Global Conference on Engineering and Technology
conference homepage: www.gcoet.org
GLOBAL CONFERENCE ON ENGINEERING & TECHNOLOGY

High-Throughput of SHA-256 Hash Function with Unfolding Transformation

Shamsiah binti Suhaili [1*], Takahiro Watanabe[2]

[1]Faculty of Engineering, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia
[2]Graduate School of Information, production and Systems, Waseda University, 2-7 Hibikino, Wakamatsu-ku, Kitakyushu-shi, Fukuoka 808-0135, Japan

ABSTRACT

Hash Function in cryptography algorithms is used to encrypt the message by giving the appropriate output based on the structure of the hash function itself. This algorithm is important for security application such as keyed-Hash Message Authentication Code (HMAC), digital signature and others. There are different types of hash function such as MD5, SHA-1, RIPEMD-160, SHA-256, SHA-224, SHA-384, SHA-512 and others. In this paper, the unfolding transformation method was proposed to improve the throughput of the SHA-256 hash function. Three types of SHA-256 hash function were designed namely SHA-256 design, SHA-256 design inner pipelining with unfolding factor 2 and SHA-256 design inner pipelining with unfolding factor 4. The designs were written in Verilog code and the output simulations were verified using ModelSim. The simulation results showed that the proposed SHA-256 inner pipelining unfolding with factor 4 provided the highest throughput which is 4196.30 Mbps, and with factor 2 was superior in terms of maximum frequency and was better than the conventional SHA-256 design.

Type of Paper: other

Keywords: Cryptography algorithm; FPGA; SHA-256 Hash Function; Unfolding transformation, Verilog

1. Introduction

Cryptography is the science of writing secret codes; to ensure none can read an encrypted message except the intended user. There are three different types of cryptographic algorithms namely symmetric cryptography, asymmetric cryptography and hash function. While symmetric cryptography uses only a key to encrypt and decrypt the message, asymmetric cryptography uses two different keys and the hash function requires no key. This paper focused on the SHA-256 hash function. It transformed a variable message input into a fixed size string hash value [1].

* Paper Info: Revised: Month, Year
Accepted: Month, Year
* Corresponding author:
E-mail: sushamsiah@unimas.my
Affiliation: Faculty of Engineering, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak