Ultra-Efficient Universal SHA-2 and BLAKE Accelerators for Decentralized Networks

Name: Pham Hoai Luan
Laboratory: Computing Architecture
Supervisor: Yasuhiko Nakashima

Abstract:
The Japanese government has set out a vision of a new super-smart society, known as Society 5.0. Accordingly, the SHA-2 and BLAKE algorithms are incredibly important in securing data integrity and security for the decentralized networks in Society 5.0. Therefore, this dissertation focuses on developing ultra-efficient universal SHA-2 and BLAKE accelerators for decentralized networks, which are presented as follows.

First, we propose an SHA-2 hardware architecture named the multimode SHA-2 accelerator (MSA), which has high performance and flexibility at the system-on-chip level. To achieve high performance and flexibility, our accelerator applies three optimal techniques, including a multimode processing element architecture, a three-stage arithmetic logic unit pipeline architecture, and nonce generator and nonce validator mechanisms. The MSA accuracy is tested on a Xilinx Alveo U280 FPGA. The experimental results on several FPGAs prove that the proposed MSA achieves significantly better performance, hardware efficiency, and flexibility than previous works. The evaluation results for energy efficiency show that the proposed MSA achieves up to 38.05 Mhps/W, which is 543.6 and 29 times better than the state-of-the-art Intel i9-10940X CPU and RTX 3090 GPU, respectively.

Second, we introduce the first fully pipelined BLAKE-256/512 accelerator to improve throughput and hardware efficiency. Moreover, based on the rates of changed words in consecutive message inputs, a compact message permutation scheme is proposed to reduce the area and energy consumption of the fully pipelined BLAKE-256/512 accelerator. To achieve these goals, the compact message permutation scheme includes two novel optimization techniques: register optimization, reducing the number of registers used by over 80% compared to conventional message permutation in a theoretical evaluation, and XOR optimization, decreasing the number of XOR gates by 93.8%. An ASIC-based experiment shows that the proposed compact message permutation scheme helps reduce the area and power consumption by up to 11.35% and 21.10%, respectively, for the fully pipelined BLAKE-256 accelerator and by up to 9.86% and 20.32%, respectively, for the fully pipelined BLAKE-512 accelerator.