Graduate School of Science and Technology Master's Thesis Abstract

Laboratory name (Supervisor)	Computing Architecture (Yasuhiko Nakashima (Professor))		
Student ID	1911419	Submission date	2021 / 7 / 28
Name	PHAN VAN DAI		
Thesis title	High Performance SHA-256 Accelerator for Society 5.0 Society 5.0実現に貢献する高性能SHA-256アクセラレータの開発と評価		

Abstract

Society 5.0 is a Super Smart Society that aims to achieve the balance between solving problems in society and sustainably developing the economy by integrating cyberspace and physical space. The technologies such as Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), or Blockchain are used in Society 5.0 to create new services for people. In addition, society 5.0 also applies digital transformation and big data to provide large and comprehensive information to solve problems in society. Applications rely on data obtained after being analyzed from cyberspace to make appropriate decisions for each specific situation. Therefore, data is an important component that determines the effectiveness of applications and the success of Society 5.0. The importance of data leads to much attention and focuses on data security in recent times. The cryptographic hash function will help to increase the security and safety of data in various applications. Secure Hash Algorithm 256 (SHA-256) is a ubiquitous cryptographic hashing function. It is an indispensable role in Society 5.0 and is used widely in applications such as Blockchain, cryptocurrencies, data integrity, digital signature, and data security.

Nowadays, the number of smart devices is increasing rapidly. Reducing power consumption in smart devices saves operating costs and helps protect the environment. In addition, the large number of devices also leads to the data processing capacity at the centralized server must be enhanced. Therefore, a high-throughput but energy-efficient accelerator is the target for IoT devices and server devices. SHA-256 needs to be calculated both at the terminal devices as well as at the servers. However, most of the research usually focuses on developing the performance of the SHA-256 algorithm and ignores other factors such as data transmission in a full system. They only develop the SHA-256 accelerator based on the standalone level. The SHA-256 function is only a small module of a large system, and the data transmission in and out of the accelerator takes a considerable amount of time.

This thesis proposes an accelerator suitable for both the accelerator level and the full system level. It has achieved high performance by applying the following methods: fully parallel and pipelined computation ALU, the multiple memory Processing Elements (PEs), and the multi-core accelerator. The pipelined ALU combines with the local memory, shift registers to reduce the critical path and significantly improve the processing rate. The accelerator is designed and verified with the System-on-Chip on a real hardware platform (Xilinx UltraScale+ ZCU102). The synthesis results on FPGA show that our proposed architecture, including ALU or full PE circuit, is the most outstanding compared with exiting works. Our accelerator has the most improvement, which is 31.2× higher in processing rate and 12.42× in hardware efficiency when comparing previous works. The accelerator is also synthesized and laid out by the Renesas SOTB 65nm standard cell library, with each PE operate at 117 Mhz, area 0.25 mm2, and consuming 20.9mW.