社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－ＳＬＤＭ－126 (16)
2006／10／26

完全自立形を指向したIPコアの設計法

畠中 浩行† 中村 次男†† 笠原 宏† 冬爪 成人† 田中 照夫†††

† 東京電機大学情報環境学部 〒270-1382 千葉県印西市武西学園台 2-1200
†† 国際短期大学情報ネットワーク学科 〒165-0022 東京都中野区江古田 4-15-1
††† 東京電機大学工学部電気工学科 〒101-8457 東京都千代田区神田錦町 2-2
E-mail: †kasahara@itl.sie.dendai.ac.jp

あらまし 集積回路技術が向上していく中，使用される多種多様なIPコアは数十～数百にもなる．これにはIPコアの再利用および流通が不可欠となる．しかも，多種多様なIPコアを一つのチップに集積化するとなると設計者はすべての仕様を知る必要があり，非常に困難である．そして，IPコアの再利用性および多種多様なIPコア間のインタフェース，バス調停機構，使用容易性，消費電力などの問題も生じてくる．これらの諸問題を解決するために，オブジェクト指向技術を用いたメッセージ通信やVC(Virtual Component)として特定の使用目的に限定されないIPコアを設計する設計法の提案を行った．

キーワード 自立形IPコア，システムLSI，再利用性，使用容易性，システム・オン・チップ

A Self-support Oriented IP Core Design Method

Hiroyuki HATAKENAKA†, Tsugio NAKAMURA††, Hiroshi KASAHARA†,
Narito FUYUTSUME†, and Teruo TANAKA†††

† Department of Information Environment Engineering School of Information Environment, Tokyo Denki University Muzaigakuendai 2-1200, Inzai-shi, Chiba, 270-1382 Japan
†† Department of Information and Network, Kokusai Junior College Egota 4-15-1, Nakano-ku, Tokyo, 165-0022 Japan
††† Department of Electrical Engineering School of Engineering, Tokyo Denki University Kandanishikichou 2-2, Chiyoda-ku, Tokyo, 101-8457 Japan
E-mail: †kasahara@itl.sie.dendai.ac.jp

Abstract For designing an integrated circuit with the scale of System LSI or SoC, it is reasonable to reuse the circulating IP cores. But it is a quite difficult work for a single designer to get to know all the details of the specifications of dozens / hundreds of IP cores. Problems, such as interfaces between various IP cores, bus mediation mechanism, power consumption are all essential issues to be considered.

To cope with these problems, the paper proposes a common IP core designing method, where 1)each core is considered to be a virtual component, not for single purpose but for general purpose uses, with the optional arithmetic accuracy 2)data transfers between IP cores are limited only by unified message-communication format. We call such a scheme of core as "self-support oriented" assimilated to object-oriented technology.

Key words self-supproting IP core, System LSI, reuse, ease-of-use, System on Chip

1. まえがき

集積回路技術が向上し，システムLSIやSoC(System on Chip)などの大規模集積回路に用いられるIP(Intellectual Property)コアは数十～数百にもなると言われている[1]．これらの大規模集積回路においては，最初からすべての回路ブロックを設計することは要する時間やコストなどを考慮すると困難である．これにはIPコアの再利用および流通が不可欠になる．しかも，多種多様なIPコアを集積化するためにはそれらの仕様をすべて知る必要があり，それは非常に困難となることからIPコアの再利用や使用容易性が求められる．そして，複数のIPコアを用いることでIPコア間のインタフェース，バス調停機

構，消費電力などの問題が生じる．これらの諸問題を解決するために，オブジェクト指向技術を用いたメッセージ通信 (メッセージとパラメータによる通信) や IP コアの用途が特定されない Virtual Component(以下 VC とする) としての IP コアを設計する設計法の提案を行う．

2. 完全自立形 IP コアの実現

SoC やシステム LSI といった大規模集積回路では，多種多様な IP コアが流通し，1 チップ上に集積化される．従って，使用用途の特定されない VC として設計されている必要がある．更に，使用者や LSI 設計者は多種多様な IP コアの仕様を知ることなく，また，再利用性や使用容易性を満足する IP コアの実現が重要性を増してくる．これからの超集積回路時代においては，従来の設計法とは異なった設計法が求められてくる．筆者らの提案する設計法は処理を行うために必要なデータのみを与えることで IP コアが外部からの制御を全く必要とせずに処理を行い，結果を返すという完全自立形 IP コアを実現することである [3]〜[7]．これにより，IP コアは部品化され，その中身を知らなくても使用することができる．自立性を持った IP コアとなる．

