解　説

数論アルゴリズムとその応用

暗号理論への応用†

黒澤　馨††　藤岡　淳†††　宮地充子††††

1. まえがき

現代暗号理論は，公開鍵暗号の誕生以来，初等整数論を軸に，急激な発展をとげてきた．素因数分解あるいは離散対数問題を基に，巧みに，公開鍵暗号，ディジタル署名あるいは真の乱数と多項式時間では区別不可能な擬似乱数など，新しい概念およびその実現法が，続々と発表されている．最近は，有限体上の楕円曲線上に定義される群構造に基づく公開鍵暗号に関する研究も盛んである．

本論文では，これらのうち，公開鍵暗号とディジタル署名（3. 藤岡），擬似乱数（4. 黒澤），および楕円曲線（5. 宮地）について解説する．

誌面の都合上割愛せざるえなかったが，ほかにも素因数分解と暗号解読の等価性が証明された公開鍵暗号[15)~17)]，選択平文攻撃に対する安定性の証明されたディジタル署名[18)]，collision free であることが証明されたハッシュ関数[19)]，秘密分散法[20)]など，興味あるテーマはつきない．本論文を通じ，数論が織りなす現代暗号理論のおもしろさを感じていただければ，幸いである．

2. 初等整数論の基礎事項

2.1 記　法

本稿では，以下の記法を用いるものとする．

PRIME：奇素数の集合

$a\in_R A$：集合 A から要素をランダムに選ぶ

Z_P：0以上 p 未満の整数の集合（$=Z/pZ$）

Z_p^*：Z_p かつ p と互いに素な整数の集合（$=(Z/pZ)^*$）

$|a|$：a のビット長

$[a]$：a 以下の最大の整数

$[a]$：a 以上の最小の整数

$a|b$：a は b を割り切る

GCD (a, b)：a と b の最大公約数

LCM (a, b)：a と b の最小公倍数

$\varphi(x)$：x の Euler 関数[1)]

$\lambda(x)$：x の Carmichael 関数[1)]

特に，$x=pq(p, q\in$ PRIME$)$ のときは，

$\varphi(x)=(p-1)(q-1)$

$\lambda(x)=\mathrm{LCM}(p-1, q-1)$

であることに注意されたい．

2.2 定義・定理

[フェルマーの定理]　p を素数とする．0でない任意の整数 $\alpha\in Z_p$ に対し，

$$a^{p-1} \bmod p=1$$

が成立する．

定義 **2.1**　任意の整数 m に対する Carmichael 関数は，以下のように定義される．整数 m が $m=2^{a_0}p_1^{a_1}\cdots p_r^{a_r}$（ただし，$p_1, \cdots, p_r$ は互いに異なる奇素数とする）のように因数分解されるときに，

$$\lambda(m)=\mathrm{LCM}(\lambda(2^{a_0}), \varphi(p_1^{a_j}), \cdots, \varphi(p_r^{a_r}))$$

$$\lambda(2^t)=\begin{cases}2^{t-1} & \text{if } t<3\\ 2^{t-2} & \text{if } t\geq 3\end{cases}$$

として与えられる．

定理 **2.1**　すべての $a\in Z_m^*$ に対して，

$$a^{\lambda(m)}\equiv 1 \pmod m$$

が成立する．

2.3 困難な問題

[素因数分解]

p, q を素数とし，$n=pq$ とする．p, q から n は多項式時間で容易に求めることができる．しかし，n から p, q を求める問題は多項式時間では

† Applications ot Modern Cryptology by Kaoru KUROSAWA (Department of Electrical and Electronics Engineering Tokyo Institute of Tcchnology), Atsushi FUJIOKA (NTT Network Information Systems Laboratories) and Atsuko MIYAJI (Matsushita Electric Industrial Co. Ltd. Communication Systems Reserch Laboratory).

†† 東京工業大学工学部電気・電子工学科
††† NTT 情報通信網研究所
†††† 松下電器産業(株)

解けない，と広く信じられている．

[離散対数問題]

p を素数，g を mod p における原始根とする．すると，任意の $y(1<y<p)$ に対しある $x(0\leq x<p-1)$ が存在し，

$$y=q^x \bmod p \qquad (1)$$

と書ける．ここで，(p, q, y) から x を求める問題を離散場数問題という．この問題も多項式時間では解けない．と広く信じられている．

3. 素因数分解・離散対数問題に基づく公開鍵暗号法

3.1 暗号・署名の原理

ここでは，数論アルゴリズムの有力な応用分野である情報セキュリティの各手法について実際例を中心に概説する．

ここで実現される方式は，鍵共有方式・暗号方式・署名方式の三つである．これらはともに，『公開鍵方式 (public key system)』と呼ばれる手法に基づいている．具体的には，素因数分解・離散対数問題などが用いられ，ユーザは，秘密鍵 (secret key) SK から公開鍵 (public key) PK を作成する．このとき，PK から SK を求める問題が，素因数分解問題であったり，離散対数問題であったりする．そして，PK を自分の公開鍵として公開し，SK を自分のみが知っている値として秘密にしておく．

《秘密鍵》SK

《公開鍵》PK

3.1.1 鍵共有方式

通信における情報の秘匿性を実現する最も重要な手段は暗号である．これは，単純には，送信者と受信者が秘密の鍵を共有することで実現できる．すなわち，鍵 K を共有している二者の間では，E を暗号化変換，D を復号化変換とし，平文 M と暗号文 C を，

$$C=E(M, K)$$
$$M=D(C, K)$$

のように変換することにより，暗号通信を行うことができる[2]．

しかしながら，ここで注意すべき点は，暗号通信を行う際には事前に鍵を共有している必要があることである．すなわち，暗号通信を行うためには，なんらかの手段で鍵の共有を実現しなければならない．

ここで数論アルゴリズムをうまく利用することにより，通信において鍵の共有が実現できる方法が示されている．これを鍵共有方式 (key distribution system) という[3]．

いま，送信者・受信者がともにそれぞれの秘密鍵 SK_i と対応する公開鍵 PK_i をもっているものとする．このとき，あるアルゴリズム H によって，

$$K=H(PK_1, SK_2)$$
$$K=H(PK_2, SK_1)$$

として鍵 K を生成できればよい．

3.1.2 暗号方式

先の鍵共有方式で鍵を生成して行われた暗号通信は，送信者・受信者ともに同一の鍵を用いる『秘密鍵暗号方式 (secret key cryptosystem)』によるものであったが，ここで述べる暗号方式は，それとは異なる暗号方式である[3]．

