

УДК 004.3:004.9

Климаков О.Є.¹, Грушко С.С.²

¹ студ. гр. КНТ-515м НУ «Запорізька політехніка»

² доц. НУ «Запорізька політехніка»

ІНТЕГРОВАНА FPGA-СИСТЕМА ВЕРИФІКАЦІЇ ДАНИХ НА ОСНОВІ ХЕШ-ФУНКЦІЇ JENKINS

FPGA-платформи поєднують продуктивність і гнучкість завдяки можливості перепрограмування логіки, глибокому паралелізму та оптимізації під конкретні криптографічні алгоритми. Порівняльні дослідження реалізацій

SHA-2, SHA-3 і BLAKE2 на FPGA підтверджують перевагу таких рішень за показником «пропускна здатність на ват» порівняно з CPU і GPU, особливо при конвеєрній та масово-паралельній обробці [1–5]. Аналіз сучасних лінійок Intel Stratix 10, Intel Cyclone 10, Intel Cyclone V і Xilinx Zynq UltraScale демонструє можливість вибору між максимальною продуктивністю, енергоспоживанням і вартістю, а також використання вбудованих криптографічних IP-ядер [6–10].

У роботі розглянуто вимоги до систем захисту інформації в контексті протоколів FIDO2 і WebAuthn, що покладаються на криптографічні примітиви, апаратні модулі безпеки та захищені середовища виконання [11]. Показано, що для задач перевірки цілісності в розподілених системах, зокрема у вузлах із консенсусом типу Proof of Authority, доцільним є застосування легших хеш-функцій, які забезпечують достатню колізійну стійкість при менших апаратних витратах порівняно з повноцінними криптографічними алгоритмами SHA-2/SHA-3. На цій основі обґрунтовано вибір хеш-функції Jenkins як компромісу між простотою реалізації, швидкодією та придатністю до FPGA-оптимізації у порівнянні з SHA-1, MD5 і SHA-256.

Мета роботи полягає у розробці інтегрованої FPGA-системи контролю цілісності даних на основі хеш-функції Jenkins, придатної для використання у вбудованих пристроях, телекомунікаційному обладнанні та вузлах блокчейн-мереж. Запропонована система повинна забезпечувати контроль цілісності в реальному часі, мінімальне використання апаратних ресурсів і можливість масштабування шляхом паралельної обробки кількох потоків даних, а модульність архітектури має спростити подальшу інтеграцію інших хеш-функцій та криптографічних блоків.

Архітектура FPGA-системи має модульну структуру та складається з інтерфейсного модуля і модуля обчислення хеш-функції Jenkins. Інтерфейсний модуль забезпечує приймання 32-бітових слів даних, задання довжини повідомлення, режиму роботи (обчислення/перевірка) та референтного хеш-значення, формуючи сигнали керування для обчислювального ядра, тоді як обчислювальний модуль виконує послідовну обробку байтів повідомлення, операції XOR і циклічні зсуви згідно зі специфікацією Jenkins hash і генерує вихідне хеш-значення.

Апаратну реалізацію виконано на базі FPGA Intel Cyclone V із використанням середовища Quartus II 13.1 та мови опису апаратури Verilog HDL, що відповідає технічній документації на сімейство Cyclone V. Модуль hashing має інтерфейс clk, reset, datain, lengthin, validin, mode, hashref, hashout, validout, hashok, що полегшує його повторне використання у системах із поточковими інтерфейсами на кшталт AXI4-Stream. За результатами синтезу реалізація займає 134 ALM при нульовому використанні DSP-блоків,

залишаючи значний резерв ресурсів FPGA для інсталяції декількох екземплярів хеш-модуля або додаткових криптографічних ядер.

Функціональну верифікацію проведено в середовищах Active-HDL і Quartus II на основі тестових наборів, що містять повідомлення різної довжини та структури [12]. Коректність роботи підтверджено порівнянням результатів апаратної реалізації з програмною реалізацією Jenkins hash: отримані хеш-значення повністю збігаються для всіх тестових векторів, а сигнал hashok правильно відображає результат перевірки цілісності. Додатково оцінено пропускну здатність при тактовій частоті до 100 МГц, що продемонструвало можливість ефективної обробки потоків даних у режимі реального часу [13].

