Ultra-Efficient Universal Cryptographic Accelerators for Blockchain-based IoT Systems

Name: Le Vu Trung Duong
Laboratory’ｓ name: Computing Architecture
Supervisor’ｓ name: Yasuhiko Nakashima

Abstract:

Nowadays, cryptographic algorithms are indispensable tools for ensuring data security and privacy in blockchain-based IoT systems. Accordingly, hash functions, block ciphers, and stream ciphers are three main types of cryptography that encompass many of the most widely used algorithms today. Therefore, this dissertation focuses on developing ultra-efficient universal cryptographic accelerators to support these three types of cryptography in blockchain-based IoT systems.

First, we propose the Flexible and Energy-efficient Crypto-Processor (FECP), a Coarse-Grained Reconfigurable Array (CGRA) accelerator designed to support hash functions, block ciphers, and stream ciphers, offering excellent performance and hardware efficiency. To achieve these goals, three new techniques are proposed: the Crypto Arithmetic Logic Unit, Dual Buffering Extension, and Local Data Memory Scheduler. Experiments show that the FECP can perform various hash functions with power consumption ranging from 0.239 to 0.676 W, throughput of 10.2 to 3.35 Gbps, and energy efficiency of 4.44 to 14.01 Gbps/W. Moreover, the FECP on FPGA outperforms modern embedded CPUs such as the ARM Cortex A53 and ARM Cortex A57 by 6.23 to 24.1 times in various algorithm computations. Compared to state-of-the-art works, the proposed FECP is 1.65 to 4.49 times better in throughput, 1.73 to 21.19 times better in energy efficiency, and 1.48 to 17.58 times better in energy-delay-product, respectively.

Second, we develop a novel resource-shared crypto accelerator (RCA) to achieve high flexibility and maximize hardware efficiency in hash function and stream cipher computations. The RCA employs two optimizations: a register-sharing approach with multi-mode digest routers and an adder-sharing approach in flexible ALUs. Theoretical evaluation reveals that the RCA achieves 72% register sharing (104 out of 136) and 78.6% adder sharing (44 out of 56). Verification of the RCA on a Xilinx ZCU102 FPGA at the system-on-chip level is conducted to demonstrate its accuracy and efficacy. Furthermore, experimental results of the RCA on multiple FPGAs show its remarkable flexibility and hardware efficiency. It outperforms existing works in terms of throughput (1.36 to 28.9 times) and area efficiency (1.14 to 2.45 times).