接触型 IC カード用セキュアプロセッサ SEP-7 の開発

伊藤 真梨子† 猪股 俊光† 新井 義和† 曽我 正和††
†岩手県立大学ソフトウェア情報学部 ††岩手県立大学地域連携研究センター

1 はじめに

市場では IC カードや USB トークン，ETC カードなどの接触型の認証媒体が増大している．これら接触型媒体の場合，外部から電力を受電することができるのでクロックを高速化することが可能である．また，一般的に認証用プロセッサでは，汎用計算機能に加えて認証のためのディジタル署名計算機能などを回路規模を小さくして実装するのが望ましい．そこで本研究では，SEP-E[1] のアーキテクチャにセキュア機能（高速暗号計算機能・秘密鍵保護機能）を組込み，接触型媒体用セキュアプロセッサ SEP-7 を開発し，暗号計算速度やゲート規模の評価を行った．

2 SEP-7 の概要

2.1 セキュアプロセッサとしての特徴

SEP-7 では秘密鍵の漏洩を防ぐために，セキュア機構と秘密鍵参照回路を実装した．

(1) セキュア機構

暗号計算途中でメモリ上に格納される中間結果が参照されると，秘密鍵を推定されてしまう．そこで，SEP-7 では，暗号計算実行途中の中間結果を参照できない機構を実装した．

セキュアモードとノーマルモード ノーマルモードでは汎用計算のみ実行可能とし，セキュアモードでは暗号計算専用命令のみ実行可能である．セキュアモードの間は割り込み，ならびに特定のメモリアドレスへのアクセス以外は禁止する．

暗号計算の中間結果のクリア ノーマルモード移行時に，暗号計算の中間結果を格納しているメモリ領域をゼロクリアし，中間結果が外部へ漏洩するのを防止する．

ダイジェストチェック機能 ダイジェスト値 160 ビットを 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し，どこか一つの組でもすべてのビットが '0' であればダイジェスト値が単純であると判断し，暗号計算を拒否する．

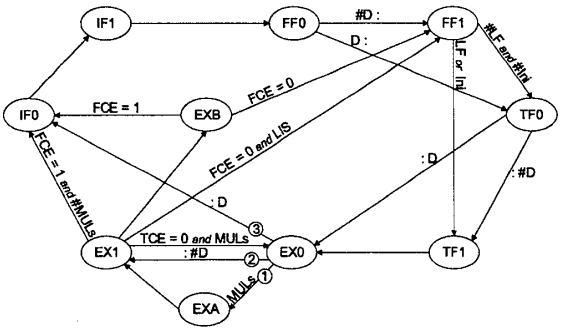
(2) 秘密鍵参照回路

RSA 暗号計算はバイナリ法 [2] とモンゴメリ乗算 [3] を基にしたアルゴリズムで行われる．秘密鍵は最上位ビットから 1 ビットずつ参照され，ダイジェスト D の指数として利用される．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，その他のレジスタや主メモリへの経路は存在せず，また秘密鍵を格納しているメモリへアクセスするための命令も用意されていない．

(3) 高速暗号計算機能

RSA 暗号計算機能 ディジタル署名計算の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 [2] とモンゴメリ乗算 [3] を用いており，この計算を効率的に行うことが出来るハードウェア回路をもつ．

状態遷移 ディジタル署名計算等に必要な多倍長乗算のための状態遷移をもうけた．図 1 の MULs は多倍長乗算の実行を，LIS はその他の多倍長演算の実行を表すフラグであり，FCE，TCE は指定された語長分，演算が実行されたとき '1' がセットされ，多倍長演算が終了する．Ini は多倍長乗算時に EXB へと遷移した際に '1' がセットされ，LF は多倍長演算時に EX0 に遷移した際に '1' がセットされる．



「#」否定，「O:」F オペランド，「:O」T オペランド

図 1: SEP-7 の状態遷移図

2.2 プロセッサ構成

SEP-7 のアーキテクチャを図 2 に示す．このうち，KC-，1024bit Select Key は秘密鍵参照回路であり，秘

Development of a Secure Processor SEP-7 for Contact Type Medium

† Mariko ITO, Toshimitsu INOMATA, Yoshikazu ARAI
†† Masakazu SOGA
Faculty of Software and Information Science, Iwate Prefectural University (†)
Iwate Prefectural University, Iwate Regional Cooperative research center (††)

密鍵 K の i 桁目を参照し，ダイジェスト値 D の指数として利用する．Address Table は，署名計算専用命令が使用する主メモリや ROM におけるアドレスを格納する．SEP-7 ではオペランドの対象をレジスタのみにしており，D モードを除き，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は常に固定であることから，命令ごとに適切なアドレスを A バスに出力し，FA+，TA+にセットする．

