氏名	魏 書剛 (Wei Shu Gang)
授与学位	工学博士
学位授与年月日	平成2年3月28日
学位授与の根拠法規	学位規則第5条第1項
研究科，専攻の名称	東北大学大学院工学研究科 （博士課程）電子工学専攻
学位論文題目	**多値演算回路に基づく暗号処理プロセッサに関する研究**
指導教官	東北大学教授 樋口 龍雄
論文審査委員	東北大学教授 樋口 龍雄　東北大学教授 斎藤 伸自 東北大学教授 高木 相　東北大学助教授 亀山 充隆

論文内容要旨

第1章 緒言

情報化社会の進展に伴い，データ通信の安全保護はますます重要となっており，その対策として暗号が利用されている。公開鍵暗号の暗号化／復合化には，極めて長い語長の演算が必要であり，例えば，RSA暗号処理に対して，極めてけた数の多いべき乗計算と剰余計算を主体としているため，その高速化が重要な問題である。

現在までいくつかのRSA暗号処理LSIアーキテクチャが提案されているが，それらはすべて通常の2進数演算を前提として構成されているので，長い語長を有するデータに対してキャリ伝搬の影響が本質的に存在している。

これに対して，Signed－Digit（SD）数演算では，語長に無関係に一定遅れ時間で加算出力が得られるため，キャリ伝搬の影響が本質的に存在しないことが知られている。本論文は，この性質を利用することにより，SD数加算器を有する極めて語長の長い暗号処理プロセッサの構成を提案し，RSA暗号処理の高速化を実現することを目的とするものである。SD数演算回路については，SD数表現の冗長性のため，通常の2値論理演算に基づく構成方法では，回路の規模および配線数が増大するという問題がある。本論文では，高速性かつコンパクト性の観点から，双方向電流モードに基づく多値SD数演算回路を中心とする暗号処理プロセッサの構成法を提案する。また，2 μm CMOSの設計ルールによるVLSIチップの試作を前提としたVLSI化設計およびその性能評価を行

い，従来の暗号処理プロセッサと比較して10倍以上高速できることを明らかにしている。

第2章　RSA公開鍵暗号処理の高速化に関する考察

公開鍵暗号の高安全性のため，暗号処理に必要とされる鍵およびデータの語長が極めて長いことが要求されている。RSA公開鍵暗号処理では，次式の演算が行われる。

$C = M^{e} \bmod F$

eとFは公開鍵であり，例えば，それぞれ10進100けたと200けた程度の大きな正整数である。M，CはFより小さい正整数であり，それぞれ通信文および暗号文である。暗号処理の高速化のため，いくつかのハードウェアアルゴリズムが提案されている。しかしながら，これらの方法が2進数加算の繰り返しによるものであり，極めて長い語長のキャリ伝搬が暗号処理の高速化を制限している。これに対し，O(1)の加算時間で加算を実行できるSD数演算に基づく暗号処理プロセッサを構成することにより暗号処理の高速化に有用であることを明らかにしている。

第3章　多値SD数演算回路

本章では，暗号処理プロセッサで使用されるSD数加算器の高速化と小型化のために，電流モード回路による実現法を考察している。双方向電流モード回路においては，結線のみにより線形加算を実現できるという性質を十分活用し，2値システム内で利用可能な2値入出力4進SD数加算器の構成法を提案している。図1は，多値4進SD数全加算器のブロック図を示している。2値電圧－多値電流変換と単方向および双方向電流の線形加算を巧みに組合せることにより構成された4進SD数加算回路は従来提案されている加算回路と比較して高速性とコンパクト性に優れていることを明らかにしている。

第4章　4進SD数演算に基づく暗号処理ハードウェアアルゴリズム

第3章で提案した2値入出力4進SD数加算器を用いることにより，高速な暗号処理ハードウェアアルゴリズムを提案する。SD数の剰余演算を容易に実行できるように，負数を含む剰余演算を定義している。すなわち，剰余演算P mod Fの結果がFより小さい正整数になるのに対し，剰余計算結果を$-F+1$から$F-1$の間の整数とすることにより，4進SD数加算の繰り返し回数が少ない暗号処理アルゴリズムを提案し，2進数演算アルゴリズムに比べてその計算量を半減できることを示している。

第5章　多値暗号処理プロセッサの構成

第4章で提案した4進SD数演算に基づく暗号処理アルゴリズムにより，多値SD数演算回路を中心とする暗号処理プロセッサを考案している。メモリ，レジスタなどを2値素子で構成することを前提とし，またSD数演算の高並列性を最大限活かしたパイプライン処理に基づき，SD数加算器とメモリおよびレジスタとのデータ転送が同時に実行できる方法を提案している。これにより，暗号処理速度はSD数加算の回数および加算時間により決定され，2進数暗号処理プロセッサの性