いま，暗号通信を利用した受信者は秘密鍵 SK と対応する公開鍵 PK を作成し，公開鍵を自分宛の暗号化鍵 (encryption key) とする．

送信者は，平文 M と受信者の公開鍵 PK とから暗号文 C を作成してこれを送信する．

【暗号化】 $C=E(M, PK)$

受信者は，自分の秘密鍵 SK を復号化鍵 (decryption key) として暗号文 C から平文 M を得る．

【復号化】 $M=D(C, SK)$

このとき，暗号文 C は SK を知る人のみが，復号できる．

3.1.3 署名方式

先の暗号方式は，正当な受信者だけが平文（メッセージ）を復元（作成）することができた．これを逆に利用したのが，ディジタル署名方式 (digital signature scheme) である[3]．

いま，署名者は秘密鍵 SK と対応する公開鍵 PK を作成し，公開鍵を自分用の署名検証鍵 (verification key) とする．このとき，システムに共通な関数としてハッシュ関数 (hash function：長いデータを一定長のデータに圧縮する関数[2]) が存在しているものとする（これを $h(x)$ とする）．

署名者は，自分の秘密鍵 SK を署名作成鍵 (generation key) としてメッセージ M から署名文 S を作成して M と S の対を送信する．

【署名生成】 $S=G(h(M), SK)$

検証者は，送られてきたメッセージ M と署名文

S, さらに署名者の公開鍵 PK とから署名の正当性をチェックする.

【署名検証】 OK/NG$=V(h(M), S, PK)$

(ここで, アルゴリズム V は, 署名 S がメッセージ M の正しい署名であったならば OK を, 署名 S がメッセージ M の正しい署名でなかったならば NG を出力するものである).

このとき, 署名文 S は SK を知る人のみが, 生成できる.

3.2 実際例

3.2.1 DH 鍵共有方式

1976年, Diffie と Hellman が画期的な論文を発表した[3]. すなわち, 公開鍵暗号方式やディジタル署名法の概念がこのとき示されたのである. 残念ながら, 彼らはこの論文では実際の暗号・署名方式を示すことはできなかったが, 離散対数問題に基づく単純で実用性の高い鍵共有方式を提案している.

[センタ] $p\in_R$ PRIME, $g\in_R Z_p^*$: 原始根

[ユーザ] $x\in_R Z_{p-1}$, $y=g^x \bmod p$

《秘密鍵》 x

《公開鍵》 y

このとき, ユーザ A とユーザ B が鍵 k を共有するアルゴリズムを考える (ユーザ A の秘密鍵を x_A, 公開鍵を y_A, ユーザ B の秘密鍵を x_B, 公開鍵を y_B とする).

【鍵生成】 $k_{AB}=(y_B)^{x_A} \bmod p$

$k_{BA}=(y_A)^{x_B} \bmod p$

$(k=k_{AB}=k_{BA})$

このアルゴリズムにより, ユーザ A-B 間で鍵 k が共有できることは,

$$k_{AB}\equiv(y_B)^{x_A}\equiv g^{x_A x_B}\equiv(y_A)^{x_B}\equiv k_{BA}(\bmod p)$$

より明らかである.

3.2.2 RSA 暗号方式

1978年に Rivest, Shamir, Adleman の三人によって提案された最初の公開鍵暗号方式である[4].

この方式は素因数分解の困難さに基づいており, 現在までのところ, 最も実用的であるとの期待があり, 実際のシステムや製品などに導入されつつある. また, この方式は暗号方式としてのみならず, ディジタル署名方式としても適用可能である.

[ユーザ] $p, q\in_R$ PRIME, $n=pq$, $k=\lambda(n)$ $(=$LCM $(p-1, q-1))$, $e\in_R Z_k$, GCD $(e, k)=1$,

$ed\equiv 1 \pmod k$ $(ed=kt+1)$

《秘密鍵》 d (または, p, q)

《公開鍵》 e, n

ユーザ B の平文 m に対する暗号化変換, ユーザ A の暗号文 c に対する復号化変換は以下のとおりである (ここで用いられる暗号化/復号化鍵はユーザ A のものである).

【暗号化】 $c=m^e \bmod n$

【復号化】 $m=c^d \bmod n$

なぜならば,

$$c^d\equiv m^{ed}\equiv m^{kt+1}\equiv(m^k)^t m\equiv m \pmod n$$

より, 上要アルゴリズムにより, ユーザ B は平文 m を得ることが保証される (ここで, 定理 **2.1** により, $m^k\equiv 1 \pmod n$ となることに注意されたい).

3.2.3 ElGamal 暗号方式

その後, 1984年に ElGamal は DH 鍵共有方式を変形することにより, 公開鍵暗号方式を構成できることを示した[5]. この方式は, 離散対数問題に基づく公開鍵暗号方式である.

[ユーザ] $p\in_R$ PRIME, $g\in_R Z_p^*$: 原始根,

$x\in_R Z_{p-1}$, $y=g^x \bmod p$

(p, q は DH 鍵共有方式と同様にシステムに共通な値としてもよい).

《秘密鍵》 x

《公開鍵》 y, g, p

いま, ユーザ B からユーザ A への平文 m に関する暗号通信を考える (ここで, 暗号文を c とし, 用いられる暗号化・復号化鍵はユーザ A のものもする).

【暗号化】 $r\in_R Z_{p-1}$: 乱数

$c = (c_1, c_2) = (g^r \bmod p, y^r m \bmod p)$

【復号化】 $m=c_2/c_1{}^x \bmod p$

この暗号化・復号化のアルゴリズムの正当性は,

$$\frac{c_2}{c_1{}^x}\equiv\frac{y^r m}{g^{rx}}\equiv\frac{y^r m}{y^r}\equiv m \pmod p$$

によって示される.

3.2.4 ESIGN 署名方式

素因数分解問題に基づく高速なディジタル署名方式であり, RSA 方式に比較して数十倍高速である[6),7)]. したがって, IC カードのような CPU パワーのないものの上でも十分に実用的である.

[ユーザ] $p, q\in_R$ PRIME, $p>q$, $n=p^2q$, $k>3$

《秘密鍵》 p, q

《公開鍵》 k, n

ユーザ A がメッセージ m に対する署名文 s を作成し，これをユーザ B に送信し，B がこれを検証する場合を考える（ここで用いられる署名作成／署名検証鍵はユーザAのものである）．いま，ハッシュ関数を $h(x)$ とする．

【署名生成】 $x\in_R Z_{pq}^*$ 乱数

$$w=\left[\frac{h(m)-(x^k \bmod n)}{pq}\right]$$

$$y=\frac{w}{(kx^{k-1})} \bmod p$$

$$s=x+ypq$$

【署名検証】 $0\leq(s^k-h(m)) \bmod n<2^{2\lfloor n/3\rfloor}$

なぜならば，

$$w=\left[\frac{h(m)-(x^k \bmod n)}{pq}\right]$$

より，

$$w\cdot pq=h(m)-(x^k \bmod n)+\delta$$

$$0\leq\delta<pq<2^{2\lfloor n/3\rfloor}$$

であり，

$$\begin{aligned}s^k-h(m)&\equiv(x+ypq)^k-h(m)\\&\equiv x^k+kx^{k-1}ypq-h(m)\\&\equiv x^k-h(m)+kx^{k-1}\frac{w}{kx^{k-1}}pq\\&\equiv x^k-h(m)+wpq\\&\equiv x^k-h(m)+(h(m)-x^k+\delta)\equiv\delta\\&\quad(\bmod n)\end{aligned}$$

