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

2006－SLDM－127 (32)
2006／11／30

非接触 IC カード用セキュアプロセッサ SEP-6 の開発

高橋 大介† 猪股 俊光† 新井 義和† 曽我 正和††

† 岩手県立大学大学院ソフトウェア情報学研究科 〒 020-0193 岩手県岩手郡滝沢村滝沢字巣子 152 番地 52
†† 岩手県立大学 地域連携研究センター 〒 020-0173 岩手県岩手郡滝沢村滝沢字巣子 152 番地 89
E-mail: †g231d015@edu.soft.iwate-pu.ac.jp, ††{inomata,arai,soga}@soft.iwate-pu.ac.jp

あらまし RSA 暗号による高速なディジタル署名計算機能をもつ，非接触 IC カード用マイクロプロセッサ SEP-6 の開発を行った．SEP-6 は，設計要件として，高速暗号計算機能，秘密鍵保護機能，汎用計算機能，低電力消費を掲げており，暗号計算用コプロセッサを用いず，汎用プロセッサのみで高速な暗号計算を実現しているのが特徴である．SEP-6 はこれまでに開発してきた SEP-4・SEP-5 の利点を合わせ持つように設計されたものである．本研究では，SEP-6 を FPGA 上に実装し，暗号計算速度の評価を行うとともに，シミュレーションにより消費電力を測定し，SEP-4・SEP-5 との比較を行った．

キーワード RSA 暗号，IC カード，ディジタル署名，汎用プロセッサ

Development of A Secure Processor SEP-6 for non-contact type IC cards

Daisuke TAKAHASHI†, Toshimitsu INOMATA†, Yoshikazu ARAI†, and Masakazu SOGA††

† Graduate School of Software and Information Science, Iwate Prefectural University
152-52, Takizawa-aza-sugo, Takizawa, Iwate, 020-0193, Japan
†† Iwate Prefecutral University Regional Cooperative Research Center
152-89, Takizawa-aza-sugo, Takizawa, Iwate, 020-0173, Japan
E-mail: †g231d015@edu.soft.iwate-pu.ac.jp, ††{inomata,arai,soga}@soft.iwate-pu.ac.jp

Abstract We have designed micro processor "SEP-6" for non-contact IC cards, which has a function of high-speed digital signature calculation by RSA cryptosystem. In developing SEP-6, we aim at a high-speed digital signature calculation, a private key protection, general-purpose calculation and low power consumption. The feature of this processor is not to use co-processor for RSA cryptosystem and realizes high-speed digital signature calculaton only use general-purpose processor. We have already developed SEP-4 and SEP-5 processors. We also develop SEP-6, which has former processors' features. In this paper, after implementing SEP-6 on FPGA boards, we evaluate calculation speed for coding, measure power consumption and compare with SEP-4 and SEP-5 in such properties.

Key words RSA cryptosystem, IC cards, Digital signature, General-purpose prosessor

1. はじめに

情報化社会の発展にともなって，電子情報の改ざんや，なりすまし，磁気カードのスキミングなどにより，個人情報の漏洩が社会的な問題となっている．個人認証は，安全で信頼のおける社会を構築するために重要な技術として各種方式が提案されている．その中でも，非接触 IC カードによる個人認証は，安全な認証が手軽に高速に行える点が社会のニーズと合致し，駅の改札などで近年急速に普及しており，その流れは今後も続くものと考えられる．非接触 IC カード上のマイクロプロセッサの設計要件としては，実用的な時間で署名計算を終了させられる高速暗号計算機能と，内部に保持している秘密鍵を絶対に外部に漏洩させない秘密鍵保護機能などが挙げられる．以上のような観点から，筆者らは，以下の要件を満たすセキュアプロセッサの開発を行っている [1], [2].

