様式Ｆ－１９

科学研究費助成事業（学術研究助成基金助成金）研究成果報告書

平成　25　年　6　月　3　日現在

機関番号：25403
研究種目：若手研究(B)
研究期間：2011～2012
課題番号：23700063
研究課題名（和文）　様々な公開鍵暗号方式を高速に実行できるプロセッサの研究

研究課題名（英文）　Development of A Processor for Accelerating Various Public Key Cryptosystem

研究代表者
谷川　一哉（TANIGAWA KAZUYA）
広島市立大学・情報科学研究科・講師
研究者番号：80382373

研究成果の概要（和文）：本研究ではインターネット上でやり取りされるデータの暗号化に使われる RSA 暗号や次世代の暗号化方式として注目されている楕円曲線暗号など，様々な暗号方式を高速に実行できるプロセッサの開発を行った．その結果，従来のプロセッサと比較して 1/10 の面積で数倍～数十倍以上の高い性能を達成するプロセッサの開発が可能である事がわかった．

研究成果の概要（英文）：In this research, a processor for accelerating various public key cryptosystem such as RSA cryptosystem which is widely used in current Internet data exchanging and Elliptic Curve cryptosystem which is focused as standard cryptosystem in next generation, was developed. As research achievement, the developed processor had only 10 times smaller chip area and achieved a few to several tens times higher performance, compared with a general processor currently used.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
交付決定額	3,000,000　円	900,000 円	3,900,000 円

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：暗号処理，RSA 暗号，デジットシリアル，再構成型プロセッサ，モンゴメリ乗算

１．研究開始当初の背景

様々な機器やシステムがネットワークで接続されるようになり，それらのネットワーク中に流れるデータを保護するなど，システム間での認証を行う上で，暗号化技術の重要性はますます増加している．このような暗号化技術には秘密鍵暗号方式と公開鍵暗号方式の 2 つがある．公開鍵暗号方式は暗号化と復号化にそれぞれ異なる鍵を使用し，片方の鍵を公開鍵，つまり知られても良い鍵として使用できるため，ネットワークを流れるデータの暗号化や電子的にやりとりされる際の認証に適しているといえる．この公開鍵暗号方式は暗号化・復号化のための計算量が秘密鍵暗号方式と比べて多いため，高速に暗号化・復号化が必要な IC(Integrated Circuit) カードの認証のような場面では秘密鍵暗号方式が使われ，よりセキュリティを高めたい場面では公開鍵暗号方式が使われている．しかしながら，今後は電子的にやりとりされるデータはますます増え，それに応じて必要なセキュリティも高いものが要求されるようになると考えられ，公開鍵暗号方式の高速化のニーズが高まっていると言える．

このような公開鍵暗号方式の安全性は計算機で解読しようとしても実用的な時間内では解けない事を前提としているが，計算機の能力は年々向上しており，それに伴って暗号化方式も解読されないように新しい方式に対応していく必要がある．例えば，アメリカ合衆国では NIST（National Institute of Standards and Technology, 米国立標準技術

研究所）と呼ばれる政府機関が 2010 年をもって新たな暗号方式への移行を打ち出している．具体的には，現在，公開鍵暗号方式では RSA 暗号が主に使われているが，NIST の打ち出した内容では，より短い鍵の長さで RSA 暗号と同等の安全性が保てる楕円曲線暗号への移行が盛り込まれている．しかしながら，従来の暗号専用プロセッサにおいては RSA 暗号と楕円曲線暗号というように複数の暗号化処理の高速化に対応したプロセッサはないという問題がある．そのため暗号化方式の変更が発生する度に莫大な費用がかかるプロセッサ開発を行う必要がある．

このように公開鍵暗号方式では処理の高速化が求められていると同時に，安全性を確保するために新しい暗号化方式への対応も求められているのが現状であった．

２．研究の目的

本研究では複数の暗号化処理に対応したプロセッサの開発を目的として，本研究ではそのプロセッサが以下の要件を満たす事を明らかにする．

(1) プロセッサ構成の優位性
本研究では暗号処理特有の特徴を元に効率的に暗号処理を行うための手法を提案し，実際にプロセッサを設計・実装をすることで，従来のプロセッサより，面積や消費電力の面で優位性があることを示す．

