ICカード向け暗号機能の開発
Cryptographic Technologies for Smart Cards

小池　正修　KOIKE Masanobu
川村　信一　KAWAMURA Shin-ichi
斯波　万恵　SHIBA Masue

高度情報社会でのセキュリティを担う技術の一端として，ICカードが注目されている。当社は1981年以来CPU内蔵のICカードの研究に取り組んできており，公開鍵(かぎ)暗号方式をはじめとした高いセキュリティ機能を搭載したカードを開発している。このたび，カードで高速に暗号を処理できるコプロセッサを新たに開発した。

新型のコプロセッサは鍵長1,024ビットのRSA(Rivest-Shamir-Adleman)暗号を約410 msで処理できるほか，鍵長2,048ビットにも対応でき，より高いセキュリティを実現できる。また次世代暗号として有力な楕(だ)円暗号の実装に向けた機能も備えているのが特長である。

Smart cards have become an important tool for providing security in today's increasingly computerized society. Toshiba has developed a series of smart cards since 1981. Our smart cards are equipped with excellent security features including public-key cryptosystems.

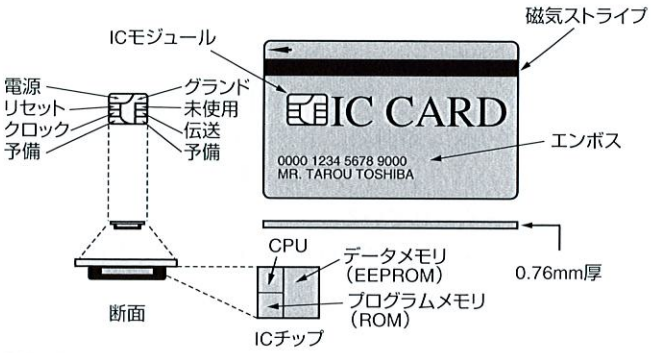
We have now developed a new crypto coprocessor, which requires only about 410 milliseconds to generate a Rivest-Shamir-Adelman (RSA) signature with a 1,024-bit key length. Moreover, RSA signatures with a 2,048-bit key length can be handled. This coprocessor also has functions enabling elliptic curve cryptosystems to be effectively implemented.

1 まえがき

私たちは日常生活で，テレホンカードや銀行のキャッシュカードをはじめとしたさまざまなカードを利用している。これらのカードのほとんどは，プラスチックなどに磁気記録媒体の付いた磁気カードである。磁気カードは記憶容量が70文字程度であること，また情報の読出しやカードの偽造が容易であることから，カード機能の拡張には安全性，記憶容量の面から限界がある。例えば，医療カルテ用に詳細な個人情報を記憶させたり，電子決済用に大きな金額を扱ったりするには記憶容量の不足やセキュリティが弱いといった問題が挙げられる。

これらの問題点を解決するために，ICカードが利用されている。ICカードは，CPUを内蔵しているものと，していないものに大別されるが，内蔵しているものは暗号のプログラムを格納・実行することができるため，高度なセキュリティ機能を実現できる。また，メモリには新聞1ページ分以上の情報を記憶でき，CPUで読書きの管理ができる。ICカードの標準的な構造を図1に示す。

現在のICカードの利用目的は，主に入退出管理のための個人認証などである。しかし，テレホンカードへの利用が始められたほか，今後は鉄道の定期券，または電子決済などでICカードの導入が予定されている。電子決済を例にとると，世界の三大クレジット会社ではクレジットカードのICカード化を決めている。わが国でもICカードを用いた電子マネーの実証実験が97年の神戸，98年の渋谷を代表に各地で行われている。その他の用途向けの実証実験も多く予定されており，ICカード市場は急速に拡大することが見込まれている。



EEPROM：Electrically Erasable and Programable ROM

図1．ICカードの構造　ICカードはCPUとメモリを内蔵し，外部から供給される電源とクロックで動作する。
Structure of smart card

当社も81年からCPU内蔵のICカードの研究・開発に取り組んでおり，前述の神戸，渋谷の実証実験にも積極的に参加している。ICカード技術のなかにはカードの偽造・変造を防ぐための物理的なセキュリティ技術も多くあるが，ここではICカードで暗号機能，特に公開鍵方式を用いた暗号機能を実現するための技術について述べる。

2 暗号技術

2.1 暗号方式

一般に，暗号技術によって実現される機能は大きく次の二つに分けられる。

(1) 通信文の内容を隠す秘匿機能

(2) 通信文の内容や相手の正当性を確認する認証機能

これらの機能を実現するための暗号方式自体も，大きく秘密鍵方式と公開鍵方式の二つに分けられる。どちらの方式にも一長一短があり，それぞれ目的に応じて使い分けられている。秘密鍵方式は高速に処理ができるため，主に通信文の暗号化に使われる。公開鍵方式は秘密鍵方式に比べ処理時間が1,000倍程度掛かるため大量の文書の暗号化には向いておらず，主に秘密鍵方式で用いる鍵の配送やディジタル署名に使われる。