1) 高速暗号計算機能 (2 節)
2) 秘密鍵保護機能 (3 節)
3) 汎用計算機能 (4 節)
4) 低電力消費 (4 節)

これまでに，コプロセッサを設けず，表 1 に示すように，単一のプロセッサによって要件，1)〜3) を実装した 64 ビットプロセッサ，SEP-4 [1]，要件 1)〜3) に加えて，要件 4) の低電力消費を実現すべく，回路規模を縮小した 32 ビットプロセッ

表 1 SEP-4, 5, 6 要件比較

Table 1 Requirements comparison among SEP-4, 5, 6.

設計要件	SEP-4	SEP-5	SEP-6
高速暗号計算機能	○	△	○
秘密鍵保護機能	○	○	○
汎用機能	○	○	○
低電力消費	△	○	○

サ SEP-5 [2] を開発してきた．SEP-5 では低電力消費を実現し，暗号計算の速度を維持するべく高速化のための工夫を加えるとともに，配線幅 0.35um の VLSI チップ化を試みた．その結果，低電力消費 (約 1.7mW) は実現できたものの，暗号計算速度は，SEP-4 の 4 倍程度の時間（約 0.94 秒）を要する結果となった．そこで，秘密鍵保護機能と汎用計算機能を実現しつつ，SEP-4 （暗号計算速度 約 0.27 秒）以上の高速暗号計算機能と，消費電力 10mW 以下を目標として，64 ビットプロセッサとして，SEP-6 の開発を試みた．

本研究で開発した SEP-6 は，駅の改札などでの瞬間的な認証が要求される状況における運用にはさらなる検討が必要と思われるが，コンピュータ，銀行端末，医療機器，販売店端末，などにおける個人認証への応用を想定している．

2. 高速暗号計算機能

2.1 RSA 暗号計算機能

公開鍵暗号方式を利用したディジタル署名は，任意のメッセージのダイジェスト値を，秘密鍵とそれに付随する公開パラメータを使用して一定のアルゴリズムに基づいて暗号化することで得られる．本プロセッサでは，ディジタル署名作成に RSA 公開鍵暗号を利用している．ダイジェスト値の生成には，SHA-1 [3] を使用している．ディジタル署名は，ダイジェスト値を D, 秘密鍵を K, 公開パラメータを N としたとき，次のように計算される．

$$D^K \bmod N \qquad (1)$$

ここで，ダイジェスト値 D は 60 ビット，秘密鍵 K は 1024 ビット，公開パラメータ N は 1024 ビットのデータ長をそれぞれもっているものとする．RSA 暗号計算を高速に実行するためにバイナリ法 [4] とモンゴメリ乗算 [5] を利用しており，両アルゴリズムによる計算を効率的に行うことができるハードウェア構成になっている．

2.2 状態遷移

状態遷移は，乗算命令とそれ以外の命令とに大別される．乗算命令以外の状態遷移を通常状態遷移と呼び，図 1 に SEP-6 の通常状態遷移図を示す．

図 1 中の，D・I・A・MI・IP・IV64・LI・LA は，SEP-6 のオペランド指定モードである．詳細については，4 節を参照されたい．SEP-6 では，オペランドとしては，F(From) オペランドと T(To) オペランドが存在し，図 1 中では，:を区切りとして，[F:T] の形で表されている．状態を表すノードに付加された ○ → ○ は，その状態時に実行される転送である．矢印に付随するラベルは，矢印で結ばれたノードへの遷移条件である．破線で描かれている矢印は，多倍長演算時専用の遷移ルートとなる．SEP-6 では多倍長演算を行う際は，1 語目の演算は，非多倍長演算時と同様に，オペランド指定で指定されたモードにしたがって遷移し，2 語目以降は，指定された語長分，破線で表されたルートを遷移し続ける．

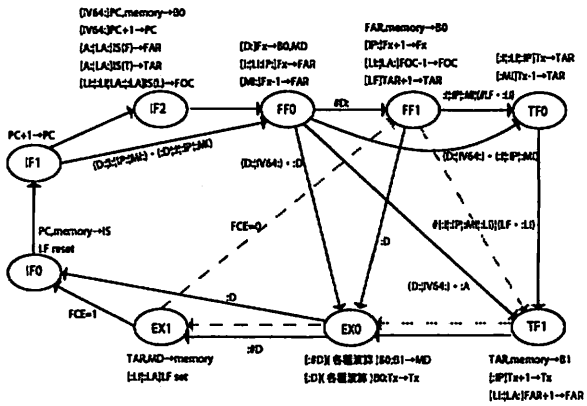

図 1 SEP-6 通常状態遷移

Fig. 1 SEP-6 Noarml State Transition.