完全自立形に求められる要素

（1） 基本モジュール (図 1)

（2） 基本モジュールの再利用による任意精度対応アーキテクチャ(図 2)

（3） 処理精度に対して効率的なクロック周波数制御 (図 5)

（4） 未使用モジュールのスタンバイモードによる消費電力の抑制 (図 7)

IP コア自身に自立性を持たせる機能を内蔵することで，使用容易性および拡張性が向上し，メッセージ通信とすることで IP コア間のインタフェースの標準化が容易になる．そのために，自立性を持った機能を備えた基本となるモジュールから成る IP コアの実現が必要となる．基本モジュールの実現において，処理精度に対して柔軟に対応できるアーキテクチャとして基本モジュール間のインタフェースを考慮し，使用用途が特定されない VC として設計されていなければならない．

基本モジュールの構成

（1） I/O インタフェース

IP コア間の接続インタフェースであり，メッセージ通信のためのメッセージ処理を行う．ここで，メッセージ内のアドレスから，自コア宛のデータなら引き続き送られてくるデータを受信し，自コア宛でないなら無視する．また，精度情報から，必要なモジュール数，クロック周波数およびクロック数の決定もこのブロックで行う (参照:2.2)．

（2） 機能モジュール

本来の IP コアとしての機能．例えば，プロセッサや暗号システムなど．

（3） モジュール間インタフェース

外部からの制御を全く必要としないアーキテクチャとするために，モジュール間で通信制御を行い，演算処理やスタンバイモード (参照:2.4) などの処理を行う．

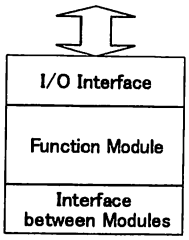


図 1 基本モジュールの構成
Fig. 1 Structure of a Basic module

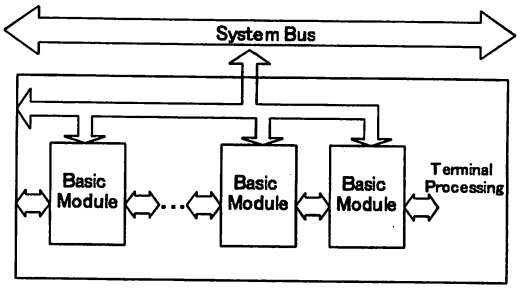


図 2 複数の基本モジュールから成る IP コア
Fig. 2 An IP core with Several Identical Basic Module

従来の外部から制御する回路と比べ，自立性を持った機能を内臓するためにインタフェース部分がゲート数増となり，オーバヘッドが生じてくるが，SoC のような大規模な集積回路において，課題となっている IP コアの再利用性，拡張性および使用容易性などを重視した設計となっており，生産性の向上が期待できる．

2.1 モジュール化のための分析

モジュール化は大きなシステムを分割し，部品化をして，保守管理を容易にしたり，生産性や品質の向上を高めることができる．しかし，提案する設計法では，設計過程におけるスケーラビリティや単純な機能分割 [8]〜[10] ではなく，1 つの基本モジュールでも自立形 IP コアとして動作が可能で，カスケード接続をすることで任意精度に対応したスケーラブルな IP コアを実現することである．これにより，再利用可能で使用容易性を持った IP コアとなり，IP コアにおける諸問題を解決できる．

ここで，重要となるのが基本モジュールの設計である．構成は前述で述べた通り I/O インタフェース，機能モジュール，モジュール間インタフェースから成る．モジュール化を行い，なおかつ，自立性を持ったアーキテクチャとするためモジュール間インタフェースでは上位モジュールおよび下位モジュールに必要となる情報を伝搬しなければならない．そして，受け取る側のモジュールも同一の基本モジュールを用いるので，基本モジュールは伝搬信号の送受信を行うことになり，それに対応した設計が必要となる．

拡張 (基本モジュールのカスケード接続) を行った場合は，モジュール間インタフェースにより，モジュール間でそのモジュールに合ったデータに対する内部レジスタへの保存および処理の

