Метод гешування з псевдовипадковою вибіркою блоків даних

Лужецький В.А.[1], Гадалін М.С.[2]

[1]Проф., д.т.н., завідувач кафедри захисту інформації, Вінницький національний технічний університет
вул. Хмельницьке шосе 95, м. Вінниця, Україна
[2]Аспірант кафедри захисту інформації, магістр з безпеки інформаційних та комунікаційних систем, Вінницький національний технічний університет
вул. Хмельницьке шосе 95, м. Вінниця, Україна, mykhailo.gadalin.vntu@gmail.com

***Анотація* — Представлено метод гешування із псевдовипадковою вибіркою блоків даних. Показана реалізація розпаралелених обчислень і зв'язування кінцевих результатів обчислень. Описано процеси гешування і вибірки блоків даних для формування окремих послідовностей.**

Ключові слова: метод гешуваннчя, розпаралелені обчислення, генератор псевдовипадкових послідовностей.

The hashing method with pseudorandom data blocks selection

Luzhetskyi V.A.[2], Gadalin M.S.[1]

[1] Prof., Head of Information Protection Department, Vinnytsia National Technical University
Khmelnytske shose str., 95, Vinnytsia, Ukraine
[2]Postgraduate of Information Protection Department, MA of Information and Communication Systems Security, Vinnytsia National Technical University
Khmelnytske shose str., 95, Vinnytsia, Ukraine, mykhailo.gadalin.vntu@gmail.com

***Abstract* — The hashing method with pseudorandom data blocks selection has been presented. Parallel calculation realization and final calculation results binding has been showed. Hashing and data blocks selection processes has been described.**

Keywords: hashing, parallel calculations, pseudorandom sequence generator.

I. Вступ

На сьогоднішній день використання геш-функцій в криптографічному захисті інформації значною мірою пов'язано з двома основними аспектами: це використання даних функцій в протоколах автентифікації та при створенні електронного цифрового підпису [1].

Проте, з розвитком технологій постійно розвиваються вимоги до забезпечення нових, швидших і безпечніших геш-функцій, значною мірою через те, що й розвиваються атаки та методи зламу даних криптографічних примітивів. Особливо ці вимоги помітні при використанні електронної комерції, електронних розрахунків та електронного банкінгу [1].

Хоча вже досить тривалий час існує новий метод гешування, відомий як геш-функція Keccak [2], багато організацій продовжують використовувати такі поширені та відомі геш-функції, як MD-5 та SHA-2 [3]. Але ці геш-функції не використовують розпаралелення обчислень, тому їх реалізація відносно повільна, а, отже, актуальною є задача створення нових швидких і надійних методів гешування [4].

Одним із перспективних підходів є власне побудова геш-функцій з розпаралеленням обчислень. При цьому, важливим питанням є організація зв'язування проміжних результатів блоків даних і реалізація функції ущільнення, як є невід'ємною складовою геш-функції [5].

II. Опис методу гешування

Вхідне повідомлення M розбивається на n блоків довжиною l кожен [6]:

$$M = \{m_1, m_2, \ldots, m_n\}.$$

З послідовності блоків M формуються дві послідовності M^0 та M^1 [7]:

$$M^0 = \{m^0_1, m^0_2, \ldots, m^0_k\};$$
$$M^1 = \{m^1_1, m^1_2, \ldots, m^1_r\};$$
$$n = k + r.$$

Формуються початкові геш-значення H^0_0 та H^1_0 довжиною l кожне для послідовностей M^0 та M^1 відповідно [7].

Процес гешування відбувається паралельно та незалежно для кожної з послідовностей M^0 та M^1.

Для отримання поточного геш-значення використовується функція ущільнення $f()$:

$$H^p_i = f(H^p_{i-1}, m^p_i),$$

де p – номер послідовності: 0 або 1;
H^p_{i-1} – попереднє геш-значення послідовності p;
m^p_i – i-й ***блок послідовності*** M^p.

Процес гешування відбувається ітеративно до моменту отримання результуючого геш-значення H^p для кожної з послідовностей M^0 та M^1. Для знаходження остаточного геш-значення H повідомлення M виконується функція ущільнення $F()$ між геш-значеннями H^0 і H^1 послідовностей M^0 та M^1 [7]:

$$H = F(H^0, H^1);$$

Довжина результуючого геш-значення H дорівнює l.

