論 文 内 容 の 要 旨

博士論文題目

Ultra-efficient Universal SHA-2 and BLAKE Accelerators for Decentralized Networks
(分散型ネットワーク用の超効率的なユニバーサル SHA-2 および BLAKE アクセラレータ)

氏 名 Pham Hoai Luan

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.

氏　名	Pham Hoai Luan

（論文審査結果の要旨）（Ａ４　１枚　１、２００字程度）

SHA-2 および BLAKE アルゴリズムは、Society5.0 の分散型ネットワークのデータ整合性とセキュリティを保護する上で非常に重要である。本論文は、分散型ネットワーク用の超効率的な SHA-2 および BLAKE アクセラレータの開発に焦点を当てている。第１に、マルチモード SHA-2 アクセラレータ（MSA）と呼ぶ SHA-2 ハードウェアアーキテクチャを提案している。システムオンチップレベルで高いパフォーマンスと柔軟性を備えている。高性能と柔軟性を実現するために、本アクセラレータは、マルチモード処理要素アーキテクチャ、３ステージの算術論理演算ユニットパイプラインアーキテクチャ、ナンスジェネレータとナンスバリデータを含む３つの最適手法を適用している。MSA の精度は、ザイリンクス製 AlveoU280 FPGA 上でテストされている。実験結果は、提案 MSA が、従来手法よりも大幅に優れたパフォーマンス、ハードウェア効率、および柔軟性を実現できることを証明している。エネルギー効率では、提案 MSA が最大 38.05 Mhps/W を達成することを示している。これは、Intel 製 CPU i9-10940X および NVIDIA 製 GPU RTX3090 よりも、各々543.6 倍および 29 倍優れていることを示している。第２に、スループットとハードウェア効率を向上させるために、完全パイプライン化された初の BLAKE-256/512 アクセラレータを提案している。また、連続するメッセージ入力において変更された単語の割合に基づき、BLAKE-256/512 アクセラレータの面積とエネルギー消費を削減するため、コンパクトなメッセージ置換スキームを提案している。メッセージ置換スキームには、２つの新しい最適化手法が含まれている。従来のメッセージ置換と比較して、使用レジスタ数を 80%以上削減するレジスタ最適化と、XOR ゲートの数を 93.8%削減する XOR 最適化である。ASIC を仮定した面積および消費電力では、完全パイプライン化 BLAKE-256 アクセラレータの場合、各々最大 11.35%と 21.10%、完全パイプライン化 BLAKE-512 アクセラレータの場合、各々最大 9.86%と 20,32%削減できることが示されている。

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。