よって，

$$0\leq(s^k-h(m)) \bmod n<2^{2\lfloor n/3\rfloor}$$

となるからである．

3.2.5 DSA 署名方式

最近，アメルカの連邦標準技術局 (NIST) により提案されたディジタル署名標準 (DSS) 案であり (digital signature algorithm と称されている)，ElGamal署名方式を基本としている[8),9)]．ElGamal 法が，メッセージに対し署名情報が長くなるという欠点があったのに対し，公開鍵のひとつである g の位数を小さくする手法によりこの点を解決している．すなわち，原始根 (位数 $p-1$) の代わりに，位数が $q(q|p-1)$ となる元 g を用いることにより，乗法群 Z_p^* の中の g が生成する部分群上で演算を考えることができる．これにより，g の指数部を位数 q 以下に抑えることができ，署名長を短くすることが可能となる．

[ユーザ] $p\in_R$ PRIME, $q\in_R$ PRIME $(q|p-1)$, $g\in_R Z_p^*$：位数 q の元，$x\in_R Z_q$, $y=g^x \bmod p$

(p, g は DH 鍵共有方式，ElGamal 暗号方式と同様にシステムに共通な値としてもよい)．

《秘密鍵》 x

《公開鍵》 y, g, p, q

いま，ユーザ A がメッセージ m に対する署名文 s を作成し，これをユーザBに送信し，Bがこれを検証するものとする（このとき，署名作成／署名検証鍵はユーザAのものを用いる）．ここで，ハッシュ関数を $h(x)$ とする．

【署名生成】 $k\in_R Z_q$：乱数

$$r=(g^k \bmod p) \bmod q$$

$$t=(k^{-1}(h(m)+xr)) \bmod q$$

$$s=(r,\ t)$$

【署名検証】 $r=(g^{h(m)t^{-1}}y^{rt^{-1}} \bmod p) \bmod q$

この署名検証アルゴリズムを解析すると，

$$\begin{aligned}(g^{h(m)t^{-1}}y^{rt^{-1}} \bmod p)&\equiv(g^{h(m)t^{-1}}g^{xrt^{-1}} \bmod p)\\&\equiv(g^{(h(m)+xr)t^{-1}} \bmod p)\\&\equiv(g^k \bmod p)\equiv r\ (\bmod q)\end{aligned}$$

となることから，この署名方式の正当性が保証される．

3.2.6 その他の暗号・署名方式

以上，素因数分解・離散対数問題に基づく代表的な暗号・署名方式について解説したが，いままでに述べてきた各種方式はその安全性が根拠となっている問題と等価であることは証明されていない．たとえば，RSA 暗号に対する素因数分解以外の簡単な解読法が存在するかもしれないのである．これに対し，Rabin 暗号方式[15)]は，受動的攻撃 (passive attack：公開鍵と暗号文から平文を求めるような攻撃) による解読法が素因数分解と同等であることが証明されている方式である．この方式を概説すれば，RSA 方式の公開鍵を 2 に限定するものとして考えられ，このとき，この復号化のアルゴリズムは，合成数 n を法とした二次式

$$x^2=c\ (\bmod n)$$

の求解アルゴリズムとなる．もし，受動的攻撃法に対して，Rabin 法を解読するアルゴリズムがあるとすれば，この解読アルゴリズムを用いて，合成数を因数分解するアルゴリズムが構成できる．しかし，Rabin 法には一意に復号できない．という欠点がある．Williams 暗号方式[16)]や逆数暗号方式[17)]は，素因数分解との等価性を保証し，かつ，

一意復号可能な方式である.

ただし，上記のような方式において，受動的攻撃法に対する安全性の証明ができることは，逆に能動的攻撃 (active attack : 暗号文を与えて平文をもらうことが許されるようなより強力な攻撃) に対しては，安全でないことをも意味してしまう. 受動的攻撃に対し安全でかつ能動的攻撃に対しても安全であることが証明されている方式も提案されている[10),11)]が，数論的手法以外の手法 (非対話型ゼロ知識証明[12)]を必要とし，実用的な構成法は知られていない.

また，素因数分解に基づく署名方式としてOng-Schnorr-Shamir 法[13)]があるが，これはすでに解読法が提案されており[14)]，この方式に対する攻撃法の研究が，合成法 n を法とした二変数二次多項式

$$x^2+ky^2=m \pmod n$$

の多項式時間求解アルゴリズムの発見につながっている.

4. 初等整数論の擬似乱数への応用

4.1 擬似乱数とは

n bit の入力 (seed) を $2n$ bit に拡張する決定性多項式時間アルゴリズム g を考えよう. 長さ $2n$ の bit 列は，全部で 2^{2n} 通りある. この集合を u_{2n} で表そう. 一方，g の出力は，全部で高々 2^n 通りある. この集合を $g(u_n)$ で表そう. すると，$|g(u_n)|/|u_{2n}| \leq 2^n/2^{2n}=1/2^n$ であるから，$g(u_n)$ は u_{2n} の非常に粗な部分集合になっている. ここで，どのような多項式時間アルゴリズムをもってしても，$g(u_n)$ と u_{2n} を区別不可能なとき，g を「暗号学的に安全な擬似乱数生成器」とよぶ. 以下，このような g を，単に擬似乱数生成器とよぶことにしよう (g の出力は n bit より長ければよいわけで，$2n$ bit である必要はない. また正確には，$g(u_n)$ と u_{2n} はランダム変数として定義される)[21)].

このようなランダム性の証明された擬似乱数は，任意の部分情報が保護できる公開鍵暗号[27)] (擬似乱数＋バーナム暗号により安全性の証明された慣用鍵暗号も可能) や擬似ランダム関数[28)]，零知識証明[29)]などに応用され，現代暗号理論の基本的なツールの一つになっている. 歴史的にみると，擬似乱数生成器は，当初整数論的仮定の下で構成された[22)]. その後，徐々に仮定が弱められ，最終的に一方向性関数という非常に一般的仮定の下で構成できる，というところまで到達している[23),24)].

ここでは，整数論的仮定に基づく擬似乱数生成器を紹介しよう[22),25),26)]. (一般の有限アーベル群上での擬似乱数の構成法も知られている[30)].)

4.2 一般的構成法

まず，一方向性置換 $f(x)$ およびそれにともなう hard core 述語 $b(x)$ を定義しよう[21)]. なお，一方向性関数に関しては，文献 31) を参照されたい.

