ВІДГУК

офіційного опонента про дисертаційну роботу Нестеренко Оксани Борисівни «Методи та засоби синтезу операцій потокового шифрування за критерієм строгого стійкого кодування», подану на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.05 – комп'ютерні системи та компоненти

Цей відгук підготовлено за матеріалами дисертації, що містить основний текст роботи на 155 стор., додатки, акти впровадження результатів дисертації, автореферат на 19 стор. і копії 18 наукових праць здобувача.

1. Актуальність теми дисертаційної роботи

Стрімкий розвиток глобального інформаційного простору нерозривно пов'язаний із багатократним збільшенням обсягів інформації які накопичуються, передаються і обробляються. Розширення зон впливу цифрових технологій і перехід на цифрову економіку насичують глобальну мережу величезною кількістю конфіденційної інформації, яку потрібно не тільки обробляти а і захищати. Сучасні реалії вимагають не лише забезпечити конфіденційність, цілісність та доступність інформації а також оперативність доступу до конфіденційної інформації.

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 шляхом досягненні максимальної невизначеності результатів потокового шифрування. З цього випливають задачі наукового обґрунтування можливості синтезу спеціальних логічних операцій, які забезпечують максимальну невизначеність результатів перетворення за рахунок виконання вимог критерію строгого стійкого кодування. Дані операції повинні забезпечити швидкі потокові криптоперетворення необхідною стійкістю до лінійного і диференційного крипто аналізу. Необхідно також розробки методи та засоби їх реалізації в алгоритмах комп'ютерної криптографії.

ЧДТУ
Вх. № 758-л
14. 06. 2019

Дисертація, що розглядається, має саме таку побудову – від вимог до криптоперетворення до синтезу операцій, від загального синтезу операцій до методів та засобів синтезу операцій мінімальної складності при їх технічній реалізації.

Тема досліджень дисертації, що розглядається, відповідає основним науковим напрями фундаментальних досліджень у галузі технічних наук Національної академії наук України і виконувалась за напрямком наукових досліджень кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету. Отримані результати включені в НДР "Методи та засоби захисту інформації МНС України на основі операцій криптографічного кодування", "Синтез операцій криптографічного перетворення з заданим характеристиками".

Таким чином, усе сказане обумовлює актуальність дисертаційної роботи Нестеренко О.Б. і наукову новизну поставлених в ній задач досліджень.

2. Наукова новизна результатів роботи

У роботі досліджено підвищення невизначеності результатів потокового шифрування за рахунок використання нових операцій криптоперетворення, синтезованих за критерієм строгого стійкого кодування.

Виходячи з того, що нові наукові результати – це нові знання в певній галузі фундаментальних чи прикладних наук, можна вважати основними науковими результатами дисертації таке:

− вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування шляхом використання таблиць мінімальних відстаней за Хеммінгом для побудови таблиць істинності дискретних моделей, які забезпечують максимальну невизначеність результатів перетворення;

− вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності на основі використання операцій перестановки і гамування, шляхом встановлених обмежень та залежностей між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення при практично мінімальній складності схемотехнічної та програмної реалізації;

− набули подальшого розвитку методи синтезу програмних і апаратних криптографічних засобів комп'ютерної техніки на основі використання нової групи операцій, побудованих за критерієм строгого стійкого кодування, шляхом застосування методів синтезу моделей операцій з новими властивостями, які забезпечили спрощення процесу синтезу програмних і апаратних крипто-

графічних засобів і дозволили реалізувати синтез аналогічних засобів мінімальної складності без побудови таблиць істинності та мінімізації.

3. Достовірність наукових результатів

Достовірність наукових результатів, положень, методів, висновків і рекомендацій обумовлені коректним використанням основних положень теорії інформації, криптографії, математичної логіки, дискретної математики, математичної статистики та комп'ютерного моделювання, а також не розбіжністю отриманих теоретичних і експериментальних результатів з практикою впровадження розроблених засобів.

4. Цінність дисертаційної роботи для науки

Цінність дисертації полягає в тому, що в ній запропоновано нове рішення важливої науково-технічної задачі в теорії побудови криптографічних засобів для захисту інформації в комп'ютерних системах і мережах з підвищеною невизначеністю результатів потокового шифрування. Змістовний аспект запропонованого рішення, який спрямований на підвищення якості функціонування систем комп'ютерної криптографії шляхом побудови методів шифрування які базуються на застосуванні критерію строгого стійкого кодування і засобів, що їх реалізують, не був відомий раніше.

5. Практична цінність роботи

Практична корисність роботи обумовлена тим, що використання запропонованих в ній формальних методів і конкретних рішень дозволяє отримувати більш досконалі, порівняно з відомими, засоби комп'ютерного криптографічного перетворення інформації. Результати роботи впроваджено на ПП "Сенсорна Електроніка" та в навчальний процес Черкаського державниого технологічного університету.

6. Структура роботи

Дисертаційна робота містить вступ, 4 розділи, висновки, додатки та перелік використаних джерел.

У вступі сформульовано актуальність теми роботи, мету задачі, предмет і об'єкт дослідження, наукову новизну і практичне значення отриманих результатів, наведено відомості про реалізацію і апробацію роботи, про публікації за її

темою.

