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

2004－ARC－160 (13)
2004／12／2

セキュアプロセッサの開発

穂積 健介† 猪股俊光†† 曽我 正和††

ディジタル署名機能をもつ非接触ICカード用のマイクロプロセッサSEP-5を設計した．SEP-5は，高速暗号計算機能，秘密鍵漏洩防止機能，汎用計算機能，低電力消費を要件として設計されたもので，コプロセッサを用いずに，単独のプロセッサで実現することが特徴である．このプロセッサをFPGAに実装し，これまでに開発をすすめてきたプロセッサSEP-4との比較を行った．

Development of A Secure Processor

KENSUKE HOZUMI,† TOSHIMITSU INOMATA†† and MASAKAZU SOGA††

We have designed a microprocessor "SEP-5", which has the function of digital signature calculation for noncontact IC-cards. It is required that a high-speed code calculation function, a private key disclosure prevention function, a general-purpose calculation function, and low power consumption. The feature of SEP-5 is realized by the independent processor not using a co-processor. We have mounted this processor on FPGA, and compared with SEP-4 which is a predecessor of SEP-5.

1 はじめに

個人認証を行うための電子的媒体としては，ディジタル署名機能をもつ非接触ICカードが最適であると考えられる．生体情報を利用する個人認証方法は，限られた範囲内ならよいが，一般的な認証に使うには，相手方へ生体情報を預けねばならないため，社会的受容性を考慮する必要がある[1]．ディジタル署名機能をもつ非接触ICカード上のマイクロプロセッサの要件としては，実用的時間内にディジタル署名を完了しうる高速暗号計算機能と，外部へ個人秘密鍵を絶対に漏洩させない機密保管機能が必要となる．さらに非接触であるための低電力消費と，ディジタル署名機能以外の若干の応用機能を持つことができる汎用性とが要求される．現在これらの要件に近いものとして，"汎用プロセッサ＋暗号計算専用コプロセッサ"の形式のものがあるが，消費電力の点で非接触ICカードとしての実現が難しい[2]．

以上のような観点から，筆者らは，次のような要件を満たすセキュアプロセッサの開発を行っている．

(a) 高速暗号計算機能
(b) 秘密鍵漏洩防止機能
(c) 汎用プロセッサとしての計算機能
(d) 低電力消費

これまでに，コプロセッサをもうけず，汎用プロセッサに部分的な工夫を加えることで上記の要件を満たすセキュアプロセッサとしてSEP-4[3]の開発を試みた．SEP-4はゲート規模約33万ゲートの64ビットセキュアプロセッサであり，要件のうちで(d)低電力消費に課題が残っていた．

そこで，本研究では，低電力消費を実現すべく，ゲート規模の縮小を目指し，SEP-4に改良を加えた．その結果としてSEP-5という32ビットセキュアプロセッサを開発した．

本研究で開発したセキュアプロセッサは，駅の改札など，瞬間的な処理が要求されるようなICカードへの搭載は想定していない．本プロセッサの汎用性を生かし，本プロセッサが搭載されたICカードの利用環

† 岩手県立大学大学院ソフトウェア情報学研究科
Iwate Prefrctural University Graduate School of Software and Information Science
†† 岩手県立大学ソフトウェア情報学部
Iwate Prefrctural University Faculty of Software and Information Science

境として主に次のようなものを考えている．

- コンピュータネットワーク上でのログイン認証
- 電子的身分証，各種証明証
- 電子的診察券など

2 署名計算アルゴリズム

一般にディジタル署名は，あるメッセージのダイジェスト値を計算し，それを秘密鍵で暗号化することによって作成される．本研究が対象とするディジタル署名の作成では，ダイジェスト値の計算にSHA–1，暗号化にRSA公開鍵暗号をそれぞれ用いることとした．SHA–1は，2^{64}ビット未満のメッセージに対してダイジェスト値と呼ばれる160ビット長のデータを出力するハッシュアルゴリズム[4]である．ダイジェスト値をD(160ビット)，秘密鍵をK(1024ビット)，公開パラメータをN(1024ビット)としたとき，ディジタル署名Sigは次のように計算される．

$$Sig = D^K \bmod N \tag{1}$$

ダイジェスト値は，自プロセッサの汎用機能を用いて計算するか，あるいは外部から受け取ることとする．

式(1)のべき乗剰余演算を効率よく行うためのアルゴリズムとしてバイナリ法とモンゴメリ乗算を用いるものがある[3]．本プロセッサでは，このアルゴリズムのために有用な機能をセキュアアーキテクチャとして実装した．ここではバイナリ法とモンゴメリ乗算の概要を述べ，アルゴリズムの詳細は文献[3]を参照されたい．

