УДК 004.056.55+ 004.424.47

В. В. Казміревський

АНАЛІЗ МЕТОДІВ КРИПТОАНАЛІЗУ ГЕШ-ФУНКЦІЙ

Вінницький національний технічний університет

Анотація

Розглянуто та проаналізовано основні методи криптографічного аналізу геш-функцій, які ґрунтуються на знаходженні колізій, відновлення прообразу та властивостях конструкції гешування. Розглянуто узагальнену структуру геш-коду. З використанням цієї структури розгянуто можливі атаки на геш-функції.

Ключові слова: *геш-функція, криптоаналіз, методи криптоаналізу, колізія, прообраз, алгоритм, бумеранг.*

Abstract

The main methods of cryptographic analysis of hash functions are considered and analyzed. The main methods of cryptographic analysis of hash functions, which are based on the finding of collisions, the restoration of the prototype and the properties of the hash structure, are considered and analyzed. The generalized structure of the hash code is considered. Using this structure, possible attacks on hash functions have been unleashed.

Keywords: *hash function, cryptanalysis, cryptanalysis methods, collision, prototype, algorithm, boomerang*.

Вступ

Сьогодні важко переоцінити необхідність криптоаналізу. Останні часом спостерігається різке збільшення числа доповідей та відкритих текстів з усіх питань криптології, а криптоаналіз стає однією з найбільш активно розвинених областей досліджень. Багато криптосистем, стійкість яких не викликала особливих сумнівів, виявилися успішно розкритими. При цьому розроблений великий арсенал математичних методів, що представляють прямий інтерес для криптоаналітика.

Проведення криптоаналізу для давно існуючих і нових, що нещодавно з'явилися, криптоалгоритмів дуже актуально, так як вчасно можна сказати, що даний криптоалгоритм є нестійким, і що його потрібно вдосконалити його або замінити новим. Для того, щоб виявляти нестійкі криптоалгоритми необхідно весь час удосконалювати вже відомі методи криптоаналізу і знаходити нові [1]. Своє місце в криптоаналізі посіли і криптографічні геш-функції.

Метою даного дослідження є збільшення швидкості розробки засобів кібербезпеки, які використовують геш-функції за рахунок вибору достатнього набору методів криптоаналізу для дослідження показників їх стійкості.

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. [2].

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.

Якщо розглядати з точки зору криптографії, то геш-функція - це така функція, яка стійка до криптографічним атакам двох типів. А саме [2]:

1. Атака на відновлення першого прообразу. Припустимо, що зловмисник знає геш-код деякого повідомлення, тобто він знає, що h - це результат обчислення геш-функції від якогось повідомлення. Складність обчислення прообразу - це складність пошуку такого повідомлення M, що для нього геш-функція дорівнює заданої.
2. Стійкість другого роду. Коли нічого не задано, окрім алгоритму криптографічного гешування, зловмисник шукає два таких повідомлення, у яких збігається геш-функція (завдання пошуку колізій). Якщо такі колізії легко знайти алгоритмічно або обчислювально, то розглянута геш-функція вважається поганою з криптографічної точки зору.

Геш-функції широко застосовуються в сучасній криптографії. Їх використовують для перевіркаи цілісності файлів або повідомлень, як ідентифікатор файлу або даних, для псевдовипадкової генерації й утворення ключів, для побудиви геш-таблиць.

В даний час запропоновані і практично використовуються різні спеціальні алгоритми для обчислення геш-функції. Найбільш відомими алгоритмами є MD5, SHA-1, SHA-2 і інші версії SHA, а також алгоритм, викладений у ГОСТ Р 34.11-94.

Криптоаналіз геш-функцій

В останні роки були витрачені значні зусилля і досягнуті певні успіхи в справі розробки криптографічних методів аналізу функції гешування. Щоб зрозуміти їх, розглянемо структуру типової захищеної функції гешування, показану на рис. 1. [3].

