早稲田大学大学院理工学研究科

博士論文概要

論文題目

カスタムアレイ型大規模並列回路の
高速・高集積・省電力化に関する研究

申請者

佐藤証

Akashi Satoh

1998年7月
(西暦)

本研究では大規模・高集積化する半導体ハードウェアリソースを最大限に利用した，高速で小型かつ電力の低い高性能 VLSI 回路のカスタム設計を目的とし，次の三つの視点から様々な回路方式を提案した．

- シンプルな基本演算ユニットの大規模並列処理による高速化
- 規則的なアレイ構成や同一機能ブロックの共有による小型化
- ダイナミック回路における電圧と動作タイミングの制御による省電力化

また提案方式を実装した高速 DRAM，データ圧縮回路，公開鍵暗号回路では，いずれも世界最高速度と小型・省電力化が達成され，その有効性が示された．

微細加工技術の進歩とチップの大規模化により VLSI 回路の性能は飛躍的に向上して来たが，それと同時に回路設計の難度が増大していることも事実である．特に1チップ内で一千万個を超えるに至ったトランジスタを効率的に使いながら，高速化に相反して増大する消費電力を如何に抑えるかといった点が設計の重要なポイントとなる．高速ハードウェアの設計において，ソフトウェアに真似のできない最大の特徴は大規模な並列性にある．しかしソフトウェアで多数の分岐命令を要するような複雑な処理を，ハードウェアで効率的に並列実行させることは難しい．そこで高速化のボトルネックとなる機能ブロックを切り出し，並列処理可能なシンプルな回路ユニットに分解し，そのユニットをアレイ状に並べた構成にすることが，ハードウェア性能の向上と効率的なカスタム設計には欠かせない．またアレイ構成も単なるフラットな並列化に止めず，信号の伝播遅延を考慮しながら各ブロックの処理内容に応じて柔軟に対処することも重要である．さらに回路のアレイ化によって処理が並列化されるだけでなく，基本ユニットのカスタムレイアウトも容易となり，ダイナミック回路の使用と電圧・動作タイミング制御，デバイスや配線の細かな調整などによる高速・小型・省電力化も可能となる．

第1章では研究の背景と目的を，2章と3章では高速 DRAM，4章と5章ではデータ圧縮回路とその応用，6章では公開鍵暗号回路について述べた．

大容量化と高速化が進む DRAM は，メモリセルが規則的に並ぶアレイ構造を持つ最も基本的な並列処理回路と捉えることができる．データの読み／書きにおいて数百～数千個の基本ユニットが並列動作するので，高速化と同時に消費電力を抑えるため，個々の回路に対しアナログ特性を重視した設計を行なった．また DRAM はコンピュータシステムの主記憶として広く用いられ，プロセッサの処理を滞らせないためにはアクセス速度と同様にデータ転送効率の向上が重要である．そこで内部処理のパイプライン化と再スケジューリングにより，バス使用効率の最適化も図った．

連想メモリはデータ検索機能を持ち，これをデータ圧縮回路の冗長データの検索・削除に応用した．ここでは連想メモリと圧縮符号の双方の特徴を生かすためアーキテクチャの視点から，検索・エンコードの様々な並列処理手法を提案するとともに，回路の共有による小型化についても検討した．

公開鍵暗号では長大な数に対する算術処理のため，より複雑な回路構成が必要となる．演算の基本回路である加算器に対しては，セルをフラットなアレイ構造ではなく，1ビットずつ大きなブロックを作りながら階層構造化し，キャリーが各ブロック上を多重伝播する高度な並列化手法を示した．また全体のアーキテクチャにおいては，演算式を様々な形にアレンジして並列処理・共通項の削除・演算の省略による高速・小型化を行なった．

以下に，各章で得られた主な結果を要約する．

第2章では，DRAM と連想メモリの高速化と省電力化のための回路方式を提案した．DRAM でキーとなる回路は数千個が同時に動作するセンスアンプであり，ビット線電圧をフルスイングさせる従来の Half-V_{DD} センス方式の代りに，イコライジング電圧をシフトし，またパルス信号で振幅を制御するパルスセンス方式を提案した．これにより無駄な電力の削減と，メモリセルからの信号出力遅延時間の短縮による高速化が実現された．またワード線をダイナミック OR 回路により直接モニターしてセンスのタイミングを最適化する方式や，データ出力回路の高速・低ノイズ化のためデータバスを事前に $1/2V_{DD}$ に設定して電圧振幅を半分とするプリコンディション方式を提案した．これらの方式を実装した 4M ビット DRAM では，世界最高速のアクセス時間 14ns が実現され，消費電力も Half-V_{DD} センス方式の 2/3 と低いことが示された．また連想メモリにおいても検索動作時の電圧振幅を抑え，貫通電流をカットして省電力化と高速化を行なった．