2.1 バイナリ法

バイナリ法[5]は，D^Kのべき乗計算において，指数Kを2進展開し，自乗演算とDを乗ずる演算を繰り返す手法である．アルゴリズムを図1に示す．アルゴリズム中lはKのビット長を表し，K_iはKの第iビット目を表す．Kの最上位ビットから最下位ビットまで順次1ビットずつ調べ，'0'であれば$A = A^2$，'1'であれば$A = A^2D$として繰り返し計算する．各乗算ごとに剰余演算することにより，中間結果の圧縮をしている．

2.2 モンゴメリ乗算

モンゴメリ乗算[6]は除算を必要とせず，加算と乗算と高々1回の減算で剰余算を実現する手法である．

Algorithm: *Binary Method*
Input: $D, N, K = (K_{l-1}K_{l-2}\cdots K_1K_0)_2 = \sum_{i=0}^{l-1} K_i 2^i$
Output: $A = D^K \bmod N$

1). **if** $K_{l-1} = 1$ **then** $A := D$ **else** $A := 1$
2). **for** $i := l-2$ **downto** 0
  2-1). $A := A \cdot A \bmod N$
  2-2). **if** $K_i = 1$ **then** $A = A \cdot D \bmod N$
3). **return** A

図1 バイナリ法アルゴリズム

図1のループ内における剰余算に適用する．

3 セキュアアーキテクチャ

本プロセッサにおけるセキュリティ機能の目的は，秘密鍵の漏洩防止である．漏洩とは，SEP–5内のソフトウェアあるいはSEP–5と接続するコンピュータのソフトウェアを任意に使用して，秘密鍵データがICカード外部へ読み出されること，あるいは間接的に推定されることをいう．さらに，鍵データは漏洩せずとも，幾つかのディジタル署名データをもとに別の任意のディジタル署名が合成偽造されることも漏洩の一種とみる．ここで漏洩防止を議論するための前提として，鍵漏洩をたくらむ攻撃者が，ICカードのメモリへ侵入して正規の署名実施のためのプログラムを書き換える攻撃を想定する．なお，プロセッサを物理的手段により観測する攻撃，すなわちサイドチャネル攻撃は別途対策を講じることとして，ここでは議論の対象とはしない．以上の前提のもとで，本プロセッサは，秘密鍵の漏洩を防止するために，次の2つの構成を有する．

- 秘密鍵参照回路
- セキュアモード

3.1 秘密鍵参照回路

秘密鍵は，あらかじめROMなどの不揮発性メモリに格納されていることとし，ここではそれを秘密鍵メモリと呼ぶ．図1のとおり，バイナリ法におけるディジタル署名計算では，秘密鍵の値は最上位ビットから1ビットずつ参照され，その値に対応した乗算が行われる．これが秘密鍵の唯一の使用方法である．したがって，図2のような，秘密鍵メモリから秘密鍵を1

ビットずつ選択して参照し，D^{Ki} に反映させる回路構造を設けた．これを秘密鍵参照回路と呼ぶ．

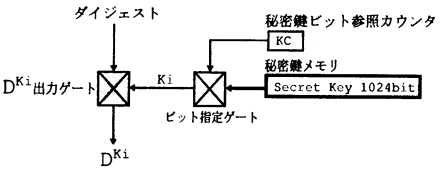

図 2　秘密鍵参照回路

図 2 の秘密鍵参照回路において，秘密鍵ビット参照カウンタ（KC：Key-bit reference Counter）は 1023 から 0 まで，順次デクリメントされる．この秘密鍵ビット参照カウンタに応じて，ビット指定ゲートから，秘密鍵メモリに格納されている秘密鍵が順次 1 ビットずつ参照される．ビット指定ゲートからの出力 Ki は，D^{Ki} 出力ゲートにのみ使用される．図 2 で表すように，秘密鍵を格納する秘密鍵メモリから，他のレジスタやメモリへデータを転送する伝送経路を設けていない．このようなハードウェア構造によって，秘密鍵の秘密鍵メモリ外部への漏洩を防いでいる．

