ВІДГУК

офіційного опонента на дисертаційну роботу

Лади Наталії Володимирівни

«Метод синтезу операцій потокового шифрування з точністю до перестановки»,

представлену на здобуття наукового ступеня

кандидата технічних наук

за спеціальністю 05.13.21 – системи захисту інформації

Актуальність

Забезпечення конфіденційності, цілісності, доступності, захисту від несанкціонованого доступу, тощо на практиці забезпечується застосуванням механізмів шифрування даних. Використання блокових симетричних шифрів має ряд недоліків: достатньо велика складність перетворень при шифруванні, недостатня швидкодія прямих та зворотних перетворень, не можливість розпаралелювання процесів крипто перетворень. У той час, як у ряді застосувань необхідно забезпечувати швидкодії в десятки та сотні Гбіт/с. Розв'язання цього протиріччя покладається на потокові симетричні перетворення - потокові симетричні шифри (ПСШ).

Зважаючи на переваги ПСШ, на міжнародному рівні проведено та виконано ряд науково-практичних результативних проектів – Nessie, eSTREAM, створено програмні потокові шифри (HC 128, Rabbit, Salsa20/12, Sosemanuk), апаратні потокові шифри (F-FCSR-H v2, Grain v1, MISKEY v2, Trivium). Для забезпечення гарантованої (обчислювальної) стійкості ПСШ гама шифрування повинна мати достатній період повторення та допустиму величину ймовірності перекриття шифру. Гама шифруюча генерується на основі початкового ключа та вектору ініціалізації. При організації зв'язку кожного разу на першому етапі здійснюється передача вектору ініціалізації , яка разом із ключем визначає правило формування гам зашифрування та розшифрування.

Дисертаційна робота Лади Наталії Володимирівни присвячена **актуальним питанням** побудови криптографічних перетворень для потокового шифрування на основі використання модифікованих операцій додавання за модулем два з точністю до перестановки, які задовольняють вимогам статистичних властивостей і структурній скритності гами шифруючої. Актуальність дисертаційної роботи визначається необхідністю розробки національного стандарту потокового шифру та підтверджується науково-дослідною роботою

"Синтез операцій криптографічного перетворення з заданими характеристиками" (державний реєстраційний номер № 0116U008714), в якій автор був виконавцем.

Метою дисертаційної роботи є підвищення криптографічної стійкості потокового шифрування на основі модифікованих операцій додавання за модулем два з точністю до перестановки. Для досягнення поставленої мети сформульовано основні задачі дослідження, які в роботі послідовно розв'язано. У результаті це дозволило дисертанту розробити метод синтезу модифікованих операцій додавання за модулем два з точністю до перестановки для застосування в потокових симетричних перетвореннях.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Ступінь обґрунтованості нових положень, висновків і рекомендацій у дисертації обумовлена коректністю застосування методів дискретної математики, теорії алгоритмів, теорії графів, теорії груп перестановки для розробки методу синтезу модифікованих операцій додавання за модулем два з точністю до перестановки, методу підвищення стійкості та надійності потокового шифрування.

Достовірність основних положень та висновків підтверджено тестуванням розроблених модифікованих операцій додавання за модулем два з точністю до перестановки на основі застосування програмних засобів.

Ідентичність змісту автореферату й основних положень дисертації

У авторефераті дисертації з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертації. Структура дисертації відповідає вимогам, які ставляться до кандидатських дисертацій. Дисертаційна робота складається зі вступу, чотирьох розділів і висновків, має загальний обсяг 194 сторінок, з яких 160 сторінок основного тексту, містить 70 рисунків, 43 таблиць, список використаних джерел з 167 найменувань, 11 додатків на 21 сторінці.

У першому оглядовому розділі виконано аналіз існуючих основних операцій, на основі яких будуються системи криптографічного захисту інформації, обґрунтовується необхідність вдосконалення захисту інформації в інформаційно-телекомунікаційних системах.

У другому розділі запропоновано модель симетричних та несиметричних модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки операндів на основі матричних алгоритмів, обчислені

цикли криптоперетворень.

У третьому розділі запропоновано метод синтезу операцій додавання за модулем два з точністю до перестановки результатів виконання операції, який забезпечує синтез модифікованих операцій, придатних для криптографічних перетворень, та уніфікує процес знаходження взаємозв'язків між матричними алгоритмами та синтезованими модифікованими операціями при їх взаємному використанні в криптографічних перетвореннях, перевірено коректність отриманих результатів.

У четвертому розділі запропоновано метод підвищення стійкості та надійності потокового шифрування на основі застосування синтезованої групи модифікованих операцій, проведено оцінку статистичних властивостей результатів шифрування з використанням пакету NIST_STS.

Для основних положень дисертації та змісту автореферату характерна повна ідентичність.

