ВІДГУК

офіційного опонента на дисертаційну роботу

Бабенко Віри Григорівни

«Методологія синтезу операцій перетворення інформації для комп'ютерної криптографії»,

представлену на здобуття наукового ступеня доктора технічних наук

за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

1. Актуальність теми. Криптоперетворення даних є найефективнішим засобом забезпечення конфіденційності інформації та контроля її цілісності в сучасних комп'ютерних системах та мережах при забезпеченні діяльності сучасного суспільства та є перспективним напрямком наукових досліджень.

Особливого значення в потоковому і блоковому шифруванні набуває створення нових та удосконалення існуючих методів захисту інформації для вирішення задач створення високоякісних криптопримітивів та псевдовипадкових послідовностей. Тому розробка придатних для практичного застосування методів підвищення ефективності таких показників криптографічного перетворення інформації, як швидкість та стійкість має високу теоретичну і практичну значимість, а її вирішення є актуальною проблемою.

Особливу значимість теми дисертаційного дослідження Бабенко Віри Григорівни підкреслює її зв'язок з науково-дослідними роботами: «Методи та засоби захисту інформації МНС України на основі операцій криптографічного кодування» (ДР № 0112U003579), «Криптографічне кодування: методи та засоби реалізації (частина 2)» (ДР № 0113U001475), «Ефективність систем інформаційної безпеки», шифр НДР «Безпека» (ДРН 0113U004731), «Ефективність систем інформаційної безпеки» (Шифр «Перетворення»), «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР № 0116U008714), «Розробка методів та засобів оцінки ефективності соціоінжинірингу» (ДР № 0116U008715), «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах» (ДР № 0115U003103).

Таким чином, враховуючи наведені аргументи, актуальність теми дисертаційного дослідження Бабенко Віри Григорівни «Методологія синтезу операцій перетворення інформації для комп'ютерної криптографії» не викликає

жодних сумнівів.

2. Ступінь обґрунтованості наукових положень дисертації та їх достовірність. Основні наукові результати дослідження: методологія синтезу операцій криптографічного перетворення інформації; технологія синтезу операцій для мультиопераційних матричних криптографічних примітивів; удосконалені методи побудови криптографічних примітивів на прикладі примітивів ковзного шифрування; удосконалені методи синтезу та аналізу криптографічних алгоритмів; розбудова методів синтез дискретних математичних моделей, елементарних функцій та операцій криптоперетворення є достатньо обґрунтованими та не викликають сумнівів. Достовірність наукових положень дисертації забезпечується:

- використанням в процесі досліджень методів теорії інформації, дискретної математики, множин, алгоритмів, математичної статистики, систем числення, криптографії, комп'ютерного моделювання, лінійного та нелінійного криптоаналізу;
- дослідженням псевдовипадкових послідовностей, що реалізують запропоновані методи формування, за допомогою статистичних пакетів тестування NIST;
- відповідністю проведених експериментальних досліджень виконаним теоретичним розрахункам.

3. Найбільш вагомі наукові результати одержані здобувачем особисто.

У дисертаційній роботі вирішена актуальна науково-технічна проблема, яка пов'язана з досягненням заданої ефективності функціонування систем комп'ютерної криптографії шляхом створення методології синтезу операцій перетворення інформації та побудови криптографічних примітивів на їх основі для вирішення протиріч між криптостійкістю, складністю та швидкістю перетворень виходячи з задач проектування.

4. Наукова новизна отриманих результатів полягає в наступному:

- вперше запропонована методологія синтезу операцій криптографічного перетворення інформації на основі існуючих та розроблених методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення шляхом їх класифікації та узагальнення, що забезпечило можливість розширення бази операцій, використання яких дозволяє

удосконалювати існуючі та синтезувати нові криптоалгоритми і криптопримітиви;

- вперше розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів на основі побудови нових груп операцій з точністю до перестановки шляхом використання запропонованої табличної моделі операції криптоперетворення, що дозволило за рахунок варіативності операцій підвищити криптостійкість існуючих криптопримітивів;
- удосконалено методи побудови криптопримітивів на прикладі примітивів ковзного шифрування на основі матричних операцій криптографічного перетворення та отриманих узагальнених рекурентних послідовностей для побудови моделей шляхом їх паралельної реалізації, що забезпечило підвищення швидкості шифрування та стійкості до лінійного криптоаналізу;
- удосконалено методи синтезу та аналізу криптографічних алгоритмів на основі узагальненої моделі криптоалгоритму, шляхом послідовно-паралельної реалізації операцій криптографічного перетворення інформації на макро- та мікрорівнях, що забезпечило можливість вирішення протиріч між криптостійкістю, складністю та швидкістю для досягнення заданої ефективності, виходячи з задач проектування;
- отримали подальший розвиток математичні моделі та методи синтезу елементарних функцій та операцій криптоперетворення на основі запропонованої методології та вибраної групи нелінійних елементарних функцій шляхом удосконалення математичного апарату для синтезу прямих та обернених матричних моделей не афінних дискретних перетворень, що в сукупності забезпечило можливість синтезу операцій нелінійних криптоперетворень.

5. Практична цінність результатів полягає у розробці алгоритмічного та програмного забезпечення для реалізації технології побудови математичних моделей операцій криптоперетворення, а також структурних і функціональних схем пристроїв шифрування, які забезпечують підвищення стійкості та швидкості криптоперетворення. Застосування синтезованих операцій криптографічного перетворення за рахунок збільшення варіативності алгоритмів забезпечує збільшення крипостійкого до 10^{1000} разів при зменшенні часу шифрування до 8 разів.

