Design and Implementation of MD5 Hash Function Algorithm Using Verilog HDL

Shamsiah Binti Suhaili, Cleopatra Chundang Anak Niam, Zainah Md. Zain, and Norhuzaimin Julai

Abstract Over the past 20 years, the demand of computers and the Internet has been increasing and people have paid a growing attention to information and network security. In result, various encryption algorithms coming into being. Cryptographic algorithm has become one of the most essential features of embedded system design. Hash functions are one of the cryptographies that can be used in both security design applications and protocol suites. A few distinct applications of hash algorithms are digital signatures, digital time stamping and the message integrity verification. Among hash algorithms, MD5 is the most used hash function algorithm. This paper proposed iterative looping architecture. The architecture includes MD5 padding block, data path, and a controller. A general concept and implementation of the MD5 hash function is described. The MD5 hash function modelling was done using Verilog, compiled with a few targeted virtual Altera Quartus devices, and simulated using ModelSim. Its performance in terms of frequency and throughput is compared with other MD5 implementations. The maximum frequency achieved is 111.45 MHz, and the throughput of iterative looping design was increased significantly to 864.58 Mbps using family device of Arria II GX. The improved performance of the implementation is the main goal of the design presented herein.

Keywords Cryptography · Hash function · MD5 · Verilog · Iterative looping

S. B. Suhaili (✉) · C. C. A. Niam · N. Julai
Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia
e-mail: sushamsiah@unimas.my

Z. Md. Zain
Robotics, Intelligent System & Control Engineering (RISC) Research Group, Faculty of Electrical and Electronics Engineering Technology, Universiti Malaysia Pahang, Pekan Branch, 26600 Pekan, Pahang, Malaysia

K. Isa et al. (eds.), *Proceedings of the 12th National Technical Seminar on Unmanned System Technology 2020*, Lecture Notes in Electrical Engineering 770,
https://doi.org/10.1007/978-981-16-2406-3_38