機能と性能を取捨選択可能なIPsecハードウェア実装の検討

山口 和哲，楯岡 孝道，阿部 公輝
電気通信大学 情報工学科

1 はじめに

近年、ネットワーク上で重要なデータ（機密情報，個人情報）を扱うようになり，高速なセキュリティ機能を実現する必要が出てきた．その為には，セキュリティ機能のハードウェア化が有効であるが，コストが問題となる．そこで，扱う情報や機器によってセキュリティ強度や機能，性能は同じレベルで保つ必要はないと考え，利用目的に応じて機能や性能の取捨選択を行う事を提案する．

これは，IPsec[1] 実装を各機能ごとに実装し，それらの取捨選択を行うことで実現できる．さらに目的に応じた性能は，同じ機能を持つ異なる実装を取捨選択することで実現できる．これにより機能，性能とコストのトレードオフが可能であり，この各機能の性能とコストを示すことにより，今後利用形態に応じて最適化したIPsecの実装を行う際の目安になる．

2 IPsec機能と性能の取捨選択の提案

IPsec機能の取捨選択を行うパーツとして大きく4つに分けることができる．図1にその概要を示す．

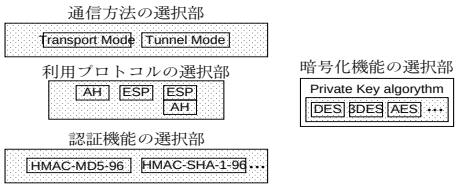

図 1: 取捨選択を行うパーツ

鍵管理，及び鍵交換機能を持つIKEについては，利用頻度が少なくハードウェア化コストが非常に高い事が予想されるので本研究では扱わない．

これらの中から，例えば「Tunnel Modeを省略し，低速だがコストの低いAESを使用する」などして，バランスの取れた実装を実現する．

3 認証機能MD5のハードウェア実装

性能とコストのトレードオフを行う為に，IPsecの中で利用頻度の高いMD5[2]について，速度重視と面積重視のMD5の実装を行った．

3.1 MD5実装の詳細

3.1.1 MD5全体の実装

MD5は，任意のデータを入力にとり，128ビットのMessege Digestを生成する．作成したMD5の構造を図2に示す．

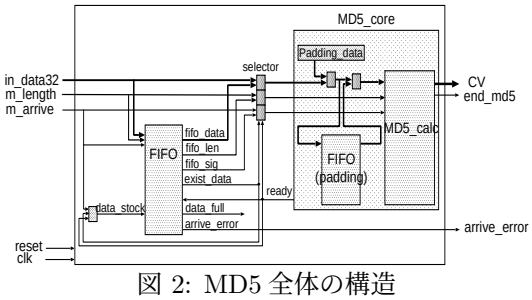

図 2: MD5 全体の構造

3.1.2 MD5_calc部の実装

処理の中心となる図2のMD5_calc（512ビット単位でMD5の計算を行う回路）についてパイプライン化したもの（MD5_pipeline_module）とそうでないもの（MD5_loop_module）を作成し性能比較を行った．

3.2 性能比較

記述言語にVerilog-HDLを用い，論理合成にはSynopsys社のDesign Compilerを用いた．また，ライブラリにはRHOM社の0.35μmデザインテクノロジーを使用した．

論理合成時の制約条件を変えることで得られたスループットと回路面積の比を表すことにより性能比較を行う．

図2のMD5_calcにMD5_pipeline_moduleとMD5_loop_moduleをそれぞれ組み込んだときの性能比較を図3に示す．

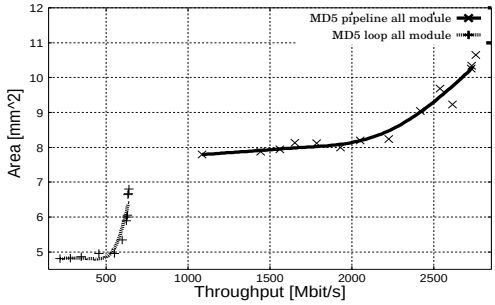

図 3: MD5 全体の性能比較

これより，図2のMD5_calc部に用いる回路を選択することで，“速度重視” または “面積重視” など設計目的に応じて選択できることが確認できた．さらに，この図2の回路において，FIFOの深さを変えることが可能であり，利用目的に応じて機能を取捨選択することでコストの削減を行うことも可能である．

また，ソフトウェア (PentiumIII 500MHz FreeBSD 4.8R) と比べ，ハードウェア化することで8倍近い処理速度の向上が見られた．

4 おわりに

IPsecハードウェア実装における各機能と性能の取捨選択によるコストとのトレードオフについての検討を行い，IPsecカスタマイズ実装について提案をした．また，2種類のMD5ハードウェア実装を行い性能比較を行った．これより，同じ機能を持つ回路でも，組み込む回路を取捨選択することにより回路面積の削減，または速度の向上が可能であることが示された．

今後は，残りの各機能についても個別に実装し性能評価を行うことにより，IPsecカスタマイズ実装を可能にする．

参考文献

[1] S. kent and R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, Nov. 1998.

[2] R. Rivest, “The MD5 Message-DIgest Algorithm”, RFC 1321, Apr. 1992.