ВІДГУК

офіційного опонента про дисертаційну роботу Навроцького Дениса Олександровича «Методи побудови симетричних криптографічних шифрів з використанням тривимірних перетворень», подану на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – Системи захисту інформації

1. Актуальність теми дисертаційної роботи

Інформаційний вибух останніх років висунув на одне з перших місць проблему захисту величезної кількості конфіденційної інформації, що оброблюється і передається в комп'ютерних системах і мережах, а також глобальній мережі Internet.

У даний час основними засобами захисту інформації в системах і мережах є криптографічні засоби, що реалізують різноманітні методи шифрування. Деякі з цих методів реалізовані як стандарти і рекомендуються для широкого використання. Однак удосконалення методів криптоаналізу і постійне підвищення продуктивності комп'ютерної техніки створюють реальну можливість зламу шифрів. Крім того, існуючі засоби шифрування не завжди задовольняють вимогам продуктивності, особливо при застосуванні у високошвидкісних комп'ютерних системах. Усе це обумовлює актуальність розробки методів шифрування інформації, які б забезпечували побудову шифрів, стійких до зламу, і створення високопродуктивних засобів шифрування для систем захисту інформації.

Відомі наукові праці, в яких доведено, що одним з перспективних напрямків забезпечення криптостійкості симетричних шифрів є використання криптографічних примітивів, в яких реалізуються керовані операції. Крім цього, перспективною тенденцією є перехід від одновимірного до двовимірного і тривимірного представлення даних. З цього випливають задачі наукового обґрунтування можливості синтезу динамічно керованих тривимірних криптографічних примітивів, що забезпечують стійкість до статистичного, лінійного і диференційного криптоаналізу, розробки методів блокового і потокового шифрування та алгоритмів і програмних засобів, що їх реалізують.

Дисертація, що розглядається, має саме таку побудову - від концепції синтезу динамічно керованих тривимірних криптографічних примітивів лінійного розсіювання, включаючи примітиви зсуву, нелінійної заміни (підстановки) та «ковзного кодування» на основі узагальнених перетворень Грея до аналізу їх криптостійкості, методів і алгоритмів шифрування та їх програмної реалізації.

Тема досліджень відповідає «Концепції інформаційної безпеки України», «Стратегії національної безпеки України» відповідно до п.4.12 «Забезпечення кібербезпеки і безпеки інформаційних ресурсів, зокрема реформування системи технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС з досліджень та інновацій», «Основним науковим напрямам та найважливішим проблемам фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014–2018 роки» в частині п.1.2.8.1 «Розробка методів та інформаційних технологій розв’язання задач комп’ютерної криптографії та стеганографії» і виконувалася за напрямком наукових досліджень Національного авіаційного університету.

Таким чином, усе сказане обумовлює актуальність теми дисертаційної роботи Навроцького Д. О. і наукову новизну поставлених в ній задач досліджень.

2. Наукова новизна результатів роботи

У роботі досліджено підхід щодо підвищення криптостійкості та швидкодії засобів шифрування інформації, який полягає у використанні динамічно керованих тривимірних криптографічних примітивів.

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 розроблений метод побудови динамічно керованих примітивів лінійного розсіювання, нелінійної заміни та «ковзного кодування» на основі узагальнених перетворень Грея та матриць Галуа для тривимірного представлення даних, використання яких забезпечує збільшення швидкості

шифрування і стійкості шифрів та зменшення обсягу пам’яті, потрібної для реалізації процесу шифрування;

– вперше розроблені методи блокового і потокового шифрування, що використовують тривимірне представлення даних;

– удосконалений метод синтезу матриць для таблиць підстановки і перестановки на основі тривимірних криптографічних примітивів;

– удосконалені методи синтезу примітивних матриць Галуа і Фібоначчі над простими полями Галуа характеристики 2, які забезпечують можливість розширення множини узагальнених генераторів псевдовипадкових послідовностей.

3. Достовірність наукових результатів

Достовірність основних наукових результатів роботи підтверджується наведеною в розд. 2, 3 і 4 системою формальних методик і перетворень, що не містить принципових помилок, а також рядом прикладів, результатами комп‘ютерного тестування з використанням загальновизнаних наборів тестів і впровадженням програмних 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 систем захисту інформації. Змістовний аспект запропонованого рішення, який спрямований на розширення класу методів блокового і потокового шифрування і засобів, що їх реалізують, не був відомий раніше.

5. Практична корисність роботи

Практична корисність роботи обумовлена тім, що використання запропонованих в ній моделей, формальних методів і конкретних рішень дозволяє отримувати більш досконалі, порівняно з відомими, засоби криптографічного захисту інформації в комп’ютерних системах та мережах.

Результати роботи впроваджено в науково-технічних розробках ТОВ «Агфар», ТОВ «Сайфер Лтд», ТОВ «Гратис Лтд», що підтверджено відповідними актами впровадження, та в навчальний процес кафедри

електроніки Національного авіаційного університету і кафедри виробництва приладів Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

6. Структура роботи

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

У вступі сформульовано актуальність теми роботи, мету і задачі дослідження, наукову новизну і практичне значення отриманих результатів, показано зв‘язок роботи з науковими програмами, планами і темами, виконуваними у Національному авіаційному університеті, наведено відомості про реалізацію і апробацію роботи, про публікації за її темою.

У першому розділі наведено аналітичний огляд існуючих методів і алгоритмів блокового шифрування. Значну увагу приділено криптографічним примітивам, використовуваним у блокових шифрах, що є стандартними в певних країнах. Розглянуто основні атаки на шифри та методи криптоаналізу.