Проведено порівняльний аналіз реалізації Jenkins hash function на FPGA Intel Cyclone V, Intel Stratix 10 та Intel Cyclone 10 з точки зору ресурсних витрат, максимальної частоти та потенційної пропускну здатності. Показано, що використання старших серій, таких як Stratix 10, дозволяє суттєво підвищити продуктивність за рахунок більшої кількості логічних ресурсів і вищих робочих частот, тоді як рішення на базі Cyclone 10 забезпечують кращий баланс між вартістю й енергоспоживанням для вбудованих застосувань. Запропоновано напрями подальшого розвитку системи, зокрема додавання підтримки SHA-3 згідно з NIST FIPS 202 та алгоритмів сімейства BLAKE з урахуванням існуючих напрацювань щодо їх FPGA-реалізації.

Отримані результати підтверджують доцільність використання FPGA як платформи для побудови інтегрованих систем контролю цілісності даних у вбудованих та мережових засобах захисту інформації. Розроблена FPGA-система на основі хеш-функції Jenkins характеризується низькими апаратними витратами, можливістю масштабування та інтеграції з сучасними криптографічними протоколами, що робить її перспективною для практичного застосування в системах кібербезпеки нового покоління.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. *NIST*. URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf> (дата звернення: 05.05.2025).
2. Cryptographic Standards and Guidelines. URL: <https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines> (дата звернення: 05.05.2025).
3. BLAKE HASH Function Family on FPGA. URL: <https://ieeexplore.ieee.org/document/5572760> (дата звернення: 05.05.2025).
4. Comparing SSH Keys - RSA, DSA, ECDSA, or EdDSA? URL: <https://goteleport.com/blog/comparing-ssh-keys/> (дата звернення: 05.05.2025).

5. Secure Hash Algorithm-3 (SHA-3) implementation on Xilinx FPGAs. URL:
https://www.researchgate.net/publication/339275421_Secure_Hash_Algorithm-3SHA-3_implementation_on_Xilinx_FPGAs_Suitable_for_IoT_Applications (дата звернення: 05.05.2025).
6. Secure and Low-Power FPGA Implementations. URL:
https://www.researchgate.net/publication/388754148_Secure_and_Low-Power_FPGA_Implementations_for_Cryptographic_Applications (дата звернення: 05.05.2025).
7. Power-Analysis Attacks on an FPGA. URL:
https://www.researchgate.net/publication/221291675_Power-Analysis_Attacks_on_an_FPGA_-_First_Experimental_Results (дата звернення: 05.05.2025).
8. Intel Stratix 10 Device Overview. URL: <https://cdrdv2-public.intel.com/670537/s10-overview-683729-670537.pdf> (дата звернення: 05.05.2025).
9. Intel Cyclone 10 Device Handbook. URL:
<https://www.intel.com/content/www/us/en/docs/programmable/683861/current/device-design-guidelines.html> (дата звернення: 05.05.2025).
10. Zynq UltraScale+ Device Technical Reference Manual. URL:
https://www.xilinx.com/support/documentation/user_guides/ug1085-zynq-ultrascale-trm.pdf (дата звернення: 05.05.2025).
11. FPGA Security Solutions. URL:
<https://www.amd.com/en/products/adaptive-socs-and-fpgas/technologies/design-security.html> (дата звернення: 05.05.2025).
12. Intel Cyclone V Device Datasheet URL:
<https://www.intel.com/content/www/us/en/docs/programmable/683801/current/cyclone-v-device-datasheet.html> (дата звернення: 12.05.2025).
13. Intel Cyclone V Device Overview. URL:
<https://www.intel.com/content/www/us/en/docs/programmable/683694/current/cyclone-v-device-overview.html> (дата звернення: 12.05.2025).