表 2 多倍長演算時の状態ステップ数の比較

Table 2 Compare number of state steps.

	SEP-4	SEP-6
LI:LI	6 × (倍語長 − 1) + 9	4 × (倍語長 − 1) + 9
LA:LA	5 × (倍語長 − 1) + 9	4 × (倍語長 − 1) + 9

PC・FAR・TAR・B0・B1・MD・IS は，SEP-6 の内部に存在するレジスタの名称である．LF は多倍長演算の実行を表すフラグであり，FCE は指定された語長分，演算が実行された時，'1' になり，多倍長演算が終了する．

SEP-6 の通常状態遷移を設計するにあたり，多倍長演算時の状態遷移を見直し，状態遷移の最適化を行った．オペランド指定モードが LI:LI のときを例として説明する．SEP-4 で多倍長演算を行うとき，IF0 → IF1 → IF2 → FF0 → FF1 → TF0 → TF1 → EX0 → EX1 と遷移した後，FF0 に遷移し，その後は指定された語長分，FF0 → FF1 → TF0 → TF1 → EX0 → EX1 → FF0···，と遷移を繰り返す．これに対して，SEP-6 の多倍長演算は，最初に EX1 まで遷移するところまでは同様であるが，その後は指定された語長分，FF1 → TF1 → EX0 → EX1 → FF1···，と遷移を繰り返す．すなわち，SEP-4 では，FF0 と FF1 の 2 ステップで行っていた動作を，SEP-6 では FF1 の 1 ステップで行う．このように回路構成を見直したことで，多倍長演算時の状態ステップ数を，1 語長につき 2 ステップ削減することができた．表 2 は両プロセッサの多倍長演算時のステップ数である．暗号計算は多倍長演算を多用するため，このステップ数削減により，若干の速度改善が達成できた（5 節参照）．

一方の，乗算専用状態遷移は，SEP-5 [2] と同じである．

表 3 各モードの動作内容

Table 3 Behaviors in each mode.

	ノーマルモード	セキュアモード
実行許可命令	汎用計算命令	暗号計算専用命令
不許可命令実行	NOP 命令に置き換え	SIE 命令に置き換え
割込み	許可	禁止
メモリアクセス	全領域アクセス可能	暗号計算時使用領域のみ

表 4 SIG, SIE 命令仕様

Table 4 Instruction specifications of SIG, SIE.

命令	動作内容
SIG	SF を '1' にセット 暗号計算プログラムの先頭番地へジャンプ 秘密鍵参照カウンタ（後述）の初期化
SIE	SF を '0' にセット 戻り番地へジャンプ

3. 秘密鍵保護機能

ディジタル署名計算を実行する IC カードにとって何より致命的なのは内部に保管している秘密鍵が漏洩することである．ここで秘密鍵の漏洩とは，以下のような行為によって，秘密鍵そのもの，もしくは秘密鍵を推定されうる情報が攻撃者の手に渡ることをいう．

i) 秘密鍵の全ビットが一度に読み出される．
ii) 暗号計算中に間接的に使用される秘密鍵の各ビット値が計測され，そこから秘密鍵が推定される．
iii) ある種の暗号計算結果を収集して，別の任意のダイジェスト値に対する署名を合成する．

秘密鍵の漏洩を防ぐために，次の 2 つの機能を実装した．

- セキュア機構
- 秘密鍵参照回路

3.1 セキュア機構

秘密鍵参照回路によって秘密鍵のレジスタ，メモリ上への漏洩を防げたとしても，暗号計算途中でメモリ上に格納される中間結果を参照することにより，そこから秘密鍵を推定されてしまう可能性がある．そこで，本プロセッサでは，暗号計算実行途中の中間結果を参照できないような機構を実装した．