Перший розділ присвячений аналізу якості систем криптографічного перетворення інформації. На основі проведеного аналітичного огляду сучасного стану та тенденцій розвитку комп'ютерної криптографії формулюються мета і задачі наукового дослідження.

Другий розділ присвячений дослідженню двохрозрядних операцій криптографічного перетворення інформації за критерієм строгого стійкого криптографічного кодування. Даний критерій запропоновано використовувати для оцінки якості операцій криптоперетворень замість строгого лавинного ефекту Криптографічний алгоритм, або операція криптографічного перетворення інформації задовольняє критерією строгого стійкого криптографічного кодування, якщо незалежно від ключової послідовності та вхідної інформації кожний біт вихідної послідовності змінюється відносно вхідної інформації з імовірністю одна друга.

Третій розділ присвячено розробці методу синтезу операцій криптографічного перетворення інформації за критерієм строгого стійкого криптографічного кодування. Встановлено, що якщо крипто перетворення відповідає вимогам критерію строгого стійкого криптографічного кодування, то виконання декількох раундів не приводить до підвищення невизначеності результатів шифрування.

Четвертий розділ присвячено розробці методу синтезу операцій криптографічного перетворення інформації мінімальної складності та оцінці можливості застосування синтезованих операцій у потоковому шифруванні. Синтез операцій, які задовольняють критерію строгого стійкого кодування і мають мінімальну складність, проводиться на основі парних перестановок та інверсії, шляхом інверсії половини бітів, за умови однієї інверсії в кожній парній перестановці. Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам до протидії лінійному крипто аналізу.

У додатках подано акти про впровадження результатів дисертаційного дослідження та приведено обов’язковий додаток.

7. Публікації за темою дисертації

Наукові положення дисертації, що пов’язані з розробкою методів та засобів синтезу операцій потокового шифрування за критерієм строгого стійкого кодування достатньо повно відображені в публікаціях автора і пройшли апро-

бацію на міжнародних науково-технічних і науково-практичних конференціях.

8. Автореферат дисертації

Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі.

9. Зауваження щодо змісту дисертаційної роботи та автореферату

1. По першому розділу, слід відмітити, відсутність порівняльного аналізу потокових криптосистем; матеріали підрозділу "Атаки на асиметричну криптосистему" (ст.. 27-30), в подальших дослідженнях не використовуються; автору було б доцільно крім надійності криптосистем приділити більше уваги їх оперативності як однієї з основних причин необхідності вдосконалення саме систем потокового шифрування.

2. В другому розділі, в підрозділі 2.2 результати дослідження дворозрядних елементарних функцій для криптоперетворенні зведені в табл..2.2 та табл..2.6 без детального пояснення наведених результатів, а підрозділі 2.3 навпаки детальний аналіз 24 операцій криптоперетворення доцільно було б скоротити, обмежившись методикою аналізу та визначеними на її основі чотирма операціями.

3. В третьому розділі надмірна формалізація результатів обчислювального експерименту не дає в повній мірі оцінити можливі подальші шляхи розвитку дисертаційного дослідження. Автор вибрав лише один із можливих шляхів розбудови систем потокового шифрування, а саме мінімальну складність реалізації. В підрозділі 3.3.2 було б доцільно крім фрагменту зведених результатів моделювання таблиць підстановок для синтезу чотирьох розрядних операцій, які відповідають критерію ССК навести алгоритм програмного забезпечення для проведення обчислювального експерименту.

4. В четвертому розділі було б доцільно навести алгоритм реалізації, методу синтезу операцій криптографічного перетворення інформації мінімальної складності за критерієм строгого стійкого кодування, з деталізацією особливостей синтезу різних груп операцій, а не переобтяжувати його приблизними теоретичними оцінками потужності груп синтезованих операцій.

5. В дисертації є несуттєві граматичні та стилістичні неточності пов’язані як з роботою автора так і з текстовими редакторами. Наприклад "…виділивши з операції базову частину і частину інверсій…" (ст..12 автореферату), замість "…представивши операцію двома операціями, базовою операцією, і операцією

інверсії…"; "Таблиця підстановки в червінковій системі числення..", замість четвіркової (ст..71 дисертації).

10. Загальна оцінка дисертації

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове рішення важливої науково-технічної задачі, спрямованої на підвищення якості систем комп'ютерного криптографічного захисту інформації за рахунок підвищення невизначеності результатів потокового шифрування на основі використання нових операцій криптоперетворення, синтезованих за критерієм строгого стійкого кодування. Дисертація є завершеною науково-дослідною роботою.

Вважаю, що за актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики дисертаційна робота задовольняє вимогам "Порядку присудження наукових ступенів", а її автор Нестеренко Оксана Борисівна заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент
професор кафедри захисту інформації
Національного університету
"Львівська політехніка",
д.т.н., професор Л. Т. Пархуць

" 12 " червня 2019 р.

Підпис професора кафедри захисту інформації Л.Т.Пархуця ***засвідчую****:*

Вчений секретар
Національного університету
"Львівська політехніка",
к. т. н., доцент Р. Б.Брилинський