Практична цінність дисертаційного дослідження підтверджується наведеними в додатках дисертації актами впровадження на підприємствах НВК «Фотоприлад», НДІ «Акорд», ПП «Сенсорна електроніка», ТОВ «Люменс-груп», та в навчальний процес Черкаського державного технологічного університету, Черкаського національного університету імені Б. Хмельницького, Національного аерокосмічного університету імені М. Є. Жуковського «ХАІ», Кіровоградського національного технічного університету.

6. Оцінка змісту та завершеності роботи. Дисертаційна робота Бабенко Віри Григорівни складається зі вступу, шести розділів, висновків (загалом 336 сторінок основного тексту), списку використаних джерел (258 найменування), додатків (76 сторінок).

Дисертаційна робота побудована логічно правильно, розділи та підрозділи роботи взаємопов’язані та чітко спрямовані на досягнення зазначеної мети. В цілому, вважаю, що дисертаційне дослідження є завершеною науковою роботою, яка знайшла практичне застосування у виробничій діяльності підприємств, і в навчальному ВНЗ МОН України, що підтверджується актами впровадження.

У додатках до дисертації автором наведені докладні результати тестування за допомогою статистичних пакетів, акти впровадження, а також обов’язкову інформацію про публікацію та апробацію результатів дослідження.

7. Основні наукові результати, що отримані в дисертації, викладені здобувачем у 90 публікаціях, серед яких 7 колективних монографій (2 закордонні), 49 статях у наукових журналах та збірниках наукових праць (з них 40 статей у наукових фахових виданнях України, 6 статей у закордонних виданнях), 30 тезах доповідей на міжнародних та всеукраїнських наукових, науково-технічних і науково-практичних конференціях. Здобувач не використовував матеріали й висновки дисертаційних досліджень, за якими захистив кандидатську дисертацію, яку я також опонував.

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. При проведенні дисертаційного дослідження автор не приділив достатньої уваги теоретичній криптостійкості, адже застосування запропонованих перетворень дозволяє використовувати операції з різних математичних груп, що вимагає збільшення довжини гамуючої послідовності. Це дозволило б отримати нові теоретичні та практичні результати, які б мали важливі результати як для комп'ютерної криптографії так і для криптології в цілому.

2. В підрозділі 1.4 «Формальна постановка наукової проблеми» доцільно було б більш детально описати протиріччя, які вирішуються в даному дослідженні, а не обмежитися лише формалізованими взаємозв'язками та їх залежностями.

3. В підрозділі 2.1 недостатньо детально розкрите поняття криптографічного кодування (ст. 73), яке по суті є основним для даної роботи, тому що саме воно поєднує в єдине ціле методи побудови систем захисту інформації і комп'ютерну інженерію. Крім того доцільно було б навести основні базові теореми необхідні для побудови моделей пристроїв прямого, оберненого та взаємного криптографічного перетворення, а не обмежитися посиланнями на них (ст. 75).

4. Автор лише на деяких прикладах показав перехід від елементарної функцій криптоперетворення до логіки виконання криптоперетворення, яка дійсно може бути використана для побудови криптоалгоритмів. Проте логіку виконання криптоперетворення чомусь було названо «фізичним змістом» перетворення. (ст. 142). Процес переходу від синтезованої елементарної до логіки виконання криптоперетворення детально не розглядався проте наведені в роботі результати доводять необхідність окремого додаткового дослідження за рамками даної роботи.

5. З тексту підрозділу 3.5.2. не зрозуміло, як автор перейшов від трьохрозрядних моделей криптоперетворення до моделей довільної розрядності, які в роботі синтезуються іншими методами.

6. В тексті дисертації відсутні правила переходу від матричних моделей перетворень ковзного шифрування до рекурентних моделей даних перетворень (розділ 4), які було застосовано автором. Детальний опис побудови даних правил сприяє, крім даного дослідження, на розбудову кодів Грея та «золотої пропорції».

7. Розроблена методологія синтезу операцій криптографічного перетворення заявлена в роботі як наукова новизна, тому цей результат не можна відносити до практичної цінності.

8. В четвертій задачі зазначена розробка технології синтезу операцій для мультиопераційних матричних криптопримітивів, але отриманий науковий результат чітко не відображений в науковій новизні, а тільки показані практичні аспекти, що пов'язані з програмною реалізацію зазначеної розробки.

Зазначені зауваження не впливають на наукову та практичну цінність проведеного дослідження.

10. Висновок. Дисертаційна робота Бабенко Віри Григорівни «Методологія синтезу операцій перетворення інформації для комп'ютерної криптографії», є актуальною завершеною науковою працею, а отримані результати вирішують важливу науково-технічну проблему, пов'язаною з підвищенням ефективності функціонування систем комп'ютерної криптографії шляхом створення відповідної методології синтезу операцій перетворення інформації та побудови криптопримітивів на їх основі.

Дисертаційна робота, представлена до розгляду, відповідає вимогам щодо докторських дисертацій, а її автор Бабенко Віра Григорівна заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент:
Завідувач кафедри безпеки
інформаційних технологій
Національного авіаційного
університету,
лауреат Державної премії України
в галузі науки і техніки,
доктор технічних наук, професор О.Г. Корченко

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
01132330
МІСТО КИЇВ

Корченка О.Г.
засвідчую
Вчений секретар
Національного авіаційного університету
Г. Ємець