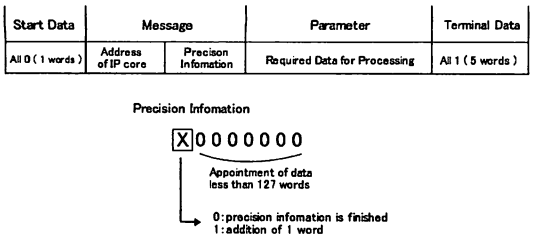


図 3　通信フォーマット
Fig. 3　Communication format

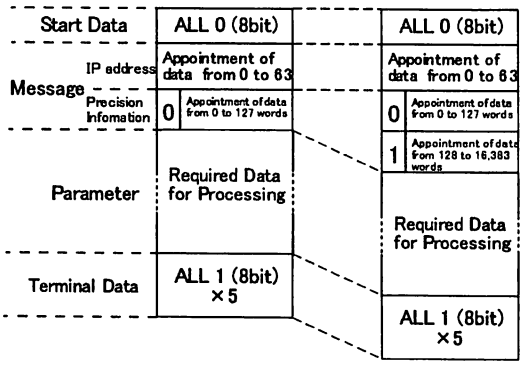


図 4　1 ワードを 8 ビットにしたときの通信フォーマット例
Fig. 4　Communication format sample by a word as 8 bit

開始/終了合図の信号を伝搬する．さらに拡張する場合は，同様に同一の基本モジュールをカスケードに接続することで可能となる．複数の基本モジュールをカスケード接続して構成した IP コアのブロック図を図 2 に示す．図 2 のようにすべて同一の基本モジュールを使用するので，最下位モジュールや最上位モジュールといった特別な設計を行っておらず，最下位モジュールで端末処理をするだけでよい．

2.2　メッセージ通信によるインタフェース

開発元の異なる多種多様な IP コアのインタフェースの標準化は大きな問題となっている．オブジェクト指向技術のメッセージとパラメータによる通信方式を用いることで，インタフェースの標準化そして使用容易性の問題を解決できる．通信フォーマットを図 3 に示す．特定の IP コアを指定する IP コア指定アドレスと処理データの精度 (ワード数) を示す精度情報をメッセージとし，処理データをパラメータとする．IP コア間ではこのメッセージとパラメータのみで通信を行い，それ以外の制御情報を必要としない．そのため，使用者は IP コア内部の詳しい構造を知る必要がなく，IP コアがどのような機能を持っているかさえ分かれば必要なデータを決められたフォーマットで与えるだけで IP コアを使用することができる．

自立形 IP コアの通信フォーマットはデータ通信開始/終了パターンを加えることで送受信データのフレームを判断する．1 ワードを n ビットとした場合，初めにデータ通信開始パターンとして 1 ワードのオール 0 を付加し，続けてメッセージとパラメータ，最後にデータ通信終了パターンとしてオール 1 を 5 ワード付加する．送信側は，パラメータ中にオール 1 が 4 ワード連続したデータがある場合は，必ず 1 ワード分のオール 0 を挿入し，受信側はそのオール 0 を取り除くことで通信終了パターンとの誤判定を防ぐ．

1 ワードを 8 ビットとしたメッセージとパラメータの例を図 4 に示す．IP コアの指定は 8 ビットの内 6 ビットを用いてアドレスとする．これで，モジュールを 64 個まで指定することができる．さらにアドレスが必要になった場合は，1 ワード追加し拡張する (精度情報の拡張と同様)．精度情報はパラメータのワード数となり，アドレスと同様に拡張が可能である．8 ビット中の最上位ビットが拡張ビットで，"0" の場合は，パラメータは 1 ワードのみとなり，そこで精度情報が終了となる．"1" の場合は，もう 1 ワード追加となる．ここで，実際の精度情報は 7 ビットなので 0～127 バイトまで指定ができる．1 ワード追加した場合は，128～16,383 バイトまでのデータに対応することが可能となる．

IP コアをカスケード接続した場合，図 2 で示した複数の同一基本モジュールから成る IP コア内では，右端の最下位モジュールのレジスタから上位モジュールのレジスタにとワード単位でデータを取り込む．

2.3　可変クロック周波数

流通する複数の IP コアを集積化すると，当然のことながらそれぞれのプロセスにおける遅延情報は付帯される．従って，SoC のプロセス遅延に換算して各 IP コアの実遅延を想定し，システムクロックを決め，集積化をすることになる．提案する設計法では，メッセージ内に含まれる精度情報からそれぞれの IP コアの処理精度に合ったクロック周波数を選定する．システムクロックを分周回路を通して，適応するクロック周波数へ変換する (図 5)．処理精度や遅延が大きい場合は分周段数の多い低周波数のクロックが選定される．このようにして，効率的な処理を行うためにクロック周波数を制御する．