2.2 ICカードへの暗号機能の搭載

ICカードはCPU，メモリをもつという点で普通のパソコン本体と基本構成は同じである。しかし，その規模を見てもわかるとおり，性能には大きな差がある。標準的なICカードチップの性能を表1に示す。

表1．ICカードチップの標準的仕様
Specifications of general smart card chip

項　目	仕　様
CPU	8ビット
RAM	256～1,024バイト
ROM	16～32Kバイト
EEPROM	8Kバイト
動作周波数	5～10 MHz

このように，能力の小さなICカードに実用的に使える暗号機能をもたせるには独特の技術が必要となる。DES(Data Encryption Standard)方式[1]に代表される秘密鍵方式は，ソフトウェアによる実装でも十分実用的な時間で処理ができ，従来のICカードにおいても通信文の暗号化などに利用されている。一方，公開鍵方式は処理が複雑なため，ICカードのCPUだけでは処理時間が掛かりすぎて実用に耐えない。次章では公開鍵方式と，ICカードに実装する際に必要となるコプロセッサ(CPUの機能強化用補助プロセッサ)について概説する。

3 公開鍵方式とコプロセッサ

3.1 公開鍵方式

これまでに，さまざまな公開鍵方式の暗号が提案されている。利用されている方式の多くは，解くのに天文学的な時間の掛かる数学の問題に安全性の根拠を置いたものである。現在の主流は素因数分解の難しさによるものと，離散対数問題によるものの二つである(図2)。それぞれRSA方式[2]，DSA(Digital Signature Algorithm)方式[3]が代表的な方式で，DFS(事実上の標準)となっている。

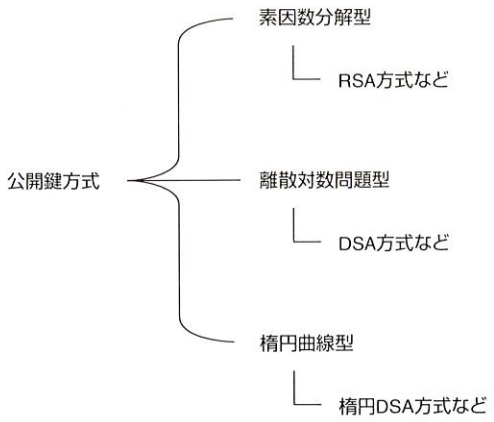


図2．公開鍵方式の系統　現在の公開鍵方式の主流は三つのタイプに分けられる。
Types of public-key cryptosystems

これらの方式での処理の大部分はべき乗剰余算

$$C = M^d \bmod N \qquad (1)$$

に費やされる。ここでM, Nなどの変数のビットサイズは暗号の安全性と深い関係があり，不正解読を防ぐためには大きくとる必要がある。そのためNのビットサイズを鍵長と呼ぶ。

従来，RSA方式では鍵長512ビットのものが広く使われてきた。しかし，コンピュータの性能の向上と解読手法の研究の進展から解読時間が短くなってきたため，現在では1,024ビットが必要とされている。ところが，鍵長の増加は安全性を向上させると同時に正規の利用者の暗号化処理時間も大きく増加させる。携帯して使うICカードでは特に暗号化処理のリアルタイム性が要求されるため，べき乗剰余算(1)式をいかに高速に処理するかが重要な課題となる。しかし，ICカードのCPUだけでは(1)式の処理をするのに数十秒掛かってしまうのが現状である。

そこで，ICカードのチップ内にCPUの処理を補助する専用の処理回路を入れて，処理時間を小さくする技術が用いられている。この専用の処理回路をコプロセッサと呼ぶ。

3.2 コプロセッサ

コプロセッサは暗号自体の処理を行うものではない。暗号処理の流れのなかで用いられる四則演算やべき乗剰余算などの個々の演算を行う回路である。ICカードのCPUから演算コマンドを受け付け，計算結果をCPUに返すという役割をもつ(図3)。個々の演算を組み合わせた上位機能はファームウェアで実現する。

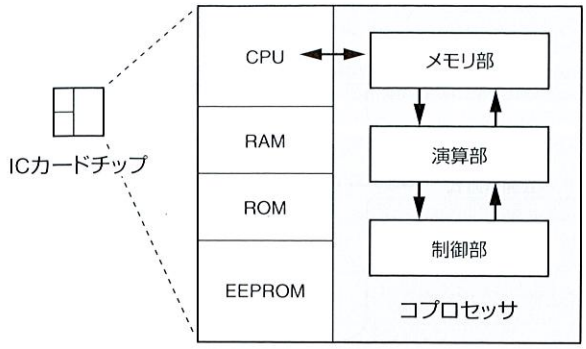


図3．コプロセッサの構成　　コプロセッサはメモリ部，演算部，制御部から構成され，ICカードCPUの処理を補助する。

Configuration of coprocessor

コプロセッサの性能を評価する項目として，次の四項目が挙げられる。

(1) チップサイズ　　カードの曲げなどからチップの割れを防ぐため，コプロセッサを含めたICカードチップ全体で5 mm×5 mmに収まる必要がある。また，カードの価格の面からもチップサイズは小さいほうが望ましい。

