

ЗАСІБ ДЛЯ ГЕШУВАННЯ ДАНИХ МЕТОДОМ HDG

Вінницький національний технічний університет

Анотація

Представлено спеціалізований апаратний пристрій, що реалізує геш-функцію HDG, призначений для використання в малоресурсних системах, зокрема в IoT-пристроях, сенсорних мережах та смарт-картах. Запропоноване рішення ґрунтується на ефективному використанні побайтової обробки даних, забезпечуючи високу ефективність при обмежених ресурсах пам'яті та обчислювальних можливостях пристроїв. Апаратну реалізацію засобу представлено у вигляді спеціалізованого процесора для гешування (HDG-процесора). Наведено структуру спеціалізованого процесора, здійснено його декомпозицію на блоки, кожен з яких реалізує відповідну функцію. Проведено оцінку апаратної складності пристрою, що підтверджує його відповідність вимогам малоресурсної криптографії та доцільність використання у системах з обмеженими апаратними ресурсами.

Ключові слова: апаратний засіб, спеціалізований процесор, малоресурсна криптографія, геш-функція, апаратна складність.

Abstract

A specialized hardware device implementing the HDG hash function is presented, designed for use in low-resource systems, including IoT devices, sensor networks, and smart cards. The proposed solution is based on efficient byte-wise data processing, ensuring efficient operation with minimal memory and computational resources. The hardware implementation of the device is presented as a specialized hashing processor (HDG processor). The structure of the specialized processor is described, and its decomposition into functional blocks is carried out, each performing a specific function. An assessment of the hardware complexity of the device confirms its compliance with the requirements of lightweight cryptography and its feasibility for use in systems with limited hardware resources.

Keywords: hardware, specialized processor, low-resource cryptography, hash function, hardware complexity.

Вступ

Захист цілісності даних є важливою складовою сучасних інформаційних систем, особливо у сфері пристроїв з обмеженими апаратними ресурсами, де традиційні криптографічні алгоритми можуть вимагати значних обчислювальних ресурсів та апаратних витрат. Використання геш-функцій дозволяє забезпечити ефективну перевірку цілісності інформації, проте стандартні рішення, такі як SHA-256 або SHA-3, вимагають значних обчислювальних ресурсів та пам'яті, що обмежує їхнє застосування у малоресурсних пристроях. Рішенням цієї проблеми є використання спеціалізованих засобів для гешування, що розроблені з урахуванням обмежень малоресурсних систем [1-2].

Метод HDG (Hash Data Generator) [3] було розроблено з метою створення ефективної геш-функції, яка потребує мінімальних апаратних ресурсів. Головною особливістю геш-функції HDG є побайтна обробка даних, що дозволяє зменшити витрати на реалізацію та водночас зберегти необхідний рівень криптографічної стійкості.

У роботі запропоновано апаратний засіб для гешування даних методом HDG, який забезпечує ефективне виконання операцій гешування в малоресурсних системах.

Результати дослідження

Апаратний засіб для гешування даних методом HDG реалізовано, у вигляді спеціалізованого процесора (HDG-процесора). Спеціалізований процесор для гешування даних інтегрується у комп'ютерну систему та призначений для прискорення операцій гешування шляхом виділення обчислювальних процедур в окремий пристрій. Центральний процесор системи забезпечує зберігання та формування послідовності байт вхідного повідомлення для гешування. HDG-процесор забезпечує виконання всіх арифметичних операцій, необхідних для обчислення геш-значень та зберігає проміжні

геш-значення.

Виходячи з особливостей геш-функції HDG структура спеціалізованого процесору для гешування даних складається з кількох функціональних блоків, кожен з яких виконує конкретні завдання:

- Блок регістрів (BRG) – відповідає за збереження проміжних геш-значень під час виконання обчислень.
- Генератор псевдовипадкової послідовності (LFSR) – забезпечує формування випадкових значень, необхідних для роботи алгоритму.
- Блок арифметичних операцій (ADDB) – реалізує додавання за модулем 256 з додатковим керуванням, що є основною операцією у формуванні геш-значень.
- Блок керування (CB) – забезпечує синхронізацію роботи всіх елементів процесора та здійснює обмін даними із центральним процесором системи.

На рисунку 1 подано схематичне зображення структури HDG-процесора.

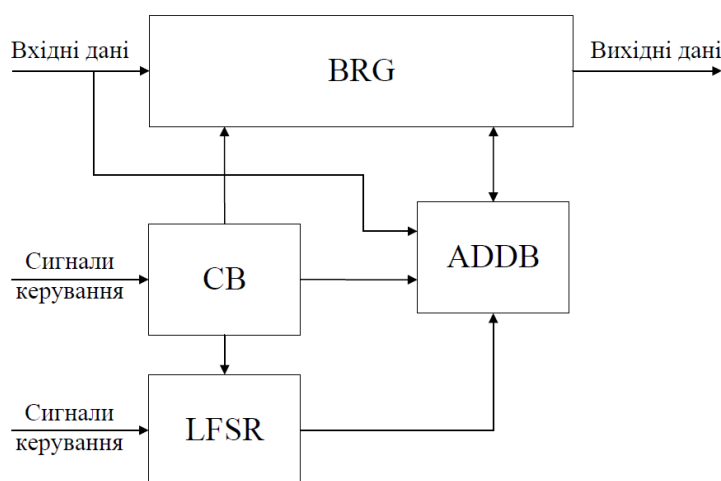


Рисунок 1 – Структурна схема апаратного засобу

Процес гешування у HDG-процесорі побудований на основі ітеративної обробки байтів вхідного повідомлення. Кожен байт змінює стан регістрів блоку BRG відповідно до внутрішньої логіки алгоритму гешування [3], що включає операції зсуву та додавання з додатковим керуванням операндом (блок ADDB) на основі псевдовипадкової керуючої послідовності біт, яка генерується блоком LFSR. Завдяки цьому формується унікальне геш-значення, яке забезпечує високий рівень криптографічної стійкості при мінімальних апаратних витратах.

