УДК 004.056

В. В. Казміревський

ДОСЛІДЖЕННЯ СТІЙКОСТІ ДО ЛІНІЙНОГО ТА ДИФЕРЕНЦІЙНОГО КРИПТОАНАЛІЗУ ФУНКЦІЙ ГЕШУВАННЯ

Вінницький національний технічний університет

Анотація

Розглянуто та проаналізовано лінійний та диференційний криптоаналіз алгоритмів гешування. Розглянуто узагальнену структуру геш-коду. З використанням цієї структури розглянуто можливі атаки на геш-функції. Досліджено стійкість ряду алгоритмів гешування.

Ключові слова: *геш-функція, криптоаналіз, прообраз, алгоритм, лінійний криптоаналіз, диференційний криптоаналіз.*

Abstract

Linear and differential cryptological analysis of hashing algorithms was considered and analyzed. The general structure of the hash code was considered. With the use of this structure, possible attacks on hash functions was considered. The infeasibility of a number of hashing algorithms has been studied.

Keywords: *hash function, cryptanalysis, prototype, algorithm, linear cryptanalysis, differential cryptanalysis.*

Вступ

2022 рік в Україні характерний низці масових кібератак. Так 14 січня, значної шкоди зазнали 22 сайти органів державної влади. 70 сайтів було відключено за вказівкою СБУ та Держспецзв'язку [1]. Згодом спостерігались потужні DDoS-атаки, було зафіксовано перебої в роботі веб-сервісів Приватбанку та Ощадбанку та інших інформаційних ресурсах України. Кібератакам також піддалися сайти ЗСУ та Міністерства оборони [2]. Таким чином, випливає завдання захисту інформації та даних. Події, наведені вище, які пов'язані з атаками на різні ресурси та сервіси показали, що засоби захисту інформації потребують удосконалення або їх розроблення з новим підходом. До таких засобів захисту інформації віносять програмні модулі криптографічного захисту даних, у яких необхідно реалізовувати вибір методів гешування стійких до лінійного та диференціального криптоаналізу. Метою даного дослідження є покращення стійкості програмних бібліотек за рахунок криптоаналізу геш-функція, які вони реалізовують.

Для досягнення мети було розв'язано такі задачі:

- проаналізовано поняття геш-функції;
- проаналізовано методи криптоаналізу щодо їх застосування для геш-функцій;
- розроблено засіб, який складається з набору тестів для аналізу стійкості геш-функцій;
- проаналізовано результати тестування.

Криптографічні геш-функції

Функція гешування H(m) або геш-функція (hash-function) – це детермінована функція, на вхід якої подається рядок бітів довільної довжини, а виходом завжди є рядок бітів фіксованої довжини n. Значення геш-функції H(m) для входу m називають геш-значенням або скорочено гешем [3]. У літературі можна широко поширені і інші назви, а саме: геш, геш-образ, геш-код, згортка, дайджест повідомлення, криптографічна контрольна сума, код автентичності повідомлення, код виявлення маніпуляцій.

Криптоаналіз функцій гешування зазвичай зосереджений на дослідженні внутрішньої структури алгоритму стиснення і спирається на спроби знайти ефективні методи виявлення колізій при одноразовому виконанні функції [4].

Якщо ця проблема вирішена, то атакуючому залишається розглянути фіксоване початкове значення. Конкретний вид атаки на алгоритм стиснення залежить від внутрішньої структури цієї функції. Зазвичай, наприклад, коли мова йде про симетричні блокові шифри, алгоритм стиснення передбачає кілька раундів обробки даних, так що краще всього виконувати аналіз зміни побітової структури даних від раунду до раунду [4].

Слід при цьому мати на увазі, що колізії повинні існувати в будь-якій функції гешування, оскільки остання відображає, як мінімум, блок довжини b в геш-код довжини n, де b> n [4].

Потрібно лише обчислювальна неможливість виявити такі колізії [4, 5].

Лінійний криптоаналіз

У криптографії лінійний криптоаналіз є загальною формою криптоаналізу, заснованого на пошуку афінних наближень до дії шифру. Атаки були розроблені для блокових шифрів і потокових шифрів. Лінійний криптоаналіз є однією з двох найбільш широко використовуваних атак на блокові шифри; інший - диференційний криптоаналіз. Відкриття приписують Міцуру Мацуї, який вперше застосував цю техніку до шифру FEAL [6, 7].