3.2　セキュアモード

図 2 のハードウェア構造により，秘密鍵を一度に取り出すことは不可能であるが，署名計算で間接的に使用される秘密鍵のビットごとの値が計測され，集められたビット列から秘密鍵を推測される可能性が残る．観測されるのが署名計算の最終結果（全 1024 ビット）ならば，それはディジタル署名であるから秘密鍵の推測が難しいことは知られている．そこで 1 ビットごとにモンゴメリ乗算結果から秘密鍵の値（0 または 1）を推測されないようにするための仕組みを用意した．

プログラム走行モード

署名計算で使用される命令を署名計算以外の目的（たとえば，秘密鍵の漏洩）に悪用されないようにするため，本プロセッサでは，プログラム走行モードをノーマルモードとセキュアモードとに分け，署名計算とその他の計算とを区別した．

どちらのモードで実行中であるのかは，セキュアフラグ（SF：Secure Flag）で表される．SF=1 の場合をセキュアモードと呼び，署名計算実行中であることを表す．SF=0 の場合をノーマルモードと呼び，各種応用プログラム，ダイジェスト計算などが行われる．

モードの切替えは，SIG(Signature) 命令と SIE 命令の 2 つの専用命令を用いて行われる．SIG 命令は，署名プログラムの先頭番地へのジャンプ，SF=1 の設定，KC=1023 の設定をする．SIE 命令は，戻り番地に復帰するとともに SF=0 を設定する．

命令セット

命令セットには，一般命令と，署名計算でのみ使用する署名計算専用命令の 2 種類がある．一般命令はノーマルモードでのみ動作し，署名計算専用命令はセキュアモードでのみ動作する．セキュアモード時の一般命令，ノーマルモード時のセキュア命令は，それぞれ SIE(Signature End) 命令，NOP(Non Operation) 命令に置き換わる．

中間結果の格納

セキュリティモード中の署名計算で使用する命令のうち，中間結果を出力する命令は，中間結果をすべて主メモリの固定番地に上書きする．ノーマルモードになったあとでは，一般命令の MOV 命令などによって固定番地の内容を他番地へ転送することができる．

また，SIE 命令は KC=0（バイナリ法において署名計算の終了）でない場合には中間結果格納領域の内容をすべて 0 クリアする．

この結果，ビットごとの中間結果は固定の番地へのみ上書きされ，ビットごとの中間結果を外部へ取り出すことはできず，秘密鍵の全ビットを走査して得られた結果のみが参照される．

署名拒否機構

本プロセッサにおいて，ダイジェスト値は，自プロセッサの汎用機能を用いて計算するか，外部から受け取ったのち，メモリの固定番地へ格納される．ダイジェスト値が任意に選択できる場合，ある一定の条件を満たすメッセージの署名を偽造することができる [8]．署名計算結果から，任意のダイジェスト値の署名を合成されないようにするため，ダイジェスト値 160 ビットの内容が単純な値である場合にはディジタル署名を拒否する機能をハードウェアとして持たせた．すなわち，ダイジェスト値 160 ビットを 16 ビット × 10 個に区分けし，1 個の区分ごとに少なくとも 1 ビット以上の 1 が存在することを署名実施の必要条件とし，1 個でも 16 ビット全零の区分があれば，ダイジェスト値は無効としてセキュアモードに移行しない．

これまで述べてきた 3.1 の秘密鍵参照回路と 3.2 のセキュアモードにより，想定した攻撃（署名プログラムの書き換えによる秘密鍵の漏洩）を防ぐことができる．

4 セキュアプロセッサ SEP-5 の設計

4.1 メモリ構成

前節で述べたセキュア・アーキテクチャを含むセキュアプロセッサ SEP-5 を実装した．語長は 32 ビット，メモリアドレス指定範囲は 0x0000 番地から 0xFFFF 番地である．主メモリとのアドレス単位は語単位，主メモリの容量は，32 ビット×64K 語 (2M バイト) とした．ただし，特定の命令にてバイト単位でのデータ転送が可能である．また，多倍長演算を 1 個の命令で行うことができる．