Процес отримання результуючого геш-значення вхідного повідомлення M шляхом утворення послідовностей M^0 та M^1 реалізує зв'язування результатів паралельних обчислень.

III. Процес формування послідовностей

На основі вхідного повідомлення M генерується початкове значення I генератора псевдовипадкових послідовностей (ГПВП):

$$I = B(M),$$

де $B()$ – функція отримання початкового значення ГПВП.

На основі початкового значення I ГПВП генерує послідовність G довжиною n [7]:

$$G = \{g_1, g_2, \ldots, g_n\},$$

де $g_i = \{0; 1\}$.

Послідовності M^0 та M^1 формуються наступним чином. Для кожного блоку m_i послідовності M перевіряється відповідне значення g_i послідовності G. Якщо $g_i = 0$, блок m_i відноситься до послідовності M^0. У випадку, коли $g_i = 1$, блок m_i відноситься до послідовності M^1.

Процес формування послідовностей є ітеративним і починається з першого блоку m_1 послідовності M. На кожній ітерації, після віднесення блоку m_i до послідовності M^p, знаходиться значення v:

$$v = C(m_i),$$

де $C()$ – функція знаходження номера блока повідомлення M для наступної обробки.

Після знаходження значення v блок m_i видаляється з послідовності m_i, а значення g_i видаляється з послідовності G. Наступна ітерація виконується над блоком m_i, де $i = v$.

Формування послідовностей M^0 та M^1 закінчується після обробки останнього блоку послідовності M.

Даний підхід дозволяє змінити значення та порядок блоків послідовностей M^0 та M^1 при зміні блоків вхідного повідомлення M.

Завдяки тому, що початкове значення ГПВП I формується на основі значення вхідного повідомлення M, то при зміні навіть одного блоку останнього, також змінюється значення I, а, отже, змінюється вигляд послідовності G, що в свою чергу змінює вміст та порядок блоків послідовностей M^0 та M^1.

Крім того, ітеративне обчислення номера блока повідомлення M перед кожним віднесенням до однієї з послідовностей M^0 та M^1 дозволяє змінити позицію останнього блоку, який є найменш впливовим на результуюче геш-значення кожної з послідовностей.

IV. Висновки

Представлений метод гешування дозволяє реалізувати розпаралелені обчислення, що, в свою чергу, забезпечує збільшення швидкості гешування порівняно з послідовним обчисленням геш-значення. Розбиття вхідного повідомлення M на дві послідовності M^0 та M^1 дозволяє виконувати обчислення над кожною із них незалежно від іншої.

При чому отримання геш-значення для кожної з послідовностей M^0 та M^1 займе приблизно однаковий час, тому що ймовірність появи 0 та 1 в послідовності G, що формується ГПВП, однакова, а, отже, кількість блоків послідовностей M^0 та M^1 приблизно однакова.

У запропонованому методі гешування може використовуватись будь яка функція ущільнення, що робить його універсальним, а також залишається можливість для подальших досліджень та удосконалень.

[1] Коробейников А. Г. Математические основы криптологии : учебное пособие / А. Г. Коробейников, Ю. А. Гатчин. – СПб : СПб ГУ ИТМО, 2004. – 106 с. : илл.

[2] Keccak implementation overview Version 3.2 [Електронний ресурс] / G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, – 69 с. Режим доступу: http://keccak.noekeon.org/Keccak-implementation-3.2.pdf. – Назва з екрану.

[3] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. 2-е изд. / Брюс Шнайер. – СПб. : Вильямс, 2000. – 789 с.

[4] Математичні основи криптографії : навч. посібник / Кузнецов Г.В. [та ін.]. – Дніпропетровськ : Національний гірничий університет, 2004. – Ч1. – 391 с.

[5] Ростовцев А. Г. Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. – СПб : Профессионал, 2005. – 490 с.

[6] Лужецький В. А. Метод гешування із зав'язуванням блоків даних / В. А. Лужецький, М. С. Гадалін // тези доповідей Четвертої Міжнародної науково-практичної конференції: «Методи та засоби кодування, захисту й ущільнення інформації». м. Вінниця, 23-25 квітня 2013 року. – Вінниця : ВНТУ, 2013. – 386 с.