Лінійний криптоаналіз складається з двох частин. Перший полягає в побудові лінійних рівнянь, що пов’язують відкритий текст, зашифрований текст і ключові біти, які мають велике зміщення; тобто ймовірності утримання (у просторі всіх можливих значень їхніх змінних) максимально наближені до 0 або 1. По-друге, використовувати ці лінійні рівняння разом із відомими парами відкритий текст та зашифрований текст для отримання ключових бітів [6, 7].

Диференційний криптоаналіз

Диференціальний криптоаналіз — це загальна форма криптоаналізу, застосовна насамперед до блочних шифрів, а також до потокових шифрів і криптографічних геш-функцій. У найширшому сенсі це дослідження того, як відмінності у введеній інформації можуть вплинути на результуючу різницю на виході. Відкриття диференційного криптоаналізу, як правило, приписують Елі Біхаму та Аді Шаміру наприкінці 1980-х, які опублікували низку атак на різні блочні шифри та геш-функції, включаючи теоретичну слабкість у стандарті шифрування даних (DES). Біхам і Шамір відзначили, що DES був напрочуд стійким до диференційного криптоаналізу, але невеликі модифікації алгоритму зробили б його набагато більш сприйнятливим [6, 7].

Диференціальний криптоаналіз, як правило, є атакою на вибраний відкритий текст, що означає, що зловмисник повинен мати можливість отримати зашифровані тексти для певного набору відкритих текстів на свій вибір. Однак, існують розширення, які дозволяють атакувати відомий відкритий текст або навіть атакувати лише зашифрованим текстом. Основний метод використовує пари відкритого тексту, пов'язані постійною різницею. Різницю можна визначити кількома способами, але операція виключне АБО (XOR) є звичайною. Потім зловмисник обчислює відмінності відповідних зашифрованих текстів, сподіваючись виявити статистичні закономірності їх розподілу [6, 7].

Криптоаналіз функцій гешування

Для криптоаналізу були вибрані такі геш-функції:

1) SHA-224,
2) SHA-256,
3) SHA-384,
4) SHA-512,
5) SHA3-224,
6) SHA3-256,
7) SHA3-384,
8) SHA3-512,
9) RIPEMD-128,
10) RIPEMD-160,
11) RIPEMD-256,
12) RIPEMD-320,
13) Scrypt.

Результати тестування алгоритмів гешування зобразимо на графіку (рис. 1), по осі X – бали, які набрали алгоритми під час аналізу, по осі Y – порядковий номер геш-функції.

