Pertanika J. Sci. & Technol. 30 (1): 581 - 603 (2022)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

FPGA-based Implementation of SHA-256 with Improvement of Throughput using Unfolding Transformation

Shamsiah Suhaili*and Norhuzaimin Julai

Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Malaysia Sarawak, 94300 UNIMAS, Kota Samarahan, Sarawak, Malaysia

ABSTRACT

Security has grown in importance as a study issue in recent years. Several cryptographic algorithms have been created to increase the performance of these information-protecting methods. One of the cryptography categories is a hash function. This paper proposes the implementation of the SHA-256 (Secure Hash Algorithm-256) hash function. The unfolding transformation approach was presented in this study to enhance the throughput of the SHA-256 design. The unfolding method is employed in the hash function by producing the hash value output based on modifying the SHA-256 structure. In this unfolding method, SHA-256 decreases the number of clock cycles required for traditional architecture by a factor of two, from 64 to 34 because of the delay. To put it another way, one cycle of the SHA-256 design can generate up to four parallel inputs for the output. As a result, the throughput of the SHA-256 design can be improved by reducing the number of cycles by 16 cycles. ModelSim was used to validate the output simulations created in Verilog code. The SHA-256 hash function factor four hardware implementation was successfully tested using the Altera DE2-115 FPGA board. According to timing simulation findings, the suggested unfolding hash function with factor four provides the most significant throughput of around 4196.30 Mbps. In contrast, the suggested unfolding with factor two surpassed the classic SHA-256 design in terms of maximum frequency. As a result, the throughput of SHA-256 increases 13.7% compared to unfolding factor two and 58.1% improvement from the conventional design of SHA-256 design.

Keywords: FPGA implementation, SHA-256, throughput, unfolding technique

ARTICLE INFO

Article history:
Received: 1 July 2021
Accepted: 15 September 2021
Published: 10 January 2022

DOI: https://doi.org/10.47836/pjst.30.1.32

E-mail addresses:
sushamsiah@unimas.my (Shamsiah Suhaili)
jnorhuza@unimas.my (Norhuzaimin Julai)
*Corresponding author

ISSN: 0128-7680
e-ISSN: 2231-8526