論文内容の要旨

申請者氏名　　LE VU TRUNG DUONG

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).

論文審査結果の要旨

申請者氏名　　LE VU TRUNG DUONG

今日、暗号アルゴリズムは、ブロックチェインベースIoTシステムにおけるセキュリティとプライバシーを確保するために不可欠なツールである。ハッシュ関数、ブロック暗号、ストリーム暗号は、今日最も広く使用されているアルゴリズムの多くを網羅する3つの主要暗号である。本論文は、ブロックチェインベースIoTシステムでこれら3種類の暗号をサポートする超効率汎用暗号アクセラレータに焦点を当てている。
まず、ハッシュ関数、ブロック暗号、ストリーム暗号に対して、優れた性能とハードウェア効率を達成する粗粒度再構成可能アレイ(CGRA)アクセラレータとして、柔軟かつエネルギー効率の高い暗号プロセッサ(FECP)を提案している。具体的には、暗号算術論理ユニット、デュアルバッファリング拡張、および、ローカルメモリスケジューラの3手法を提案している。実験の結果、FECPは、消費電力0.239～0.676W、スループット10.2～3.35Gbps、エネルギー効率4.44～14.01Gbps/Wにより、様々なハッシュ関数を実行できることが示されている。さらに、FPGAに実装されたFECP は、様々なアルゴリズムにおいて、ARM Cortex-A53やARM Cortex-A57などの最新組み込みCPU より、6.23～24.1 倍優れている。SOTAと比較すると、FECP は、スループットでは1.65～4.49倍、エネルギー効率では1.73～21.19倍、エネルギー遅延積では1.48～17.58倍優れている。
次に、ハッシュ関数とストリーム暗号計算において高い柔軟性と、高いハードウェア効率を達成するために、新しいリソース共有暗号アクセラレータ(RCA)を提案している。RCAは、マルチモードダイジェストルータを使用した、レジスタ共有と、柔軟なALUによる加算器共有という2つの最適化を行っている。事前評価の結果、RCAは72%のレジスタ共有(136個中104個)と78.6%の加算器共有(56個中44個) を達成している。RCAの精度と有効性を実証するため、Xilinx製ZCU102 FPGAにRCAを実装した。複数FPGAによる実験の結果、優れた柔軟性とハードウェア効率が明らかになった。具体的には、スループットにおいて1.36～28.9倍、面積効率において1.14～2.45倍となり、既存研究を上回った。
以上、本論文は学術上、実際上寄与するところが少なくない。よって、本論文は博士（工学）の学位論文として価値あるものと認める。