汎用レジスタは R0～R31 までの 32 本を有する．秘密鍵メモリは ROM として実装し，中間結果の格納番地は 0x0000～0x003F 番地までとした．

4.2 命令フォーマット

命令フォーマットには図 3 の 2 オペランド形式と，図 4 の 3 オペランド形式の計 2 種類がある．

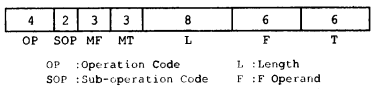

図 3 命令フォーマット（乗算を除く）

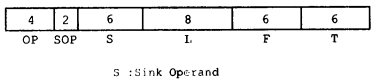

図 4 乗算命令フォーマット

図 3 のフォーマットは乗算以外の命令フォーマットである．OP(4 ビット) と SOP(2 ビット) には命令コードを，MF(3 ビット)・MT(3 ビット) のフィールドにはオペランド指定モードをそれぞれ指定する．本プロセッサでは，オペランドの対象をすべてレジスタとし，オペランド指定モードは表 1 に示す 5 つのモードとした．

D・I・MI・IP の各モードは直交しているが，LI モードは LI:LI の組合せのみである．

L(8 ビット) は多倍長演算が可能な命令において LI モードが指定されたときのみ有効となるフィールドで，多倍長データのワード数を指定する．F(6 ビット)・T(6 ビット) の両フィールドにはそれぞれ演算対象となるレジスタ番号を指定する．

図 4 のフォーマットは，乗算用の命令フォーマットである．オペランド指定モードは表 1 の I モードまたは LI モードと等価になる．F・T フィールドに演算対象データ，S フィールドに演算結果の格納先を指定する．

表 1 オペランド指定モード

	モード名称	動作
D	レジスタ直接	EA=Rn
I	レジスタ間接	EA=[Rn]
MI	-1&レジスタ間接	Dec(Rn), EA=[Rn]
IP	レジスタ間接&+1	EA=[Rn], Inc(Rn)
LI	多倍長レジスタ間接	先頭アドレス=[Rn]

n=0～31,sp,pc,
EA=実効アドレス，[ ]：内容を示す，
Inc(Rn)：Rn ← Rn+1，Dec(Rn)：Rn ← Rn−1

4.3 プロセッサ構成

本研究で設計したプロセッサ SEP-5 のブロック図を図 5 に示す．

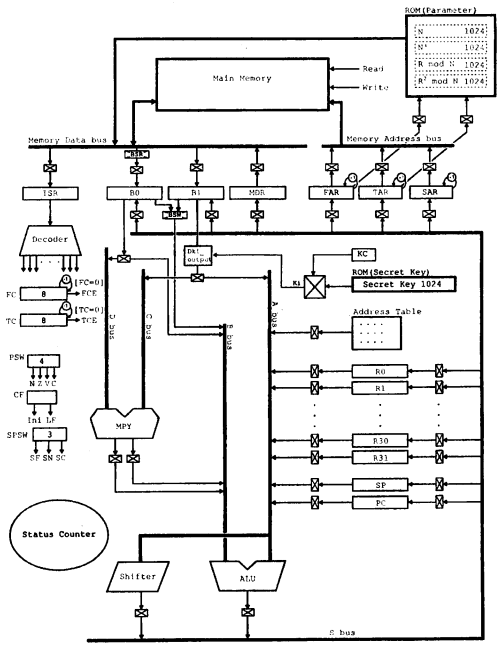

図 5 プロセッサ構成図

ALU, Shifter, MPY ：ALU は加算・減算・論理演算を行い，Shifter は算術・論理・ローテートの各シフト演算を行い，MPY(Multiply Unit) は 32 ビット×32 ビットの乗算を行う．

BSR・BSW(Byte Selecter Read・Write)：主メモリからバイト単位で読み書きをするゲートである．

SPSW(Secure PSW) ：セキュアモードで使用されるフラグ群である．SF はセキュアフラグ，SN，SC はそれぞれ N，C フラグに相当する．

Address Table： 署名計算専用命令が使用するアドレスを格納する．本プロセッサではオペランドの対象をレジスタのみに限定しているため，D モードを除き，一度オペランドアドレスをレジスタに格納する必要がある．署名計算専用命令が使用するアドレスが常に一定であることから，命令により適切なアドレスを A バスに出力し，FAR・TAR にセットする構成とした．

