Метод малоресурсного гешування типу «генератор-дані»

Володимир Лужецький
кафедра Захисту Інформації
Вінницький національний технічний університет
Вінниця, Україна
v.luzhetskyi@vntu.edu.ua

Віталій Селезньов
кафедра Захисту Інформації
Вінницький національний технічний університет
Вінниця, Україна
seleznov.vitalii@mail.com

Method of low-resource hashing type «generator – data»

Volodymyr Luzhetskyi
Doctor of Technical Science, Professor, Head of Information Security Department
Vinnytsia National Technical University
Vinnytsia, Ukraine
v.luzhetskyi@vntu.edu.ua

Vitalii Seleznov
Information Security Department
Vinnytsia National Technical University
Vinnytsia, Ukraine
seleznov.vitalii@mail.com

***Анотація* — Запропоновано новий метод малоресурсного гешування, що базується на конструкції Меркла-Демґарда та використовує новий підхід типу «генератор-дані», особливість якого полягає у обчисленні геш-значень на основі станів генератора псевдовипадкових чисел, для вибору яких використовуються вхідні дані для гешування.**

***Abstract* — A new lightweight hashing method is proposed, based on the Merkle-Damgård construction and utilizing a new "generator-data" approach. Its key feature is the computation of hash values based on the states of a pseudo-random number generator, with input data for hashing used to select these states.**

Ключові слова — метод гешування; малоресурсна криптографія; функція ущільнення; геш-значення

Keywords — hashing method; low-resource cryptography; compression function; hash value

I. Вступ

У сучасному світі широкого розповсюдження набули пристрої Інтернету речей, серед яких зростає частка тих, що вимагають обмежених апаратних витрат для їх реалізації. Водночас, до таких пристроїв висувається вимога забезпечення захисту даних, що обробляються та передаються мережею Інтернет. Сучасні криптографічні алгоритми, що реалізуються як правило програмно є непридатними для побудови апаратних засобів малоресурсної криптографії [1-3].

Малоресурсне гешування використовується у пристроях з обмеженими ресурсами (RFID пристроях) для контролю цілісності даних та в різних протоколах автентифікації користувачів і повідомлень. Останні дослідження та публікації, присвячені малоресурсному гешуванню, демонструють необхідність розробки нових й оптимізації існуючих методів та підходів до малоресурсного гещування, що змогли б відповідати сучасним вимогам до безпеки, забезпечувати оптимальну продуктивність та мінімальну апаратну складність реалізації [2].

В роботі запропоновано метод малоресурсного гешування типу «генератор-дані», що дозволяє обчислювати геш-значення довжини 128, 192 або 256 біт, забезпечуючи при цьому складність апаратної реалізації, що не перевищує 2000 GE (gate equivalent) [4].

II. Основна частина

Запропонований метод малоресурсного гешування використовує підхід «генератор-дані», що є альтернативою до підходу «дані-генератор», який використано в геш-функції HDG та описано авторами у статті [2].

Процес гешування виконується відповідно до конструкції Меркла-Демґарда. Дані, що підлягають гешуванню, подано у вигляді масиву *M*, що складається з блоків довжини 1 байт [6].

$$M = \{m_1, m_2, ..., m_n\}, \quad (1)$$

Гешування є ітераційним процесом. Початкове геш-значення h_0 є сукупністю восьми *k*-розрядних блоків ($k = \frac{l}{8}$, де l – довжина геш-значення в бітах).

Проміжні геш-значення h_i визначаються, як значення функції ущільнення:

$$h_i = f(m_i; h_{i-1}), \quad (2)$$

де $m_i = \{m_{i,0}, m_{i,1}, ..., m_{i,7}\}$.

Процес реалізації функції ущільнення для *i*-го байту даних передбачає виконання таких дій:

1. Для j від 0 до 7 виконати:

2. Згенерувати *k*-розрядне псевдовипадкове число g_j

3. Виконати обчислення:

$$h_{i,j} = h_{i-1,j} \oplus (g_{7-j} \cdot m_{i,(7-j)}) \quad (3)$$

Схему обрахунку функції ущільнення за методом гешування наведено на рис. 1.

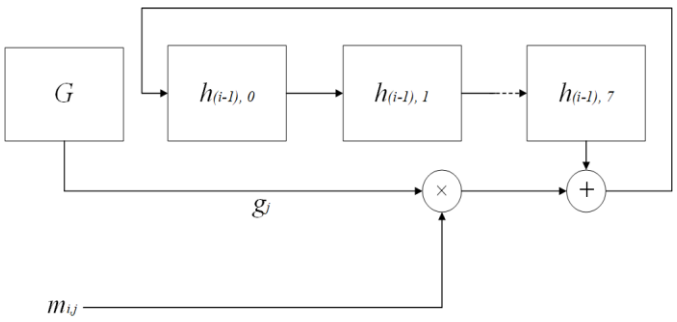

Рис. 1. Схема обчислення геш-значень

Результат *n*-го ущільнення f є остаточним геш-значенням $h_n = \{h_{n,0}, h_{n,1}, ..., h_{n,7}\}$ для даних *M*.