ノーマルモードとセキュアモード

プログラムの走行モードを，表 3 に示すように，汎用命令実行時のノーマルモードと，暗号計算実行時のセキュアモードの 2 つに分けている．二つのモードはプロセッサ中の SF(*Secure Flag*) によって制御されており，SF が '0' の時はノーマルモード，'1' の時はセキュアモードになる．モードの切り替えは 表 4 の SIG(Signature) 命令と SIE(Signature End) 命令で行われる．

本プロセッサで実行される命令は，ノーマルモードの汎用計算命令か，セキュアモードの暗号計算専用命令のいずれかの命令群に属し，それぞれモードの変更で動作は，表 3 のように制限が課せられる．

表 5 暗号計算専用命令

Table 5 Instruction set for the RSA cryptosystem calculation.

命令	動作
ADI	2 つの多倍長データと 1 の和を求める．
IBN	多倍長データをインクリメントする．
CSB	多倍長データと，公開パラメータ N を比較し， N より大きい場合のみ，多倍長データから N を減算する．
PKS	使用する秘密鍵の番号を PKS レジスタに格納する．(3.2 節)
MLS	多倍長データの自乗を求める．
MDK	多倍長データと D^{K_i} の積を求める．KC をデクリメント．
MLP	多倍長データと $R^2 \bmod N$ の積を求める．
MLH	多倍長データと N の積の上位半分を求める．
MLL	多倍長データと $N'(= N^{-1} \bmod R)$ の下位半分を求める．

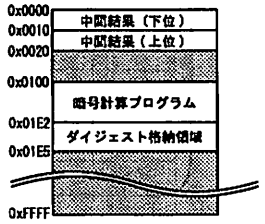

図 2 主メモリのメモリマップ

Fig. 2 Memory Map of Main Memory.

暗号計算専用命令は，表 5 に示すように，SEP-6 アーキテクチャ上で，RSA 暗号計算を高速に行うことに特化した命令群である．

暗号計算の中間結果のクリア

セキュアモードで実行する暗号計算専用命令は，命令時にアクセスするメモリアドレスが図 2 に示すようにあらかじめ決められている．すなわち，暗号計算を行うときは，常にメモリ上の同じ領域を使用して計算を行っている．暗号計算終了時や，暗号計算プログラム中に汎用命令が含まれていた場合など，ノーマルモード移行時にメモリ上に暗号計算の中間結果が残っていると，攻撃者に秘密鍵を推定する情報を与えてしまうことになる．そのため，SIE 命令が実行されノーマルモードに移行する時は，同時に暗号計算の中間結果格納領域をゼロクリアすることで，計算途中の中間結果が外部に漏洩するのを防止している．

ダイジェストチェック機能

ダイジェスト値はプロセッサ内部で汎用機能を用いて生成するか，外部から生成したものを受け取ったのち，メモリ上の固定番地に格納することで，暗号計算時に使用される．ダイジェスト値を任意に選択できる場合，ある一定の条件を満たす署名を偽造できることが報告されている [6]．よって，ダイジェスト値 160 ビットをチェックし，ダイジェスト値が単純である場合には暗号計算を拒否する機能を実装した．具体的には，ダイジェスト値を 16 × 10 の組に分け，各組に必ず 1 ビット以上 1 が存在することをチェックする．もしどこか一つの組でも，すべてのビットが 0 の組があれば，単純なダイジェスト値と判断

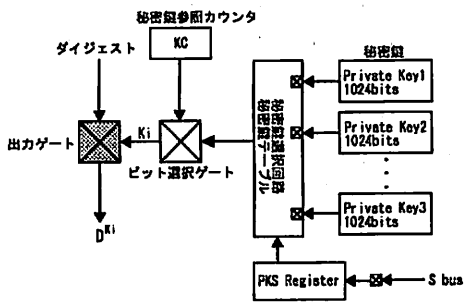

図 3 秘密鍵選択回路と秘密鍵参照回路

Fig. 3 Architecture of selecting and referring private key.