定義 **4.1** 以下の条件を満たす関数 f を一方向性置換と呼ぶ.

1. $f(x)$ は集合 X から集合 X への 1 対 1 写像
2. x から $f(x)$ を計算する多項式時間アルゴリズムが存在する.
3. $f(x)$ から x を計算するのは難しい (意味のある確率以上で計算する確率的多項式時間アルゴリズムは存在しない).

定義 **4.2** 以下の条件を満たす述語 B (0 or 1 の値をとる) を，関数 f の hard core と呼ぶ.

1. x から $B(x)$ を計算する多項式時間アルゴリズムが存在する.
2. $f(x)$ から $B(x)$ を 1/2 より **意味のある** 確率以上良い確率で計算する確率的多項式時間アルゴリズムは存在しない.

Blum と Micali は，擬似乱数生成器 $G(x)$ の以下のような一般的構成法を示した[22)]. G は n ビットの random seed x を入力とし，$m=Q(n)$ ビットの擬似乱数を出力するものとする. ここで，$Q(n)$ は任意の多項式である.

$x_0 \leftarrow x$
$x_{i+1} \leftarrow f(x_i)$
$b_i \leftarrow B(x_i)$
$G(x) \leftarrow b_0 b_1 \cdots b_{m-1}$

(例)

前章で示したRSA暗号，すなわち $f(x)=x^e \bmod n$ は，一方向性置換である ((n, e) で parameterize されているので，正確には一方向性置換の族として定義したほうがよい，より正確には，一方向性置換の族の候補，というべきであろう). $B(x)=lsb(x)$ は，RSA 暗号の hard core である[26)]. (但し，$lsb(x)$ は x の最下位ビット)

上記の G がなぜ，擬似乱数生成器の条件を満

たすのか，あるいは，上記の $B(x)$ がなぜ RSA 暗号の hard core になるのか，といった証明は，紙面の都合上，省略する．整数論的観点からは，おのおのの（整数論的仮定に基づく）一方向性置換に付随する hard core をいかに（効率的に）構成するか，がポイントになる．次節において，この点を離散対数問題に焦点を当ててやや詳しく説明しよう．

4.3 離散対数問題に基づく擬似乱数

4.3.1 離散対数問題の Hard Core

先に進む前に，初等整数論を少し復習しておこう．フェルマーの定理（**2.**）より，ただちに次式が成り立つ．

$$y^{(p-1)/2} \bmod p = \pm 1 \qquad (2)$$

上式の左辺を $\left(\frac{y}{p}\right)$ という記号で表そう（ルジャンドルの記号）．さらに一歩踏み込んで，次の補題が成り立つ．

補題 **4.1**

1. $y=g^x \bmod p$ とする．このとき

$$\left(\frac{y}{p}\right)=y^{(p-1)/2} \bmod p = \begin{cases} 1 & \text{if } x=0 \bmod 2 \\ -1 & \text{if } x=1 \bmod 2 \end{cases}$$

が成り立つ．

2. $(y/p)=1$ のときかつそのときに限り，ある整数 a が存在し，

$$y=a^2 \bmod p$$

と書ける．このような y を平方剰余，そうでない y を平方非剰余と呼ぶ．

この補題は，(p, g, y) から x の最下位ビットが多項式時間でもとまってしまう，ということを示している（式(2)の左辺を高速べき乗法で計算すればよい）．では，x のどのビットが難しいのであろうか．

述語 $B_1(p, g, x)$ を以下のように定義しよう．

$$B_1(p, g, x)=\begin{cases} 0 & \text{if } 0\le x<(p-1)/2 \\ 1 & \text{if } (p-1)/2\le x\le p-1 \end{cases}$$

(p, g, y) から $B_1(p, g, x)$ を求めることは，離散対数問題を解くのと同程度に難しいことが証明できる．より正確には，以下の定理が成り立つ[22]．

定理 **4.1**　ε を任意に小さい正定数とする．$p-1$ 個のうち $1/2+\varepsilon$ の割合の y に対し，$B_1(p, g, x)$ の値を正しく答えてくれるオラクル（神様）$MB(y)$ を仮定する．すると，離散対数問題を平均多項式時間で解く確率的アルゴリズムが存在する（ε は $1/(poly(|p|))$ におきかえられる）．本定理よりただちに，離散対数問題に基づく擬似乱数生成器は，一般的構成法の節で示した方法で構成できることになる．さて，この定理の証明は多少複雑なので，ここでは以下のより簡単な定理を証明しよう．

定理 **4.2**　すべての y に対し $B_1(p, g, x)$ の値を正しく答えてくれるオラクル（神様）$MB(y)$ を仮定する．すると，離散対数問題を多項式時間で解くアルゴリズムが存在する．

補題 **4.2**　y が平方剰余のとき，y の平方根を z_1, z_2 とする．すると，

$MB(z_1)=0$, $MB(z_2)=1$　または，その逆が成り立つ．

（証明）

簡単のため，$MB(z_1)=0$ としよう．つまり，

$$z_1=g^{x_1} \bmod p \quad (0\le x_1<(p-1)/2)$$

とする．さて，$g^{(p-1)/2}=-1 \bmod p$ であるから，

$$z_2=-z_1=g^{(p-1)/2}g^{x_1}=g^{(p-1)/2+x_1} \bmod p$$

が成り立つ．ここで，

$$(p-1)/2\le(p-1)/2+x_1<p-1$$

となり，よって，$MB(z_2)=1$ である．

定理 **4.2** の証明の準備として，$\bmod p$ の下で平方根を求めるアルゴリズムが必要になる．それを次節で説明しよう．

4.3.2 2次方程式 mod p の解き方

一般的に，

$$x^2+ax+b=(x-x_1)(x-x_2) \bmod p$$

とし，x^2+ax+b から x_1, x_2 をもとめる方法を示す．

定理 **4.3**　$\left(\frac{x_1}{p}\right)\left(\frac{x_2}{p}\right)=-1$ のとき，

$$\gcd(x^2+a^9x+b,\ x^{(p-1)/2}-1) = c(x-x_1) \text{ or } c(x-x_2)$$

ただし，c はある定数．

（証明）

$\left(\frac{x_1}{p}\right)=1$, $\left(\frac{x_2}{p}\right)=-1$ とすると，

$$x_1^{(p-1)/2}=1,\quad x_2^{(p-1)/2}=-1$$

であるから，$x-x_1$ は $x^{(p-1)/2}-1$ の因数であり，$x-x_2$ は因数でない．

系 **4.1**　$\left(\frac{x_1+r}{p}\right)\left(\frac{x_2+r}{p}\right)=-1$ のとき，

$$\gcd((x+r)^2+a(x+r)+b,(x+r)^{(p-1)/2}-1)$$

$$=c(x-(x_1+r)) \text{ or } c(x-(x_2+r)) \quad (3)$$

【2次方程式を解く確率的多項式時間アルゴリズム】

step 1: r をランダムに選ぶ.

step 2: 式(3)の左辺を計算する.

step 3: その結果が一次式であれば，系 4.1 から x_1, x_2 がもとまる．そうでなければ，step 1 へ．このアルゴリズムは，1回の繰り返しにつき，確率 1/2 で成功する．通常，数回の繰り返しで解がもとまる.