(2) RSA 暗号方式に置ける優位性
(1)で開発したプロセッサが現在よく使われている RSA 暗号の処理に置いて，従来のプロセッサよりも性能において優位性がある事を示す．

(3) 楕円曲線暗号に置ける優位性
(1)で開発したプロセッサが今後主流になると考えられる楕円曲線暗号においても，従来のプロセッサよりも性能において優位性があることを示す．

３．研究の方法

本研究では上記の研究目的を達成するために(1)RSA 暗号や楕円曲線暗号に必要な多倍長整数演算の問題点の洗い出し，(2)その問題点を解決するために提案プロセッサで採用した手法の決定，(3)提案するプロセッサの詳細設計，という手順で研究を行う．以下に各項目の詳細について説明する．

(1) 多倍長整数演算の問題点

通常のプロセッサで使用されている演算は 32 ビット，あるいは，64 ビットであるが，本研究で取り扱う RSA 暗号では 2048 ビット以上の乗算が必要であり，楕円曲線暗号においても 160 ビットの演算が必要である．このようにビット幅の大きい整数演算を多倍長整数演算と呼ぶ．多倍長整数演算では①ビット幅が長いためキャリーによる伝搬遅延が膨大になるという問題，②1 回の演算で使用するデータ量も多くなり，外部からのデータ転送時間がボトルネックになる，という問題がある．以下ではこれらの多倍長整数演算の問題について詳細に述べる．

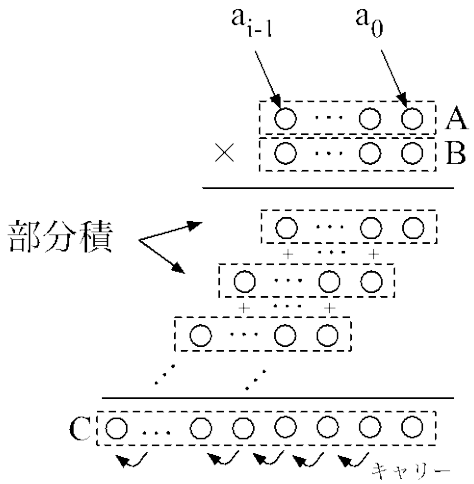

図 1　多倍長乗算のキャリー伝搬

①キャリーによる伝搬遅延の問題

多倍長整数演算では下位桁での計算結果により生じるキャリーを上位桁の計算で使うため，そのキャリーを下位桁から上位桁に順番に伝搬しなければならず，多倍長整数演算ではその伝搬遅延が長くなりがちである．

図 1 に多倍長乗算のキャリー伝搬の様子を示す．図 1 に示すように乗算結果の各ビットの値を求めるには部分積の結果の和を取る必要がある．この部分積の和をとる演算において下位桁から上位桁へのキャリーの伝搬が発生する．具体的には 2048 ビットの RSA 暗号では 2048 ビットの乗算が使われるため，このキャリー伝搬が 2048 ビット分も必要になる．この問題を軽減するために，1 ビットずつの計算ではなく数ビットまとめたデジット単位で計算する手法もあるが，基本的に下位桁から上位桁へのキャリーの伝搬は残っており，この遅延の問題は解決されない．

②データ転送量の問題

RSA 暗号の様に 2048 ビット同士の多倍長整数演算を行うには，1 回の演算で 4096 ビットのデータが必要となる．そして，剰余計算を除算で行う場合には，1 回 4096 ビットのデータを外部から投入することで，剰余計算が 1 回終了する．しかし，剰余計算をモンゴメリ乗算で実行する場合は，乗算 3 回，加算が 1 回となり，合計で 16384 ビットのデータを外部から投入する必要がある．RSA 暗号はべき乗計算を 1 回行う毎に剰余計算を行

