特許ビジネス市

案件名称　：　セキュア･プロセッサ

(独) 科学技術振興機構

(岩手県立大学　地域連携センター　曽我正和)

技術内容

① 従来技術とその問題点

電子的個人認証の現状

認証方法	鍵コードの所在場所	推定される危険度	盗聴される危険度	サーバ漏洩時の対策
暗証番号	本人の記憶	**危険あり** 推定手掛りあり	**危険あり** キータッチ追跡	番号変更
ID番号	IDカード上のメモリ媒体	危険小	**危険あり** スキミング	番号変更
生体認証	本人の身体	危険小	危険小 ただし指紋はトレース可能	**変更不可能**
デジタル署名	IDカード上のプロセッサ	危険小	危険小 秘密鍵は外へ出さない仕組み	サーバには公開鍵のみ

危険大

危険中

不安感

仕組強

技術内容

② 技術の主要部説明

認証用ICチップ

デジタル署名は、安全強固な認証方式なので、住基カードに使われている

しかし、SUICA や ETC にはまだ使われていない

何故か

$D^{K}Mod\ n$

通信用／暗号用

認証の計算時間が膨大 → デュアルプロセッサで十数秒 → 遅い

ICチップの消費電力大 → 接触型カード → 不便

これを解決！

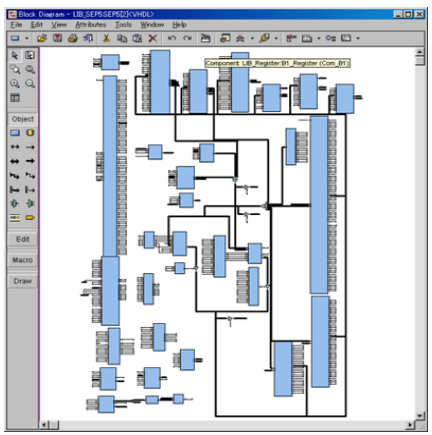
技術内容

③ 効果

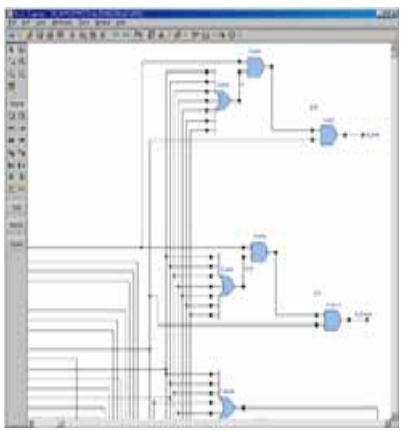
特許部分

メインプロセッサのアーキテクチャを署名計算向きにして

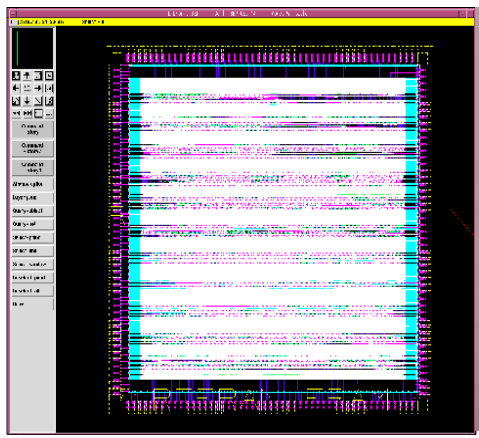
単一プロセッサとし、**高速化・低電力・安全性を同時に達成**



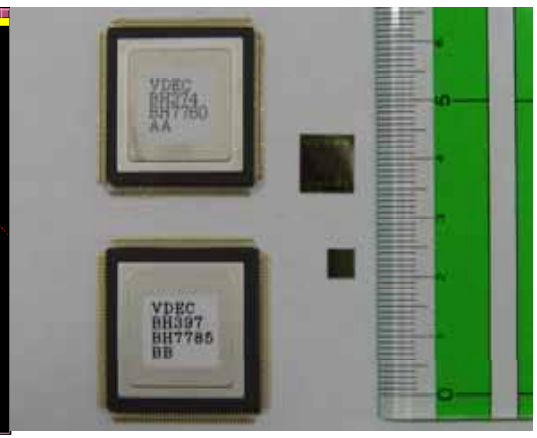
アーキテクチャ設計



論理設計



LSI設計



上段 SEP-5(9.8mm角)

下段 SEP-6(4.9mm角)

■ 本研究は東京大学大規模集積システム設計教育研究センターを通し、シノプシス株式会社の協力で行われたものである。

特許内容

① 特許情報

1、発明の名称	セキュア･プロセッサ			
2、出願	出願番号	特願２００３－３８０１１４	出願日	２００３．１１．１０
	出願人	独立行政法人 科学技術振興機構	審査請求有無	有
3、公開･登録情報	公開番号	特開２００５－１４１１６０	登録番号	
4、権利者	曽我 正和、猪股 俊光			
5、関連特許				