以上，このアルゴリズムにより，mod p の下での y の平方根を，二次方程式 $x^2=y$ の求解により求めることができる.

4.3.3 定理 4.2 の証明

具体例で示そう．x の2進表現を

$$(x_1x_2x_3x_4)_2=(1010)_2$$

とする.

1. 補題 4.1 より，y の指数部 x の最下位ビット x_4 をもとめる．この場合，$x_4=0$ ともとまる.

2. $x_4=0$ なので y は平方剰余．そこで，前節のアルゴリズムで y の平方根 y_1, y_1' をもとめる．ここで，オラクル MB の助けを借りて，$MB(y_1)=0$ となるほうを y_1 と定める（補題 4.2 参照）．すると，$y_1=g^{(101)_2} \bmod p$ である.

3. 補題 4.1 より，y_1 の指数部の最下位ビットをもとめる．この場合，$x_3=1$ ともとまる.

4. $x_3=1$ なので y は平方非剰余．そこで，$y_1=g^{-1}y_1=g^{(100)_2} \bmod p$ とおく．この y_1 は，平方剰余.

5. 前節のアルゴリズムで y_1 の平方根をもとめる．以下同様に x_2, x_1 と x のすべての bit をもとめることができる.

4.3.4 擬似乱数生成器

定理 4.1 および一般的構成法より，離散対数問題に基づく擬似乱数生成器 $G_{(p,g)}(x)$ は以下のアルゴリズムで与えられる.

$x_0 \leftarrow x$

$x_{i+1} \leftarrow g^{x_i} \bmod p$

$$b_i \leftarrow \begin{cases} 0 & \text{if } 0 \le x_i < (p-1)/2 \\ 1 & \text{if } (p-1)/2 \le x_i < p-1 \end{cases}$$

$G_{(p,g)}(x) \leftarrow b_0b_1 \cdots b_{m-1}$

この擬似乱数生成器の安全性は，以下のように証明される.

もし，この擬似乱数発生器の出力の集合と U_m を区別するアルゴリズムがあったらならば，そのアルゴリズムを用いて，擬似乱数発生器の出力中の1bit を予測することができる．この1bit が予測できると，この予測アルゴリズムを用いて，離散対数問題を解くアルズリズムを構成できる（定理 4.2 参照）.

よって，離散対数問題が困難であれば，この擬似乱数発生器は非常にランダムな出力をするものと結論付けられる.

5. 楕円曲線に基づく公開鍵暗号

5.1 楕 円 曲 線

楕円曲線は，1985年に離散対数問題に基づく公開鍵暗号に用いる手法（文献 34), 42)）が発表され，暗号分野に応用されるようになった．この公開鍵暗号は有限体上の楕円曲線を用いて定義されるのであるが，安全性の根拠になる楕円曲線上の離散対数問題に有限体上の離散場数問題に対する強力な解法である「指数計算法 (Index Calculus)」が直接適用できないことから盛んに研究されるようになった．「指数計算法」については[37]，に解説されている.

一方これとは別に楕円曲線は，1986年に素因数分解に用いる手法（文献 40)）が発表されている．これについては 37) を参照されたい．この原理を用いて，1991年に素因数分解の安全性に基づく楕円曲線上の RSA 暗号が発表された(文献 33))．これは環上の楕円曲線を用いて定義され，有限体上の RABIN 暗号も同様に定義される.

この章では楕円曲線に基づく離散対数問題ベースの公開鍵暗号の基本原理と研究の流れについて述べる．そこでまず公開鍵暗号が定義される有限体上の楕円曲線について簡単に述べる．有限体上の楕円曲線の元の集合は，F_q (q は5以上の素数 p の r 乗）を q 個の元をもつ有限体とし，$a, b \in F_q$ を $4a^3+27b^2 \neq 0$ なる元とするとき，

$$\{(x, y) \in F_q^2 \mid y^2=x^3+ax+b\} \cup \{\mathcal{O}\}$$

と表される．以後これを $E(F_q)$ と表す．ここで $\mathcal{O}$ は無限遠点で，楕円曲線にはこれが零元になるような加法が定義される．q が2もしくは3の r 乗の場合および楕円曲線の詳細については文献 41), 51) を参照されたい．これにより $E(F_q)$ は有限体と同様に有限可換群になり，有限体上と同様に離散対数問題 (EDLP) が定義される．EDLP の詳細については，37) に解説されている.

5.2 原　理

楕円曲線に基づく公開鍵暗号は，有限体上の離散対数問題に基づく公開鍵暗号において有限体の元を楕円曲線の元に，有限体上の乗法を楕円曲線上の加法に対応させることにより定義される．このとき有限体の元の r 乗は楕円曲線の元の r 倍に対応し，通常有限体の元の r 乗を計算するのに用いる高速指数演算法も楕円曲線の元の r 倍を計算するのに用いることができる．次に楕円曲線に基づく公開鍵暗号の具体的な構成例を二つ紹介する(文献 35))．以下 $E: y^2=x^3+ax+b$ を F_q 上定義された楕円曲線とし，$f(x)=x^3+ax+b$ とし，また $P\in E(F_q)$ を位数 ($nP=\mathcal{O}$ となる最小の正整数 n) が大きな素数で割れる元（ベースポイント）とする．また $\Gamma(F_q)$ および P はシステム内で公開する．

- DH 鍵共有方式

A と B が鍵を共有する場合を考える．

【鍵生成】 A は正整数 x_A を選びこれを秘密鍵として保持し，E 上で

$$Y_A=x_AP$$

を計算し，$E(F_q)$ の元 Y_A を公開鍵として公開ファイルに登録する．同様に B も正整数 x_B を秘密鍵として保持し，$E(F_q)$ の元 Y_B を公開鍵として公開ファイルに登録する．

