要 旨

セルフタイム型パイプラインによる AES 回路の設計

久保 竜宏

情報通信処理システムの小型化や高性能化では，計算処理資源 (トランジスタ) をいかに性能の向上へ転換するかが鍵となる．計算処理資源を利用した性能の向上手段としては，同一モジュールを複数設置することによる処理性能の向上や，同一の処理を単一モジュールに重畳させることによる回路規模の縮小がある．これらを実現するためにはモジュール間の柔軟な接続が必要であり，セルフタイム型パイプライン (STP) は同期式パイプイランに比べ，柔軟な構成 (接続) を容易に実現することが可能となる．そして，その柔軟な構成を利用することにより，モジュール単位での自由な設計の変更や，処理のデータフローに沿ってモジュールを接続することが可能となる．しかし，設計の際に必要となるパイプライン構成の検討には，性能と面積のバランスを見抜くエキスパートの洞察力が必要とされ，経験の乏しい設計者には難しい作業となってしまう．そこで，本研究ではアプリケーションのデータフローに着目し，要求性能に応じたパイプライン構成を導き出す手法として，パターンベースパイプイラン構成法について提案する．そして，提案手法を AES 回路に適用して小面積で実装可能なデータフローを検討し，65nm CMOS プロセスを利用して設計を行った．結果，8.0Gbps の性能を得ることができ，評価対象として設けた映像・通信分野の 5 項目と比較することにより，比較対象とした 5 項目について有効であることを確認した．また，評価後の考察として，本研究で用いたパイプライン構成よりもさらに複雑なパイプライン構成にも適用可能な構成法へと改良していく余地があるという結論に至った．

キーワード　セルフタイム型パイプライン，パターンベースパイプライン，AES

Abstract

Design of AES Circuit by Self-Timed Pipeline

Tatsuhiro KUBO

Effective use of high performance transistor is a key factor in designing a high performance or smaller ICT system. The performance of circuit can be improved by increasing the processing modules or by cutting down the size with superposition of same module of circuits by using high performance transistor. In order to realize these, adaptable connection between modules is necessary. Self-timed pipeline (STP) provides more adaptable connection than pipeline of synchronous circuit. Thus, STP enables the designers to make easy design changes to each module, and connect modules along the data flow. However, designing the optimal pipeline requires much expertise in detecting the balance between the throughput and the area of the circuit, which will be a difficult task for inexperienced designers. This study focus on data flow, we proposed the pattern-based pipeline architecture method, which generate the optimal pipeline architecture according to the required performance. And so, we designed the AES circuit used the proposed method and 65nm CMOS process. As a result, AES circuit brought out 8.0Gbps throughput. It is confirmed that this designed circuit brought out better throughput in required performance compared to wire communication, wireless communication, Blu-ray Disc, digital broadcast and USB3.0. Finally, it is discussed that further study is necessary in applying this study to more complicated pipeline architecture.

key words self-timed pipeline, pattern based pipeline , AES