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

Цей відгук підготовлено за матеріалами дисертації, що містить основний текст роботи на 336 стор., додатки, акти впровадження результатів дисертації та автореферат на 40 стор.

1. Актуальність теми дисертаційної роботи

Розвиток інформаційних технологій і глобалізація інформаційних процесів сумісно з впровадженням комп'ютерних систем в усі сфери людської діяльності стали причиною стрімкого росту обсягів інформації. Ці процеси не лише характеризуються позитивними наслідками, але водночас спричиняють появу нових негативних інформаційних впливів, зокрема – сприяють стрімкому розвитку кіберзлочинності. У зв'язку з цим зростає потреба захисту інформації, яка має відповідну цінність як для держави, так і для окремих користувачів, а також набувають особливої актуальності для сьогодення проблеми інформаційної безпеки та захисту інформаційних ресурсів.

Провідна роль у забезпеченні інформаційної безпеки інформаційно-телекомунікаційних систем і кіберпростору відводиться криптографії, одними з головних задач якої є забезпечення конфіденційності, цілісності та автентичності даних, що збираються, передаються і обробляються. Однак існуючі засоби шифрування не завжди задовольняють вимогам криптостійкості та продуктивності, особливо при захисті великих обсягів інформації. Все це обумовлює актуальність розробки методів шифрування інформації, які б забезпечували побудову шифрів, стійких до зламу, і створення високопродуктивних засобів шифрування.

Одним з перспективних напрямків розвитку криптографії є побудова та використання операцій криптографічного перетворення на основі застосування булевих функцій, які забезпечують побудову високошвидкісних криптографічних примітивів з надвисокою варіативністю.

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
Вх. № 520
07. 09. 2020

Проте залишається цілий ряд задач і проблем, пов'язаних з відсутністю теорії побудови дискретних моделей груп перестановок, які забезпечать виконання вимог до якості криптоперетворення та можливість синтезу пристроїв шифрування з заданими властивостями. Розбудова даної теорії неможлива без створення методології синтезу операцій криптоперетворення, яка об'єднає на основі єдиного підходу процеси дослідження і синтезу як відомих, так і невідомих груп операцій криптографічного перетворення інформації.

Вирішення поставленої проблеми дозволить вдосконалити існуючі криптоалгоритми та створити нові, основними перевагами яких будуть висока швидкість, що базується на простоті реалізації булевих функцій, та криптостійкість, обумовлена значним збільшенням варіативності процесу шифрування.

Дисертація, що розглядається, має таку побудову – від формування методології синтезу операцій криптоперетворення до побудови методів синтезу груп моделей операцій на основі застосування методології, з наступною розробкою примітивів на їх основі та програмно-апаратних засобів реалізації, а також оцінкою ефективності отриманих результатів на фінальній стадії дослідження.

Тематика дослідження дисертації, що розглядається, відповідає державній науковій програмі розвитку технічного захисту інформації в Україні і виконувалась за напрямком наукових досліджень кафедри «Інформаційна безпека та комп'ютерна інженерія» Черкаського державного технологічного університету.

Таким чином, усе сказане обумовлює актуальність дисертаційної роботи Бабенко Віри Григорівни.

2. Наукова новизна результатів дисертаційної роботи

У роботі досліджено підвищення ефективності функціонування систем комп'ютерної криптографії шляхом створення методології синтезу математичних моделей операцій перетворення інформації та побудови криптографічних примітивів на основі їх застосування.

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

1. 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 вдосконалювати існуючі та синтезувати нові криптоалгоритми і крипто примітиви.

2. 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 крипто-примітивів.

3. Удосконалено методи побудови криптографічних примітивів 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 (до двох разів) та стійкості до лінійного крипто аналізу.

4. 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.

5. Отримали подальший розвиток математичні моделі та методи синтезу елементарних функцій та операцій криптоперетворення на основі запропонованої методології та вибраної групи нелінійних елементарних функцій шляхом вдосконалення математичного апарату для синтезу прямих та обернених матричних моделей неафінних дискретних перетворень, що в сукупності забезпечило можливість синтезу операцій нелінійних криптографічних перетворень.

3. Достовірність наукових результатів

Достовірність основних наукових результатів роботи підтверджується коректним застосуванням вибраного наукового апарату, зрозумілим трактуванням отриманих результатів, а також рядом прикладів, комп'ютерним моделюванням крипто перетворень, результатами їх статистичної оцінки та впровадженням розроблених методів та засобів.

4. Цінність дисертаційної роботи для науки

Цінність дисертації полягає в тому, що в ній запропоновано рішення важливої науково-технічної проблеми в теорії побудови систем комп'ютерної криптографії, пов'язаної з протиріччями між швидкістю, складністю, криптостійкістю та варіативністю. Змістовний аспект запропонованого рішення, який спрямований на підвищення ефективності функціонування систем комп'ютерної криптографії шляхом створення методології синтезу операцій перетворення інформації та побудови криптографічних примітивів на їх основі, не був відомий раніше.

5. Практична корисність роботи

Практична корисність роботи обумовлена тим, що використання запропонованих в ній формальних методів і конкретних технічних рішень дозволяє отримувати більш досконалі, порівняно з відомими, засоби комп'ютерної криптографії для захисту інформації в кіберпросторі. Результати роботи впроваджено на підприємствах та в навчальний процес закладів вищої освіти України.

6. Структура роботи

Дисертаційна робота містить вступ, 6 розділів, висновки, перелік використаних джерел та додатки.

У вступі обґрунтовано актуальність теми роботи, сформульовано мету і задачі дослідження, описано наукову новизну та практичне значення отриманих результатів, показано зв'язок з наукового-дослідними роботами в рамках яких виконано дане дослідження, наведено відомості про реалізацію і апробацію роботи, про публікації за її темою.