(2) 扱える演算の種類　　ハードウェア的に回路を準備することでの処理の高速化，ファームウェアを開発するときの利便性に関係する。

(3) 扱える整数のビットサイズ　　ファームウェアの対象となる暗号方式の鍵長，すなわち暗号の強度につながるため大きいほうが望ましいが，チップサイズや処理速度からの制約を受ける。

(4) 処理速度　　コプロセッサの性能をもっとも端的に表す項目である。通例べき乗剰余算の処理時間が比較対象とされる。当社は(1)式が0.5 s程度，また有力な暗号方式が1 s以内で処理できることを目ざした。

カードの性能を決めるこれらの要素は独立に決められるわけではなく，それぞれ互いに関係している。どのようにするかを決めるのは各メーカーの裁量である。

4 新型コプロセッサ

当社では，今までに鍵長512ビットのRSA暗号を実用的な時間内に処理できるコプロセッサを開発している。今回，新たに鍵長1,024ビットのRSA暗号と，後述する楕円暗号を扱うことを見据えたコプロセッサを開発した。新型コプロセッサの性能について述べる。

(1) サイズ　　コプロセッサを含めたICカードチップ全体で3 mm×5 mmに収まる。これは前章の要求を十分満足する大きさである。

(2) 扱える演算の種類　　四則演算，べき乗剰余算のほかに剰余乗算，モンゴメリ乗算，拡張ユークリッド互除法による逆元計算など豊富な種類を扱える。最初の三種類の演算は，RSA暗号など従来の暗号を実装する際に必要となる基本的な演算である。最後の二種類の演算は楕円暗号を実装する際に有効なものである。

(3) 扱えるビットサイズ　　すべての演算が1,024ビットまで，加減除算は2,048ビットまで扱える。これは多くの有力な公開鍵方式を安全な鍵長で実装するのに十分な長さである。

(4) 処理速度　　図4から読み取れるように，鍵長1,024ビットのRSA暗号を約410 msで処理できる。中国剰余定理(注1)を用いて高速化した場合には約130 msで完了する。さらに鍵長2,048ビットのRSA暗号にも対応できて，中国剰余定理を用いて約830 msで処理できる。この処理速度は世界トップクラスといえる。

ここではRSA方式を例に述べたが，多倍長整数の演算で実現される公開鍵方式の暗号は，このコプロセッサを用いて容易に実装することができる。

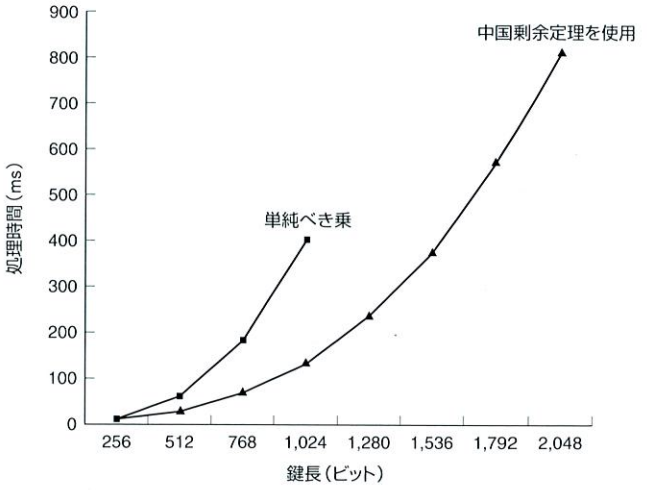


図4．RSA暗号処理時間　　上側はべき乗剰余算だけを用いた場合を示す。下側は中国剰余定理を用いた場合で処理速度を大幅に向上できる。

Computation time for RSA

5 楕円暗号

現在主流のRSA方式，DSA方式では，安全性の根拠においている素因数分解，離散対数問題の解法の研究が進んでいるため鍵長が増加傾向にある。しかも，この増加は2,048ビット，4,096ビットと加速的である。

(注1)　余り(剰余)演算を高速で行うアルゴリズムの一種。

表2．楕円DSA方式とRSA方式の比較
Comparison of elliptic curve digital signature algorithm（DSA）and RSA

