楕円曲線暗号

Elliptic Curve Cryptosystems

あらまし

次世代の公開鍵暗号として注目されている楕円曲線暗号について，その概要と富士通研究所の取組みについて述べる。

楕円曲線暗号は，1985年に発明された暗号で，公開鍵暗号のデファクトスタンダードであるRSA暗号に比べ，より短い鍵長で同等の安全性を提供できる暗号である。鍵長が短いため，高速処理が可能であり，またハードウェア実装を行った場合に，より小規模な実装が可能である。本稿では，まず楕円曲線暗号の原理について概要を述べ，代表的な署名アルゴリズムを紹介する。つぎに，楕円曲線暗号の安全性と最新の攻撃法に関して概要を述べる。最後に，富士通研究所で取り組んでいる安全な楕円曲線暗号のパラメタ生成技術，およびソフトウェアとDSPによる楕円曲線暗号の高速演算エンジンの実装結果について述べる。今後，楕円曲線暗号は，広く電子情報を用いたサービスの基盤技術として利用されていくと思われる。

Abstract

This paper describes elliptic curve cryptosystems (ECCs), which are expected to become the next-generation public key systems. This paper also describes Fujitsu Laboratories's studies of ECCs.

The ECC was invented in 1985. It requires a shorter key length than the RSA crytopsystem, which is the defacto standard of public key cryptosystems, but provides equivalent security. Because of the shorter key length, ECC can be implemented with less processing time and less hardware.

First, we outline the principle of ECC, and describe a typical digital signature algorithm. To explain the security of ECC, we also report on the latest attacks on ECC. Then, we describe the results of our study concerning safe parameter generation for ECC and the fast implementation of ECC using software and a digital signal processor (DSP).

We think that ECC will be used widely as a base technology of electronic information services.

鳥居直哉（とりい　なおや）

1983年大阪大学大学院工学部通信工学科博士課程前期了。同年(株)富士通研究所入社。以来，音声スクランブラ，各種暗号アルゴリズムの高速実装，鍵管理システムなど，情報セキュリティ関連の研究開発に従事。
コンピュータシステム研究所セキュアコンピューティング研究部

横山和弘（よこやま　かずひろ）

1983年東京大学大学院理学系研究科修士課程専攻了。1985年同大学院博士課程２年中退，同年富士通国際情報社会科学研究所入社。以来，数式処理とその応用(数学，工学)に従事。理学博士(1991年)，日本数式処理学会監事。
コンピュータシステム研究所セキュアコンピューティング研究部

楕円曲線暗号

ま え が き

オープンなネットワークで展開する電子情報を使用した各種サービス，すなわち電子商取引，音楽や映像などの電子情報販売，およびCALS/EDIなどは，今後広く社会に浸透し，より豊かで効率的な生活を提供する手段として大いに期待されている。これらの各種サービスに不可欠な基盤技術が暗号技術である。暗号技術には，送信者と受信者が同じ鍵を使用する共通鍵暗号と異なる鍵を用いる公開鍵暗号がある。公開鍵暗号系として代表的なものは，1978年に発明されたRSA暗号[(1)]と1984年に発明されたエルガマル暗号[(1)]がある。

楕円曲線暗号は，1985年にKoblitz博士[(2)]とMiller博士[(3)]とにより独立に発明された暗号技術であり，次世代の公開鍵暗号として注目されている。実用化に向けてISO，IEEE，ANSI，IETFなどの標準機関でも積極的に標準化作業が行われている。一方で，安全性に関する研究活動も盛んに行われている。

本稿では，最先端の暗号技術である楕円曲線暗号について，その概要と富士通研究所の取組みについて概説する。

楕円曲線暗号

● 公開鍵暗号

公開鍵暗号とは，暗号用の鍵と復号用の鍵が異なる暗号である。暗号通信するためには，送信者は，暗号用鍵(公開鍵)をもち，受信者は復号用鍵(プライベート鍵)をもつ。公開鍵から，プライベート鍵を導き出すには莫大な計算を必要とし，実用上不可能であるように設計される。公開鍵暗号では，受信者の公開鍵を知っていれば，暗号通信のための秘密の鍵を送受信者間で共有しなくても暗号通信が行える。つまり，受信者のプライベート鍵を送信者に通知することなく暗号通信ができるために，不特定多数との通信に向いているといわれている。