Другий розділ присвячено питанням синтезу узагальнених перетворень тривимірних даних і побудови керованих криптографічних примітивів, які базуються на цих перетвореннях. Спочатку наводяться відомі положення з теорії багатовимірних матриць, на яких базуються подальші дослідження. Далі розглядаються методи синтезу S-блоків підстановки в тривимірному просторі та метод синтезу тривимірних узагальнених матриць Галуа.

У третьому розділі розглядаються питання синтезу і аналізу тривимірних криптографічних примітивів: перемішування, арифметичне, логічне і змішане «ковзне кодування». Досліджуються статистичні властивості перетворень «ковзного кодування» і нелінійної заміни. Показано, що нелінійна заміна на основі тривимірної моделі S-блоку має більш рівномірну щільність порівняно з нелінійною заміною на основі S-блоків шифру AES. Наводиться приклад оригінального шифрування з використанням «ковзного кодування». Розглядаються алгоритми блокового і потокового шифрування, в яких використовуються тривимірні криптографічні примітиви. Наводиться приклад

криптографічного протоколу обміну даними, який використовує запропоновані автором шифр і хеш-функцію.

Четвертий розділ присвячений результатам досліджень стійкості шифрів. У перший частині розділу наводяться результати експериментальних досліджень статистичних властивостей відомих і запропонованих автором шифрів. Для проведення експериментів автор розробив програмний засіб, який забезпечує тестування шифрів з використанням загальновизнаних тестів NIST STS і Dieharder. Результати експериментальних досліджень показали, що запропоновані автором шифри мають таку саму стійкість до статистичного аналізу як і широко використовувані шифри. Отримані аналітичні верхні межі стійкості відносно лінійного і диференційного криптоаналізу шифрів, запропонованих автором, свідчать про те, що ці шифри задовольняють сучасним вимогам.

У додатках подано комп'ютерні програми для експериментальних досліджень та акти про впровадження результатів дисертаційного дослідження.

7. Публікації за темою дисертації

Наукові положення дисертації, що пов'язані з розробкою динамічно керованих тривимірних криптографічних примітивів, методів і алгоритмів шифрування на їх основі, а також з аналізом їх криптостійкості, достатньо повно відображені в публікаціях автора і пройшли апробацію на міжнародних науково-технічних конференціях.

8. Автореферат дисертації

Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі.

9. Зауваження щодо змісту дисертаційної роботи

1. У списку використаних джерел відсутні роботи майже половини вчених, згадуваних автором у вступі як таких, що «…зробили значний внесок у розвиток криптографічних методів захисту інформації».

2. У тексті часто використовуються поруч поняття «шифрування» і «розшифрування». Однак з контексту випливає необхідність вживання поняття

«зашифрування». Крім того, автор часто вживає поняття «шифр» і «шифратор» як синоніми. Однак під шифром розуміють алгоритм, а шифратором називають засіб, який реалізує алгоритм шифрування.

3. Автор некоректно використовує як синоніми «шифр Rijndael» і «шифр AES», оскільки шифр AES є стандартом США і допрацьованою версією шифру Rijndael, який є переможцем міжнародного конкурсу претендентів на стандарт блокового шифру. Наприклад, таблиця 1.5, яка має назву «Таблиця підстановок для шифратора Rijndael», наведена на рис. 2.9 з назвою «S-блок AES».

4. У табл. 1.3. не вказано одиницю вимірювання наведеної характеристики, тому незрозуміло, про яку саме характеристику йде мова. Характеристикою шифру може бути або швидкість шифрування, або кількість операцій, використовуваних для шифрування одиниці даних (біт або байт). Вказана автором характеристика «швидкодія» стосується пристроїв, а не алгоритмів.

5. Посилаючись на рис. 1.10 «Структурна схема плати … з уразливістю шифру AES» автор відзначає, що «Виявлені апаратні уразливості шифраторів», однак не наводить їх перелік.

6. Підрозд. 1.4 «Паралельні обчислення в тривимірному просторі» містить загальновідому популярно викладену інформацію, яку можна вилучити без шкоди змісту роботи.

7. Таблиці 3.1 і 3.2 є неінформативними і подані без дотримання існуючих правил оформлення. Рис. 3.1 і 3.25 мають однакові назву і зміст.

8. Зі змісту підрозд. 3.3 не зрозуміло, яким чином здійснюється множення тривимірних матриць, оскільки відсутній опис криптографічного примітиву «3D matrix multiplication», а зміст рис. 3.19 не відповідає його назві «Множення матриць по перетинах за обраним напрямком».

9. У табл. 4.5 числові значення різниць ентропій шифрограми і вхідного файлу мають занадто велику кількість цифр після коми. Достатньо було б чотири-п’ять цифр.

10. Відсутні оцінки апаратної складності шифраторів, що реалізують

запропоновані автором шифри, тому неможливо визначити на скільки вони задовольняють вимоги низькоресурсної криптографії, зокрема, вимоги до апаратури безпілотних літальних апаратів, про які неодноразово згадується в роботі.

11. Деякі наукові результати досліджень представлені не в статтях, а в патентах України на корисну модель.

12. У переліку публікацій, наведеному в авторефераті, праці [10, 12, 13] присвячені питанням стеганографії, а тому не пов'язані з темою дисертаційного дослідження.

10. Загальна оцінка дисертації

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове рішення важливої науково-технічної задачі, спрямованої на підвищення швидкості процесу шифрування і криптостійкості шифрів, використовуваних у системах захисту інформації. 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 п. 9, 10, 12 «Порядку присудження наукових ступенів», затвердженого постановою КМУ від 19 серпня 2015 року № 656, а її автор Навроцький Денис Олександрович заслуговує присудження наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – Системи захисту інформації.

Офіційний опонент
завідувач кафедри захисту інформації
Вінницького національного
технічного університету,
д.т.н., професор В.А. Лужецький