# Graduate School of Science and Technology Master's Thesis Abstract

| Laboratory name (Supervisor) | Computing Architecture (Yasuhiko Nakashima (Professor )) | | |
|---|---|---|---|
| Student ID | 1911418 | Submission date | 2021 / 7 / 27 |
| Name | PHAN TRIDUNG | | |
| Thesis title | Design and Evaluation of High-performance SHA-3 System on Chip for Society 5.0<br>Society5.0向けの高性能SHA-3システムオンチップの設計と評価 | | |


Abstract

Secure Hash Algorithm 3 (SHA-3) plays an important role in developing smart systems because of the requirement of data security. Unfortunately, current researches are mostly focused on improving the speed of SHA-3 as a stand-alone core. In contrast, the performance of the SHA-3 SoC is affected by the core's processing rate and the data transfer rate between the SHA-3 core and external memory. In this research, we develop a high-performance SHA-3 SoC by increasing the processing rate of both the SHA-3 core and its outside data flow. We enhance the processing speed of the SHA-3 core with a fully unrolled 24-round architecture. Also, Direct Memory Access (DMA) is applied to shorten the data transfer time between SHA-3 core and external memory. Furthermore, some parts of the SHA-3 algorithm is implemented in software to reduce hardware cost. Our system is implemented and evaluated on FPGA Zynq UltraScale+ MPSoC ZCU102, and proofed maximum frequency performance is improved 380$¥%$, throughput is increased 206.25$¥%$. Besides, we also design the SHA-3 accelerator part as an Application-specific integrated circuit (ASIC) for evaluation.