また，公開鍵暗号は，ディジタル署名に適している。例えばRSA暗号を用いた署名では，メッセージの署名として，そのメッセージをプライベート鍵で暗号化したものを署名データとする。署名の確認には，公開鍵で署名データを復号し，メッセージと比較し，同じかどうか確認することで署名の確認が行える。本処理により，公開鍵に対応するプライベート鍵を持ったユーザがメッセージの変換を行ったこと，および署名を行ったメッセージに改ざんがないことが確認できる。公開鍵暗号による署名は，署名者のプライベート鍵を知らなくても公開鍵があれば署名確認ができることが特徴である。

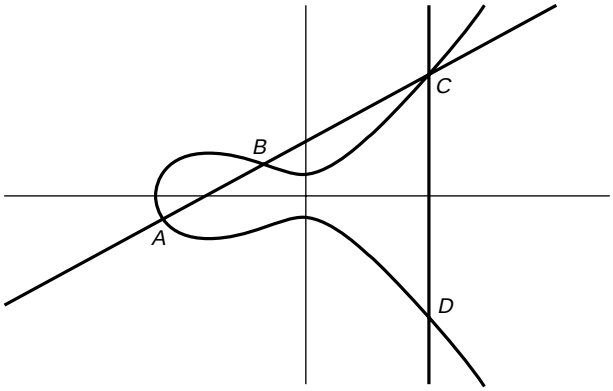

図-1　楕円曲線上の点の加算
Fig.1-Addition rule over the elliptic curve.

公開鍵暗号は，プライベート鍵を明かさずに暗号通信やディジタル署名が可能であるため，不特定多数の情報が行き交うオープンなネットワークでの安全な通信や相手認証やデータの認証のために必須の暗号技術の一つといえる。

● 楕円曲線

楕円曲線暗号は，楕円曲線における有理点の加算を用いた暗号系である。暗号に用いられる楕円曲線は，素数q (>3)で決められる素体 {GF(q)} 上の楕円曲線とよばれ，以下の式で表現される。

$$E: y^2 \equiv x^3 + ax + b \bmod q$$

ここで，a，$b \in GF(q)$であり，$4a^3 + 27b^2 \neq 0$を満たしている。また，mod qとは，qで割った余りを表わすこととする。

楕円曲線上の有理点とは，上記方程式を満たすGF(q)上の点であり，{a，b，q}が決まれば，上記楕円曲線上の点の数は決まる。これを曲線の位数と呼び，#Eで表す。有理点の集合全体は以下で定義する加法について群をなすことが知られている(曲線の位数はこの群の位数である)。

曲線上の加法を定義する(図-1)。曲線上の点Aと点Bを足した点Dは，点A，Bを結ぶ直線が再び曲線と交わる点(C)のy座標の符号を反転した点で定義される。点A，Bが同じ点である場合は，その点での接線を引く。また，楕円曲線上の点として無限遠点O = (∞，∞)も定義する。無限遠点とある点Pの加算結果は，点Pになると定義する。

ある決められた楕円曲線上の点Gがある場合に，その点を上記の方法でk回加算した結果，点Wが得られたとする。これをGのスカラ倍と呼ぶ。kとGからWは計算により容易に求まるが，GとWからkを求めるのは困難である。素数qの大きさを160ビット程度に選べば，現在知られている最も効率の良いアルゴリズムを用い，最新のコンピュータで計算しても現実的な時間で解は求まら

ない。点Gと点Wが与えられたときにkを求めることを楕円曲線上の離散対数問題という。楕円曲線暗号は，この「楕円曲線上の離散対数問題」を用いて構成される暗号である。

また，楕円曲線上の点Gが与えられたとき$nG = O$となる正の整数nが存在する。このような(最小の)nを点の位数と呼ぶ。nは曲線の位数の約数となる。

楕円曲線は，素体のほか，GF(2)の拡大体上の曲線についても実現可能で標準化されつつある。

● 署名アルゴリズム

楕円曲線上の離散対数問題を利用して通信相手の公開鍵を用いて秘密鍵を共有するための鍵配送アルゴリズム，メッセージの秘匿のための暗号アルゴリズム，メッセージの改ざん検出，および署名者の認証を行うための署名アルゴリズムを実現することができる。ここでは，例として署名アルゴリズム(ECDSA[4])を示す。