【鍵共有】 A は公開ファイルから B の公開鍵 Y_B を取ってきて E 上で

$$K_{A,B}=x_AY_B=x_Ax_BP$$

を計算する．同様に B は公開ファイルから A の公開鍵 Y_A を取ってきて E 上で

$$K_{B,A}=x_BY_A=x_Bx_AP$$

を計算する．A と B は $E(F_q)$ の元 $K_{A,B}=K_{B,A}$ を鍵として共有する．

- ElGamal 暗号方式

送信者 A が平文 M を受信者 B に秘密に送信する場合を考える．ここで M は $E(F_q)$ の元とする．

【鍵生成】 受信者 B は正整数 x_B を選びこれを秘密鍵として保持し，E 上で

$$Y_B=x_BP$$

を計算し $E(F_q)$ の元 Y_B を公開鍵として公開ファイルに登録する．

【暗号化】 送信者 A は乱数 r を選び，E 上で

$$C_1=rP$$

$$C_2=M+rY_B$$

を計算し，二つの $E(F_q)$ の元 (C_1, C_2) を送る．

【復号化】 受信者 B は，自分のみが知る秘密鍵 x_B を用いて E 上で

$$C_2-x_BC_1=M$$

を計算し平文 M を得る．

次に平文 m を $E(F_q)$ の元 M に対応させる方法を述べる．ここで平文 m は $0\le m<l$ の整数とする．正整数 k を $0<lk<q$ となるようにとる．$1\le i\le k$ なる整数 i に対して $x_{m,i}=mk+i$ とおき，これを p 進展開したときの係数を用いて $x_{m,i}$ を F_q の元に対応する F_p 上の $r-1$ 次の多項式に対応させる．こうして得られる F_q の元を $\tilde{x}_{m,i}$ とする．すなわち，

$$x_{m,i}=\sum_{i=0}^{r-1}a_ip^i(0\le a_i\le p-1)$$

と展開し，これを F_p 上の多項式

$$\sum_{i=0}^{r=1}a_iX^i$$

に対応させることにより F_q の元 $\tilde{x}_{m,i}$ を得る．そこで $f(\tilde{x}_{m,i})$ が F_q の平方根となる最小の i に対して $x_{m,i}=x_m$ とし，この x_m を用いて平文 m を $E(F_q)$ の元

$$M=(\tilde{x}_m, \sqrt{f(\tilde{x}_m)})$$

に対応させる．このとき，逆に $E(F_q)$ の元 M の x 座標 $\tilde{x}_m$ から，$m=\lfloor(x_m-1)/k\rfloor$ とおくことにより元の平文 m を得ることができる．また任意の $1\le i\le k$ なる i に対して $f(\tilde{x}_m)$ $(x_m=mk+i)$ が平方数になる確率は，ほぼ 1/2 であることより，この方法により平文が $E(F_q)$ の元に対応できない確率は約 $(1/2)^k$ であることが分かる．

5.3 構成法の主要なアルゴリズム

楕円曲線に基づく公開鍵暗号が十分安全であるようにするには，次の条件 1 を満たすように楕円曲線を構成する必要がある．

条件 1：楕円曲線のベースポイントの位数が大きな素数で割れる．

つまり，楕円曲線の元の個数は大きな素数で割れる必要がある．このためには，楕円曲線の元の個数を知らなければならない．楕円曲線の元の個数を求める一般的なアルゴリズムとしては文献 50) が知られているが，これはあまり実用的でない．このため，条件 1 を満たすような楕円曲線の構成方法の研究が行われた．

Menezes-Vanstone (文献 44)) は次の楕円曲線の構成方法を提案している.

【Menezes-Vanstone の方法】

step 1: E の候補の決定

F_2 上の超特異楕円曲線

$E: y^2+y=x^3$

を取る.

step 2: 拡大次数 l の決定

上記の楕円曲線の F_{2^l} 上の元の個数は $\sharp E(F_2)$ を用いて容易に求められ, l が奇数のとき,

$\sharp E(F_{2^l})=2^l+1$

で与えられる. そこで元の個数が大きな素数で割れるような奇数 l を求め, $E(F_{2^l})$ を求める楕円曲線とし, その大きな素数を位数にもつ元をベースポイントとする.

上記のような F_2 上の超特異楕円曲線は, 通常の楕円曲線に比較して2倍の計算が簡単になるという利点をもつ. 超特異 (supersingular) の定義及び $\sharp E(F_{2^l})$ については文献 51) を参照されたい. 特に上記の楕円曲線を用いると2倍点の計算が, $2(x, y)=(x^4, y^4+1)$ で与えられるためその計算量が少なくてすみ, 高速な暗号/復号化が望める.

さらに Menezes-Vanstone は平文 m を楕円曲線 $E(F_q)$ の元 M に対応させることなく暗号化する一般的な方法も提案している. 簡単のため, 平文 m は F_q の元とする. 送信者 A は乱数 r を選び, E 上で $C_1=rP$ と $C_2=rY_B$ を計算し, C_2 の x 座標 $x(C_2)$ と m との積 $m*x(C_2)$ を求め, C_1 と $m*x(C_2)$ を送信する. 受信者 B は, 秘密鍵 x_B を用いて E 上で $x_BC_1=C_2$ を計算し平文 m を得る. 楕円曲線の元のデータサイズは, x, y 座標が必要なため定義体 F_q の大きさの2倍になる. そこで送信データを減少させるため, C_1 の代わりに, x 座標 $x(C_1)$ と y 座標を復元させるための $y(C_1)$ の符号の1ビット $sign(y(C_1))$ を送信することもできる. この際受信者は, $x(C_1)$ と $sign(y(C_1))$ から C_1 を復元してから復号化することになる.

Morain (文献 45)) は条件1を満足するために Menezes-Vanstone とは違う構成方法を提案している.

【Morain の方法】

step 1: 大きな素数 p の決定

step 2: 楕円曲線の元の個数 n の決定

ある整数 x, y に対して次の二つを満たすような正整数 d を見つける.

1. $4p=x^2+dy^2$ となる.
2. $n=((x-2)^2+dy^2)/4$ が squarefree (素数の2乗で割れない) で, かつ大きな素数で割れる.

step 3: 元の個数が n となる楕円曲線の構成

有限体上の楕円曲線は, 巡回群か二つの巡回群の直積になる[45]. 条件1を満たす楕円曲線をより小さな素体上で構成するには, 巡回群となる必要がある. 上記の方法はこの点に着目し, 元の個数が n で巡回群になる楕円曲線を構成するという方法である. step 3 における与えられた元の個数をもつ素体上の楕円曲線については Deuring により研究されている[32]. これについて文献 39) に詳しく解説されている. Morain の方法は Menezes-Vanstone の場合のように2倍点, もしくは和計算が高速にできるというわけではない.

楕円曲線上の公開鍵暗号は, 上記のように構成すると特に強力な解法がなかった. ところが1991年になって, Menezes-岡本-Vanstone らにより新しい解法アルゴリズム (MOV-reduction) が提案された (文献 47)). MOV-reduction は EDLP を構成する群をある単射準同型写像を用いて有限体の群と同一視し, DLP に変換して解法する方法である. これについては 37), 48) にも解説されている. この結果, 楕円曲線は条件1に加えて, 次の条件2を満たすように構成することが必要となった.

条件 2: MOV-reduction により楕円曲線 E/F_q 上の EDLP が変換される DLP が F_q の小さい拡大体上定義されない.