2.4　スタンバイモード機能

基本モジュールをカスケード接続して拡張するにあたって，単に拡張をしていくだけでは処理データの容量によっては全く使用しないモジュールが存在することになる．そこで，使用していないモジュールの消費電力を抑制するためにスタンバイモードとし，動作を行わないようにする．これは，メッセージに含まれている精度情報から使用モジュールと未使用モジュールを判断する．I/O インタフェースが精度情報から判断を行うので，I/O インタフェースから情報を得て，スタンバイモード

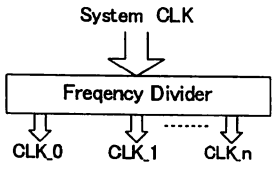


図 5　クロック周波数の分周
Fig. 5　Frequency divider clock

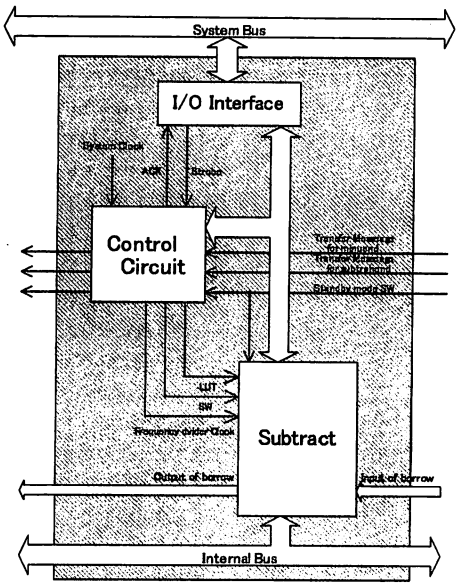


図 6　自立形基本減算モジュール構成
Fig. 6　A self-supporting Subtract module

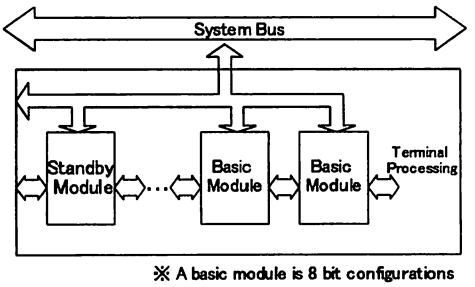


図 7　スタンバイモード
Fig. 7　Standby mode

のスイッチを制御する．

例えば，64 ビット構成の IP コアで 16 ビットの処理データの処理を行う場合，メッセージに含まれている精度情報を確認して使用モジュールが 16 ビット分ということを認識し，使用しない上位 48 ビット分のモジュールを図 7 のようにスタンバイモードにして消費電力を抑える．演算処理などで桁上げによるビット変動が生じた場合は，スタンバイモードは解除され，正常通りの動作を行う．これは下位モジュールのモジュール間インタフェースからの伝搬信号を受け取ることで動作を開始する．

3.　自立形減算モジュール

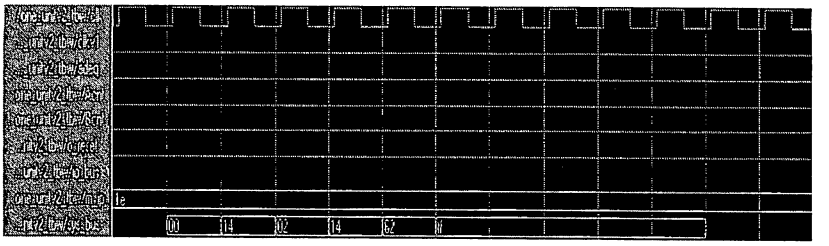
前述までに完全自立形に求められる要素について詳しく述べてきた．この章では，実際に 4 つの要素を満たし，機能モジュールを減算器に適用させて自立形減算コアの設計を行った．自立形基本減算モジュールの構成を図 6 に示す．

初めに，1 モジュールを 8 ビットとし，4 モジュールをカスケード接続して 32 ビット対応の自立形減算コアとする．メッセージ通信方式でメッセージとパラメータを減算コアに与えると，I/O インタフェースはメッセージ開始パターン (Start Data) である 1 ワードのオール 0 を検知して処理を開始する．メッセージ内のアドレスから自コア宛のデータであるかを判断する．自宛でない場合は図 8.a) のように残りのデータを無視をして処理を行わない．自宛である場合は，I/O インタフェースから制御回路に strobe(ラッチ信号) を送る．それを受け，制御回路は LUT 信号を減算器へ送り，データを 1 ワードずつ取り込む．1 ワードずつ取り込んでいるシミュレーションを図 8.b) に示す．すべてのデータが取り込まれると，減算器は演算を開始する．減算器には演算を行うときのみクロックを与え，消費電力を抑制している．演算中に桁借りが生じると borrow 信号が発生して処理が行われる．このとき，上位モジュールがスタンバイモードの場合，Standby mode SW により解除され，減算処理を行う．減算が終了すると，制御回路から減算結果のデータが出力される．それを I/O インタフェースが受け取り System Bus に送出して処理終了となる．自立形減算コアのシミュレーション波形を図 8.c) に示す．

