

平成25年度 卒業研究報告書概要

課程, 学籍番号, 氏名	課程: 電気・電子情報工学課程, 学籍番号: B123204, 氏名: 鮎澤 勇介		
工学分野名: 情報通信システムコース	指導教員名: 市川 周一, 藤枝 直輝		
題 目: セキュアハッシュ関数 SHA-3 のパイプライン回路実装と性能評価 (Pipeline implementation and performance evaluation of the secure hash function SHA-3)			
Abstract In November 2007, NIST announced that they began a competition to select a new cryptographic hash function SHA-3. In October 2012, Keccak was selected as SHA-3. Pipelined implementation has been proposed to cope with multiple small messages efficiently. This paper presents a pipelined implementation of SHA-3 with the performance evaluation results. The evaluation criterion in this work is “Throughput / Area”. First, the pipeline was optimized to achieve high frequency. Secondly, the calculation of round constants were retimed for higher operational frequency. Thirdly, DSP units of FPGAs were adopted for both high frequency and area reduction. The improved circuit achieved 102.4 [%] improvement of “Throughput / Area” over the reference circuit, while a precedent study reported 51.7 [%] improvement.			
概 要 ハッシュ関数は、任意長のデータやメッセージから固定長のハッシュ値を生成する。情報が正確に伝達されたかを判定するためにハッシュ値は広く使われている。代表的なハッシュ関数として 2012 年 10 月に SHA-3 に選定された Keccak が挙げられる。ハッシュ関数の応用先として、ネットワークルータの伝送チェックやネットワークストレージの暗号化キーなどが挙げられる。これらの応用では、多数の小容量データのハッシュ値を得ることが必要である。 本研究では SHA-3 のハードウェア実装の改良を提案し、面積あたりの処理速度を評価基準として性能を評価する。複数メッセージを取り扱う回路にするため、SHA-3 にパイプライン化を施しハードウェア実装する。実装は Xilinx 社の Virtex-5 FPGA を対象とする。 本研究での改良は 3 つの点から成る。1 つ目はパイプラインの構成変更である。Abdulkadir Akin らの関連研究ではパイプラインステージ数 5 で実装されている。Akin らのパイプライン構成を追実験したところリファレンス回路に対し評価値は 51.7 [%] 向上した。他のパイプライン構成を検討したところ、パイプラインステージ数 3 で実装したときリファレンス回路に対し評価値は 72.2 [%] 向上した。 2 つ目の改良はラウンド定数を計算するタイミングを変更することである。これにより動作周波数の向上を図る。パイプラインステージ数 4 でラウンド定数の計算タイミングを変更したところ、リファレンス回路に対し評価値は 88.3 [%] 向上した。 3 つ目の改良は FPGA に搭載されている DSP (Digital Signal Processor) ユニットの使用である。Provelengios George らの関連研究では FPGA に搭載されている DSP を演算処理の一部に使用することにより動作周波数向上を図った。George らと同様に非パイプライン環境で DSP を使用し追実験を行ったところ、リファレンス回路に対し評価値は低下した。しかしパイプライン環境では、DSP を使用することにより動作周波数向上と面積削減が期待できる。パイプラインステージ数 5、ラウンド定数の計算タイミング変更、DSP 使用、という条件を組み合わせで実装したところ、リファレンス回路に対し評価値は最大 102.4 [%] 向上した。 本研究で用いた Virtex-5 以外の FPGA であっても、類似の DSP 回路が搭載されていれば性能向上が期待できる。DSP が搭載されていない FPGA であっても、パイプラインステージ数の変更、ラウンド定数の計算タイミングの変更で評価値の向上が期待できる。			

発表する際の課程を記入

電気・電子情報工学

課程

発表番号

3

(学籍が他課程所属の学生も発表する課程を記入すること)