ВІДГУК

офіційного опонента професора Пархуця Л.Т. про дисертаційну роботу

Козловської Світлани Григорівни

"Методи синтезу груп симетричних операцій для потокового шифрування",

подану на здобуття наукового ступеня кандидата технічних наук

за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

1. Актуальність теми дисертаційної роботи

Раніше розвиток засобів захисту інформації був орієнтований на вимоги державних структур, особливо армії, розвідки, дипломатичного корпусу. Проте створення єдиного кіберпростору на фоні інформаційного вибуху останніх років висунув на одне з перших місць проблему захисту величезної кількості конфіденційної інформації, що обробляється і передається в глобальних і корпоративних комп'ютерних системах і мережах.

Розвиток технічного прогресу потребує невпинного створення нових та вдосконалення вже наявних методів та засобів захисту інформації, в тому числі і криптографічного захисту. Одним із шляхів захисту інформації в хмарних сховищах є потокове шифрування, яке в змозі забезпечити необхідний рівень оперативності доступу до конфіденційної інформації. Розвиток потокових шифрів пов'язаний з вирішенням задач генерації високоякісних псевдовипадкових послідовностей та побудови нових логічних операцій потокового шифрування. Проте на сьогоднішній день комплексне дослідження можливостей синтезу груп криптографічних двохоперандних операцій потокового шифрування не проводилося. Застосування двохоперандних операцій потокового шифрування приводить до підвищення стійкості та надійності криптоперетворення, а збільшення їх кількості до збільшення варіативності перетворення.

З цього випливають задачі наукового обґрунтування можливості синтезу нових груп спеціальних двохоперандних логічних операцій, які є стійкими до лінійного і диференційного криптоаналізу і забезпечують швидкі криптоперетворення, а також розробки методів та засобів їх реалізації в алгоритмах потокового шифрування. Дана дисертація, має наступну побудову - від методу синтезу та дослідження окремих операцій до синтезу груп операцій потокового криптоперетворення та засобів, що їх реалізують до оцінки якості практичного використання операцій.

Тема досліджень дисертації, що розглядається, відповідає державній науковій програмі розвитку технічного захисту інформації в Україні і

ЧДТУ
Вх. 727-п
14. 06. 2019

виконувалась за напрямком наукових досліджень інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету. Отримані результати включені в НДР «Метод синтезу швидкодіючих систем захисту інформації на основі спеціалізованих логічних функцій», «Метод синтезу механізмів захисту інформації в спеціалізованих автоматизованих системах», «Синтез операцій криптографічного перетворення з заданим характеристиками»

Таким чином, усе сказане обумовлює актуальність дисертаційної роботи Козловської С.Г. і наукову новизну поставлених в ній задач досліджень.

2. Наукова новизна результатів роботи

У роботі досліджено підвищення якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та варіативності перетворення на основі додаткового використання груп двохоперандних двохрозрядних операцій, синтезованих на основі додавання за модулем два та чотири.

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

– вперше розроблено метод побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту шляхом формалізації, класифікації та математичного перетворення, що забезпечило встановлення нових взаємозв'язків між операндами й результатами, а також можливість застосування одноперандних операцій у потоковому шифруванні;

– вперше розроблено методи синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування на основі результатів обчислювального експерименту шляхом застосування результатів реалізації розробленого методу побудови та дослідження двохоперандних операцій, що забезпечило синтез математичних груп симетричних двохоперандних операцій на основі додавання за модулем два та додавання за модулем чотири;

– удосконалено метод підвищення стійкості та надійності потокового шифрування на основі додаткового застосування синтезованих груп симетричних двохоперандних операцій криптографічного перетворення інформації, що забезпечило підвищення стійкості та варіативності потокового шифрування.

3. Достовірність наукових результатів

Достовірність основних наукових результатів роботи підтверджується наведеною в розділах 2, 3 і 4 системою формальних методик і перетворень, що не містить принципових помилок, результатами комп'ютерного моделювання і впровадженням 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 засобів комп'ютерної криптографії з підвищеною стійкістю та варіативністю перетворення. Змістовний аспект запропонованого рішення, який спрямований на підвищення якості функціонування систем криптографічного захисту інформаційних ресурсів шляхом розширення класу методів синтезу операцій потокового шифрування і засобів, що їх реалізують, не був відомий раніше.

5. Практична корисність роботи

Практична корисність роботи обумовлена тим, що використання запропонованих в ній формальних методів і конкретних рішень дозволяє отримувати більш досконалі, порівняно з відомими, засоби потокового криптографічного перетворення інформації для комп'ютерних систем і мереж. Результати роботи впроваджено в Центральному конструкторському бюро «Сокіл» Науково-виробничого комплексу «ФОТОПРИЛАД» та в навчальний процес кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету.

