УДК 004.056 : 004.424.47

Слободян С. О.
Науковий керівник: к. т. н., доц. Баришев Ю. В.

КОНСТРУКЦІЇ ГЕШУВАННЯ ІЗ ЗАВ'ЯЗУВАННЯМ БЛОКІВ ДАНИХ

Вінницький національний технічний університет

Анотація: *У даній роботі представлено аналіз атак, які грунтуються на знаходженні мультиколізій та методів протидії ним. Проаналізовано відомі підходи підвищення стійкості гешування до мультиколізій. Запропоновано новий підхід до побудови конструкцій гешування стійкого до мультиколізій.*
Ключові слова: *конструкція гешування, мультиколізії, атака Жу.*

Abstract: *This work presents an analysis of attacks which are based on multicollision finding and their counteraction methods. Known approaches were analyzed to improve the hash infeasibility against multicollision. The new approach of multicollision resistant hash constructions designing.*
Key words: *hash construction, multicollisions, Joux attack.*

Для функціонування інформаційних технологій періодично необхідно розв'язувати задачі автентифікації користувачів та перевірки цілісності даних. Для забезпечення криптографічностійкої стійкості при реалізації поставлених задач використовують алгоритми гешування [1].

Оскільки існують загальні атаки на конструкції гешування й загрози аналізу та підбору геш-значення, усі методи гешування що мають однакові конструкції будуть чутливі до цих атак.

Метою дослідження є підвищення стійкості гешування до загальних атак.

Відома низка методів підвищення стійкості гешування до загальних атак. Зокрема відомий метод Правіна Гаураварама, який передбачає підвищення стійкості за рахунок формування контрольної суми з блоків повідомлення та проміжних значень геш-функції (рис. 1) [4].

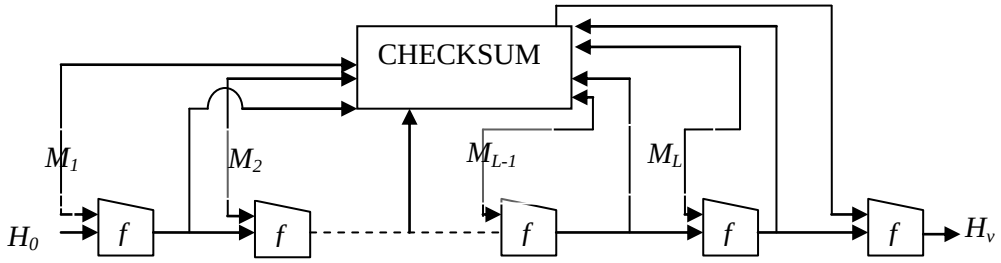

Рисунок 1– Конструкція гешування з лінійною контрольною сумою

Отримане значення контрольної суми подається вхідний аргумент функції ущільнення на останній ітерації . Однак аналіз таких підходів показав несуттєве зростання стійкості внаслідок їх реалізації [3]. Такий підхід дещо ускладнює роботу зловмисника за рахунок введення додаткових обчислень на кожному з проміжних етапів, але не відіграє значної ролі в подоланні геш-атак загалом. Алгоритм гешування передбачає використання лінійних операційдля зав'язування блоків даних тому зловмисник, як і перед вдосконаленням функції має можливість реалізовувати загальні атаки.

Для покращення методів гешування запропоновано конструкцію, наведену на рис. 2.

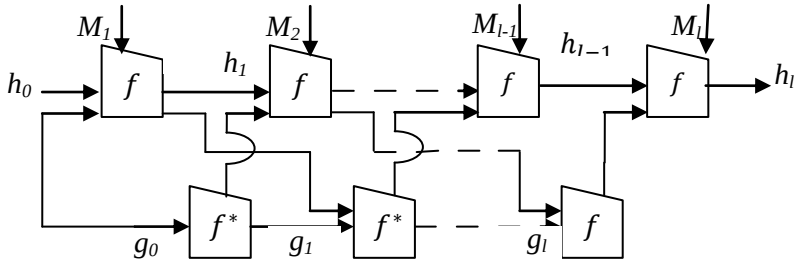

Рисунок 2– Конструкція гешування, що усуває лінійні залежності в зав'язуванні блоків даних