能を大幅に向上できることを示している。図2は，マイクロプログラム制御方式に基づく本暗号処理プロセッサのブロック図を示している。個別ICによる16ビットプロセッサを試作し，暗号処理の動作原理を確認している。

第6章　多値暗号処理プロセッサのVLSI化設計と性能評価

本多値暗号処理プロセッサに対し，VLSIチップの試作を前提として，2 μmCMOS設計ルールによるVLSI設計，および性能評価を行っている。まず，2値入出力4進SD数加算器のレイアウトを行い，レイアウトパターンから配線容量などのパラメータを抽出し，電子回路解析プログラムSPICE 2によるシミュレーション結果を2進数加算器と比較することにより，本SD数加算器が高速性およびコンパクト性に優れることを明らかにしている。ついで，極めて長い語長の暗号処理VLSIを設計するため，SD数演算の局所性と規則性に着目し，Digit－Sliceと呼ぶ設計法を考案している。この方法により，実用的暗号処理プロセッサのVLSI化設計が容易になり，VLSIチップが非常にコンパクトに構成される。図3は512ビット語長の暗号処理VLSIレイアウトを示しており，チップサイズは，9.1×7.4㎟となり，VLSI化が十分可能となっている。さらに，シミュレーションなどによる性能評価を行った結果，暗号処理速度は85kbit／sとなり，2進数演算に基づく暗号処理プロセッサより10倍以上高速化できることが明らかになった。

第7章　結　　言

結論として本論文を要約した。本多値暗号処理プロセッサが画像通信のような高速データ伝送に応用でき，さらに，提案したSD数演算回路およびSD数演算アルゴリズムは語長の長い演算に極めて適合するため，他の公開鍵暗号処理の高速化にも有用であると考えられる。