4.4 多倍長演算機能

FAR・TAR・SAR(F・T・S operand Address Register) の各レジスタは，それぞれ自己インクリメント機能を持っている．多倍長演算を行う場合，図 3 と図 4 の L フィールドで指定されたワード数分，順次自己インクリメントを行う．FAR・TAR・SAR の各レジスタ値をアドレスとして，オペランドが主メモリから次々に読み書きされるようにしたことで，多倍長語の演算を 1 個の命令で実現した．

FC・TC(F・T operand Counter) は多倍長演算時のワード数を保持するデクリメントカウンタである．1 語分の演算が終了するたびにデクリメントされ，それぞれカウンタ値が 0 になると FCE・TCE 信号を出力し，状態遷移の多倍長ループが終了する．

CF(Control Flag) は状態遷移を制御するフラグ群で，Ini は乗算時，LF は乗算以外の多倍長演算時に使用される．

4.5 MPY 構成

MPY は図 6 に示すように，1 つの 32 ビット乗算器と 2 つの加算器から構成される．演算時間短縮のために，文献 [3] の多倍長乗算アルゴリズムを改良したアルゴリズム [7] を実装した．

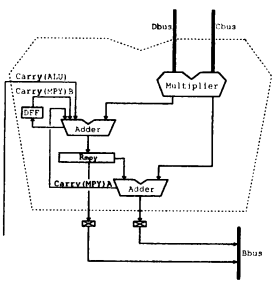

図 6 MPY 構成図

4.6 状態遷移

状態遷移（図 5：Status Counter）は乗算の場合と，乗算を除く場合で 2 つに大別される．ここでは乗算を除く場合の状態遷移を，通常状態遷移と呼ぶ．

図 7 に通常状態遷移図を示す．命令はオペランド

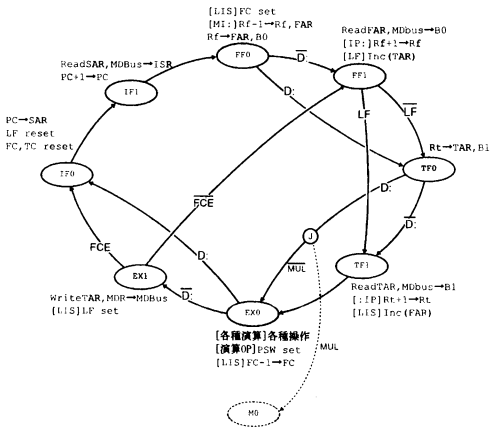

図 7 通常状態遷移図

指定モードの組合せによって，5〜8 クロックステップにて実行される．同図中 LIS は多倍長演算であることを意味する信号である．遷移条件におけるオペランド指定モードの表記は ':' の位置で F オペランドと T オペランドの区別を付けている．Inc( )，Dec( ) はそれぞれ自己インクリメント，自己デクリメント機能により計算されることを示している．Rf-1 → Rf，Rt+1 → Rt は ALU により計算される．

乗算の場合，図 7 の TF0 後に，図 8 の乗算専用の状態遷移へと遷移する．図 8 に乗算専用の状態遷移を示す．図中 Rx は汎用レジスタの x 番を指す．

5 評価

SEP-5 は，Summit Design 社の Visual Elite(ver. 3.5.1) を使用し，VHDL 言語で記述した．論理合成は Synplicity 社の Synplify Pro(ver. 7.5.1)，配置配線には Altera 社の QuartusII(ver. 2.0) を使用して設計した．設計データは，三菱マイコンソフトウェア社の実験ボード PowerMedusa AP1500 上に搭載された FPGA(Altera 社 EP20KE-1500EBC652-3) に実装した．

