ВІДГУК

офіційного опонента
про дисертацію Грицака Анатолія Васильовича
на тему «Методи побудови ефективних криптографічних функцій гешування», що представлена на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації»

Актуальність теми дисертаційного дослідження

Сучасна криптографія застосовується для розв'язання таких основних задач: 1) забезпечення конфіденційності даних; 2) перевірка справжності відправника (автентифікація); 3) не заперечення авторства; 4) забезпечення цілісності даних. Остання задача полягає у тому, що отримувач може перевірити несанкціоновану модифікацію в тексті, а зловмисник не може видати змінений текст за справжній. Одним із найбільш ефективних способів розв'язання зазначеної задачі є використання методів гешування, тобто перетворення вхідних даних довільної довжини у вихідні дані (бітовий рядок) фіксованої довжини (процес перетворення називається геш-функцією, а вихідні дані геш-кодом, або дайджестом). Криптографічні функції гешування дають змогу перевірити відповідність вхідних даних дайджесту, проте не дозволяють відновити вхідні дані за наявним дайджестом – саме ця властивість дозволяє забезпечити цілісність даних. Крім зазначеної, ефективна функція гешування має забезпечувати такі властивості, як висока швидкість обчислення та стійкість до колізій першого і другого роду. Серед сучасних геш-функцій варто відзначити Keccak, SHA-2, BCA, MD-5, Haval, N-hash, RIPE-MD, Kupyna (чинний національний стандарт України) та інші. Не зважаючи на велику номенклатуру існуючих методів і рішень, розробка та дослідження нових ефективних геш-функцій, які при достатньо високій швидкодії забезпечуватимуть необхідний рівень стійкості є актуальною науково-технічною задачею, що має теоретичне і практичне значення. Саме розв'язанню цієї науково-технічної задачі і присвячена дисертаційна робота Грицака Анатолія Васильовича, яка на мою думку, має важливе теоретичне і прикладне значення.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Викладені наукові положення, методики, висновки і рекомендації є повністю обґрунтованими, а достовірність запропонованих гіпотез і математичних моделей підтверджується відповідними експериментальними даними та результатами верифікації запропонованих методів і алгоритмів. Отримані, під час експериментів, дані відповідають теоретичним висновкам роботи і повністю підтверджують їх. До того ж, коректно застосовані методи теоретичної криптографії (дослідження швидкості і стійкості геш-функцій), скінченних полів та елементів теорії чисел (побудова функцій

гешування і криптоалгоритмів), об'єктно-орієнтованого програмування та математичної статистики (розробка програмних засобів, проведення експериментів і обробка їх результатів, аналіз колізійних властивостей геш-функцій).

Ідентичність змісту автореферату й основних положень дисертації

Проаналізувавши автореферат і дисертацію здобувача, можна зробити висновки, що в авторефераті з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертаційної роботи. Для основних положень дисертації та змісту автореферату характерна повна ідентичність. Крім того, варто зауважити, що усі компоненти дисертаційної роботи оформлено відповідно до чинних вимог.

Оцінка змісту та структури дисертації.

У **вступі** автором представлена загальна характеристика роботи, обґрунтована актуальність наукової теми, сформульовані мета і задачі дослідження, відображено наукову новизну та практичну цінність отриманих результатів і висновків, наведено дані щодо їх апробації та впровадження.

У **першому розділі** дисертації проведено аналіз сучасних методів і алгоритмів побудови та реалізації ефективних криптографічних функцій гешування, що дозволило виявити їх недоліки і формалізувати завдання наукового дослідження. Серед виявлених недоліків основними є уразливість відомих геш-функцій до криптоаналітичних атак, низька швидкість шифрування і високі вимоги до обчислювальних засобів. Також, визначено, що у сучасній криптографії необхідно виділити такі додатки геш-функцій, як протоколи електронного цифрового підпису, контроль цілісності даних з використанням спільного секрету, контроль цілісності даних без використання спільного секрету, генерація псевдовипадкових послідовностей (ПВП), протоколи встановлення ключів, протоколи автентифікації за паролем тощо.