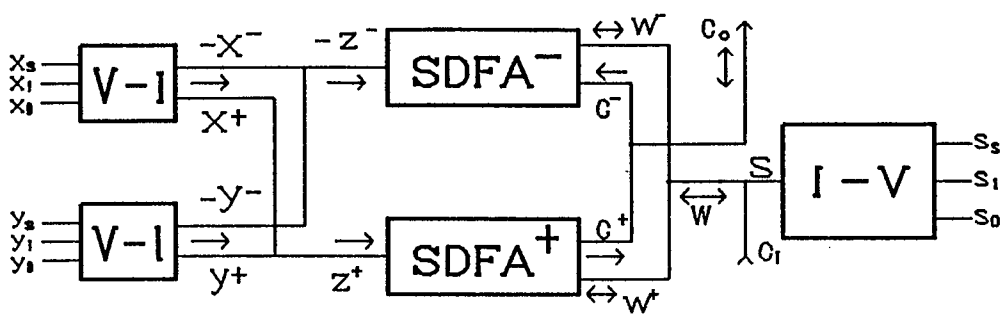

図1　2値入出力多値SD数全加算器

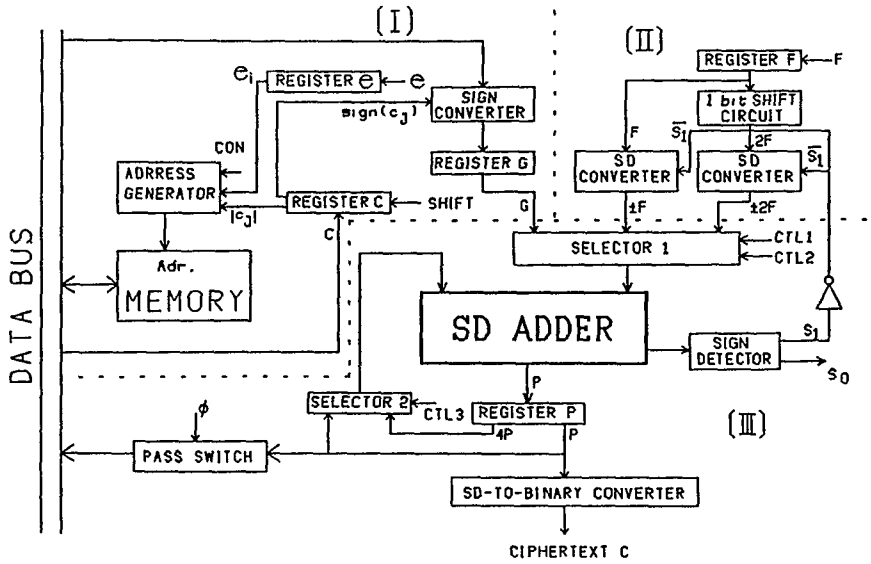

図2　多値暗号処理プロセッサの構成

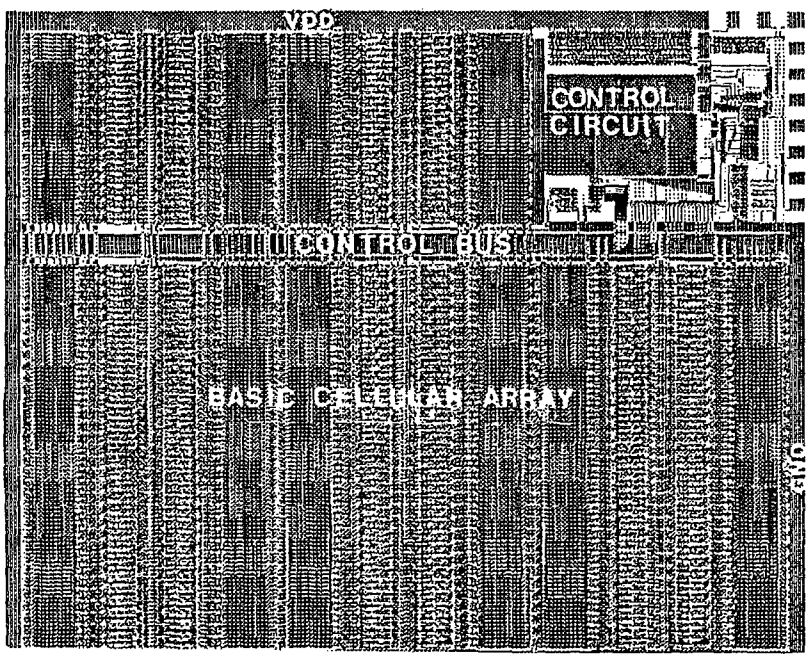

図3　多値暗号処理 VLSI のレイアウト
（チップサイズ：9.1×7.4㎟，トランジスタ数：120k）

審 査 結 果 の 要 旨

情報ネットワーク化の進展に伴い，暗号を用いた情報セキュリティが重要となってきている。特に，画像通信などを可能にするためには高速暗号処理VLSIプロセッサの開発が望まれている。

著者は，安全性確保のため極めて長い語長の演算が必要とされる暗号処理に対し，4進Signed−Digit（SD）数演算の高並列性が適合することに着目し，新しい多値演算回路に基づく暗号処理プロセッサの構成法を提案し，チップ設計による評価を行い，その有用性を明らかにした。本論文はその成果をとりまとめたもので，全文7章よりなる。

第1章は緒言である。第2章では，極めて長い語長の算術演算に対し語長に依存しない高速加算が可能である4進SD数加算回路をサブシステムとして利用することが公開鍵暗号処理プロセッサの構成に有用であることを明らかにしている。

第3章では，多値単方向および多値双方向電流モードCMOSを巧みに組み合わせることにより，暗号処理プロセッサの構成に重要となる2値出力インタフェース容易性を具備する4進SD数全加算器（SDFA）の新しい構成法を提案している。回路解析プログラムを用いた計算機シミュレーションによる評価の結果，従来の双方向電流モードSDFAの構成法と比較しても高速化と小型化が達成できることを明らかにしている。

第4章では，4進SD数加算に基づく暗号処理ハードウェアアルゴリズムを考案した結果を示している。冗長な剰余表現と4進数の利用により，暗号処理に要する加算回数を2進数演算と比較して半減できることを明らかにしている。これは有用な成果である。

第5章では，本ハードウェアアルゴリズムに対し，パイプライン処理により暗号処理速度が加算回数のみで決定されるプロセッサアーキテクチャを提案している。これに基づくモデルプロセッサを個別ICを用いて試作し，良好に動作することを確認している。

第6章では，2 μmCMOS設計ルールに基づき，本暗号処理VLSIプロセッサのレイアウトと計算機シミュレーションによる性能評価を行った結果を示している。4進SD数加算器の局所並列演算性を巧みに利用したDigit−Slice法と呼ぶ設計法を考案し，規則性のあるレイアウトが可能であると共に，その性能は従来までの暗号処理プロセッサの10倍程度になることを明らかにしている。これは重要な成果である。第7章は結言である。

以上要するに本論文は，多値電流モード4進SD数演算回路の新しい構成法を考案し，この演算回路を巧みに利用することにより従来にはない高性能な暗号処理を達成するVLSIの構成法を確立したものであり，電子工学および情報工学の発展に寄与するところが少なくない。

よって，本論文は工学博士の学位論文として合格と認める。