うため，1 回毎に 4096 ビットのデータが必要となる．そのため，剰余計算 1 回毎にデータを外部から演算を行うプロセッサに供給するには，大きな負荷となる．

また，公開鍵が 160 ビットの場合の楕円曲線暗号においても，1 度の演算では 320 ビットのデータ転送量でよいが，高速化のために 2 並列，3 並列と同時に複数の演算を行えば行うほどデータ転送量が増えるといった問題がある．そのため，多倍長整数演算の高速化にはデータ転送量の改善が必要となる．

(2) 提案プロセッサでの手法

今回開発を行うプロセッサのアーキテクチャについて述べる．まず，これまでに述べた多倍長整数演算の問題点の改善策と開発するプロセッサに要求される事項について述べる．次に，要求を満たすための基本アーキテクチャについて述べる．

①設計方針

まず，本研究が解決すべき問題点を以下に示す．

- 多倍長整数演算による通信量の増加(問題点 1)
- 多倍長整数演算で生じるキャリーの伝搬遅延（問題点 2)

問題点 1 解決するために，他の研究では除算や剰余テーブルを使用することで演算回数を減らしている．しかし，前者の手法では演算時間，ハードウェア面積共に有利とはいえず，後者はハードウェア面積が膨大過ぎて現実的とはいえない．そこで，本研究で開発を行うプロセッサは A) データ通信回数を低減する点を要求事項とする．

問題点 2 を解決するために，他の研究では，冗長 2 進表現を用いて演算を行っていた．しかし，冗長 2 進表現はハードウェア面積が大きくなる欠点がある．そこで，本研究では，通常の 2 進表現を用いることとする．しかし，通常の 2 進表現だとキャリーの伝搬による遅延が生じてしまう．そこで，プロセッサの要求事項として，B) 搭載する演算器(FU)にキャリー伝搬の遅延を少なくなる構成を設計する．

また，序論で述べたように，様々な公開鍵暗号に対応する必要がある．そのため，C) 回路構成をアプリケーションにあわせた構成に切替えることが可能な再構成型アーキテクチャにする必要がある．以下に要求事項をまとめる．

- データ通信回数を低減する（要求事項 A)
- 搭載する演算器(FU) にキャリー伝搬の遅延を少なくなる構成を設計する(要求事項 B)
- 再構成可能なアーキテクチャにする(要求事項 C)

これら 3 つの要求事項を満たすプロセッサを開発することにした．以下は 3 つの要求事項を満たすための構成について述べる．

②ビットシリアル演算方式の採用

本節では上記で述べた要求事項 A を満たす方針の 1 つとして FU の基本演算方式にビットシリアル演算方式を採用した．ビットシリアル演算方式とは，1 ワードのデータを 1 ビット毎の演算に分割して，複数サイクルに分けて計算する手法である．そのため，ビットシリアル演算方式はビットパラレル演算方式と比較して，約 4 倍の個数の FU を搭載できる．その結果，複数の多倍長整数演算を一度に再構成型プロセッサ上に実装できる．そのため，再構成回数が少なくなり，再構成情報間でのデータの受渡しが少なくなり，要求事項 A のデータ通信回数を低減することが可能となる．

③キャリー伝搬遅延を削減した手法の採用

キャリー伝搬を削減するための手法として演算器から出力されるキャリーを単純に伝搬するのではなく，演算器内部に保持し，そのキャリーを次サイクルに使うように多倍長整数演算の計算方法を見直すことで，キャリーの伝搬遅延の問題を解決した．

