ВІДГУК

офіційного опонента на дисертаційну роботу

Бреус Роксолани Василівни

«Генерація псевдовипадкових послідовностей операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда»,

представлену на здобуття наукового ступеня

кандидата технічних наук

за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

1. Актуальність теми.

Криптографічні засоби захисту інформації в комп'ютерних системах і мережах на сьогоднішній день є одними з основних. Проте існуючі алгоритми шифрування не завжди забезпечують необхідних вимог крипостійкості, а самі засоби необхідної оперативності доступу, особливо при захисті великих обсягів інформації. Все це створює необхідні передумови і робить актуальною розробку методів комп'ютерного шифрування інформації, які б забезпечували побудову стійких до зламу шифрів, і створення високопродуктивних засобів шифрування орієнтованих на захист великих обсягів інформації.

Одним із можливих шляхів підвищення якості доступу до конфіденційної інформації може бути забезпечено за рахунок високошвидкісної генерації псевдовипадкових послідовностей операцій прямого і оберненого криптографічного перетворення інформації. Використання двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування, в генерованих послідовностях, забезпечує досягненні максимальної невизначеності потокового шифрування. З цього випливають задачі наукового обґрунтування можливості генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда: розробити метод синтезу обернених операцій; розробити метод синтезу групи операцій і на їх основі розробити методу генерації псевдовипадкових послідовностей прямих і обернених операцій на основі перетворення другого операнда.

Актуальність і особливу значимість теми дисертаційного дослідження

Бреус Роксолани Василівни підкреслює її зв'язок з науково-дослідними роботами «Синтез операцій криптографічного перетворення з заданими характеристиками» (ДР № 0116U008714), «Розробка методів та засобів оцінки ефективності соціоінжинірингу» (ДР № 0116U008715).

Таким чином, враховуючи наведені аргументи, актуальність теми дисертаційного дослідження Бреус Роксолани Василівни «Генерація псевдовипадкових послідовностей операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда» не викликає жодних сумнівів.

2. Ступінь обґрунтованості наукових положень дисертації та їх достовірність. Основні наукові результати дослідження, запропонований методу синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда; розроблення методу синтезу групи двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі перетворення другого операнда відомої операції; розроблення методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда достатньо обґрунтовані та не викликають сумнівів. Достовірність наукових положень дисертації забезпечується:

- використанням в процесі досліджень методів дискретної математики, теорії інформації, комп'ютерної криптографії, теорії ймовірності і математичної статистики, логіки. теорії алгоритмів і теорії цифрових автоматів;
- наведеною в розділах 2, 3 і 4 системою формальних методик і перетворень, які забезпечують побудову дискретних моделей операцій, які співпадають з результатами комп'ютерного моделювання;
- відповідністю проведених теоретичних розрахунків результатам впровадження.

3. Найбільш вагомі наукові результати одержані здобувачем особисто.

У дисертаційній роботі вирішена актуальна науково-технічна задача, яка полягає в підвищенні швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда.

4. Наукова новизна отриманих результатів полягає в наступному:

- вперше розроблено метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда шляхом реалізації моделі автомата побудови другого операнда оберненої операції, що забезпечило можливість практичного застосування даних операцій;
- вперше розроблено метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда відомої операції шляхом виконання над ним двохрозрядної одноопераднної операції, що забезпечило можливість збільшення варіативності криптопримітивів при практичному застосуванні даних операцій;
- вперше розроблено метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда, що дозволяє значно спростити процес дослідження та синтезу групи операцій строгого стійкого криптоперетворення та робить можливим використання його при вдосконаленні методу підвищення криптостійкості і надійності потокового шифрування.

5. Практична цінність результатів полягає в доведенні розроблених методів до дискретних моделей операцій та алгоритмів автоматичної генерації псевдовипадкових послідовностей операцій строгого стійкого кодування для систем потокового комп'ютерного шифрування, що дозволило розширити варіативність криптографічних перетворень за рахунок збільшення кількості

операцій з 12 до 24, синтезувати операцій на 15–20 % швидше порівняно з табличним методом синтезу, а також забезпечити період псевдовипадкової послідовності операцій, який складає $(24!)^2$.

Додатково практична цінність дисертаційного дослідження підтверджується наведеними в додатках дисертації актами впровадження у навчальний процес Черкаського державного технологічного університету та КНП «Черкаська міська консультативно-діагностична поліклініка» (філія №2), ТОВ «Нова Пошта», ПАТ «Черкасиобленерго».

