セキュア・ハッシュ・アルゴリズムの高性能でコンパクトなパイプライン設計

HOANG ANH TUAN

本論文はハッシュアルゴリズムのいくつかの細粒度のパイプライン実装と評価を述べており、高性能でコンパクトなハードウェアを実現している。本研究はパイプラインのステージを均衡させることによって、許容できるハードウェア量でハッシュアルゴリズム実装のスループットの制限に打ち勝つことを目的としている。

ハッシュアルゴリズムはメッセージと鍵を用いて、多数の繰り返しでハッシュ値を生成する。その繰り返しで生成される巨大な計算の遅延が、システム全体のスループットを制限する。ハッシュアルゴリズムの実装には、基本的なパイプラインとループアンローリングの２つがあるが、各ステージの処理時間はまちまちで、ハードウェアのサイズが大きい。従来の研究では、ループアンローリングのスループットは高いが、ハードウェアをコピーするのでハードウェアサイズが大きい。基本的なパイプラインはステージ間が不均衡なので、スループットに制限がある。

我々は２つの逐次的な繰り返し計算におけるデータ依存性とデータ転送を分析することにより、クリティカルパスを均衡したステージに分割する方法を提案する。MD5の１つの繰り返し計算はデータフォワーディングと２つのメッセージ処理により、３段と４段のパイプライン処理に分割して実現する。SHA-2の繰り返し計算は、データフォワーディングと計算の延期により、２段と３段のパイプライン処理に分割して実現する。さらに、SHA-2の２つのバージョン（SHA-384とSHA-512）を結合して設計し、デバイスの使用率を向上させる。これらの設計をいくつかのFPGAボード上で実装し、ハードウェアサイズ、スループット、エリアパフォーマンスレートの観点から評価した。我々の実装は最高のエリアパフォーマンスレート（スループット÷エリア）を達成しているだけではなく、殆どすべての関連研究よりも高いスループットを実現している。実験結果はハッシュアルゴリズムの高性能でコンパクトなハードウェア設計を示している。