そのキャリーの伝搬遅延を解決した手法の概略を図 2 に示す．これまでの乗算の手法（図 1 の手法）は部分積を求めながら計算し

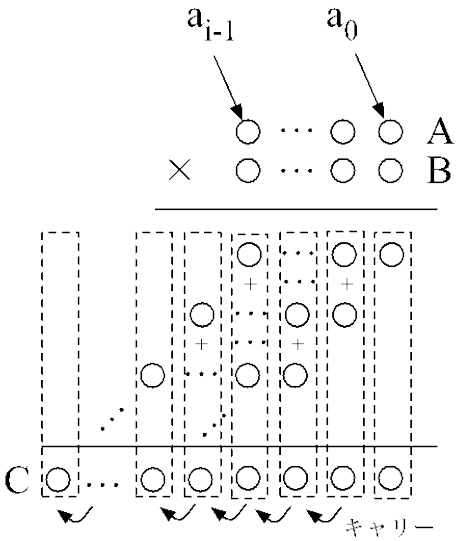

図 2　キャリー伝搬遅延を削減する手法

ていたため，各部分積を求める度にキャリーの伝搬をビット幅分必要であり，この遅延が問題であった．それに対して本研究で使用した手法は計算結果の桁毎に計算する手法に

することで，キャリーの伝搬が 1 回の計算内には存在せず，異なる計算の間でのみ発生するようになった．その結果，1 度に発生するキャリーの伝搬はたかだか 1 つ分だけでよくキャリー伝搬遅延が膨大になるという問題を解決できている．よって，本手法を採用する事で要求事項 B を満たすことができる．

④DS-HIE アーキテクチャの採用
本節ではビットシリアル演算を採用しつつ，再構成可能なアーキテクチャとして DS-HIE アーキテクチャを採用した．DS-HIE アーキテクチャの特徴を以下に示す．

- FU にビットシリアル演算方式を採用（特徴 1）
- 小面積で高い配線制を持った配線構造の採用（特徴 2）
- スループット重視での性能向上（特徴 3）

DS-HIE アーキテクチャは特徴 1 により本研究の目的に適しているといえる．次に多くの演算器が必要な再構成型アーキテクチャにおいて演算器間の配線を実現する配線資源が持つ面積は膨大なものになりがちである．しかしながら DS-HIE アーキテクチャではビットシリアル演算の採用と配線資源に多段非閉塞網である Benes 網を使用する事で面積の増加を抑えている．またビットシリアル演算ではレイテンシの増加が問題となるが，それを隠蔽するためにスループット性能で高い性能が出るように設計されており，暗号処理の用に膨大なデータを扱う処理に向いていると言える．このように DS-HIE アーキテクチャを採用する事で要求事項 A と要求事項 C の要求を満たす事ができる．

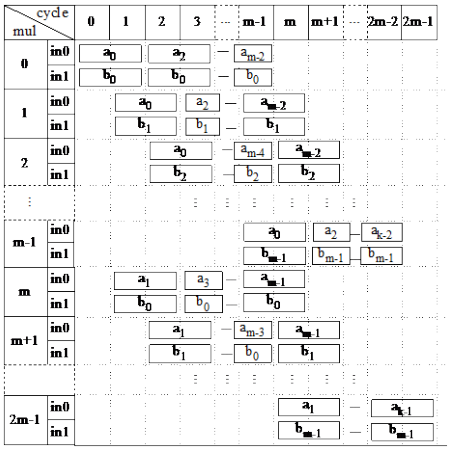

図 3　データ転送の規則性

⑤データ転送量を削減するための手法
本研究で取り扱っている多倍長整数乗算を③で採用した手法を用いて実現する場合，データの転送に規則性がある事がわかった．その規則性を図 3 に示す．図 3 に示すようにデータB（b_0, b_1, …）にしてはサイクルが異なっていても常に同じ乗算器に入力されている．そのため各乗算器には一度データを入力したら，そのデータを保存する機構を用意する事で 2 回目以降のデータ転送をする必要がなくなる．またデータA（a_0, a_1, …）に関してはあるサイクルでデータが入力された後は次のサイクルでは隣接する乗算器で同じ入力が使用されている．そのためある乗算器に入力されたデータを隣接する乗算器に転送する機能があればデータの転送量を減らす事ができると考えられる．このような手法を実現できるデータ供給機構を提案プロセッサに搭載する事で要求事項Aを満たす事ができる．