SEP-5 を使用してディジタル署名計算を行い，SEP-4 と比較を行った．署名計算は，ダイジェスト値を 160 ビット，秘密鍵長を 1024 ビットとし，文

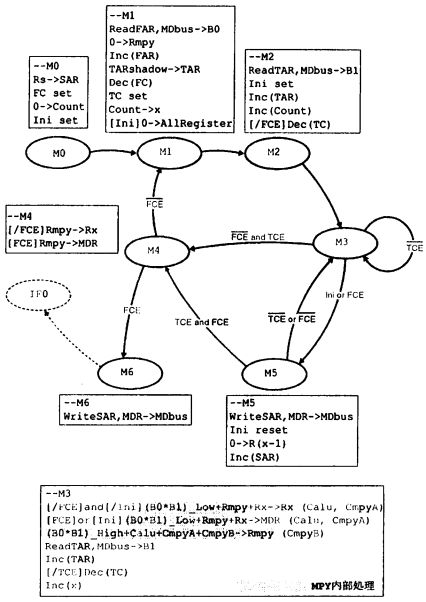

図 8　乗算専用状態遷移図

献 [3] と同じ署名プログラムを実行した．表 2 に，総クロックステップ数と，非接触（近傍型）IC カードの動作周波数である 13.56MHz 時での署名計算時間の換算値，ゲート規模の比較を示す．

表 2　ディジタル署名計算の比較

	SEP-4 [3]	SEP-5
総クロックステップ数	約 702 万ステップ	約 1273 万ステップ
署名計算時間 (13.56MHz)	約 517ms	約 939ms
ゲート規模	約 33 万ゲート	約 18.5 万ゲート

6　まとめ

ディジタル署名機能をもつ非接触 IC カード用のセキュアプロセッサ SEP-5 を設計した．SEP-5 は，高速暗号計算機能，秘密鍵漏洩防止機能，汎用計算機能，低電力消費を要件とするもので，コプロセッサをもうけずに，単独のプロセッサとして実装されている．これまでに開発をすすめてきた SEP-4 に比べ，署名計算時間の増加を約 1.82 倍におさえながらゲート規模を約 44% 縮小することができた．これにより，消費電力の低下が期待される．

今後は，消費電力の測定と改善，秘密鍵漏洩防止機能の安全性の検証，汎用計算機能を利用したアプリケーション開発が課題である．現在は VDEC[9] を利用した LSI チップの試作を行っている．

最後に，本プロセッサについては，「セキュアプロセッサ」という名称で，特許出願 [10] したことを付記する．

謝辞　本研究は，財団法人いわて産業振興センター育成試験助成金，岩手県学術研究振興財団展開研究助成金の補助を受けて行われた．

参考文献

[1] 菅 知之，“本人認証の全体像とバイオメトリクスの位置付け”，情報処理，vol.40，No.11，pp.1073-1077，1999.

[2] 吉田 壱，平田 真一，“IC カードシステム技術の現状と課題”，情報処理，vol.43，No.3，pp.296-303，2002.

[3] 浜尾仁志，曽我正和，猪股俊光，“RSA 暗号の秘密鍵保護機能と暗号計算機能をもつ IC カード用汎用プロセッサの設計”，信学技報 ISEC2003-94，pp.67-73，Dec.2003.

[4] FIPS 180-1 – Secure Hash Standerd, http://www.itl.nist.gov/fipspubs/fip180-1.htm

[5] Cetin Kaya Koc, “High-Speed RSA Implementation Version 2.0”, RSA Security, pp.10-11.1994. ftp://ftp.rsasecurity.com/pub/pdfs/tr201.pdf

[6] P.L.Montgomery, “Modular Multiplication without Trial Division”, Mathematics of Computation, vol.44, no.170, pp.519-512, Apr.1985.

[7] 浜尾仁志，“RSA 暗号の秘密鍵保護機能と暗号計算機能をもつ IC カード用汎用プロセッサの設計”，岩手県立大学大学院ソフトウェア情報学研究科，修士論文，2004.

[8] Desmedt,M.,and A.M.Odlyzko “A chosen text attack on the RSA sryptosystem and some discrete logarithm schemes”, Advances in Cryptology–proceedings of CRYPT'85, Lecture Notes in Comuputer Science, Vol.218, Springer-Verlag, pp.1-12, 1986.

[9] “VLSI Design and Education Center”, http://www.vdec.u-tokyo.ac.jp/

[10] 曽我正和，猪股俊光，“セキュアプロセッサ”，特願 2003-380114. 2003-11-10.