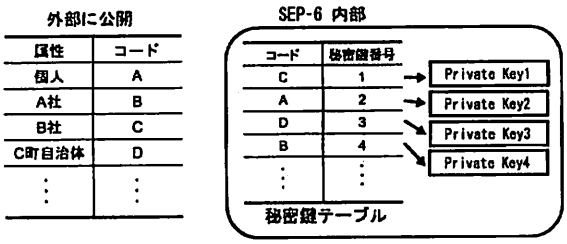

図 4 秘密鍵テーブル

Fig. 4 Private key table.

して，セキュアモードに移行しない．

3.2 秘密鍵選択回路と秘密鍵参照回路

秘密鍵選択回路

SEP-6 では，あらかじめ秘密鍵を複数個保持しておき，必要に応じて暗号計算時に使用する鍵を変更することで，属性認証にも対応できるようにした．

図 3 に秘密鍵選択回路と後述する秘密鍵参照回路の構成図を示す．暗号計算に使用する秘密鍵の選択には，PKS(*Private Key Select*) 命令を使用する．プロセッサ内部の秘密鍵にあらかじめ固有の番号を割り当てておき，PKS 命令で使用する鍵の番号を指定することとした．PKS で指定された鍵番号は，PKS Register に格納され，暗号計算時に秘密鍵選択回路により参照される．秘密鍵選択回路は PKS Register に格納された値に対応した秘密鍵のゲートを開放する．

プロセッサ内部に保持することになる秘密鍵の例としては，持ち主自身を表す個人認証用の秘密鍵の他に，たとえば，持ち主の所属する会社の従業員であることを証明する秘密鍵や，持ち主が暮らす地域の自治体に所属することを証明する秘密鍵などが挙げられる．

これら複数個の秘密鍵を格納している IC カードで認証を行う際，秘密鍵の固有番号の付け方が大切となる．そこで，図 4 のように，秘密鍵にはあらかじめ，属性ごとに固有のコードを設定しておき，秘密鍵を登録する際に，プロセッサ内では秘密鍵登録時に秘密鍵番号を割り当て，コードと秘密鍵番号の対応を秘密鍵テーブルとして保持しておく．

利用者が認証を行う際には，秘密鍵の指定に固有のコードを使用し，プロセッサ内部では秘密鍵テーブルからコードと対応する秘密鍵を引き出して，認証に使用する．

なお，プロセッサ内部への秘密鍵の安全な登録方法は今後の課題である．

秘密鍵参照回路

前述のとおり，本プロセッサでは，RSA 暗号計算をバイナリ法とモンゴメリ乗算を組み合わせたアルゴリズムを利用して行う．バイナリ法を利用した RSA 暗号計算では，秘密鍵 K は最上位ビットから 1 ビットずつ参照されて，ダイジェスト D の指数として利用されるのみである．そこで，図 3 に示す，秘密鍵を 1 ビットずつ参照して，その値を D^{K_i} に反映させる秘密鍵参照回路をプロセッサ内部に設けた．ここで，i は秘密鍵中の i 桁目を示す．

図 3 中の秘密鍵参照カウンタは，暗号計算中に参照する秘密鍵のビットを示すカウンタで，1023 を初期値として 0 までデクリメントされる．秘密鍵選択ゲートでは，秘密鍵参照カウンタの値から秘密鍵中の 1 ビットを選択し，ダイジェストの指数として使用し，出力ゲートより D^{K_i} を出力する．

秘密鍵を格納しているメモリとプロセッサはこの秘密鍵参照回路で結ばれているのみで，その他のレジスタや主メモリへの経路は存在しない．

以上に述べた機構により，i)〜iii) に挙げた行為による，プロセッサ外部への秘密鍵情報の漏洩を防いでいる．

この機構を別途，国際特許出願している [10].