(3) 提案プロセッサの詳細設計
上記の(2)で述べた手法を採用し，実際に開発したプロセッサのブロック図を図 4 に示す．この全体のブロック図は上記(2)④で採用した DS-HIE アーキテクチャをベースにしている．図 4 において制御部は外部プロセッサからの命令やデータを受信し，各機構の制御を行う機構である．次に，Input Buffer は外部プロセッサから制御部を通してデータを受信し，各 FU にデータを投入する機構である．この Input Buffer に上記(2)⑤で採用した手法を実現している．この提案プロセッサでは FU で乗算や加減算などの演算を実現し，演算器間のデータ転送は Benes 網を使って接続する事で，上記(2)③で説明した乗算手法を実現することができる．また各 FU は上記(2)②で説明したビットシリアル演算を採用している．

また本プロセッサでは FU 数を 512 個とし

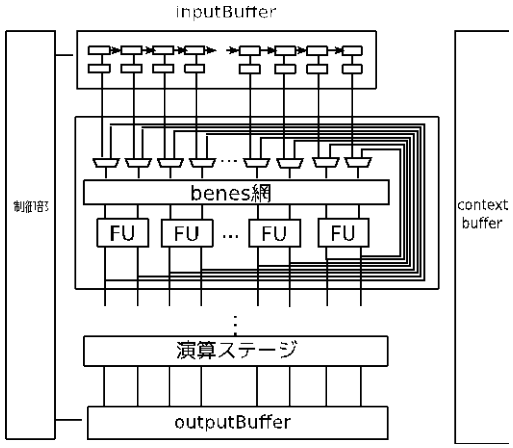

図 4　提案プロセッサのブロック図

た．これは 2048 ビットの RSA 暗号で必要となるモンゴメリ乗算を効率的に行うのに必

表 1 従来手法とキャリー伝搬遅延削減手法の比較

	使用FU数	実行サイクル数
従来手法	559	1600
キャリー伝搬遅延削減手法	41	400

要なFU数を確保するためである．

４．研究成果

本研究の成果として，(1)本研究で採用したキャリー伝搬遅延を防ぐ手法の有効性，(2)本研究で開発したプロセッサの小面積性，(3)本研究で開発したプロセッサの暗号処理に置ける高性能性，の3つを示す．

(1) キャリー伝搬遅延を防ぐ手法の有効性

本研究で採用したキャリー伝搬遅延を防ぐ手法の有効性を示すために，従来の多倍長整数乗算において従来手法を採用した場合と理論的に比較する．具体的には，楕円曲線暗号で必要となる 160 ビットの乗算において，使用する FU 数と予測される実行サイクル数で比較する．ここで FU 数が少なければ少ない程，プロセッサの面積が小さくなると考えられ，実行サイクル数が少なければ少ない程，高性能だと考えられる．このような内容で性能比較を行った結果を表1に示す．

表1の結果より，本研究で使用しているキャリー伝搬遅延削減手法は従来手法より1/14個のFU数で実現でき，性能は4倍高性能であるという事が分かった．以上より，本研究で採用したキャリー伝搬遅延削減手法の有効性が示されたと言える．

(2) 本研究で開発したプロセッサの小面積性

本研究で開発したプロセッサは0.18μmCMOSプロセスでチップ試作し実際に必要な面積を求めた．提案プロセッサのレイアウト図を図5に示す．その結果，提案プロセッサのチップ面積は 7.3mm×7.3mm であることが分かった．この面積を現在デスクトップパソコン