На вхід функції ущільнення подається значення елементів масиву, проміжних значень h_i та g_i. В основі побудови нового методу лежить ідея введення залежності проміжних геш-значень від певного виразу, що обчислюється на кожній ітерації, наприклад таким чином:

$$\begin{cases} h_i = f(h_i, g_i, m_i) \\ g_i = f^*(h_{i-1}, g_{i-1}) \end{cases},$$

де g_i обчислюється для кожної ітерації окремо та формується із значень отриманих на попередній ітерації .

Дану конструкцію пропонується удосконалити шляхом введення додаткових залежностей між проміжними геш-значеннями з метою протидії атаці Нострадамуса, представлена в роботі [5]:

$$\begin{cases} s = rand(h_{i-2}, g_{i-1}) \\ g_i = f^*(h_{i-1}, s) \\ h_i = f(h_{i-1}, g_{i-1}, m_i) \end{cases},$$

де s – псевдовипадкове значення, що формується на основі попередніх ітерацій g_i та h_i. В свою чергу значення g_i обчислюється для кожної ітерації окремо та формується із власного попереднього проходу та попередньої ітерації h_i.

Оскільки значення h_i залежить від інших аргументів, що обчислюються на кожній ітерації, утруднюється атака Kelsey–Kohno, адже для її реалізації важливою є незалежність геш-значення на *i*-й ітерації від геш-значень, отриманих на всіх ітераціях, крім попередньої [1].

Введення залежностей h_i від інших аргументів дозволяє підвищити стійкість геш-функції до загальних атак, зокрема до атаки Нострадамуса [5], однак дані конструкції мають недолік, пов'язаний із несуттєвим зростанням стійкості до атаки Жу, що обумовлює необхідність подальших досліджень в даній галузі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В. А. Лужецький. Конструкції гешування стійкі до мультиколізії / В. А. Лужецький, Ю. В. Баришев // Наукові праці ВНТУ. – №1–2011. – 8 с. – Режим доступу до ресурсу : praci.vntu.edu.ua/article/download/1032/62

2. В. А. Лужецький. Методи та засоби паралельно керованого гешування /В. А. Лужецький, Ю. В. Баришев// Наукові праці ВНТУ. – № 2–2011. – 6 с. – Режим доступу до ресурсу : http://praci.vntu.edu.ua/article/view/1372

3. Kelsey J. Second preimages on *n*-bit Hash Function for Less than 2^n Work. / J. Kelsey, B. Schneier //Cryptology ePrint Archive. – 2004. – 15 с. – Режим доступу до ресурсу : http://eprint.iacr.org/2004/304.pdf

4. P. Gauravaram. Cryptanalysis of a class of cryptographic hash functions / P. Gauravaram, J. Kelsey //Cryptology ePrint Archive. – 30 с. – Режим доступу до ресурсу : http://eprint.iacr.org/2007/277.pdf

5. J. Kelsey. Herding Hash Functions and the Nostradamus Attack / J. Kelsey, T. Kohno // National Institute of Standards and Technology. – 18 с. – Режим доступу до ресурсу : https://eprint.iacr.org/2005/281.pdf

Слободян Світлана Олександрівна факультет інформаційних технологій так комп'ютерної інженерії, студент групи БС-12б, Вінницький національний технічний університет, Вінниця, feride.fe@list.ru.

Баришев Юрій Володимирович кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, yuriy.baryshev@gmail.com.

Slobodyan Svitlana faculty of Information Technologies and Computer Engineering, student group BS-12b, Vinnytsya National Technical University, Vinnytsya, feride.fe@list.ru.

Baryshev Yurii ph.d asosiate professor of information protection Vinnytsya National Technical University, Vinnytsya, yuriy.baryshev@gmail.com.