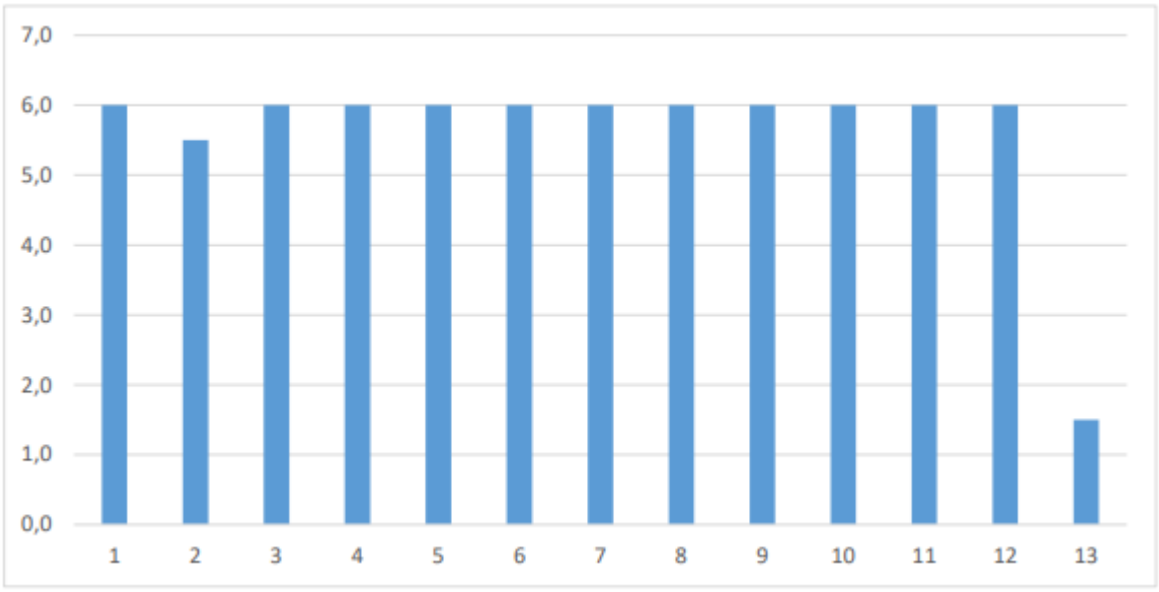

Рисунок 1 – Зображення графіку порівняння алгоритмів гешування

Криптоаналіз алгоритмів гешування показало, що найстійкішими алгоритмами є SHA-224, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RIPEMD-128, RIPEMD-160, RIPEMD-256, RIPEMD-320. Менш стійкою виявилася геш-функцій SHA-256. Алгоритм Scrypt показав найменший результат.

Висновки

Отже, розглянуто та проаналізовано основні методи лінійного та диференційного криптографічного аналізу геш-функцій. Таким чином, результатом проведеної робити є дослідження стійкості ряду функцій гешування SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RIPEMD-128, RIPEMD-160, RIPEMD-256, RIPEMD-320, Scrypt. Більшість геш-функцій показали відмінний результат, але необхідно памятати про те, що однозначно криптостійкого алгоритму не існує, криптостійкість алгоритму швидкоплинна, тому алгоритми постійно потребують свого криптоаналізу та вдосконалення. Математична ймовірність злому системи завжди вище, ніж інуїтивна оцінка цієї ймовірності. Даний висновок справедливий для всіх видів і типів криптографічних геш-функцій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кабінет Міністрів України - Від кібератаки 14 січня постраждали 22 державних органи, -Держспецзв'язку. (б.д.). Головна | Кабінет Міністрів України. https://www.kmu.gov.ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnih-organi-derzhspeczvyazku (дата звернення: 18.05.2022)

2. Кабінет Міністрів України - Щодо кібератаки на сайти військових структур та державних банків. (б.д.). Головна | Кабінет Міністрів України. https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv (дата звернення: 18.05.2022)

3. Баришев Ю. В., Лужецький В. А. Методи та засоби швидкого багатоканального гешування даних в комп'ютерних системах : монографія за заг. ред. В. А. Лужецького. м. Вінниця, ВНТУ, 2016. 144 с.

4. Казміревський В. В. Аналіз методів криптоаналізу геш-функцій: матеріали L науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії, м. Вінниця, 2021 р. URL: https://conferences. vntu.edu.ua/index.php/all-fitki/all-fitki-2021/paper/ view/12543 (дата звернення: 18.05.2022).

5. Антон Кудін, Богдан Коваленко. Диференційний аналіз функцій хешування та блокових шифрів: узагальнений підхід. URL: http://jrnl.nau.edu.ua/index.php/Infosecurity/ article/view/8734 (дата звернення: 18.05.2022).

6. Gaetan Leurent. Improved Differential-Linear Cryptanalysis of 7-round Chaskey with Partitioning. URL: https://www.iacr.org/archive/eurocrypt2016 /96650217/96650217.pdf (дата звернення: 18.05.2022).

7. Howard M. Heys. A Tutorial on Linear and Differential Cryptanalysis. URL: https://ioactive.com/wp-content/uploads/2015/07/ldc_tutorial.pdf (дата звернення: 18.05.2022).

Казміревський Віталій Віталійович — студент групи БС-21м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: kazmirevskiy1999@gmail.com

Науковий керівник: ***Баришев Юрій Володимирович*** – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця. email: yuriy.baryshev@vntu.edu.ua

Vitaliy Kazmirevs'kiy — Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: kazmirevskiy1999@gmail.com

Scientific supervisor: ***Yurii Baryshev*** – PhD (Eng), Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia. email: yuriy.baryshev@vntu.edu.ua