Наукове та практичне значення результатів дисертаційної роботи

Наукова новизна отриманих результатів дисертаційної роботи, на мою думку полягає в наступному:

1. Вперше розроблено модель симетричних та несиметричних модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки операндів на основі матричних алгоритмів, що дає змогу формалізувати встановлені взаємозв'язки між матричними алгоритмами та синтезованими операціями при їх взаємному використанні в криптографічних перетвореннях та довести їх коректність.

2. Вперше розроблено метод синтезу операцій додавання за модулем два з точністю до перестановки результатів виконання операції, яка забезпечує синтез модифікованих операцій, придатних для криптографічних перетворень, та уніфікує процес знаходження взаємозв'язків між матричними алгоритмами та синтезованими модифікованими операціями при їх взаємному використанні в криптографічних перетвореннях.

3. Вперше розроблено метод підвищення надійності потокового шифрування на основі застосування групи модифікованих операцій додавання за модулем два з точністю до перестановки шляхом використання додаткової гамуючої послідовності для вибору операцій на кожному етапі шифрування, що надає можливість забезпечити збільшення надійності до 12,5%, а при однократних відмовах до 41% і забезпечити формування зашифрованої гамуючої послідовності при відмові вхідної відкритої інформації.

Практичне значення результатів дисертації полягає у наступному:

1. Побудовано алгоритми функціонування, структури, схеми реалізацій криптоперетворень на основі матричних алгоритмів операції додавання за модулем два з точністю до перестановки, визначені властивості крипто перетворень.

2. Побудовано схему потокового шифрування з використанням групи модифікованих операцій криптографічного додавання за модулем два.

3. Отримано оцінки статистичних властивостей результатів шифрування на основі пакету тестів NIST_STS.

Результати дисертаційної роботи впроваджені у державному підприємстві «Науково-виробничий комплекс «ФОТОПРИЛАД» (м. Черкаси), НДІ «Акорд» та в навчальний процес Черкаського державного технологічного університету, Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ», Кіровоградського національного технічного університету.

Повнота викладу результатів дисертаційної роботи в опублікованих працях та їх апробація

Результати виконаних досліджень опубліковано у 7 статтях у фахових виданнях, що входять до переліку МОН України, 7 матеріалах і тезах наукових конференцій, 2 колективних монографіях.

Дисертація Лади Н.В. має достатній рівень апробації на наукових конференціях і семінарах. Опубліковані праці повністю відображають зміст та висновки дисертаційної роботи.

Зауваження

1. На мою думку назва першого розділу «ПРОБЛЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ» не вдала, так як має узагальнене визначення, та не відображає проблематику дослідження щодо базових операцій для побудови крипто перетворень за темою роботи. Назви другого, третього, четвертого розділів практично співпадають та не відповідають тематично цільовим дослідженням.

2. В роботі використовуються поняття «якість систем потокового шифрування», «якість шифрування», «надійность роботи» що не є технічними показниками. Бажано було визначити показники за якими робиться оцінка щодо порівняння та переваг розроблених методів та визначити як ці показники пов'язані з вимогами до реалізації.

3. Для підтвердження достовірності отриманих результатів в роботі не представлено приклади обчислення потокового шифрування з використанням

групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки та відсутні чисельні оцінки щодо підвищення секретності шифрування за запропонованим методом побудови потокового шифру.

4. Висновки за розділами мають констатуючий характер, не представлені кількісні та якісні оцінки отриманих результатів.

5. В роботі є деякі помилки технічного характеру, наприклад в таблиці 4.15 на стор 133, щодо позначення операндів, додатки A, B, C, D не містять пояснюючих коментарів, що ускладнює їх розуміння.

Висновки

Зазначені недоліки не є суттєвими та критичними і не впливають на загальну позитивну оцінку здобувача. У цілому дисертаційна робота Лади Наталії Володимирівни є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для забезпечення секретності та надійності систем потокового шифрування конфіденційної інформації.

Вважаю, що дисертаційна робота «Метод синтезу операцій потокового шифрування з точністю до перестановки» повністю відповідає вимогам «Порядку присудження наукових ступенів», затвердженого Постановою КМ України від 24.07.2013р. №567 (із змінами, внесеними згідно з Постановами КМ України №656 від 19.08.2015, №1159 від 30.12.2015 №567 від 27.07.2016р.), а її автор Лада Наталія Володимирівна заслуговує присудження наукового ступеня кандидата технічних наук за науковою спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент
завідувач кафедри безпеки інформаційних технологій
Харківського національного університету радіоелектроніки,

доктор технічних наук, професор Г.З. Халімов

ПІДПИС ЗАСВІДЧУЮ:
Начальник відділу кадрів
«12» 07 2018.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ
ВІДДІЛ КАДРІВ №1
№02071107