Другий розділ присвячений розробці двох методів побудови функцій гешування – перший метод орієнтований на застосування у системах, для яких критичним є параметр стійкість, а другий – у системах, для яких критичним є параметр швидкість. Розроблено метод побудови функцій гешування, який за рахунок доповнення вхідного повідомлення розміром цього повідомлення та ПВП salt (розраховується на основі вхідного повідомлення), використання у функції стиснення нової послідовності операцій (на основі 6-ти нелінійних функцій, операцій підстановки, додавання за модулем 2 і 2^n, циклічних і лінійних зсувів), дозволив будувати крипостійкі функції гешування. Розроблено метод побудови функцій гешування, який за рахунок доповнення вхідного повідомлення ПВП salt (розраховується на основі вхідного повідомлення та його розміру), використання у функції стиснення додаткового вектору внутрішнього стану та нової послідовності операцій (на основі 4-х не лінійних функцій, операцій підстановки, перестановки,

додавання за модулем 2 і 2^n та циклічного зсуву), дозволив будувати швидкісні функції гешування.

У третьому розділі розроблено метод побудови генераторів псевдовипадкових послідовностей та метод криптографічного захисту інформації. Удосконалено метод побудови генераторів ПВП, який за рахунок обробки вектора внутрішнього стану та ключового вектору операціями підстановки, циклічного зсуву, складання за модулем 2 і 2^n та 4-ма нелінійними функціями, дозволив будувати ефективні генератори ПВП. На основі цього методу розроблено і реалізовано програмно три генератори ПВП, які будуть корисними як для функцій гешування, так і для інших криптографічних застосувань (генерування ключів, потокові шифри тощо). Удосконалено метод криптографічного захисту інформації, що за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дає можливість забезпечити конфіденційність і цілісність даних в ІКС.

Четвертий розділ дисертації присвячено практичним реалізаціям та експериментальним дослідженням розроблених рішень. Розроблено методику проведення експерименту, обґрунтовано доцільність вибору бази експерименту, визначено мету та задачі експерименту, вхідні та вихідні параметри, гіпотезу і критерії дослідження, достатність експериментальних об’єктів та послідовність необхідних дій. Для проведення експериментів на базі розроблених у другому розділі методів побудови функцій гешування було розроблено шість функцій гешування, а на базі розробленого у третьому розділі методу побудови генераторів ПВП було розроблено три генератори. Над розробленими криптографічними алгоритмами були проведені експериментальні дослідження згідно розробленій методиці. Розроблено спеціалізоване програмне забезпечення у вигляді консольних додатків на мові програмування C++ (середовище розробки Microsoft Visual Studio 2013 (Release Version)) та методику, що дозволило провести експерименти і верифікувати запропоновані методи.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи.

Наукова новизна результатів роботи

Наукова новизна отриманих результатів роботи полягає у наступному:

– вперше розроблено метод побудови функцій гешування, який базується на структурі Меркла-Демґарда та за рахунок доповнення вхідного повідомлення розміром цього повідомлення та псевдовипадковою послідовністю salt (розраховується на основі вхідного повідомлення), використання у функції стиснення нової послідовності операцій (на основі 6-ти не лінійних функцій, операцій підстановки, додавання за модулем 2 і 2^n, циклічних і лінійних зсувів), дозволив будувати криптостійкі функції гешування;

– вперше розроблено метод побудови функцій гешування, який базується на структурі Меркла-Демґарда та за рахунок доповнення вхідного повідомлення псевдовипадковою послідовністю salt (розраховується на основі вхідного повідомлення та його розміру), використання у функції стиснення додаткового вектору внутрішнього стану та нової послідовності операцій (на основі 4-х не лінійних функцій, операцій підстановки, перестановки, додавання за модулем 2 і 2^n та циклічного зсуву), дозволив будувати швидкісні функції гешування;

– удосконалено метод побудови генераторів псевдовипадкових послідовностей, який за рахунок обробки вектора внутрішнього стану та ключового вектору операціями підстановки, циклічного зсуву, складання за модулем 2 і 2^n та 4-ма нелінійними функціями, дозволив будувати ефективні генератори псевдовипадкових послідовностей;

– удосконалено метод криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в інформаційно-комунікаційних системах.

Повнота викладу основних результатів та висновків в опублікованих працях

Основні положення дисертації опубліковано в 11 наукових працях, у тому числі 6 наукових статей (1 – у міжнародному рецензованому періодичному виданні, що входить до бази даних Scopus, 5 – у вітчизняних і закордонних фахових наукових журналах), а також 5 матеріалів і тез доповідей на конференціях.

Крім того, зазначені положення дисертаційної роботи пройшли обов’язкову і достатню апробацію на наукових конференціях та семінарах в Україні і закордоном, зокрема на МНПК молодих учених і студентів «Політ. Сучасні проблеми науки» (м. Київ, 2016-2020 роки), МНТК «Проблеми експлуатації та захисту інформаційно-комунікаційних систем» (Київ, 2017 рік), МНПК «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації» (Верхній Студений, 2018 рік), МНТК «Сучасні засоби зв’язку» (Мінськ, 2019 рік) тощо.