署名アルゴリズムは，送信者がメッセージmに署名を行い，受信者Bが署名確認を行うためのアルゴリズムである。メッセージ全体に署名処理を行う代わりにハッシュ関数$h()$を用いてデータを固定長に圧縮する。

楕円曲線暗号では，システム共通のパラメタとして素数q，曲線パラメタ(a，b)，基準となる曲線上の点$G = (x, y)$，点Gの位数rがある。これらは，通信に際して相互に知っているものとする。

【準備】

送信者は，プライベート鍵Sと公開鍵Wを作成する。

(1) 乱数s ($1 \leqq s \leqq r - 1$)生成

(2) 公開鍵生成$W = sG$の計算を行う

【署名作成】

(1) メッセージのハッシュを計算し，ハッシュ値$f = h(m)$を得る

(2) 乱数u ($1 \leqq u \leqq r - 1$)生成

(3) $V = uG = (x_v, y_v)$を計算し，$c = x_v \bmod r$とする

(4) $d = u^{-1}(f + sc) \bmod r$を計算する

(5) mの署名として(c, d)を出力

送信者は，メッセージm，署名(c, d)，公開鍵Wを送る。

【署名確認】

受信者は，受信したメッセージm，署名(c, d)，公開鍵Wを用いて以下の計算を行う。

(1) ハッシュ計算$f = h(m)$

(2) $h = d^{-1} \bmod r$

(3) $h_1 = fh \bmod r$，$h_2 = ch \bmod r$

(4) $P = h_1 G + h_2 W = (x_P, y_P)$，$c \fallingdotseq x_P \bmod r$

(5) $c = c$なら“有効”，そうでないなら“無効”を出力

● 特徴

楕円曲線暗号のメリットは，公開鍵暗号のデファクトスタンダードであるRSA暗号に比べ短い鍵長で同等の安全性が確保できることである。そのため高速処理が可能であり，またハードウェアを実装した場合も，より小規模で実現可能である。ただし，楕円曲線暗号の安全性は，鍵の長さだけでなく曲線パラメタの選択に大きく左右される。よって楕円曲線暗号の実現のためには，安全な曲線パラメタを用いた高速実装が不可欠である。以下では，これらについての取組みを述べる。

安　全　性

● 暗号の安全性

一般に暗号の安全性は，その暗号を破る(解読する)のに必要な計算時間で評価される。暗号を「破る」というのは，暗号に使われている鍵(秘密鍵)を見つけることで，「破る方法」をここでは「攻撃法」と呼ぶことにする。「暗号を破るのに必要な計算時間」というのは実測値ではない。なぜなら実測できるということは，その暗号は破れたことを意味しているため，そのような暗号は危険なので使用されないからである。では，実測できない「暗号を破るのに必要な計算時間」はどういうものかというと，ある「攻撃法」を選択した場合の計算量から算出する期待値なのである。複数の「攻撃法」がある場合は，その中のもっとも計算時間の少ないものを用いてその暗号の安全性を評価する。計算時間が期待値であるため平均量であり，この評価方法では特殊な場合の安全性は評価できない。

● 楕円曲線暗号の一般的安全性

楕円曲線暗号の安全性は前述したように「楕円曲線上の離散対数問題」に依っている。「楕円曲線上の離散対数問題」の解法は一般的離散対数問題の解法である平方根法と，曲線の位数を素因数分解して小さな離散対数問題に帰着させるPHS法(Pohlig-Hellman-Silverman法)を利用した攻撃法しか見つかっていない。[5]

平方根法は，最も汎用的な解法で，その計算時間は鍵のビット長の半分のべき乗に比例する時間が必要である(つまり，指数時間が必要となる)。公開鍵暗号の攻撃に必要な計算時間が指数時間であることは，非常に安全であると言われている。