У запропонованому методі проміжні та остаточні значення геш-функції обчислюється шляхом додавання за модулем два псевдовипадкових чисел довжиною *k*-біт у позиціях, що відповідають значенню біта вхідних даних $m_{i,j} = 1$. Якщо $m_{i,j} = 0$, то відбувається лише циклічний зсув блоків послідовності h_i. Враховуючи те, що геш-значення залежать від псевдовипадкових чисел g_j, що формуються генератором *G* та бітів вхідних даних $m_{i,j}$, що слугують для визначенням позицій, в яких виконується операція додавання за модулем два, тому такий метод гешування автори називають метод «генератор – дані».

Для апаратної реалізації цього методу потрібно використати генератор псевдовипадкових чисел на основі регістра зсуву з лінійним зворотнім зв'язком розрядністю *k*, вісім регістрів для зберігання проміжних геш-значень, загальної розрядності *l*, 8-розрядний регістр зсуву для зберігання m_i, *k* логічних елементів «І» та *k* суматорів за модулем 2. У разі використання реалізації пристрою у вигляді мікросхеми за технологією 0.18 μm з використанням бібліотеки UMCL18G212T3 [7] маємо таку загальну складність в умовних одиницях *GE*:

$$S_{\text{ПР}} = 51.97k + 42{,}64. \quad (4)$$

Для реалізації з *k=32* (довжина геш-значення 256 біт) $S_{\text{ПР}} = 1706GE$, що відповідає вимогам до апаратної складності засобів малоресурсної криптографії.

III. Висновки

Запропонований підхід до гешування даних є байт-орієнтованим, тому не потрібно доповнювати останній блок даних до певної довжини перед початком процесу гешування, як це робиться в багатьох відомих геш-функціях. Крім того, забезпечується можливість формування геш-значень будь-якої довжини кратної байту. Другою особливістю запропонованого методу є використання криптографічної «солі», що є однією з основних складових формування проміжних геш-значень. Малі апаратурні витрати на реалізацію пристрою гешування зокрема забезпечуються використанням лише двох порозрядних операцій «І» та сума за модулем 2.

Література References

[1] Селезньов В. І. АНАЛІЗ МЕТОДІВ МАЛОРЕСУРСНОГО ГЕШУВАННЯ. LII науково-технічна конференція підрозділів ВНТУ: матеріали наук. конф., м. Вінниця, 21–23 черв. 2023 р. Вінниця, 2023. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2023/paper/download/18664/15557 (дата звернення: 25.04.2024).

[2] Al-Odat Z. A., Al-Qtiemat E. M., Khan S. U. An Efficient Lightweight Cryptography Hash Function for Big Data and IoT Applications. 2020 IEEE Cloud Summit, м. Harrisburg, PA, 21–22 жовт. 2020 р. 2020. URL: https://doi.org/10.1109/ieeecloudsummit48914.2020.00016 (дата звернення: 25.04.2024).

[3] Differential Analysis of a Cryptographic Hashing Algorithm HBC-256 / K. Algazy та ін. Applied Sciences. 2022. Т. 12, № 19. С. 10173. URL: https://doi.org/10.3390/app121910173 (дата звернення: 26.04.2024).

[4] Селезньов В. І., Лужецький В. А. Метод малоресурсного гешування типу «дані – генератор». Кібербезпека: освіта, наука, техніка. 2023. 2(22). С. 84-95.

[5] Lightweight Cryptographic Hash Functions: Design Trends, Comparative Study, and Future Directions / S. Windarta та ін. IEEE Access. 2022. С. 1. URL: https://doi.org/10.1109/access.2022.3195572 (дата звернення: 27.04.2024).

[6] Лужецький В. А., Слободян С. О., Кисюк Д. В. "Методи байт-орієнтованого хешування даних низькоресурсної криптографії." Інформаційні технології та комп'ютерне моделювання: матеріали міжнар. наук.-практ. конф., м. ІваноФранківськ, 15-20 травня 2017 р., 2017. С. 216 – 219. URL: https://itcm.comp-sc.if.ua/2017/Luzhetskyi2.pdf (дата звернення: 28.04.2024).

[7] Poschmann A. Y. Lightweight cryptography cryptographic engineering for a pervasive world. 2009. URL: https://eprint.iacr.org/2009/516.pdf (дата звернення: 02.05.2024).