Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 3, No. 1. Pages 18-28, 2016

Design of Optimized Pipelined RIPEMD-160 with High Frequency and Throughput

S. Suhaili[*,a], *T. Watanabe*[b]

[a,*]Electronic Department, Faculty of Engineering, Universiti Malaysia Sarawak (UNIMAS), 94300 Kota Samarahan, Sarawak

[b]Graduate School of Information, Production and Systems, Waseda University,2-7 Hibikino, Wakamatsu-Ku, Fukuoka 808-0135, Japan

[a,*]*sushamsiah@unimas.my*, [b]*watt@waseda.jp*

Abstract –*The main objective of this paper is to design optimized pipelined RIPEMD-160 with efficient design strategies. There are two proposed designs in this paper such as iterative design and pipelined design. The results show the pipelined design provides high frequency as well as throughput of the design. The improvement of these designs based on HDL design style where the placement of register need to be considered, by adding the several register to the design and by using Quartus II Advisor tools. Furthermore, by using TimeQuest Timing Analyzer, timing requirement of the design such as setup and hold time of the design can be achieved and the maximum frequency of the design can be obtained. This paper focuses on maximum frequency of the designs. Therefore, the methodology on how to improve the speed of the design needs to be taken into consideration. In addition, nowadays high throughput of the hash function design is important since all the design need to be fast enough through some application. By using pipelined design, the frequency and throughput of the design can be improved which is about 250 MHz and 7.805 Gbps respectively with small area implementation.*

Keywords: Hash Function, iterative, pipelined, RIPEMD-160

1.0 INTRODUCTION

Hash Function is widely used for some cryptographic application. It receives arbitrary input and provides fixed length of the output based on the structure of hash function. The output of hash function known as hash code or message digests. There is no key for hash function as shown in Figure 1 which is the block diagram of hash function. There are several different types of hash function such as MD5, SHA-1, RIPEMD-160 and etc. Design and implementation of these hash functions on reconfigurable hardware have been done by many researchers [2,3,4,5,6]. Nowadays, efficient design of hash function is important for some application. Therefore, some techniques need to be taken into consideration in order to improve the performance of hash function in terms of frequency and throughput of the design.

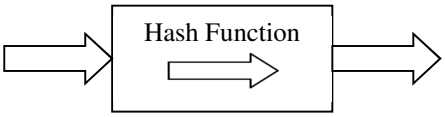

Figure 1: Hash Function