4. SEP-6 のアーキテクチャ

4.1 命令フォーマット

SEP-6 の命令フォーマットを図 5 に示す．SEP-6 では SEP-4・SEP-5 の見直しを行いながら，冗長性を取り除いて設計した．

SEP-6 のオペランド指定モードを表 6 に示す．乗算命令とそれ以外の命令とで異なる命令フォーマットを使い分け，乗算以外の命令フォーマットでは，OP(4 ビット) と SOP(4 ビット) で命令を指定し，MF・MT(各 4 ビット) でオペランド指定モードの指定を行う．F・T(各 16 ビット) は，それぞれ，演算対象となるレジスタ，メモリアドレスを指定する．L*Length* は多倍長演算時の語長数の指定に使用される．

オペランド指定モード中，多倍長演算に用いる LI，LA モー

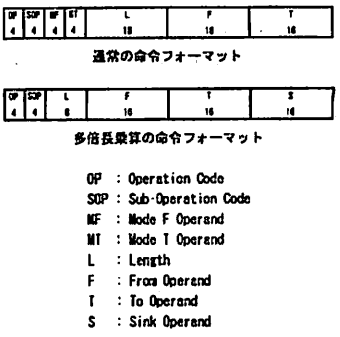

図 5 SEP-6 命令フォーマット

Fig. 5 Instruction formats on SEP-6.

表 6 SEP-6 オペランド指定モード
Table 6 Addressing modes on SEP-6

	モード名称	動作
D	レジスタ直接	EA = R_n
I	レジスタ間接	EA = [R_n]
A	アドレス直接	EA = IA
MI	−1&レジスタ間接	Dec(R_n) EA = R_n
IP	レジスタ間接&＋1	EA = R_n Inc(R_n)
LI	多倍長レジスタ間接	先頭アドレス = [R_n]
LA	多倍長アドレス直接	先頭アドレス = IA
IV64	直接即値指定	実行データ = IV

n ：1〜16, sp, pc
EA：実効アドレス，[]:内容を示す
IA：命令コードに直接書かれたアドレス，IV：即値
Dec(R_n) $R_n \leftarrow R_n - 1$, Inc(R_n) $R_n \leftarrow R_n + 1$

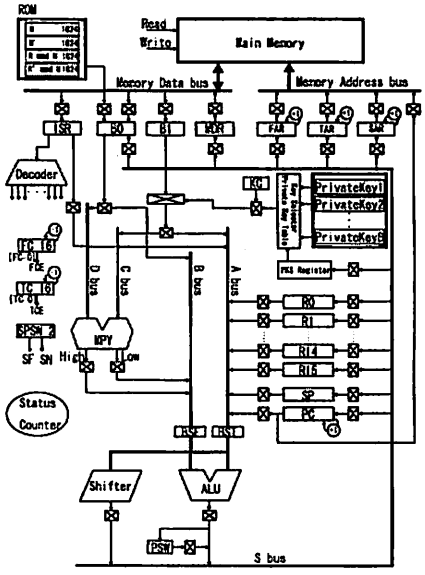

図 6 SEP-6 アーキテクチャ構成
Fig. 6 Architecture of SEP-6

ドのみ，他のオペランド指定モードと組み合わせて使うことができず，それぞれ，F オペランド，T オペランドともに LI:LI か，LA:LA の組合せのみで運用を行う．

乗算命令時は，オペランド指定モードが LI:LI に固定され，MF，MT の指定に使用していた領域を，乗算結果を格納するためのアドレス指定に使用する．

4.2 プロセッサ構成

図 6 に SEP-6 のアーキテクチャ構成を示す．SEP-6 は語長 64 ビット，メモリアクセスに用いるアドレスは語単位，容量は 64 × 64K 語 (512K バイト) とした．ただし，特定の命令を使用することでバイト単位でデータ転送が可能である．演算に使用できる汎用レジスタの数は 16 個（各 64 ビット）である．また，加減算，乗算，シフト命令など一部の命令は，1 命令で多倍長演算 [2] が可能である．

主メモリの構成は，図 2 に示すとおりで，暗号計算中間結果と暗号計算プログラムはそれぞれ，固有の番地に格納される．秘密鍵は，主メモリ中ではなく，専用の ROM に格納される．