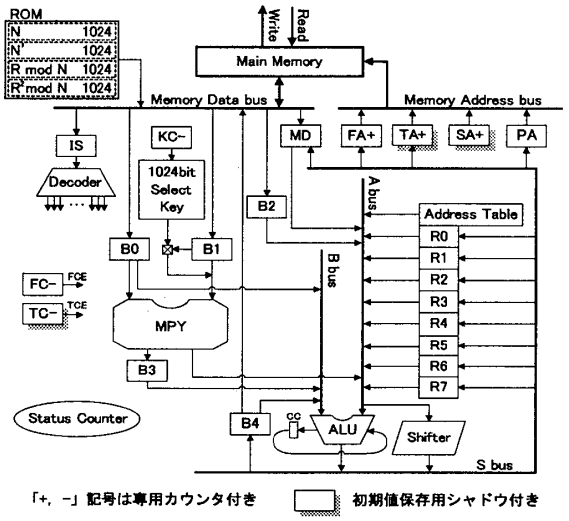


図 2: SEP-7 のプロセッサ構成図

2.3 ゲート規模の縮小

SEP-6[4] では 64 ビットレジスタを 16 個用意し，多倍長乗算時の部分積を格納して計算をするが，LSI 上でメモリやレジスタなどの記憶素子は巨大な面積を占有するためコストが非常に高くなる．そこで，SEP-7 ではゲート規模を縮小するため，部分積を汎用レジスタを用いず主メモリへ格納することとした．

3 SEP-7 の性能評価

表 1: 開発環境

工程	ツール名
VHDL 記述	MentorGraphics 社 VisualElite 3.5.1
論理合成	Synplicity 社 Synplify Pro 7.5.1
配置配線	Altera 社 QuartusII 4.2

SEP-7 の設計データは，FPGA（Altera 社 Cyclone EP1C6Q240C8：LE（Logic Element）数 5,980 個）に実装した．SEP-7 の FPGA 向け論理合成結果は LE の使用率約 60 %，ASIC 向けの論理合成では 12,132 ゲート（2NAND 換算）と推定される．SEP-7 と SEP-6 で署名計算（ダイジェスト値 160 ビット，秘密鍵長 1024 ビット）を実行した際の，総クロックステップ数，署名計算時間の比較を表 2 に示す．SEP-7 の語長は 16 ビットで，SEP-6 の 4 分の 1 であり，演算の中で繰り返される乗算の回数が単純計算で 16 倍増大する．さらに，多倍長乗算の部分積は主メモリに格納されており，SEP-6 に比べて 3 倍遅くなる．SEP-7 の動作周波数は 70MHz で，SEP-6 より約 5 倍高速であるが，署名計算時間は約 6 倍遅くなった．一方，ゲート規模（ASIC 向けの論理合成：2NAND 換算）を比べると，SEP-6 とくらべ 4 分の 1 程度までゲート規模を縮小することができた．

表 2: SEP-7 と SEP-6 の性能比較

	署名計算		ゲート規模
	ステップ数	時間	(2NAND 換算)
SEP-7 (接触型)	約 12,070 万	約 1,644ms (70MHz)	12,132
SEP-6 (非接触型)	約 350 万	約 258ms (13.56MHz)	51,694

4 おわりに

本研究では，チップサイズ 2.5mm 角（配線幅 0.18μm）への搭載を目指し，SEP-E のアーキテクチャに高速暗号計算機能，秘密鍵保護機能，汎用計算機能を実装した接触型媒体用セキュアプロセッサ SEP-7 の開発を行った．現在，VDEC[5] を利用して，SEP-7 のチップを試作する予定である．

今後は，消費電力の推定を行うと共に，SEP-7 の設計データを見直し，暗号計算の高速化を図っていく．

参考文献

[1] 高橋大介，猪股俊光，新井義和，羽倉淳，曽我正和，「組込みソフトものづくり塾の取り組み」，第 8 回組込みシステム技術に関するサマーワークショップ SWEST8 ポスターセッション，SWEST8 予稿集，pp.87-92 (2006)

[2] Cetin Kaya Koc ,"High-Speed RSA Implementation Version 2.0", RSA Security, pp.10-11 (1994)

[3] P.L.Montgomery,"Modular Multiplication without Trial Division", Mathematics of Computation, Vol.44, No.170, pp.519-512 (1985)

[4] 高橋大介, 猪股俊光, 新井義和, 曽我正和,「非接触 IC カード用セキュアプロセッサ SEP-6 の開発」，電子情報通信学会技術研究報告，Vol.106 No.389 pp.61-66 (2006)

[5] "VLSI Design and Educational Center" http://www.vdec.u-tokyo.ac.jp/