先に紹介した Menezes-Vanstone の方法は超特異楕円曲線を用いているため上記の条件2を満たさない. そこで Koblitz (文献 36)) はこの問題を解決する構成法を提案している. これは先述の Menezes-Vanstone の方法を, step 1 で超特異でない楕円曲線でトレースが1になるものを用い, step 2 でさらに条件2を満たすように改良した方法である. トレースが1であることから, $2^k(k\leq 4)$ 倍の計算が1回の和の計算でできるという利点がある.

これに対し筆者 (文献 43)) は楕円曲線 E/F_q 上の EDLP がどんな単射準同型によっても DLP に変換されない楕円曲線を提案している. これは素体 Fp 上の楕円曲線 E で元の個数 $\sharp E(Fp)=p$ と

なる楕円曲線である．以下 $\sharp E(F_p)=p$ となる楕円曲線の構成法のひとつを述べる．

【宮地の方法】

step 1：$p=11b^2+11b+3$ (b は正整数) と表される大きな素数の決定

step 2：$j_0=-2^{15}$ を j-不変数にもつ F_q-同型でない楕円曲線の構成

求める楕円曲線は，

$$E: y^2=x^3+ax+b,\ E_t: y^2=x^3+ac^2x+bc^3$$

$$\left(a\equiv\frac{3j_0}{1728-j_0},\ b\equiv\frac{2j_0}{1728-j_0}\pmod p\right)$$

の二つで与えられる．ここで c は F_q の任意の平方非剰余元である．

step 3：元の個数が p となる楕円曲線の決定

$E(F_p)$ から任意に一つ $\mathcal{O}$ と異なる元 X を取り，pX を計算する．このとき，$pX=\mathcal{O}$ であれば $\sharp E(F_p)=p$ となり，$pX\neq\mathcal{O}$ であれば $\sharp E_t(F_p)=p$ となる．

step 2 の j-不変数および F_p-同型については，文献 51) を参照されたい．また Morain の方法で述べたように，与えられた元の個数をもつ楕円曲線については Deuring により一般的に研究されている．上記のような楕円曲線では元の個数が素数なので任意の元がベースポイントにとれるという利点がある．しかし F_{2^l} 上の楕円曲線と違い，和計算が高速にできるというわけではない．

5.4 問題点と他の代数曲線への展開

一般に楕円曲線では，r 倍の計算に必要な和計算が何回かの乗法を要求する．このため暗号／復号化に時間がかかるという問題がある．そこで楕円曲線では加法の逆演算である減法が加法と同じ計算でできるということを用いて，r 倍の計算を高速にするという方法も提案されている（文献 38)，46))．楕円曲線は種数 1 の代数曲線であるが，一般に種数 ≥ 2 の代数曲線にも同様にして公開鍵暗号を定義することができる[52]．しかしこの場合，楕円曲線以上に和計算が複雑になる．この問題を解決すると，種数 ≥ 2 の代数曲線上の暗号の実現も可能になる．

6. あ と が き

現代暗号理論は，数論を軸に発展してきたが，一方で，コンピュータ・サイエンスの立場からの理論の体系化も猛烈な勢いで進んでいる．本格的に現代暗号理論の研究を志す学生（あるいは研究者）諸氏には，文献「本誌小特集ゼロ知識証明とその応用」(1991 年 6 月号) もあわせて参照されたい．

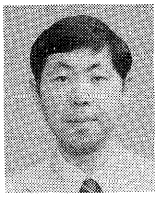
参 考 文 献

1) Kranakis, E.: *Primality and Cryptography*, Wiley-Teubner Series in Computer Science, John Wiley & Sons (1986).
2) Davis, D. W. and Price, W. L.: *Security for Computer Networks*, John Wiley & Sons (1984).
3) Diffie, W. and Hellman, M. E.: New Directions in Cryptography, *IEEE Transactions on Information Theory*, Vol. T-22, No. 6, pp. 644-654 (Nov. 1976).
4) Rivest, R., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126 (Feb. 1978).
5) ElGamal, T.: A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms, *IEEE Transactions on Information Theory*, Vol. 1 T-31, No. 4, pp. 469-472 (July 1985).
6) Okamoto, T.: A Fast Signature Scheme Based on Congruential Polynomial Operations, *IEEE Transactions on Information Theory*, Vol. IT-36, No. 1, pp. 47-53 (Jan. 1990).
7) Fujioka, A., Okamoto, T. and Miyaguchi, S.: ESIGN: An Efficient Digital Signature Implementation on Smart Card, in *Advances in Crypotlogy—EUROCRYPT '91*, Lecture Notes in Computer Science 547, Springer-Verlag, pp. 446-457 (1991).
8) National Institute for Standards and Technology: Specifications for a Digital Signature Standard, *Federal Information Processing Standard Publication XX*, draft (Aug. 1991).
9) National Institute for Standards and Technology: The Digital Signature Standard, *Communications of the ACM*, Vol. 35, No. 7, pp. 36-40 (July 1992).
10) Naor, M. and Yung, M. Public-Key Cryptosystems Provably Secure against Chosen Ciphertext Attacks, Proceedings of 22nd annual ACM Symposium on Theory of Computing, pp. 427-437 (May 1990).
11) 太田和夫，藤岡 淳：ゼロ知識証明の応用，情報処理，Vol. 32, No. 6, pp. 654-662 (June 1991).
12) 静谷啓樹，伊東利哉，桜井幸一：ゼロ知識証明モデルと計算量理論，情報処理，Vol. 32, No. 6, pp. 673-681 (June 1991).
13) Ong, H., Schnorr, C. and Shamir, A.: An Efficient Signature Scheme based on Quadratic Equations Proceedings of 16th annual ACM Symposium on Theory of Computing, pp. 208-

