УДК 681.12

В. І. Смішко[1]
Л. В. Крилик[1]

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ГЕШУВАННЯ ЦИФРОВИХ ДАНИХ НА ОСНОВІ ЛІЧИЛЬНИКА

[1] Вінницький національний технічний університет;

Анотація

Запропоновано математичну модель та інформаційну технологію гешування цифрових даних на основі лічильника, яке дозволило підвищити швидкодію гешування за рахунок меншого використання ресурсів комп'ютера на обчислювальні операції, а тому відповідає вимогам малоресурної криптографії.

Ключові слова: геш-функція, математична модель, інформаційна технологія, малоресурна криптографія.

Abstract

The mathematical model and information technology of digital data hashing on the basis of a counter was proposed, which allowed to increase the speed of hashing due to less use of computer resources for computational operations, and therefore meets the requirements of low-resource cryptography.

Keywords: hash function, mathematical model, information technology, low-resource cryptography.

Вступ

Більшість сучасних алгоритмів захисту інформації і, зокрема, шифрування, розраховані на застосування в електронно обчислювальній техніці (ЕОТ) у складі програмних комплексів без урахування оптимізації на рівні апаратного забезпечення. Цей факт унеможливлює застосування більшості існуючих криптографічних алгоритмів у пристроях з обмеженою обчислювальною потужністю, малим обсягом і малим енергоспоживанням. Ці системи також мають назву «системи з низькою вартістю», а методи криптографічного захисту даних в них «методи малоресурсної криптографії». Таким чином, сьогодні є актуальними дослідження з позицій малоресурсної криптографії таких базових примітивів як геш-функції [1].

Метою роботи є розроблення інформаційної технології та математичної моделі геш-функції, яка має підвищену швидкодію та зменшене використання ресурсів процесора.

Результати дослідження

Пропонується новий підхід до побудови геш-функцій [2] з байт-орієнтованою обробкою даних. Вхідне повідомлення M розглядається як послідовність байтів $M=\{ m_1, m_2, \ldots, m_L\}$. Геш-функція – це функція, яка певним чином пов'язує ASCII-коди байтів m_i та номери позицій l (l = 1, 2, …) цих байтів у повідомленні.

Передбачається гешування даних довільної довжини та отримання геш-значення розміру 128 біт. Геш-значення формується з ASCII-кодів байтів з урахуванням номерів позицій l.

Виходячи із заданої довжини геш-значення l_h визначається кількість байт, що будуть використовуватися для обчислень:

$$g = l_h / 8 \tag{1}$$

Наприклад, при довжині геш-значення 128 біт, це геш-значення представляється у вигляді набору з 16 елементів, кожен з яких є байтом (128=8×16), відповідно для довжини 192 біт набір складається з 24 елементів (192=8×24), а для 256 – з 32 елементів (256=8×32).

При цьому, номер позиції байта, використовуваний у подальшому, визначається за формулою:

$$q = l \bmod 2^g . \tag{2}$$

Початкове геш-значення h_0 є сукупністю псевдовипадкових чисел і має вигляд:

$$h_0 = \{h_{0,0}, h_{0,1}, \ldots, h_{0,(g-1)}\}. \tag{3}$$

Номер позиції q байта у повідомленні розглядається як двійковий код:

$$q = \sum_{i=0}^{g-1} a_i \cdot 2^i \cdot \tag{4}$$

Проміжні геш-значення $h_l = \{h_{l,0}, h_{l,1}, ..., h_{l,(g-1)}\}$ обчислюється на основі попереднього геш-значення h_{l-1}, двійкового представлення номера позиції q та ASCII-кода байта n_l :

$$\begin{aligned} h_{l,j} &= h_{(l-1),(j-1)} \bigoplus (n_l \cdot a_{j-1}), \\ h_{l,0} &= h_{l,(g-1)} \bigoplus (n_l \cdot a_{g-1}), \end{aligned} \tag{5}$$

де $j = 1,2,...,(g-1)$.

Схему обчислень геш-значень за даним методом наведено на рис. 1

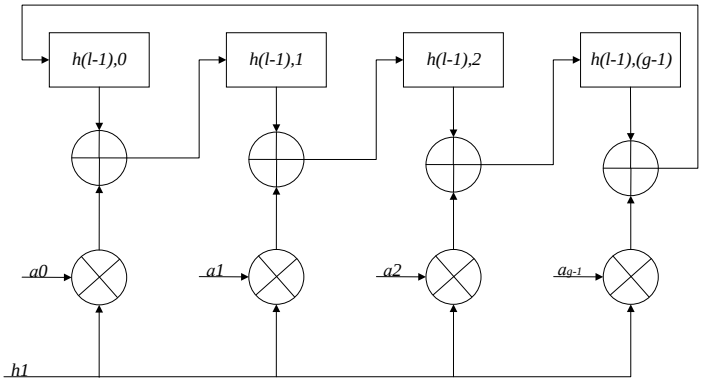

Рисунок 1 – Схема обчислень геш-значень

Для гешування одного байту даних потрібно виконати g операцій додавання за модулем 2 двох кодів байтів і $(g+1)$ операцій запису коду в регістр.

Було спроектовано власне програмне забезпечення гешування цифрових даних на основі запропонованої математичної моделі. Програму написано мовою програмування високого рівня C# під операційну систему Windows. Розроблене програмне забезпечення має більшу швидкодію (у середньому в 1,26 раз, тобто на 26%), ніж аналогічна програма HashTab.

Висновки

Встановлено, що запропонований метод та математична модель гешування цифрових даних дозволяє підвищити швидкодію (у середньому в 1,26 раз, тобто на 26%) за рахунок меншого використання ресурсів комп'ютера на обчислювальні операції.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Малоресурсна криптографія [Електронний ресурс]. – Режим доступу: URL: http://www.intuit.ua/informaciini-tehnologiyi_-metodi-zahistu_-legkovagova-kripto-std37839.html – Назва з екрану.

2. Горбенко І. Д. Сучасні підходи до побудування геш-функцій з підвищеною стійкістю./ І. Д. Горбенко, А. О. Бойко.– Київ: Рожко, 2009р. – 447 с.

Смішко Віталій Ігорович — студент групи 1КН-17м, факультет інформаційних технологій та компютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vitaliksmile777@gmail.com

Науковий керівник: ***Крилик Людмила Вікторівна*** — к.т.н., доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця

Smishko Vitaliy I. — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : vitaliksmile777@gmail.com

Supervisor: ***Krylyk Liudmila V.*** — PhD (Eng.), docent, Chair of Computer Sciences, Vinnytsia National Technical University, Vinnytsia