- ALU · Shifter · MPY

ALU は，加減算および論理演算が可能である．Shifter は算術，論理，循環の各シフト動作を左右両方向に任意のビット数 (1〜63 ビット) 行うことができる．MPY(Multiplier) は 64 × 64 ビットの乗算を行う．

- PSW · SPSW

PSW はノーマルモード時のフラグ管理を，SPSW はセキュアモード時のフラグ管理を行う．

- BSF · BST

メモリやレジスタからデータを 1 バイトのみ移動させるためのゲートである．

これらの命令と，前述の豊富なオペランド指定モードの組合せにより，本プロセッサは汎用計算機能を実現している．

4.3 ダイジェストレジスタの削除

SEP-4 では，暗号計算に用いるダイジェスト値は，メモリ上の任意のアドレスに格納しておき，暗号計算実行開始時に，プロセッサ中のダイジェストレジスタに格納して使用していた．一方，SEP-6 では，ダイジェストレジスタを削除し，暗号計算実行中にダイジェスト値を参照する必要が生じた場合はメモリ上から直接読み出して使用することとした．ダイジェストレジスタを削除することにより，ゲート規模の削減が実現された．

4.4 汎用計算命令の見直し

本研究で開発したプロセッサを，これまでに研究室内で行われている演習で試用した．ユーザからは，命令セットに対して，いくつかの改善案が寄せられた．そこで，ユーザからの要望に応え，汎用命令を見直し，新規命令の追加を行った．

APUSH 命令，APOP 命令

多倍長乗算を行う際には，汎用レジスタが乗算の中間結果の一時格納場所として使用される．プロセッサ内部の機構の簡単化のため，語長がどのようなサイズの場合でも，乗算命令開始時に，汎用レジスタの値をゼロクリアする仕様としている．このため，汎用命令を使用してプログラムを組む場合，乗算を行うたびに，使用しているレジスタをすべて退避させる必要があり，わずらわしいとの意見が多数よせられた．そこで，ハードウェアレベルで汎用レジスタの退避，復旧を 1 命令で実行する APUSH(*All Push*)，APOP(*All Pop*) 命令を実装した．これらの命令は，乗算命令の実行時に呼び出されると考え，実行時間の短縮のため，サブルーチンではなく，SEP-6 の多倍長演算機能を利用して，ハードウェアレベルで実装を行った．表 7 に，APUSH，APOP 命令の実行ステップ数と，同等の機能をサブルーチンで実装した場合の実行ステップ数の比較を示す．

表 7 実行ステップ数の比較
Table 7 Comparison of execution steps.

	ハードウェア	サブルーチン
APUSH	83 ステップ	112 ステップ
APOP	51 ステップ	80 ステップ

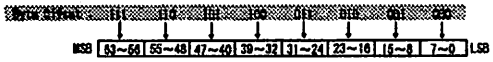

図 7 MOVB 命令のバイトオフセット
Fig. 7 Byte offset of MOVB.

表 8 SEP-4, 5, 6 の比較
Table 8 Comparison among SEP-4, 5, 6.

	SEP-4	SEP-5	SEP-6
バス幅	64 ビット	32 ビット	64 ビット
ゲート規模	53,046 ゲート	29,492 ゲート	51,694 ゲート
暗号計算速度	約 0.270 秒	約 0.939 秒	約 0.258 秒
消費電力	-	約 1.7mW	約 6.7mW

MOVB 命令

SEP-4 は基本的に語長単位のデータの受け渡ししか想定していなかったが，実際にプログラムを組む際にはバイト単位でデータの受け渡しを行えた方が都合の良い場合が多い．そこで，SEP-6 では，図 7 に示すように，F オペランド，T オペランドへの任意のバイトオフセットを指定して，1 バイト単位でデータの受け渡しが可能となる MOVB（*Move Byte*）命令を実装した．汎用レジスタ中の R14，R15 にあらかじめ F，T オペランドで指定したバイトオフセットを指定しておき，MOVB 命令実行時には，そこに格納された値をもとにして各オペランドのバイトオフセットを決定し，バイト単位での転送がされるようにした．

