Journal of Optimization in Industrial Engineering
Vol.15, Issue 1, Winter & Spring 2022, 207-216
DOI:10.22094/JOIE.2021.1941138.1896

Research Article

Throughput Improvement of RIPEMD-160 Design Using Unfolding Transformation Technique

Shamsiah Binti Suhaili [a,*], Takahiro Watanabe [b], Norhuzaimin Julai [c]

[a] *Faculty of Engineering, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia,*
[b] *School of Information, Production and Systems, Waseda University, 2-7 Hibikino, Wakamatsu-ku, Fukuoka 808-0135, Japan*
[c] *Faculty of Engineering, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia*

Received 23 September 2021; Revised 09 November 2021; Accepted 18 November 2021

Abstract

RIPEMD-160 hash functions are widely used in many applications of cryptography such as digital signature, Hash Message Authentication Code (HMAC) and other data security application. There are three proposed RIPEMD-160 design namely RIPEMD-160 iterative design, RIPEMD-160 unfolding with factor two and RIPEMD-160 unfolding design with factor four. These techniques were applied to RIPEMD-160 designs to examine the inner structure of RIPEMD-160 in terms of area, maximum frequency and throughput of the design. In this project, RIPEMD-160 hash function using unfolding transformation technique with factor four provided high throughput implementation. The throughput of the RIPEMD-160 unfolding design increase significantly. The objective of this project is to enhance the performance of RIPEMD-160 in terms of throughput. By using unfolding transformation factor four technique, the throughput of RIPEMD-160 can be improved which is about 1753.50 Mbps. The percentage of performance to area ratio of RIPEMD-160 unfolding with factor four designs increase 1.51% if compared with RIPEMD-160 design. The results show performance of proposed designs give the highest value compare with other designs. The simulation results were obtained from ModelSim Altera-Quartus II to verify the correctness of the RIPEMD-160 designs in terms of functional and timing simulations.

***Keywords**: FPGA; Hash Function;* RIPEMD-160; Throughput; Unfolding

1. Introduction

There are different types of hash functions such as SHA-1, MD5, RIPEMD-160, SHA-2 and others (Rodriguez-Henriquez and et al., 2006). Hash function is important for some security application such as Hash Message Authentication Codes (HMAC), digital signature and others. The RIPEMD-160 hash function can also be used in the implementation of cryptocurrency. Cryptocurrency is a digital currency that transfers the coin in blockchain where each block consists of hash of the previous block. Therefore, RIPEMD-160 hash function becomes important especially in recent peer-to-peer electronic cash system like Bitcoin.

Nowadays, the security process of money transaction becomes important aspect. No matter whether it is traditional currency or cryptocurrency transaction. There are lots of problem occur during transaction where the original data is modified by some users. Therefore, the data accuracy is very important, and it needs security design to avoid this problem. Security on the network is a major issue in data transmission. A network layer needs to be secure enough with cryptographic algorithms so that it can be used to accommodate encryption and authentication processes. Hash function can be used for some applications such as Message Authentication Code (MAC) and digital signature. Therefore, high performance of cryptographic hash function algorithm is one of the important aspects of security algorithm. Hence, designing an efficient implementation of RIPEMD-160 hash function algorithm on reconfigurable hardware needs to be considered. Thus, the implementation of efficient design of hash function needs to be applied to network security (Abu Bakar, Rosbi & Uzaki, 2017). In this project, the design focuses on RIPEMD-160 design. The scope of research for this project is to design and implement the optimized RIPEMD-160 using Verilog HDL which is based on FPGA device. The designs need to be improved to obtain the high performance RIPEMD-160 hash function. Therefore, several types of techniques are applied to this design such as iterative and unfolding transformation. The design must meet the timing requirement where setup and hold time will give the positive value. Thus, there is no violation in the slack from the timing report. This leads to the frequency maximum which is the longest path of the design. The optimized design can be obtained by giving appropriate clock constraint to the RIPEMD-160 design. The RIPEMD-160 design is simulated and tested by using ModelSim with different testbench files. The motivation of this research is to provide the improvement of RIPEMD-160 design. The inner structure of RIPEMD-160 algorithm is different from other hash function. In this design, there are two parallel design for both left and right parts. The complexity of RIPEMD-160 design is more complex in terms of shift and constant value.

*Corresponding author Email address: rai.naveed@mountsafa.com