第3章では DRAM をパイプライン化し，リード／ライト／リフレッシュ処理を内部で再スケジュールすることで，バーストデータ転送時にアイドル状態が生じるのを防ぎ，バス使用効率を最適化する方式を提案した．さらにシングルアクセスに対しても，リフレッシュアレイへの外部アクセスを小さなキャッシュでハンドルし，リフレッシュ動作を完全に隠蔽することが可能なことを示した．これに2章の DRAM 高速化方式を組み合わせれば，バースト SRAM に対しても速度的に遜色のないメモリを，わずか 1/4 のサイズで実現することが可能となる．

第4章では2章で提案した高速な連想メモリに可変長文字列検索機能を付加し，それを LZ77 符号の高速回路実装に応用した．文字列検索には一致した次のアドレスに対してだけ検索を許可する“ローカルプリチャージ方式”と，文字と文字列の検索結果を別々のレジスタに保持してレジスタ間で演算を行なう“2段パイプライン方式”を提案した．さらにクリティカルパスである一致検出ロジックの見直しによる高速化と小型化，圧縮率向上を目的としたプライオリティエンコーダの改良方式も提案した．LZ77 符号は様々なデータに対して高い圧縮率を示す反面，その処理速度に問題があったが，提案方式により 100MB/秒と極めて高速なデータレートが実現された．これはソフトウェア実装に比べ 2～3 桁，またハッシュテーブルを用いた従来のハードウェアに対しても一桁高速である．

第5章では高速データ圧縮 LSI によって可能となるアプリケーションとして，

ディスクス圧縮と PostScript プリンタ内のメモリ圧縮について述べた．従来のソフトウェアによるディスク圧縮は，データの読み書きにプロセッサ占有されてしまうこと以外にも，OS のファンクションコールを横取りしているためディスク破壊の危険性やソフトの互換性などの問題があった．ディスクにデータ圧縮 LSI を組み込めばこれらの問題が解決され，さらにフラッシュメモリを用いる半導体ディスクでは書き込みに長い時間と大きな電力が必要なことから，データ圧縮によって容量が増加した上に，高速かつ低電力という大きな効果が得られる．

PostScript プリンタの作業メモリはカラー化・高画質化によって増大している．しかしラスタ処理によってアクセスされる領域には局所性があるため，処理エリア周辺のイメージだけを作業メモリ上に持ち，残りの部分を圧縮しておくことでメモリが大幅に削減可能なことを示した．各種パラメータの最適化も行なうことで，ビジネス文書に対するオーバーヘッド時間を 1～5%と低く抑えながら，メモリを 1/5 に削減することが可能となった．

第 6 章では，情報セキュリティに欠くことのできない公開鍵暗号の高性能な回路実装方式について述べた．キャリーを多重伝播する高速加算器と，乗算・べき乗算の並列処理による 1024 ビットの RSA 暗号 LSI では，23ms という極めて高速な処理をわずか 4.9mm^2 のアクセラレータコアで実現することができた．これは既存の専用 LSI の 2 倍，スマートカードチップと比較すると 30 倍も高速である．さらに乗剰余算中の部分積加算と剰余補正減算をスキップして高速化する方式や，加算器のシェアによる小型化方式も提案した．これらの手法を RSA の次世代の公開鍵暗号である楕円暗号に適用すれば，RSA と同等の暗号強度が 1/7 のサイズのコアによって，10.5ms と 2 倍の速度で実現できることも示した．また既存の楕円暗号実装と比較するならば，これは 60 倍も高速な値である．

近年のパーソナルコンピュータの低価格化と各種モーバイル機器の性能向上，そしてインターネットを始めとする通信網の発達により，日常生活において様々なハイテク機器を使用する機会が一段と増している．これら電子情報化社会の急速な発展を支えている大きな要因の一つが半導体回路設計・製造技術の進歩であり，これをさらに推し進めるために一層の回路の高速化・小型化・省電力化が求められている．また本研究における三つの LSI 実装をアプリケーションの視点から見るならば，高速な DRAM はプロセッサ性能を最大限に引き出してシステム全体のパフォーマンスを向上させ，また SRAM を置き換えることでコストの削減も行なえる．データ圧縮はメモリやディスクの仮想容量を増加させるだけだけでなく，ネットワーク上の送受信データ量を減らして高速かつ低コストな通信を実現することができる．さらに高速な暗号 LSI は，不特定多数のユーザーが介在するセキュアでない通信網での機密保護や本人認証を可能とする．このように本研究の成果はコンピュータシステムの性能向上と，情報通信網の発展においても非常に重要な位置を占めるものと思われる．