項　目	楕円DSA	RSA
安全性の根拠となる問題	楕円曲線上の離散対数問題	素因数分解
現在の標準的鍵長	160ビット	1,024ビット
処理時間*	小	大
プログラムサイズ*	大	小
歴史*	浅い	深い

＊：相対的な比較を示す。

これに対し，85年に新たな方式として楕円暗号が提案された。楕円暗号は楕円曲線における離散対数問題に基づいた方式の総称である。RSA方式やDSA方式への強力な解読法が適用できないことに加え，一般の楕円暗号自体の有効な解読法が見つかっていないため，暗号に使うパラメータを適正に選べば比較的小さな鍵長で安全性の確保ができる。具体的には，鍵長1,024ビットのRSA暗号と同程度の安全性を160ビットで実現できる。また，暗号強度を上げるための鍵長の増分がRSA方式よりはるかに小さい。以上のメリットから楕円暗号は次世代の暗号方式として有望視されている。楕円暗号とRSA暗号との比較を表2に示す。

楕円暗号を実現する方式は，楕円曲線の定義体の違いから素体版と2の拡大体版に分けられる。楕円曲線の定義体とは，楕円暗号での処理に用いる演算体系を定めるものである。

5.1　素体版楕円暗号

素体とは，素数pに対し整数をpで割った余り，すなわち0, 1, 2,…，$p-1$からなる数の体系である。素体版楕円暗号は素体の元の四則演算で構成されており，素数pのビットサイズを鍵長と呼ぶ。

このように，素体版楕円暗号は多倍長の整数演算が基本演算となるので，新型コプロセッサを利用することができる。

当社は，素体版楕円暗号へモンゴメリ演算を適用することで処理の高速化を図る方法を提案している[4]。この手法での実装を考え，前章で述べたように新型のコプロセッサにモンゴメリ乗算と拡張ユークリッド互除法による逆元計算を演算コマンドとして用意した。その結果，剰余乗算，逆元計算はともに約2.5倍高速化され，楕円暗号のなかでも標準的な楕円DSA署名を署名生成が約130 ms，署名検証が約580 msで処理できる見通しである。

5.2　2の拡大体版楕円暗号

2の拡大体での元は，2進数を係数とするn次未満の多項式を指す。2の拡大体版楕円暗号はこのような多項式の四則演算で構成されており，nを鍵長と呼ぶ。

したがって，2の拡大体版での演算は今まで述べた暗号方式の演算とは大きく異なっている。ハードウェア的な回路も通常シフトレジスタが用いられ，整数演算に用いる乗算器とともに，この回路もICカードチップに載せるにはサイズ的に困難である。

当社では，前節までに述べた整数演算ができるコプロセッサに少しの回路を付け加えることで，2の拡大体版楕円暗号も扱える方法を提案している[5]。

6　あとがき

ICカードは，今後のカード社会になくてはならない技術の一つである。当社の新型コプロセッサは，現在主流の鍵長1,024ビットのRSA暗号と次世代有力暗号の楕円暗号を実用的な時間で処理でき，ICカードで高いセキュリティを実現することができる。

しかし，現在の技術や安全性の基準は将来も有効であるわけではなく，数年のうちに陳腐化することになる。そのため，より優れた技術を求めて研究・開発を継続していく必要がある。

文　献

(1) Data Encryption Standard, National Bureau of Standard, Federal Information Processing Standards Publications, 1977.
(2) Rivest, R. L., et al. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, **21**, 2, 1978, p.120-126.
(3) Proposed Federal Information Processing Standard for Digital Signature Standard（DSS）, Federal Resister, **56**, 169, 30, 1991, p.42980-42982.
(4) 新保　淳．“楕円曲線暗号へのモンゴメリ演算の適用”．暗号と情報セキュリティシンポジウム．電子情報通信学会．福岡，1997-01，電子情報通信学会情報セキュリティ研究専門委員会．1997, 14 D.
(5) 斯波万恵，他．“GF(2^m)演算及び整数演算を処理可能なハイブリッド・コプロセッサの提案”．暗号と情報セキュリティシンポジウム．電子情報通信学会．神戸，1999-01，電子情報通信学会情報セキュリティ研究専門委員会．1999, p.819-824.

小池　正修　KOIKE Masanobu
情報・社会システム社 SI技術開発センター SI技術担当。暗号・情報セキュリティの研究・開発に従事。情報処理学会会員。
System Integration Technology Center

川村　信一　KAWAMURA Shin-ichi, D.Eng.
研究開発センター コンピュータ・ネットワークラボラトリー主任研究員，工博。暗号・情報セキュリティの研究・開発に従事。電子情報通信学会，IEEE, IACR会員。
Computer & Network Systems Lab.

斯波　万恵　SHIBA Masue
情報・社会システム社 SI技術開発センター SI技術担当。暗号・情報セキュリティの研究・開発に従事。電子情報通信学会会員。
System Integration Technology Center