Цю структуру, яка називається ітерованою функцією гешування, запропонував Меркле (Merkle), і саме таку структуру має більшість використовуваних сьогодні функцій гешування, включаючи MD5, SHA-1 і RIPEMD-160.

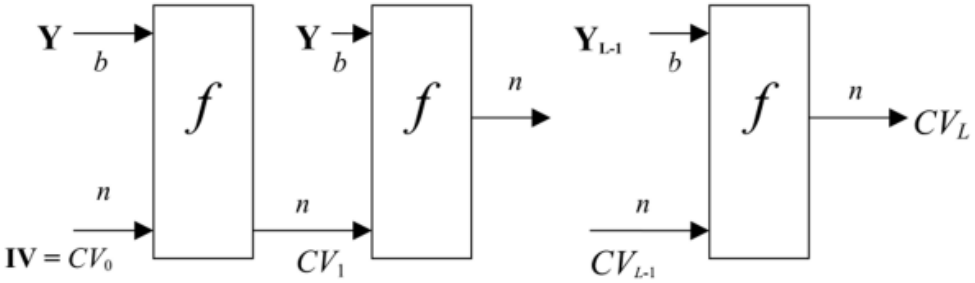

Рис. 1 – Загальна структура захищеного геш-коду

На рис. 1 прийняті позначення:

- IV - початкове значення;
- CV- змінна зчеплення;
- У - блок, що вводиться;
- / - алгоритм стиснення;
- L - число блоків;
- N - довжина геш-коду;
- b - довжина блоку.

Функція гешування отримує на вхід повідомлення і ділить його на L - 1 блоків рівній фіксованої довжини по b бітів кожен. Якщо необхідно, останній блок доповнюється до b бітів. В останній блок також включається значення сумарної довжини введення функції гешування. Це робить задачу противника ще більш складною. Противник повинен знайти або два повідомлення рівної довжини, що мають однакові значення функції гешування, або два повідомлення різної довжини, які разом з відповідними їм значеннями довжини матимуть однакові значення функції гешування.

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

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.

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.

Потрібно лише обчислювальна неможливість виявити такі колізії [3].

Методи криптоаналізу геш-функцій

Різниця у методах та особливостях криптоаналізу функцій гешування та блокових шифрів випливає з різних цілей аналізу. Головна відмінність криптоаналізу геш-функцій від криптоаналізу блокових шифрів полягає в тому, що в алгоритмах гешування відсутні невідомі для криптоаналітика ключі, замість них використовуються константи [4].

Для алгоритмів гешування найхарактернішими є такі атаки:

1. Атаки побудови колізії:

− пошук слабкої колізії,

− пошук колізії з вибраним префіксом,

− пошук сильної колізії.

2. Атаки пошуку прообразу:

− пошук прообразу,

− пошук псевдопрообразу.

Атака побудови колізії.

Зважаючи на велику різноманітність способів побудови геш-функцій, універсальних методів пошуку колізій не існує. Для багатьох функцій єдина можливість знаходження ефективних алгоритмів пошуку колізій полягає в аналізі відповідних математичних задач.

Для геш-функцій, у яких довжина геш-значення невелика, універсальним методом пошуку колізій є метод, заснований на так званому "парадоксі дня народження". Цей метод добре відомий і був описаний ще в 1979 р Ювалом [5].

Парадокс днів народження - це твердження, що ймовірність збігу днів народження (дати) хоча б у двох членів групи з 23 і більше осіб, перевищує 0,5 [6].

Атака знаходження прообразу.

У криптографії, атака знаходження прообразу криптографічної геш-функції - це спроба відшукати повідомлення із заданим значенням геш-кодування. Існують два типи подібних атак [6]:

1. Атака знаходження першого прообразу: за даним значенням хешу h знайти таке повідомлення m, що hash (m) = h.
2. Атака знаходження другого прообразу: по даним повідомленням m1 знайти відмінне від нього повідомлення m2 таке, що hash (m2) = hash (m1). Для ідеальної n-бітової геш-функції складність знаходження першого прообразу становить 2^n.