Перший розділ присвячений аналітичному огляду систем криптографічного захисту. На основі вибраних комплексних показників якості та ефективності функціонування криптосистеми визначено протиріччя між складністю, криптостійкістю та швидкістю. Для вирішення зазначених протиріч сформульовані мета та задачі дисертаційного дослідження.

Другий розділ присвячений розробці та узагальненню методів синтезу операцій криптографічного перетворення, а також побудові та формалізації методології синтезу логічних операцій для криптографічного перетворення інформації. В даному розділі було отримано перший науковий результат.

У третьому розділі проведена класифікація трирозрядних елементарних

функцій для криптографічного перетворення інформації за складністю та функціональними особливостями перетворення. На основі розробленої методології і вибраної групи класифікованих неафінних елементарних функцій отримали подальший розвиток математичні моделі та методи синтезу нелінійних елементарних функцій та операцій криптоперетворення, що дозволило отримати п'ятий науковий результат.

Четвертий розділ присвячений реалізації криптопримітивів ковзного шифрування на основі матричних операцій криптографічного перетворення. В даному розділі було отримано третій науковий результат.

П'ятий розділ присвячений моделюванню операцій для мультиопераційних матричних криптографічних примітивів і в ньому отримано другий науковий результат.

Шостий розділ присвячено синтезу криптоалгоритмів на основі операцій криптографічного перетворення інформації. В ньому отримано четвертий науковий результат.

У висновках наведено основні найбільш вагомі наукові і практичні результати проведеного дослідження.

У додатках подано акти впровадження результатів дисертаційного дослідження, результати обчислювальних експериментів та результати тестування криптоалгоритмів, наведено інформацію про публікації та апробацію результатів дослідження.

7. Публікації за темою дисертації

Наукові положення дисертації, що пов'язані з розробкою методології та методів і моделей синтезу операцій для підвищення швидкості, стійкості та варіативності криптоалгоритмів, достатньо повно відображені в публікаціях автора, пройшли апробацію на міжнародних і вітчизняних наукових, науково-технічних та науково-практичних конференціях і семінарах.

8. Автореферат дисертації

Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі.

9. Відповідність роботи встановленим кваліфікаційним вимогам.

За важливістю і актуальністю обраної теми, обсягом і рівнем одержаних результатів, їх новизною і практичною цінністю дисертація Бабенко В.Г.

відповідає вимогам до кваліфікаційних робіт, які подаються на здобуття наукового ступеня доктора технічних наук.

Дисертація відповідає паспорту спеціальності 05.13.05 –комп'ютерні системи та компоненти.

Матеріали й висновки кандидатської дисертації Бабенко В.Г. не використовуються в її дисертації, поданої на здобуття наукового ступеня доктора технічних наук.

10. Зауваження щодо змісту дисертаційної роботи та автореферату

1. У розділі 1 дисертаційного дослідження відсутній огляд сучасних стандартів блокового та потокового шифрування та існуючих базових операцій перетворення інформації, які в них використовуються.
2. З тексту підрозділу 2.2.1 «Систематизація повної множини логічних функцій для криптографічного перетворення інформації» не зрозуміло, за якими правилами проводилась нумерація операцій криптоперетворення, що наведена в табл. 2.5 «Структуровані результати обчислювального експерименту», адже від цього залежать моделі блоків логічних функцій та модулі взаємного перетворення інформації.
3. На мою думку авторка не зовсім коректно назвала процес перетворення результатів виконання однієї заданої операції в результаті виконання іншої, наперед заданої операції, як перекодування. Адже дана назва не відповідає сутності операції, яка виконується, адже кодування інформації є лише окремим випадком (ст. 94 – 95).
4. Розділ 3 переповнений моделями операцій, частина з них може бути видалена, так як використовується лише для побудови узагальнених моделей операцій прямого і оберненого перетворення. Доцільно було б привести лише узагальнені моделі, де це можливо, а інші перенести в додатки.
5. В підрозділі 4.3 автору було б доцільно детальніше описати спрощення узагальненої моделі побудови результатів багатораундового шифрування, а не обмежитися посиланням на теорему Шеннона.
6. Наведені в табл. 5.8 результати моделювання операцій над двома операндами потребують не тільки подальшого представлення формальними моделями операцій перетворення інформації, яке було зроблено автором, а більш детального опису як самих результатів так і технології їх отримання шляхом обчислювального експерименту.

7. Недостатньо обґрунтована вимога симетричності табличного представлення двохоперандної операції відносно головної діагоналі як необхідна умова її застосування в криптоперетвореннях.
8. Підрозділ 6.2 переповнений статистичними портретами результатів тестування. Було б доцільно їх розділить на декілька груп і привести зведені результати до таблиць узагальнення тестування. Даний підхід дозволив би спростити проведення аналізу і забезпечив би наглядність порівняльного аналізу для прийняття рішення.

11. Загальна оцінка дисертації

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано рішення важливої науково-технічної проблеми, спрямованої на підвищення ефективності функціонування систем комп'ютерної криптографії шляхом створення методології синтезу операцій перетворення інформації та побудови криптографічних примітивів на їх основі.

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 авторка Бабенко Віра Григорівна, заслуговує присудження наукового ступеня доктора технічних наук зі спеціальності 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент

професор кафедри інформаційних
технологій та кібербезпеки факультету № 4
Харківського національного
університету внутрішніх справ Міністерства
внутрішніх справ України,
доктор технічних наук, професор О.О. Можаєв

ПІДПИС ЗАСВІДЧУЮ
Відділ документування службової діяльності ХНУВС
01 09 2020 р.