В середовищі Logisim-evolution здійснено моделювання HDG-процесора з використанням бібліотеки [4], що відповідає елементам технології FPGA. Результати тестування моделі HDG-процесора підтвердили коректність роботи спеціалізованого процесора.

Обчислення складності апаратної реалізації спеціалізованого процесора здійснено в умовних одиницях GE (Gate Equivalent), які фактично описують кількість логічних вентилів, що необхідні для реалізації засобу. Загальна апаратна складність реалізації HDG-процесора, що обчислює геш-значення довжиною 256 біт на мікросхемі за технологією 0.18 μm з використанням бібліотеки UMCL18G212T3 [5] становить 1683 умовних одиниць (GE), що значно нижче порівняно з іншими малоресурсними геш-функціями, такими як SPONGENT-256 (2012 GE), PHOTON-256 (2177 GE) або S-Quark (2296 GE). Таким чином HDG-процесор задовольняє вимогам щодо апаратної складності засобів малоресурсної криптографії.

Висновки

Розроблений засіб для гешування даних методом HDG у вигляді спеціалізованого процесору дозволяє забезпечити захист цілісності даних в малоресурсних пристроях завдяки простій байт-орієнтованій архітектурі. Запропонована структура HDG-процесора складається з чотирьох функціональних блоків, кожен з яких виконує конкретні завдання відповідно алгоритму геш-функції HDG.

Отримані результати обчислення складності апаратної реалізації спеціалізованого процесора демонструють, що геш-функція HDG, у разі її апаратної реалізації, вимагає на 16-27% менших апаратних витрат у порівнянні з іншими відомими малоресурсними геш-функціями.

Подальші дослідження можуть бути спрямовані на удосконалення HDG-процесора, а також реалізацію геш-функції HDG на універсальних сучасних малоресурсних процесорах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. William J. Buchanan, Shancang Li & Rameez Asif. "Lightweight cryptography methods." Journal of Cyber Security Technology, 1:3-4, 187-201, 2017. URL: <https://www.tandfonline.com/doi/pdf/10.1080/23742917.2017.1384917?needAccess=true> (дата звернення: 07.03.2025)
2. Селезньов В. І., Аналіз методів малоресурсного гешування / Матеріали ЛІІ науково-технічної конференції підрозділів ВНТУ, Вінниця, 21-23 червня 2023 р. URL: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2023/paper/download/18664/15557> (дата звернення 20.02.2025)
3. Лужецький В. А., Селезньов В. І. Метод малоресурсного гешування типу 'дані – генератор', Кібербезпека: освіта, наука, техніка, т. 28, с. 84–95, грудень 2023 р. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/488> (дата звернення: 05.02.2025).
4. Logisim-evolution: Digital logic design tool and simulator. URL: <https://github.com/logisim-evolution/logisim-evolution> (дата звернення: 10.02.2025).
5. Poschmann A. Y., Lightweight cryptography cryptographic engineering for a pervasive world 2009 р. URL: <https://eprint.iacr.org/2009/516.pdf> (дата звернення: 15.03.2025).
6. ISO/IEC 29192-5, "Information technology – Security techniques – Lightweight cryptography – Part 5: Hash-functions," Official Standard, Aug. 2016, 26 pages.
7. A. Bogdanov, M. Knežević та G. Leander, "SPONGENT: The Design Space of Lightweight Cryptographic Hashing" 2011. URL: <https://eprint.iacr.org/2011/697.pdf> (дата звернення: 21.02.2025).
8. Windarta S., "Lightweight Cryptographic Hash Functions: Design Trends, Comparative Study, and Future Directions", IEEE Access, 2022, с. 1. URL: https://www.researchgate.net/publication/362502388_Lightweight_Cryptographic_Hash_Functions_Design_Trends_Comparative_Study_and_Future_Directions/link/62fdb058ceb9764f72046d21/download (дата звернення: 21.02.2025).
9. Tobias Meuser, Larissa Schmidt, Alex Wiesmaier. "Comparing Lightweight Hash Functions – PHOTON & Quark." Technische Universität Darmstadt, Germany AGT International, 2015. URL: https://download.hrz.tu-darmstadt.de/pub/FB20/Dekanat/Publikationen/CDC/2015-07-06_TR_PhotonQuark.pdf (дата звернення 22.02.2025)

Селезньов Віталій Ігорович — аспірант групи 125-22а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: seleznov.vitalii@gmail.com

Науковий керівник – **Лужецький Володимир Андрійович** — д. т. н., професор, завідувач кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: v.luzhetskyi@vntu.edu.ua

Seleznov Vitalii — Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: seleznov.vitalii@gmail.com

Scientific supervisor – **Luzhetskiy Vladimir** — Doctor of Technical Science, Professor, Head of Information Security Department, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, e-mail: v.luzhetskyi@vntu.edu.ua