Значення результатів для практики

Отримані в дисертаційній роботі результати можуть бути використані для підвищення ефективності забезпечення цілісності даних в ІКС та інших завданнях криптографічного захисту даних. Зокрема, практична цінність роботи полягає у такому:

– розроблено і реалізовано програмно шість нових функцій гешування (Oberih-1, Oberih-2, Oberih-3, Barvinok-1, Barvinok-2, Barvinok-3), які дозволяють забезпечити стійкість, підвищити швидкість у 1.15-1.36 разів (Oberih) або у 1.16-1.53 разів (Barvinok) і можуть бути використані для забезпечення цілісності

даних в ІКС, блокчейн системах, електронній пошті, системах миттєвого обміну повідомленнями (месенджерах) та інших сучасних застосунках;

- розроблено і реалізовано програмно три генератори ПВП (Viriy-1, Viriy-2, Viriy-3), які є швидшими у 1.02-1.22 разів в порівнянні з аналогами, що можуть бути використанні для криптографічних застосувань (генерування ключів, потокові шифри тощо) для підвищення їх ефективності;
- подано заявку на отримання патенту України на корисну модель «Спосіб побудови стійких функцій гешування» від 27.05.2020 року;
- результати дисертації використовуються у навчальному процесі Вінницького національного технічного університету, науковому процесі Національного авіаційного університету та ННВК «Інформаційно-комунікаційні системи».

Зауваження та недоліки

1. У першому розділі дисертації та в авторефераті наведено порівняльну таблицю сучасних функцій гешування за різними критеріями. Проте, на мою думку, у цій таблиці було б доцільно навести порівняння не лише із загальновідомими міжнародними стандартами і популярними алгоритмами, а й з розробками науковців, яких автор згадує у вступі до дисертаційної роботи.

2. Перші два наукові результати здобувача базуються на структурі Меркла-Демґарда, було б добре, щоб у другому розділі автор навів оригінальну структуру перед власною розробкою – це дало б можливість краще зрозуміти зміни в структурі, що пропонує автор.

3. Четвертий науковий результат, на мою думку, не у повній мірі відповідає предмету дослідження, зокрема у четвертому результаті вказано «удосконалено метод криптографічного захисту інформації…», а предмет на 15 стор. дисертаційної роботи визначено як «методи, способи та алгоритми побудови ефективних криптографічних функцій гешування».

4. У четвертому розділі дисертації здобувач наводить результати дослідження алгоритмів SHA-256, SHA-512, Snow, Trivium, Oberih, Barvinok, Viriy за методикою DIEHARD (стор. 100-104), проте не зрозуміло, як необхідно інтерпретувати ці результати. Наприклад, що стосується тестів NIST STS (рис. 4.1 – 4.14), то автор детально описує й тлумачить кожен отриманий результат тестування.

5. У п. 3.2 на стор. 71 дисертації прототипом для розробки методу побудови генераторів ПВП обрано MTProto Mobile Protocol v.1.0. Проте, не зрозуміло чому було обрано саме цей протокол і за якими критеріями. Добре було б, якби автор навів оригінальну схему цього протоколу для порівняння зі схемою, відображеною на рис. 3.3.

6. Тексти дисертаційної роботи та автореферату містять велику кількість скорочень, абревіатур, спеціальних позначень та формул, що ускладнює загальний процес оцінки роботи при її читанні. До того ж, не всі абревіатури та скорочення пояснені у відповідному переліку, що наведений у дисертації.

Висновки

Дисертаційна робота Грицака Анатолія Васильовича є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для розвитку теорії й практики систем захисту інформації. Усі одержані наукові результати можуть застосовуватися у різних галузях для забезпечення цілісності даних, які циркулюють в інформаційно-комунікаційних системах. Дисертація повністю відповідає спеціальності 05.13.21 – «Системи захисту інформації».

Отже, вважаю, що дисертаційна робота «Методи побудови ефективних криптографічних функцій гешування» повністю відповідає чинним вимогам МОН України, зокрема «Порядку присудження наукових ступенів», а її автор Грицак Анатолій Васильович заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент,
директор навчально-наукового інституту
Кібербезпеки, комп'ютерних і радіо технологій
Одеської національної академії зв'язку ім. О. С. Попова,

доктор технічних наук, професор Є.В. Василіу

ПІДПИС ЗАВІРЯЮ:
УЧЕНИЙ СЕКРЕТАР
ОНАЗ ім. О.С. Попова
Рудь Г.В.