PHS法は，曲線の位数が小さい素因数の積の形で表されるときに効率的に「離散対数問題」を解くことが可能になる。逆に位数が素因数分解されない場合にはその計算量は平方根法と同等になる。そこで，楕円曲線暗号に使

用する曲線の位数を素数かほぼ素数(素因数に大きな素数が含まれる)にすれば，楕円曲線暗号への攻撃に必要な計算時間は指数時間となり，非常に高い安全性が確保できることになる。

ここで現在のデファクトスタンダードであるRSA暗号の安全性と比較してみる。RSA暗号の安全性は大きな整数の素因数分解に依っている。大きな素因数分解には数体ふるい法と呼ばれる効率的な攻撃法が存在し，そのためRSA暗号への攻撃に必要な計算時間は準指数時間となる。準指数時間とは計算が容易とされる多項式時間と大変困難とされる指数時間の中間に位置するもので，数体ふるい法の場合には鍵のビット長の３乗根のべき乗にほぼ比例するもので，同じ鍵長の場合，指数時間より効率的に計算できる。1,024ビットRSA暗号と160ビット楕円曲線暗号は同等の安全性をもつと言われているのは，このためである。

● 特殊性を利用した攻撃と安全性

楕円曲線暗号の一般的な安全性評価について述べてきたが，前述したとおりこれはあくまで平均量であり，この評価方法では特殊な場合の安全性は評価できない。実際，極めて特殊な楕円曲線に対して，その特殊性により，平方根法より効率的な攻撃法が見つかっている。[5]

楕円曲線の位数の性質を表す指標の一つにtraceと言うものが存在する。このtraceの値が０～２と極めて小さい場合，その特性を利用した攻撃法が存在し，それらを用いると，前節の攻撃法より非常に効率的に計算することが可能となる。

● 安全な曲線の生成

上記より，楕円曲線暗号に使う安全曲線として，

(1) 曲線の位数が素数，またはほぼ素数であること

(2) 特殊な曲線にならない(とくにtraceは０～２にはならない)

ことが必須である。これらの条件は皆，曲線の位数#Eに関する条件であり，安全な曲線は位数計算により判定できる。

安全な曲線の生成では，現在二つの方法が提案されている。

(1) 曲線をランダムに選び，その位数を計算し，上記の条件を満たすものを探す方法

(2) あらかじめ，条件を満たす良い位数を計算し，その位数になるような曲線を構成する方法

(1)項の位数計算にはSchoof法と呼ばれる方法が使用される。Schoof法の計算量は理論的には多項式時間であり，計算可能である。しかし実際に計算する場合，非常に時間がかかるという問題があった。

表-1 パラメタ生成時間

	GF(2)の拡大体(多項式基底)		素体（$p = 2^a - \alpha$のもの）	
ビット長	160	239	160	224
生成時間(秒)	266	3,783	367	2,566

(2)項では虚数乗法法(CM法)とよばれる方法が使用される。CM法の一般解法の計算には指数時間必要で，計算不可能である。そこで使用する曲線の位数を特殊な形にすることで，計算可能にする方法が知られている。しかし，前節の例が示すように，位数が特殊な曲線を生成することは，特殊性を利用した攻撃法が見つかる可能性が高く，(2)項の方法で生成された曲線がその特殊性により今後も安全かどうかに問題が残る。そこで著者らは，Schoof法を高速化することで(1)項の方式を実現した。

● 楕円曲線の安全なパラメタ生成技術

著者らは，Schoof法の高速化に取り組み，新たな改良であるIC法により，素体，GF(2)の拡大体ともに現在使用されている160～240ビットの楕円曲線暗号に使われる曲線の実用的な時間での生成を実現した。[6), (7] 表-1には，PentiumII 400 MHz，Windows NT 4.0，Risa/Asirの環境での測定結果を示している。これにより，安全なパラメタを必要な数だけ生成できることになり，楕円曲線暗号を用いたシステム構築がより容易になったと考える。