6. Структура роботи

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

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 Черкаському державному технологічному університеті, наведено відомості про реалізацію і апробацію роботи, про публікації за її темою.

У першому розділі визначено, що одним із перспективних напрямів розвитку систем криптографічного захисту інформації є використання операцій криптографічного перетворення на основі логічних функцій. Розглянуто

сучасний стан досліджень операцій криптографічного перетворення інформації з виділенням особливостей застосування в потоковому та блочному шифруванні. Наводяться результати дослідження двохоперандних операцій криптоперетворення. Формулюється мета і задачі наукового дослідження.

Другий розділ присвячений математичному моделюванню та дослідженню двохоперандних операцій криптографічного перетворення інформації на основі відомих таблиць істинності. Побудовано математичні моделі для всіх операцій першої математичної групи, а також перестановочні схеми побудови даних операцій. На основі аналізу отриманих результатів було побудовано узагальнюючі перестановочні схеми для першої математичної групи двохоперандних операцій крипто перетворення. Розроблено метод побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту.

Третій розділ присвячений дослідженню другої математичної групи двохоперандних операцій крипто перетворення. Встановлено, що застосування повної групи побудованих перестановочних схем забезпечить побудову повної групи наборів двохоперандних операцій крипто перетворення, невідомої групи, та їх таблиць підстановки, якщо взяти будь яку операцію з даної невідомої групи.

Четвертий розділ присвячений присвячено розробці методів синтезу груп двохоперандних операцій криптоперетворення. Показано, що синтезовані моделі операцій та засоби їх застосування доцільно застосовувати в блоці крипто перетворення при реалізації методу підвищення стійкості та надійності потокового шифрування Наведені результати статистичних досліджень практичних результатів дисертаційної роботи.

У додатках подано акти про впровадження результатів дисертаційного дослідження, результати тестування та обов'язків додаток.

7. Публікації за темою дисертації

Наукові положення дисертації, що пов'язані з розробкою методів синтезу груп симетричних операцій для потокового шифрування достатньо повно відображені в публікаціях автора і пройшли апробацію на міжнародних науково-технічних конференціях і семінарах.

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 відзначити, відсутність порівняльного аналізу одно та двохоперандних операцій криптоперетворення виходячи з особливостей їх застосування в комп'ютерній криптографії; підрозділ 1.1. «Сучасні напрями розвитку методів криптографічного захисту інформації» (ст. 11-17) переповнений загальновідомими фактами та визначеннями які в подальших дослідженнях не використовуються; автор вживає поняття «симетрична операція» не наводячи визначення даного класу операцій, адже в криптографії властивість «симетричності» відноситься до оцінки крипто алгоритмів в цілому.

2. В другому розділі недостатньо формалізовано метод метод побудови та дослідження двохоперандних операцій крипто перетворення, етапи його реалізації наведено в підрозділах 2.1 -2.3 сумісно з прикладами синтезу, перетворення операцій та їх дослідження. Було б доцільно узагальнити етапи побудови методу в кінці розділу, наприклад алгоритмом його реалізації. Слід зауважити що наведені 24 математичних перетворення груп одноперандних операцій в двохоперандні ускладнюють сприйняття даного матеріалу в цілому.

3. В третьому розділі автор недостатньо уваги приділив опису порядку переходу від перестановочних схем до узагальнюючих перестановочних схем а також перестановочних схем для побудови таблиць істинності операцій, не достатньо розкриті взаємозв'язки між даними перестановочними схемами. Автор нажаль не виніс в основні наукові результати дослідження розроблений ним метод побудову повної групи наборів двохоперандних операцій крипто перетворення невідомої групи, та їх таблиць підстановки, на основі будь якої операції з даної невідомої групи. Даний метод було названо припущенням (ст..71, 106), справедливість якого доведена в даному розділі.

4. В четвертому розділі доведення коректності методу синтез операцій крипто перетворення групи двохрозрядних операцій додавання за модулем два на повній множині операцій (ст.111-117), а також аналогічне доведення методу синтез операцій крипто перетворення групи двохрозрядних операцій додавання за модулем чотири (ст.119-127) обтяжують математичними викладками дисертаційну роботу. Було б доцільно значну частину доведень коректності перетворення операцій винести в додатки.

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

10. Загальна оцінка дисертації

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове рішення важливої науково-технічної задачі, спрямованої на підвищення якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та варіативності перетворення на основі додаткового використання груп двохоперандних двохрозрядних операцій, синтезованих на основі додавання за модулем два та чотири. 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 Козловська Світлана Григорівна 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