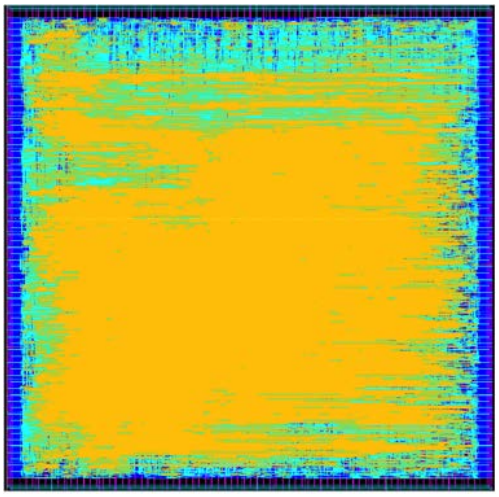

図 5 提案プロセッサのレイアウト図

で広く使用されている Intel Core i7 プロセッサと比較する．

Core i7 プロセッサは 32nmプロセスで20.8mm×20.8mmの大きさを持つ．これはCPU Core を 8 コアとその他周辺回路の面積も含んだ値であるが，CPU Core単体の面積は公開されているチップレイアウト図などから推測すると5.6mm×3.2mmだと考えられる．これに対して本研究で開発したプロセッサを32nmプロセスで試作した場合を想定すると，一辺の長さは7.3mm×32/180=1.3mmとなり，1つのCPU Coreよりも小さい面積になると考えられる．その結果，32nmプロセスで提案プロセッサとCore i7 プロセッサのCPU Coreの面積を比較した場合，1.3×1.3=1.69mm^2:5.6×3.2=17.92mm^{2}となり，面積は1/10.6になると予測される．実際に試作した場合はこのような理論通りにシュリンクしないことも多いが，それでも圧倒的に面積を小さくできると考えられる．

(3) 本研究で開発したプロセッサの暗号処理における高性能性

本研究で開発したプロセッサの暗号処理に置ける性能を評価した．評価に用いたアプリケーションはRSA暗号で使用されるモンゴメリ乗算と，楕円曲線暗号で使用される楕円曲線上の加法と2倍算である．これらの評価アプリケーションを Intel Xeon プロセッサ2.66 GHzで実行した場合の処理時間と比較した．その比較結果を表2に示す．

表 2　暗号処理に置ける性能評価結果

	提案プロセッサ@200MHz	Xeon@2.66GHz
2048bit モンゴメリ乗算	70.8 μs	1470.32μs
4096bit モンゴメリ乗算	372.74μs	11851.98μs
160bit 楕円曲線・加法	37.23 μs	39.09μs
320bit 楕円曲線・加法	73.53μs	203.95μs
160 bit 楕円曲線・2 倍算	34.51μs	37.19μs
320 bit 楕円曲線・2 倍算	68.18μs	187.21μs

表 2 の結果より，提案プロセッサの実行時間は Xeon プロセッサと比べ，モンゴメリ乗算では 21～32 倍の性能，楕円曲線上の演算では 1～2.7 倍の性能を達成した．提案プロセッサの動作周波数は 200MHz であり，Xeon プロセッサの動作周波数は 2.66GHz であるが，この差は提案プロセッサが構造上高い動作周波数を達成できないという理由ではなく，単純に使用可能な試作環境によるものである．原理的には提案プロセッサで使用している演算のビット幅は 1 ビットと Xeon プロセッサで使用している演算ビット幅 32 ビットより小さく，より高い動作周波数での動作が期待できる．そのことより提案プロセッサの動作周波数は少なくとも Xeon プロセッサと同等程度には引き上げる事が原理的に可能だと考えられ，その場合，提案プロセッサは Xeon プロセッサと比較し，モンゴメリ乗算においては 54.6～83.2 倍，楕円曲線上の演算において 2.6～7.02 倍の性能となる．この結果より，DS-REMIE は公開鍵暗号をより短時間で実行できるアーキテクチャであることが示されたといえる．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔学会発表〕（計１件）

(1) 福寿綾乃，谷川一哉，弘中哲夫，「粗粒度再構成型プロセッサDS-HIEのFPGA実装　～CPUとの通信制御部の設計開発～」，平成 24 年度(第 63 回)電気･情報関連学会中国支部連合大会，2012 年 10 月 20 日～2012 年 10 月 20 日（島根大学）．

[その他]

(1) 玉置貴俊，谷川一哉，弘中哲夫，「公開鍵暗号向け再構成型プロセッサ DS-REMIE の実装」，2012 年度版東京大学大規模集積システム設計教育研究センター年報，p.161，2012 年.

６．研究組織
(1)研究代表者
谷川　一哉（TANIGAWA KAZUYA）
広島市立大学・情報科学研究科・講師
研究者番号：80382373