохоперандної 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 3Сі-квантів інформації (3 біт інформації). Стійкість результатів шифрування до статистичного криптоаналізу відповідає вимогам методики NIST STS.

3. Практичне значення одержаних результатів.

Практична цінність дисертаційної роботи полягає в наступному:

1. В побудові придатних в практиці захисту комп'ютерних криптографічних систем нових моделей СЕТ-операцій, їх функціональних схем

і криптографічних алгоритмів впровадження потокового СЕТ-шифрування на основі елементарних функцій операцій, керованих інформацією.

2. Отримані результати забезпечують побудову криптографічних систем з подвійним управлінням процесом криптографічного перетворення і збільшують варіативність криптографічних алгоритмів шляхом використання 192 таблиць підстановки для перетворення 3Сі-квантів інформації. Для побудови симетричних криптографічних систем може бути використано 4096 варіантів двооперандних СЕТ-операцій, які реалізують лише симетричні однооперандні СЕТ-операції;

3. Впровадженням система потокового СЕТ-шифрування, на рівні програмного модуля, в систему управління роботизованим комплексом "MOROZ-02L".

4. Структура роботи, оцінка змісту дисертації та її завершеність

Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків.

У вступі показано актуальність теми дослідження, сформульована мета, предмет і об'єкт наукового дослідження, визначена наукова новизна і практичне значення результатів роботи, наведено методи, відомості про публікації, особистий внесок здобувача та інформація щодо апробації результатів на міжнародних і вітчизняних конференціях.

У першому розділі розглянуті області застосування малоресурсного шифрування, проаналізовано методи та засоби малоресурсного захисту інформації. Досліджено поняття малоресурсного СЕТ-шифрування, встановлено можливості його подальшого розвитку. Сформульовано мету і завдання дисертаційного дослідження.

Другий розділ присвячено дослідженню елементарних функцій операцій, керованих інформацією. На основі аналізу функціональних схем досліджуваних функцій розглядається їх багатоваріантне представлення. Розробляється метод синтезу моделей елементарних функцій операцій, керованих інформацією, на основі дискретно-алгебраїчного і дискретно-казуального представлення. Робиться висновок про перспективність використання дискретно-казуального представлення в подальших дослідженнях

У третьому розділі розглядаються варіанти побудови базових симетричних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. Досліджуються алгоритми побудови груп СЕТ-

операцій на основі елементарних функцій операцій, керованих інформацією, за критеріями простоти їх побудови та відмінності відповідних елементарних функцій. Розробляється метод синтезу групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

В четвертому розділі синтезуються дискретно-казуальні моделі двохоперандних СЕТ-операцій на основі симетричних базових груп, які відповідають критеріям простоти побудови та відмінності відповідних елементарних функцій. Будуються криптографічні системи на основі синтезованих дискретно-казуальних моделей СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. Проводиться оцінка стійкості результатів шифрування даними системами до лінійного криптоаналізу.

У висновках відображаються основні наукові і практичні результати, дисертаційного дослідження.

Представлені у розділах результати відповідають меті та поставленим завданням дисертаційного дослідження. Дана робота має теоретичне і практичне значення для перспективних малоресурсних систем комп'ютерної криптографії.

5. Повнота викладення дисертації в опублікованих працях.

Основні положення дисертації опубліковано у 15 друкованих працях, зокрема: у 4 статтях фахових видань України; статті опубліковані за результатами конференції, яку проіндексовано в науково-метричній базі SCOPUS; 2 колективних монографіях, в одній з яких опубліковано одноосібний розділ; в матеріалах двох міжнародних наукових конференцій, і науково-практичній конференції Харківського національного університету Повітряних Сил ім. Івана Кожедуба.

6 Відсутність (наявність) порушень принципів академічної доброчесності.

Дисертаційна робота містить коректні посилання на використані джерела інформації та опубліковані результати наукових досліджень здобувача. Ознак порушення академічної доброчесності не встановлено.

7. Зауваження та недоліки дисертації щодо її вмісту й оформлення.

1. При визначенні мети та задач дослідження автор визначає актуальність підвищення варіативності малоресурсних потокових шифрів за рахунок впровадження методу синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. Але, нажаль, не розглядає вплив варіативності на стійкість і швидкість криптоалгоритмів.

2. При аналізі малоресурсних криптографічних алгоритмів у першому розділі автор дуже багато уваги приділяє загальному їх опису. При цьому, нажаль, практично не наводить показників для їх порівняльної оцінки.

3. У розділі 2 в таблицях 2.1 (стор. 47) наведено інформацію без достатніх пояснень, що ускладнює сприйняття подальшого матеріалу.

4. Розділ 2 перевантажений варіантами побудови карт Карно та варіантами побудови функціональних схем елементарних функцій операцій, керованих інформацією. На мою думку, було б доцільно представити детальне дослідження варіантів побудови однієї елементарної функції і обмежитися детальним описом дискретно-алгебраїчних моделей, які наведені в табл.2.32 на стор. 72.

5. В тексті дисертації відсутнє трактування терміну «дискретно-казуальна логіка» та не наведені її відмінності від «дискретно-каузальної логіки».

6. Розділ 3 перевантажений формалізованими алгоритмами синтезу базових груп та прикладами їх реалізації. На мою думку, частину даних алгоритмів (наприклад ст.. 101 -103, 107-111, 118-122), доцільно було б винести в додатки.

7. В підрозділі 4.4 доцільно було б не обмежуватися лише формальним описом запропонованих криптоалгоритмів обміну конфіденційною інформацією між абонентами, а доповнити його прикладами перетворення інформації при їх реалізації або представити дані приклади в додатках для підвищення практичної цінності роботи.

8. В роботі наявні стилістичні і орфографічні помилки та неточності.

Вказані недоліки не впливають на наведені наукові і практичні результати дисертаційної роботи, яка заслуговує позитивної оцінки.

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

Дисертаційна робота Підласого Дмитра Андрійовича «Метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих

інформацією» є завершеним науковим дослідженням в якому розв'язано науково-прикладне завдання підвищення варіативності малоресурсних потокових 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.

За актуальністю теми, науковою новизною і практичним значенням отриманих результатів, теоретичною обґрунтованістю, повнотою їх опублікування і апробації, та відповідністю спеціальності 123 – Комп'ютерна інженерія 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, а також “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, Підласий Дмитро Андрійович заслуговує на присудження ступеня доктора філософії за спеціальністю 123 – комп'ютерна інженерія.

Рецензент:

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

Тетяна МИРОНЮК

Підпис Палагіна В.В. засвідчує:

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



Ірина МИРОНЕЦЬ