特許内容

② 請求範囲

項	概要	内容
1	プロセッサ構造	署名用の秘密鍵を安全に保管し、かつ高速に署名演算を実行するための専用レジスタをもつ構造
2	プロセッサ動作方式	署名専用の機械語命令のみが作動するセキュリティモードと、署名以外の一般命令のみが作動する一般モードをもつ動作方式
3	セキュリティモードの動作方式	セキュリティモード/一般モードの切り替えは特殊な命令とプロセッサ状態が整わないと実行できず、結果としてセキュリティモードは開始すると中断できない動作方式
4	セキュリティモードの動作方式	署名をつける対象データは圧縮されビットパターンが攪拌されているが、或る特異なパターンのとき対象から除外する方式
5	セキュリティモードのデータ記憶方式	署名計算が完了したとき、署名計算の途中結果がメモリ上にもレジスタ上にも残らないような途中データの記憶方式
6	製品化	これらの特徴を備えたセキュアプロセッサを搭載したICカード

特許内容

③ 効果

1. 高速署名アルゴリズムを H/W 化

高速化

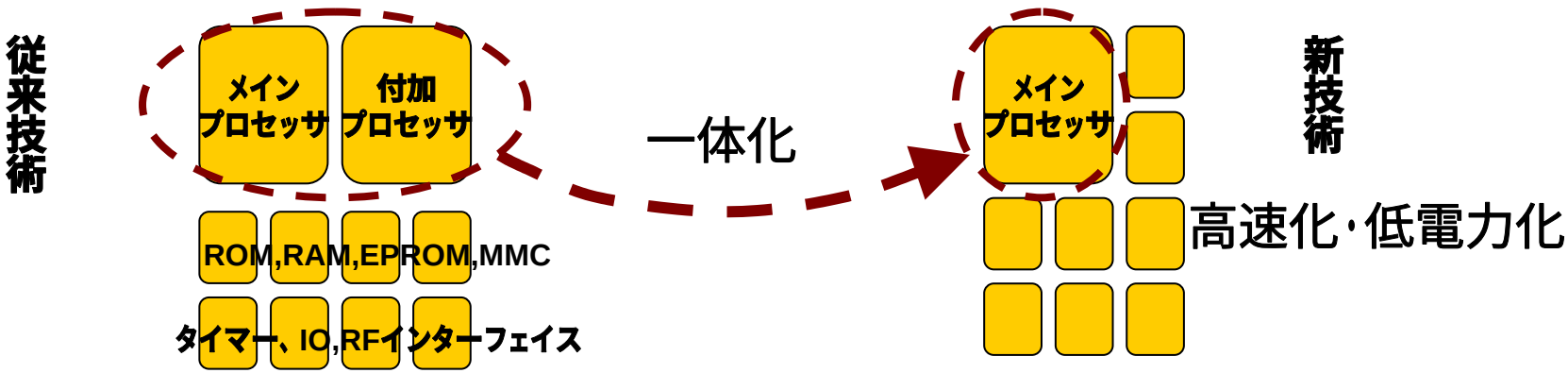
降順バイナリ式べき乗算、モンゴメリ式剰余算

フルH/W 化でなく要素動作を機械語命令化

HW縮小

機械語命令を専用付加プロセッサでなくメインプロセッサへ

更に縮小



2. 認証鍵のガードを強化

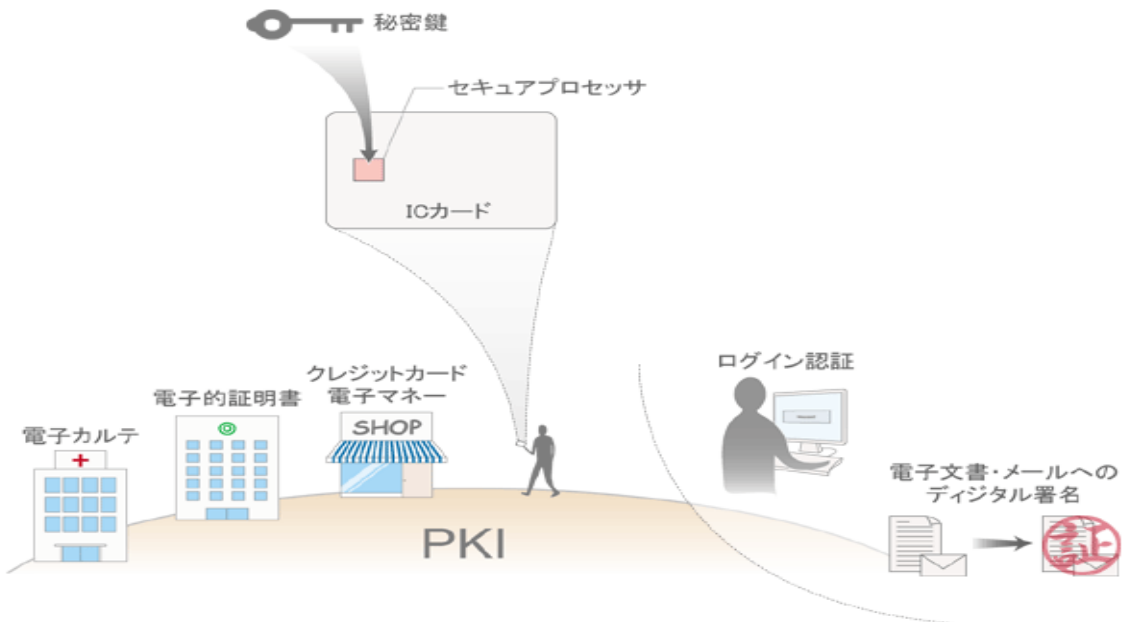
メインプロセッサに万一侵入あっても独自セキュリティモードで防御

スキミング不可能

特許内容

③ 効果-2

セキュリティ機能で署名演算を行うばかりでなく、キャッシュカード機能、クレジットカード機能、改竄防止機能、通行料金支払い機能、予約チケット機能、等々の応用に対して、異なる汎用の応用プログラムをプロセッサの上で走行することにより、対応することができる。



ビジネスプラン

① 商品特徴

品種	語長	ゲート規模	チップ規模	クロック	署名計算時間	消費電力	その他
住基カード					数秒？ 通信含み10数秒	10mw超？	接触
某社カード	32	周辺アナログ含 4,000,000Tr.	0.25μ	13.56MHz	？	デジタル部 10mw	非接触
セキュアプロセッサ SEP-6	64	51,700gate 96端子	0.18μ4.9mm² 試作すみ	13.56MHz	258ms	4.9mw	非接触 ICカード
セキュアプロセッサ SEP-7	16	約14,000見込 48端子	0.18μ2.4mm² 設計中	70MHz	約825ms	約4.0mw	USBトークン目的 設計中