Розроблені на сьогоднішній момент атаки на прообраз не є практично придатними. Якщо таку атаку можливо буде застосувати на практиці, то це сильно вплине на багато протоколів мережі Інтернет. У цьому ключі, слово «практичний» означає, що атака може бути проведена за розумний час при розумних витратах [6].

Крім методів пошуку колізій, криптоаналіз геш-функцій включає в себе також широкий спектр методів аналізу слабкостей алгоритмів гешування. Хоча ці слабкості не призводять до прямих атак на геш-функції, вони впливають на оцінку стійкості останніх. І більшість геш-функції реалізовані на основі блокових шифрів. Тому можливо застосувати до них ще атаку методом бумеранга. Хоча тут існують і свої перешкоди. Проте, атака методом бумеранга, а саме посилена атака методом бумеранга, може бути практично застосована для злому геш-функції. Це свого роду диференційна атака.

Основна ідея адаптації атаки полягає в використанні ретельно підібраного глобального диференційного шляху, який використовується в класичних атаках диференційного криптоаналізу [7]. Дана атака була успішно застосована до алгоритму SHA-1.

Також при аналізі геш-функцій варто звернути увагу на саму конструкцію гешування та її властивості. Адже на конструкцію геш-функцій також можливі атаки. Складність реалізації цих атак не залежить від способу реалізації геш-функції, а тому вони можуть бути використані для всіх геш-функцій певної конструкції. Сьогодні в основному розглядаються геш-функції конструкції Меркля–Дамгаарда, а також деякі її модифікації. Але й інші геш-функції конструкцій, відмінних від конструкції Меркля–Дамгаарда, також є вразливими. До таких атак належать: стала атака збільшення довжини повідомлення, яка обумовлюється ітеративністю процесу гешування та полягає у дописуванні до повідомлення блоків даних доти, доки геш-значення початкового та доповненого повідомлень не збігаються; атаки, що використовують мультиколізії (стала атаку Жу, знаходження певних аналогів фіксованих точок). [8].

Висновки

Отже, розглянуто та проаналізовано основні методи криптографічного аналізу геш-функцій. Таким чином, порівнюючи інтуїтивну оцінку ймовірності порушення криптостійкості геш-функцій можна зробити висновок про те, що однозначно криптостійкості систем не існує. 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 А. В. Казимиров. Методы и средства генерации нелинейных узлов замены для симметричных криптоалгоритмов. URL: https://okazymyrov.github.io/assets/attachments/theses/2014/daaa5576d6c6ecb227c6ae888cdce3.pdf дата звернення: 23.02.2021).

2 Лекция 5. Криптографические хеш-функции. [Електронний ресурс]. – Режим доступу: https://mipt.lectoriy.ru/file/synopsis/pdf/CompTech-InforSecur-M05-Vladim-131005.01.pdf (дата звернення: 23.02.2021).

3 Франчук В.М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. URL: https://vfranchuk.fi.npu.edu.ua/images/files/statty/32_ZIR_cript.pdf (дата звернення: 23.02.2021).

4 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: 23.02.2021).

5 Захист інформації. Криптографічні методи : Підруч. для вищ. навч. закл. / І.І. Маракова, А.І. Рибак, Ю.С. Ямпольський; Одес. держ. Політехн. ун-т, Ін-т радіоелектрон. і телекомунікацій. - О., 2001. - 174 с.

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

7 О.Н. Жданов, В. В. Золотарев. Методы и средств криптографической защиты информации.]. URL: http://window.edu.ru/catalog/pdf2txt/755/66755/39526?p_page=1 (дата звернення: 23.02.2021).

8 Баришев Ю. В., В. А. Лужецький Методи та засоби швидкого багатоканального гешування даних в комп'ютерних системах : монографія за заг. ред. В. А. Лужецького. Вінниця, ВНТУ, 2016. 11 с.

Казміревський Віталій Віталійович — студент групи 1БС-17б, 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

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

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