Throughput Improvement of RIPEMD-160 Design using Unfolding Transformation Technique

Shamsiah binti Suhaili[1], Takahiro Watanabe[2], Norhuzaimin Julai[1]
[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, Fukuoka 808-0135, Japan
[1]sushamsiah@unimas.my, [2]watt@waseda.jp, [1]jnorhuza@unimas.my

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 [1]. 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-