高速エンジン

楕円曲線暗号の実用化にあたり，とくに高速な実装が必要とされるサーバ向けエンジンとして高速な楕円曲線暗号エンジンの開発について述べる。

● ソフトエンジン

楕円曲線暗号の実装については，従来から様々な高速手法が提案されており，基本的な関数のアルゴリズムについては各種標準にも記述されている。

富士通研究所では，サーバ向けに様々な楕円曲線パラメタに対応可能なソフトエンジンを開発した。これはIEEE P1363 draft[4]の楕円曲線暗号に準拠しており，基礎体として素体，GF(2)の拡大体(正規基底，多項式基底)のすべてに対応している。また，メモリの許す限りの任意のビット長の楕円曲線暗号アルゴリズムを実現可能であり，取りうるすべてのパラメタに対応可能な汎用のソフトエンジンである。このソフトエンジンの処理性能を表-2に示す。これは，Pentium Pro 200 MHz Windows NT 4.0の環境で測定したものである。エンジン開発に当たっては，シンプルかつ高速実装可能な独自の各種高速化手

表-2　ソフトライブラリ処理性能

基礎体	素　体		GF（2）の拡大体（多項式基底）		GF（2）の拡大体（正規基底）	
鍵長(ビット)	160	239	163	239	162	191
署名作成(ms)	4.1	10	8.4	17	7.7	10
署名確認(ms)	18	43	34	66	30	37

表-3　ハードエンジン諸元

DSP			TMS320C601
処理クロック			200 MHz
ファームサイズ			32 Kバイト
処理性能	署名作成	160 ビット	1.1 ms
		239 ビット	2.7 ms
	署名確認	160 ビット	3.8 ms
		239 ビット	10 ms

法を開発し搭載している。

● ハードエンジン

サーバ向け高速ハードエンジンとしてDSP(Digital Signal Processor)による高速エンジンも開発している。[8] これは，素体上の楕円曲線暗号を実現するハードエンジンであり，ソフトライブラリと同様，任意の楕円パラメタに対応可能であり，最大320ビットまでの任意のビット長の楕円曲線暗号に対応可能である。本エンジンの諸元を表-3に示す。

今後の課題

近年，特殊性を利用した攻撃法が次々に発見されており，「特殊な曲線」の安全性の議論が盛んになっている。とくに，CM法で生成した曲線の安全性の検討を行う必要があると考える。さらに，今までの安全性の根拠は耐攻撃に関するものであり，今後も新たな攻撃法が発見されるたびに評価が変わっていくことが予想される。このため，未知の攻撃にも対処できる理論的な評価法が望まれている。

一方，楕円曲線暗号が広く用いられるためには，標準的な枠組みが重要になってくる。電子商取引プロトコルや各種暗号通信のための楕円曲線暗号の標準的な仕様やフォーマットなど，今後の議論が待たれる。

む　す　び

次世代の公開鍵暗号系として注目されている楕円曲線暗号について概要を述べた。楕円曲線暗号は，安全性の評価が完全に固まったわけではないが，ハード実装時のコンパクト性，高速の処理性能により，今後様々な分野で広く用いられると考えられる。

参考文献

(1) 小山ほか：現代暗号理論．初版，東京，社団法人電子情報通信学会，1986.
(2) N. Koblitz：Elliptic curve cryptosystems．Mathematics of Computation．48，pp.203-209(1987)．
(3) V. Miller：Use of elliptic curves in cryptography．Advances in Cryptology-CRYPTO '85，Lecture Notes in Computer Science，218，1986，Springer-Verlag，pp.417-426.
(4) IEEE P1363/D9(Draft Version 9) Standard Specifications for Public Key Cryptography．1998.
(5) 岡本ほか：楕円曲線暗号の安全性について．情報処理，39，12，pp.1252-1257(1998)．
(6) T. Izu，J. Kogure，M. Noro，K. Yokoyama：Efficient implementation of Schoof's algorithm．Advances in Cryptology-ASIACRYPT '98，Lecture Notes in Computer Science，1514，1998，Springer-Verlag，pp.66-79.
(7) 伊豆ほか：安全な楕円曲線暗号パラメータ設計（標数２の場合）．F1-1.2，1999年暗号と情報セキュリティシンポジウム，1999，pp.779-784.
(8) 伊藤ほか：DSPを用いた楕円曲線暗号の高速実装．T3-1.6，1999年暗号と情報セキュリティシンポジウム，1999，pp.591-596.