УДК 004.4

Д. В. Кисюк
В. А. Лужецький

ПРОГРАМНИЙ ЗАСІБ ДЛЯ ПОБУДОВИ ХЕШ-ЗНАЧЕННЯ ЗА ДОПОМОГОЮ БАЙТ-ОРІЄНТОВАНОЇ ОБРОБКИ ДАНИХ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Вінницький національний технічний університет

Анотація

В роботі був виконаний аналіз найбільш сучасних методів розробки додатків для побудови хеш-функцій без використання ітеративної процедури на основі побайтових операцій.

Ключові слова: Java, хешування, гешування, хеш-функція, неітеративне хешування, побайтова обробка даних.

Abstract

The analysis of the most modern methods of application development for the new byte-oriented method of non-iteration hash-function creation.

Keywords: Java, application, hashing, hash - function, noniterrate hashing, byte-oriented hashing.

Вступ

Криптографічні хеш-функції є одними з найважливіших видів криптографічних перетворень. Вони широко застосовуються у розробці програмного забезпечення, зокрема як один з базових принципів збереження та пошуку інформації у мові Java та задачах криптографічного захисту інформації. Натепер існує велика кількість різноманітних хеш-функцій. Проте, зростаючі вимоги, що висуваються до швидкості хешування даних, а також необхідність реалізації у пристроях з невеликими обчислювальними можливостями, приводять до необхідності розробки нових методів хешування, з можливою їх спеціалізацією для певних пристроїв чи повідомлень особливого виду. Відомі програмні засоби, що реалізують хеш-функції передбачають їх виконання у вигляді ітераційних процедур. Проте, у зв'язку з тим, що питання про лавиноподібний ефект з початковим заповненням при великій кількості ітерацій недостатньо досліджений, і, відповідно, використання цих додатків та функцій є недостатньо обґрунтованим.

Результати розробки

В процесі розробки був створений програмний засіб для реалізації запропонованого раніше методу хешування інформації для мобільних гаджетів, у яких найчастіше використовуються 8-розрядні мікропроцесори, тому потрібні хеш-функції, які орієнтуються на байтове представлення даних. У доповіді пропонується новий Java-додаток, який передбачає саме таку форму представлення даних. Відомі на теперішній час методи хешування базуються на ітераційній процедурі обчислення хеш-значення, яка передбачає на кожному кроці ітерації використання проміжного попереднього хеш-значення і наступного блоку даних, що підлягають хешуванню. Пропонується принципово новий підхід до хешування даних, який не передбачає ітераційний процес обчислення хеш-значень.

Суть методу полягає у тому, що спочатку вхідне повідомлення розбивається на послідовність байтів, далі підраховується кількість байтів однакового змісту, а потім обчислюється хеш-значення з урахуванням цих кількостей та номерів позицій, у яких розташовані ці байти.

Для реалізації запропонованого методу необхідно виконати таку кількість операцій. Вважаємо, що L - довжина вхідного повідомлення. Для формування масивів K та S потрібно виконати L зчитувань, L додавань та L записів. Обчислення хеш-значення H вимагає виконання 256 зчитувань, додавань та записів для формування масиву Q. Для формування значень сум str0 – str7 потрібно 256 зчитувань і додавань та 8 записів. Формування масиву Q* вимагає виконання 264 зчитувань, 256 додавань та 32 записи. Тобто, всього 2608 операцій. Загальна кількість операцій дорівнює 3L+2608. І чим більша довжина повідомлення, тим ближче до 3 оцінка кількості операцій потрібних для обробки 1 байта. Для порівняння метод хешування BLAKE вимагає близько 65 операцій на обробку 1 байта.

На основі описаного методу розроблено програмне забезпечення, яке дозволяє отримувати хеш-значення довжиною 256 біт.

Висновки

Розроблений додаток симулює роботу хеш-генератора на мобільному пристрої і є повністю готовим до використання. Він має консольний інтерфейс та є дуже зручним і зрозумілий, так як не потребує значних ресурсів для його виконання, та додаткових дій для встановлення і налаштування. Він найкраще підходить для швидкого генерування хеш-коду та дає змогу пристроям з байт-орієнтованою обробкою даних швидко обробити вхідну інформацію та значно зменшити апаратні витрати на реалізацію.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Лужецький В. А. Новий підхід до побудови криптографічних хеш-функцій / В. А. Лужецький, Д. В. Кисюк // «Інформаційні технології та комп'ютерна інженерія»; матеріали статей п’ятої міжнародної науково-практичної конференції, м. Івано-Франківськ, 27-29 травня 2015 року. – Івано-Франківськ: Супрун В. П., 2015 р. – с. 206-208.
2. Лужецький В. А. Узагальнений метод хешування байтової форми представлення інформації / В. А. Лужецький, Д. В. Кисюк // IV міжнародна науково-практична конференція «Інформаційні технології та комп'ютерна інженерія». – Вінниця: ВНТУ, 2014., -275с.
3. Pratik Das. Creating Hashes in Java. / P. Das. – 2021.
4. Aumasson J. P. SHA-3 proposal BLAKE / Henzen L., Meier W., Phan R. - 2010.
5. Bos J. W. Performance analysis of the SHA-3 candidates on exotic multi-core architectures / J. W. Bos, D. Stefan. – 2010.

Кисюк Дмитро Васильович — старший викладач кафедри обчислювальної техніки, Вінницький національний технічний університет вул. Хмельницьке шосе 95, м. Вінниця, Україна, kneimad@gmail.com

Лужецький Володимир Андрійович — проф., д.т.н., завідувач кафедри захисту інформації, Вінницький національний технічний університет вул. Хмельницьке шосе 95, м. Вінниця, Україна, v.luzhetskyi@vntu.edu.ua

Kysiuk Dmytro V. — Senior Lecturer, Department of Computer Science, Vinnytsia National Technical University Khmelnytske shose str.,95, Vinnytsia, Ukraine, kneimad@gmail.com

Luzhetskyi Volodymyr A. — Prof., Head of Department ofInformation Protection,Vinnytsia National Technical University Khmelnytske shose str., 95, Vinnytsia, Ukraine, v.luzhetskyi@vntu.edu.ua