シフト命令の拡張

シフト命令はこれまで，1 命令で算術シフト，論理シフト，ローテートシフトを左右どちらかの方向に 1 ビットだけシフトさせることができるだけだった．このため，多段シフトを行う場合は，シフト命令を複数回繰り返さなければならず，効率が悪いとの意見があった．そこで，Shifter を改良し，1 命令で任意のビット数（1 ビット〜63 ビット）シフトできるようにシフト命令の拡張を行った．

各シフト命令は，T オペランドで指定されたデータをシフトし，再び T オペランドへ格納する命令になっている．そこで，シフト命令時には使われていなかった F オペランドを，シフトビット数の指定に利用して，シフト命令の拡張を実現した．

5. 評　価

表 8 に，SEP-4，SEP-5，SEP-6 のゲート規模 (2NAND 換算) と，非接触 IC カードの動作周波数である 13.56MHz で動作させたときの RSA 暗号計算（秘密鍵長 1024 ビット）の計算速度，暗号計算実行時の消費電力を Cadence 社 [7] のシミュレーションツール verilog と，Synopsys 社 [8] の Power Compiler を使用してシミュレーションした結果の比較を示す．

ゲート規模は，32 ビットプロセッサとして開発した SEP-5 が最小となっている．同じ 64 ビットプロセッサである SEP-4 と比較すると，通常遷移の見直しや，ダイジェストレジスタの削除などによる効果でゲート規模が削減されている．しかしながら，大幅なゲート規模の削減にならなかったのは，汎用計算機能の充実のために MOVB 命令などを実装したことによる，ゲート規模の増加が生じたためである．

SEP-6 は 2.2 節で述べている多倍長演算時の状態遷移の遷移数を削減した効果で，SEP-4 と比較して暗号計算速度の面で約 0.12 秒の改善があった．

消費電力は，32 ビットプロセッサである SEP-5 と比較すると増加しているが，ダイジェストレジスタの削減やプロセッサの構成の見直しなどにより，当初目標としていた 10mW 以下を達成することができた．以上のことから，設計要件 1)〜4) を実現できたといえる．

6. ま と め

本研究では，これまで開発してきた SEP-4·SEP-5 の両プロセッサの利点を継承し，更に複数個の秘密鍵を扱うための秘密鍵選択回路の実装，状態遷移，汎用命令の見直しを行ったセキュアプロセッサ SEP-6 の開発を行った．SEP-6 の設計要件は，1) 高速暗号計算機能，2) 秘密鍵保護機能，3) 汎用計算機能，4) 低電力消費であり，いずれも実現された．SEP-6 の暗号計算時間は約 0.258 秒，消費電力約 6.7mW である．

現在，VDEC [9] を利用して，SEP-6 のチップを試作中である．今後は，更なる低電力消費化を推し進めるとともに，サイドチャネル攻撃に対する耐タンパ性の調査，非接触 IC カード以外への用途の検討などを行っていく予定である．

文　献

[1] 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.67-73，2003.
[2] 穂積健介，猪股俊光，曽我正和，「セキュアプロセッサの開発」，情処研報，2004-ARC-160，pp.71-76，2004.
[3] FIPS 180.1 . Secure Hash Standard, http://www.itl.nist.gov/fipspubs/fip180-1.htm
[4] Cetin Kaya Koc, "High-Speed RSA ImplementationVersion 2.0", RSA Security, pp.10-11.1994. ftp://ftp.rsasecurity.com/pub/pdfs/tr201.pdf
[5] P.L.Montgomery, "Modular Multiplication without Trial Division", Mathematics of Computation,Vol.44, No.170, pp.519-512, Apr.1985.
[6] Desmedt.M,and A.M.Odlyzko "A chosen text attack on the RSA cryptosystem 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.
[7] "Cadence Design Systems" http://www.cadence.com/
[8] "Synopsys World Leader in EDA Software and Services" http://www.synopsys.com/
[9] "VLSI Design and Educational Center" http://www.vdec.u-tokyo.ac.jp/
[10] 曽我正和，猪股俊光，"SECURE PROCESSOR", PCT/JP2004/016589.