6. Оцінка змісту та завершеності роботи. Дисертаційна робота Бреус Роксолани Василівни складається зі вступу, чотирьох розділів, висновків (загалом 154 сторінки основного тексту), списку використаних джерел (127 найменування), додатків (8 сторінок).

Дисертаційна робота побудована логічно правильно, розділи та підрозділи роботи взаємопов'язані та чітко спрямовані на досягнення задекларованої мети. В цілому, вважаю, що дисертаційне дослідження є завершеною науковою роботою, яка знайшла практичне застосування в навчальному процесі та на підприємствах, що підтверджується актами впровадження.

У додатках до дисертації автором наведені акти впровадження результатів дисертаційного дослідження та обов'язковий додаток.

7. Основні наукові результати, що отримані в дисертації, викладені здобувачем у 10 друкованих працях, у тому числі: в 4 статтях у фахових виданнях України, 1 статті в закордонному виданні; колективній монографії, в матеріалах трьох міжнародних науково-технічних конференцій та в збірнику матеріалів міжнародного симпозіуму, проіндексованому в Scopus.

8. Автореферат дисертації оформлений згідно з вимогами положення про "Порядок присудження наукових ступенів". Зміст автореферату в достатній мірі відображає основні положення дисертаційної роботи.

9. Зауваження по дисертації.

1. Матеріали підрозділу «Проблеми комп'ютеризованого захисту інформації в Україні» в подальших дослідженнях не використовуються. Автору було б доцільно при аналізі сучасного стану захисту інформації в комп'ютерних системах і мережах приділити більше уваги швидкості криптоперетворення, як однієї з основних причин необхідності вдосконалення саме систем потокового шифрування.

2. По першому розділу, слід відмітити, відсутність порівняльного аналізу одно та двохоперандних операцій криптоперетворення виходячи з особливостей їх застосування в комп'ютерній криптографії. На мою думку автором проведено дуже стислий огляд розвитку досліджень, пов'язаних з побудовою та використанням двохоперандних двохрозрядних операцій строгого стійкого криптографічного кодування.

3. В підрозділі 2.1. «Технологія дослідження взаємозв'язків між прямими і оберненими двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування» вхідні дані для проведення дисертаційного дослідження зведені до таблиці без додаткових пояснень. Посилання автора на свої публікації без однозначного трактування в роботі використаних позначень в наведених 24 дискретних моделях значно зменшує інформативність табл. 2.1.

4. В третьому розділі доведення коректності методу синтез груп двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі перетворення другого операнда відомої операції виконане для декількох груп на повних множинах операцій. Доцільно було б обмежитися лише декількома прикладами взаємоперетворення операцій, зробивши посилання на інші аналогічні приклади винесені в додатки.

5. За своєю структурою робота перевантажена математичними викладками побудови моделей при недостатньому їх описі, що погіршує сприйняття отриманих результатів.

6. На мою думку підрозділ 4.3 необхідно було б доповнити формалізованими моделями генерації операцій, а рис. 4.4 – рис.4.7, на яких наведено варіанти генерації псевдовипадкових послідовностей операцій використати для пояснення цих моделей.

7. У четвертому розділі, автор не розкрив особливості реалізації отриманих результатів, лише наведена структурна схема удосконаленого методу підвищення стійкості та надійності потокового шифрування шляхом генерації псевдовипадкових послідовностей прямих та обернених операцій криптоперетворення, приводяться лише переваги та недоліки даного рішення.

8. В дисертації і автореферати є несуттєві граматичні та стилістичні неточності які не впливають на якість виконаного наукового дослідження.

10. Висновок. Дисертаційна робота Бреус Роксолани Василівни «Генерація псевдовипадкових послідовностей операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда», представляє собою завершену наукову роботу на актуальну тему, а отримані результати вирішують важливу науково-технічну задачу підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда.

Дисертаційна робота, представлена до розгляду, відповідає вимогам щодо кандидатських дисертацій, а її автор Бреус Роксолана Василівна заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент:
професор кафедри інформаційних
технологій факультету № 4
Харківського національного університету
внутрішніх справ Міністерства внутрішніх справ України,
доктор технічних наук, професор

О.О. Можаєв

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ПІДПИС ЗАСВІДЧУЮ
Відділ документування службової діяльності ХНУВС
"19" 01 2021 р.