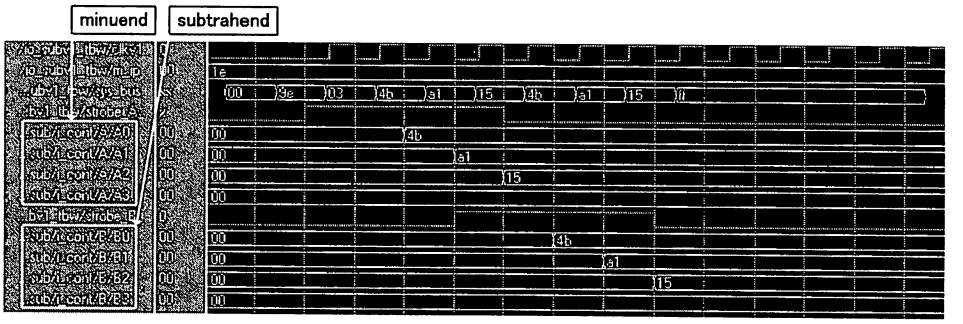
4.　楕円曲線暗号への適用例 [7], [11]〜[13]

提案する IP コアの設計法は対象とするコアの機能に限定されるものではない．ここでは適用例として，楕円曲線暗号アクセラレータの開発を行ったので報告する．楕円曲線暗号のような多精度の複雑な演算を行うコアでは，内部にローカルバスを用いて，複数の自立形 IP コアを接続した構成となる．

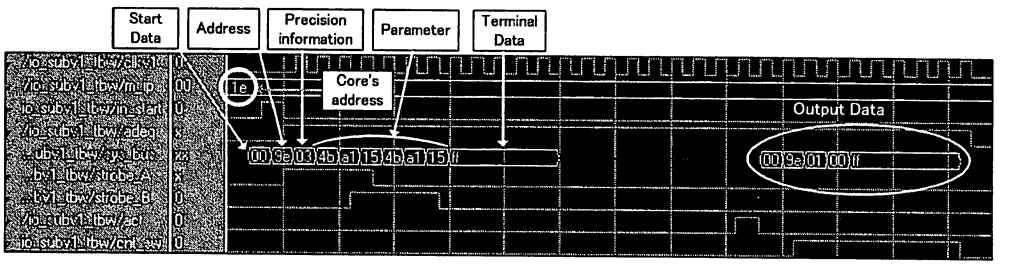
楕円曲線暗号の処理には多くの多項式演算が用いられ，剰余



a) コア指定アドレスが自宛でない場合



b) 入力部分



c) 入 出 力

図 8 自立形減算コアのシミュレーション波形

Fig. 8 Simulation of a self-supporting Subtract core

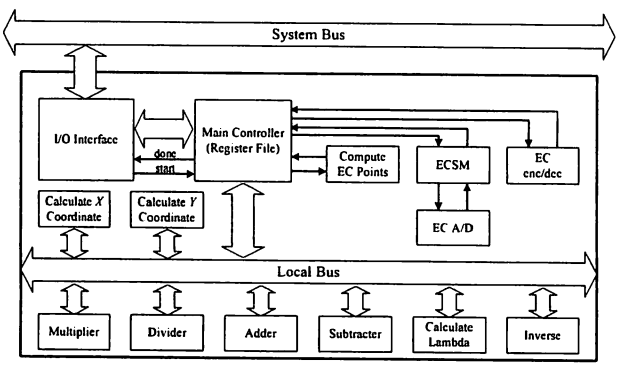


図 9 楕円曲線暗号アクセラレータの構成

Fig. 9 Structure of ECC Accelerator

表 1 楕円曲線暗号に必要となる演算コア

Table 1 Necessary Arithmatic Cores for ECC

Cores	Arithmatic Specification
Add	$x + y$
Subtract	$x - y$
Multiple	$x * y$
Divide	x/y
Residue	$Y mod P$
Quadratic Residue	$Y^2 mod P$
Square	Y^2
Rresidue of Multiple	$(x * y) mod P$
Calculate Lambda	$(3x^2 + a) mod P$
Calculate X Coordinate	$\lambda^2 - x_1 - x_2$
Calculate Y Coordinate	$\lambda\ (x_1 - x_3) - y_1$
Residue of Inverse	$x^{-1} mod P$