セキュアプロセッサ SEP-8	16	約24,000見込 48端子	0.18μ2.4mm² 計画中	70MHz	約280ms	約7.0mw	おサイフケータイ 目的で計画中

共通特長　強い暗号

小さい

速い

省電力

ビジネスプラン

② 対象市場

色々な場面での電子的個人認証

サーバが、端末側の相手が誰なのか、顔や実印を見ないで、確認する。

ログイン

銀行カード

ETC カード

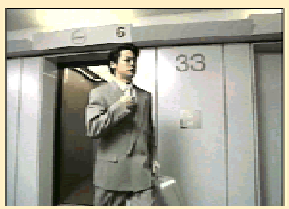
ビジネスプラン

② 対象市場-2

自宅に居ながらいつでもインターネットでオンラインショッピング

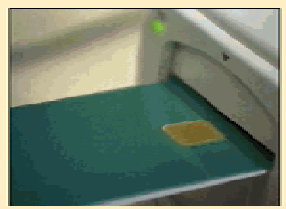
企業内のセキュリティチェックにICカードを利用（不正侵入者排除）

企業内のセキュリティに



セキュリティチェック

インターネットで
オンラインショッピング



オンラインショッピング

ビジネスプラン

③　予想売上高

サービス名	市場		初年度	2年度	3年度
非接触型ＩＣカードの製造と販売	ｶｰﾄﾞ：6億2千万枚発行 ICｶｰﾄﾞ：8400万枚発行 ｶｰﾄﾞ→ICｶｰﾄﾞ： 4億4千万枚市場	販売枚数	1,000枚	1万枚	10万枚
		売上高 (1,000円/枚)	100万円	1,000万円	1億円
	おさいふ携帯市場： 3190万枚				
セキュア・プロセッサの販売	チップ化	個数	1万個	10万個	100万個
		売上高 (200円/個)	200万円	2,000万円	2億円
その他（USBトークンなど）	ﾊﾞｲｵﾒﾄﾘｸｽ、ﾊｰﾄﾞｳｪｱ認証など 14億1000万ﾄﾞﾙ市場	個数	1万個	10万個	100万個
		売上高 (200円/個)	200万円	2,000万円	2億円
売上高			500万円	5,000万円	5億円
当期利益			250万円	2,500万円	2億5千万円

ビジネスプラン

④ 実用化に向けた課題

分類	課題内容	協力希望
SEP本体開発	認証鍵（秘密鍵）のカストマイズ回路の設計	半導体メーカ
SEP周辺開発	RFインターフェイス、電源、クロック、IOポート、の設計	ICカードメーカ
SEP基本ソフト	ICカードを盗難・紛失したときに備える具体的対策	
SEP応用ソフト開発環境	シミュレータ、C-コンパイラ	
SEP応用ソフト	具体的な応用システムの開発	システムメーカ システムユーザ

SEP： セキュアプロセッサ

ビジネスプラン

④ 実用化に向けた課題-2

1. セキュア・プロセッサ搭載ICカード製造販売体制の整備

2. 大手のICカード製造会社に特許権の売り込みとバックアップ体制の整備

3. セキュア・プロセッサの改良と特許出願

4. バイオメトリクス・アプリケーションの需要が高まっている米国での特許取得