演算などの複雑な処理が行われるため，高速化が求められている．本方式の自立形 IP コアを用いることで，完全ハードウェア化にも関わらず，鍵長が任意に対応可能で高速なアーキテクチャを比較的容易に実現できる．

楕円曲線暗号アクセラレータは，まず基本となる四則演算機能を持った自立形 IP コアを用意して，それらを組み合わせて構成する．必要となる演算コアの一覧を表 1 に示す．これにより，ハードウェアの高速性を活かし，使用容易性や再利用性を実現し，演算精度に制限のないスケーラブルな IP コアを実現することができる．

5. ま と め

年々大規模化していく集積回路に向けて，多種多様な IP コア間のインタフェースの標準化，設計する際の時間やコストを考慮した再利用性，使用容易性および拡張性などといった SoC において課題となっている諸問題を解決し，外部からの制御を全く必要としない完全自立形 IP コアの設計法を提案した．完全自立形に求められる要件を提示し，それらを満たすことで提案する設計法の必要性および有効性を実際に楕円曲線暗号アクセラレータの IP コア化に適用して確認した．

そして，筆者らの提案する設計法は任意精度計算機，データフロー計算機および NoC(Network OnChip) に基幹となる設計法であり，更に開発を進めていく計画である．

文 献

[1] Bimaum, M.and Sachs, H.: How VSIA Answers the SOC Dilemma, IEEE Computer, Vol.32, No.6, pp.42-50(1999).

[2] Luca Benini, Giovanni De Micheli, "Networks on Chips:A New SoC Paradigm", IEEE, Computer, pp.70-78, Jan 2002.

[3] 中村次男，笠原 宏：オブジェクト指向手法をハードウェア設計に導入する提案と VSI 向きコアのモジュール化，電学論 (C)，Vol.121-C, No.3, pp.567-573(2001).

[4] 中村次男，鈴川敦之，冬爪成人，笠原 宏，田中照夫：超高集積 LSI 時代に向けたハードウェア設計法，電学論 (C)，Vol.124, No.4, pp.995-1003(2004).

[5] 佐藤正幸，中村次男，冬爪成人，笠原 宏，畠中浩行，田中照夫：自立形モジュールの実現法，電子情報通信学会第 4 回リコンフィギャラブルシステム研究会論文集，pp.79-86(2004).

[6] Sato, M., Nakamura, T., Hatakenaka, H., Hayakawa, M., Fuyutsume, N., and Kasahara, H. : Hardware Implementation of Elliptic Curve Cryptosystem Adaptive to Infinite Key Length, 電子情報通信学会ソサイエティ大会講演論文集，C-12-10, p.90(2005).

[7] 畠中浩行，中村次男，佐藤正幸，早川雅文，冬爪成人，笠原 宏，田中照夫：SoC 内 IP コアの設計-楕円曲線暗号システムモジュール化への適用例-，電気学会電子・情報・システム部門講演論文集，GS2-1, pp.741-745(2005).

[8] Tenca, A. and C.K.Koc: A Scalable Architecture for Modular Multiplication Based on Montgomery's Algorithm, IEEE Trans. on Computers, Vol.52, No.9, pp.1215-1221(2003).

[9] Satoh, A. and Takano, K.: A Scalable Dual-Field Elliptic Curve Cryptographic Processor, IEEE Trans. on Computers, Vol.52, No.11, pp.449-460(2003).

[10] Crowe, F., Daly, A. and Marnane, W.: A Scalable Dual Mode Arithmetic Unit for Public Key Cryptosystems Proc. IEEE Int. Conf. on Information Technology: Coding and Computing, pp568-573(2005).

[11] Douglas R. Stinson 著，櫻井幸一監訳：「暗号理論の基礎」共立出版社 (1996)

[12] 中村次男，笠原 宏：超高精度整数乗算器の高速化とモジュール化，電学論 (C)，Vol.121-C, No.7, pp.1212-1219(2001)

[13] 中村次男，笠原 宏：任意精度向き準並列形高速除算機構，電学論 (C)，Vol.120-C, No.1, pp.158-167(2000)