216 (May 1984).
14) Pollard, J. M. and Schnorr, C.: An Efficient Solution of the Congruence $x^2+ky^2=m \pmod n$, *IEEE Transactions on Information Theory*, Vol. IT-33, No. 5, pp. 702-709 (Sep. 1987).
15) Rabin, M. O.: Digitalized Signatures and Public-Key Functions as Intractable as Factorization. Technical report, LCS/TR-212 (1979).
16) Williams, H. C.: A Modification of the RSA Public Key Encryption Procedure, IEEE, Trans. IT-26, No. 6, pp. 726-729 (1980).
17) 黒沢, 伊東, 竹内: 素因数分解の困難さと同等の強さを有する逆数を利用した公開鍵暗号, 電子情報通信学会論文誌, J 70-A, No. 11, pp. 1632-1636 (1987).
18) Goldwasser, S., Micali S. and Rivest, R.: A Digital Signature Scheme against Adaptive Chosen Message Attack, SIAM J. on Computing, Vol. 17, No. 2, pp. 281-308 (1988).
19) Damgärd, I.: Collision Free Hash Functions and Public Key Signature Schemes, Eurocrypt '87, pp. 203-216 (1987).
20) Shamir, A.: How to Share Secret, Communication of the ACM, Vol. 22, No. 11, pp. 612-613 (1979).
21) Goldreich, O.: Foundation of Cryptography, Technical report, Technion (1989).
22) Blum, M. and Micali, S.: How To Generate Cryptographically Strong Sequences Of Pseudo Random Bits, FOCS '82, pp. 112-117 (1982).
23) Impagliazzo, R., Levin, L. and Luby, M.: Pseudorandom Generation from One Way Functions, STOC '89, pp. 12-24 (1989).
24) Hästad, J.: Pseudorandom Generators under Uniform Assumption, STOC '90, pp. 395-404 (1990).
25) Blum, L., Blum, M. and Shub, M.: Comparison of Two Pseudorandom Number Generators, Crypto '82, pp. 61-79 (1982).
26) Chor B, and Goldreich, O.: RSA/Rabin Least Significant Bits are $1/2+1/\mathrm{poly}(n)$ Secure, Crypto '84, pp. 303-313 (1984).
27) Blum, M. and Goldwasser, S.: An Efficient Probabilistic PKCS as Secure as Factoring, Crypto '84, pp. 288-299 (1984).
28) Goldreich, O., Goldwasser, S. and Micali, S.: How to Construct Random Functions, FOCS '84, pp. 464-479 (1984).
29) Goldwasser, S., Micali, S. and Rackoff, C.: The Knowledge Complexity of Interactive Proof Systtems, SIAM Journal of Computing, Vol. 18, No. 1, pp. 186-298 (Feb. 1989).
30) Kaliski, B. S.: A pseudo-Random Bit Generator Based on Elliptic Logarithm, Crypto '86, pp. 84-103 (1987).
31) 渡辺 治: 一方向性関数のお話し, 情報処理, Vol. 32, No. 6, pp. 704-713 (1991).
32) Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkorper, *Abh. Math. Sem. Hamburg*, 14, pp. 197-272 (1941).
33) Koyama, K., Maurer, U. M., Okamoto, T. and Vanstone, S. A.: New Public-Key Schemes Based on Elliptic Curves over the Ring Zn, *Advances in Cryptology-Proceedings of CRYPTO '91*, Lecture Notes in Computer Science, 576, Springer-Verlag, pp. 252-266 (1992).
34) Koblitz, N.: Elliptic Curve Cryptosystems, *Mathematics of Computation*, 48, pp. 203-209 (1987).
35) Koblitz, N.: *A course in Number Theory and Cryptography*, GTM 114. Springer-Verlag, New York (1987).
36) Koblitz, N.: Cm-Curves with Good Cryptographic Properties, *Advances in Cryptology-Preceedings of CRYPTO* '91, Lecture Notes in Computer Science, 576, Springer-Verlag, pp. 279-287 (1992).
37) 小山, 静谷: 素因数分解と離散対数問題アルゴリズム, 本特集号.
38) Koyama K. and Tsuruoka, Y.: Speeding Up Elliptic Cryptosystems by Using a Signed binary Window Method, *Abstract of proceeding of CRYPTO '92* (1992).
39) Lang, S.: *Elliptic Functions*, GTM 112, Springer-Verlag, New York (1987).
40) Lenstra, H. W., Jr.: Factoring Integers with Elliptic Curves, Report 86-18, Mathematisch Instituut, Universiteit van Amsterdam (1986).
41) リード, M. 著, 若林 巧訳: 初等代数幾何学講義, 岩波書店.
42) Miller V. S.: Use of Elliptic Curves in Cryptography, *Advances in Cryptology-Proceedings of Crypto '85*, Lecture Notes in Computer Science, 218, Springer-Verlag, pp. 417-426 (1986).
43) Miyaji, A.: On Ordinary Elliptic Curves, *Abstract of proceedings of ASIA-CRYPT '91* (1991).
44) Menezes, A. and Vanstone, S.: The Implementaion of Elliptic Curve Cryptosystems, *Advances in Cryptology-Proceedings of Auscrypt '90*, Lecture Notes in Computer Science, 453 Springer-Verlag, pp. 2-13 (1990).
45) Morain, F.: Building Cyclic Elliptic Curves Modulo Large Primes, *Advances in Cryptology-Proceedings of Eurocryp '91*, Lecture Notes in Computer Science, 547, Springer-Verlag, pp. 328-336 (1991).
46) Morain, F. and Olivos, J.: Speeding up the Computations on an Elliptic Curve using Addition-Subtraction Chains, Theoretical Informatics and Applications, Vol. 24, No. 6, pp. 531-544 (1990).
47) Menezes, A., Okamoto T. and Vanstone, S.: Reducing Elliptic Curve Logarithms to Lograithms in a Finite Field, *Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing*, pp. 80-89 (1991).
48) 岡本, 桜井: 代数幾何学的アルゴリズム, 本特集号.

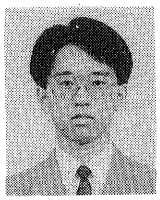
49) Pohlig, S. C. and Hellman, M. E.: An Improved Algorithm for Computing Logarithm over $GF(p)$ and Its Crytographic Significance, *IEEE Trans. Inf. Theory*, IT-24, pp. 106-110 (1978).
50) Schoof, R.: Elliptic Curves Over finite Fields and the Computation of Square Roots Mod p, *Mathematics of Computation*, Vol. 44, pp. 483-494 (1985).
51) Silverman, J. H.: *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, New York (1986).
52) Koblitz, N.: Hyperelliptic Cryptosystens, Journal of Cryptolog, Vol. 1, No. 3, pp. 139-150 (1989)

(平成4年11月6日受付)



黒澤 馨

昭和 52 年東京工業大学工学部電子工学科卒業. 昭和 57 年同大学院博士課程修了. 同年同大助手. 昭和 60 年同講師. 平成元年同助教授. 多種フロー問題, デジタル信号処理, 通信プロトコル, 情報セキュリティに関する研究に従事. 昭和 55 年度電子通信学会論文賞, 昭和 60 年度同学会篠原記念学術奨励賞各受賞. 電子情報通信学会, IEEE 学会各会員.



藤岡 淳

昭和 60 年東京工業大学工学部電気・電子工学科卒業. 平成2年同大学院理工学研究科博士課程修了. 工学博士. 同年日本電信電話(株)入社. 情報セキュリティ, 主に, IC カードにおけるセキュリティ・モジュールの研究開発に従事. 現在, NTT 情報通信網研究所データベース研究部研究主任. International Association for Cryptologic Research (IACR), 電子情報通信学会各会員.

宮地 充子

1988 年大阪大学理学部数学科卒業. 1990 年同大学院理学研究科数学専攻修士課程修了, 同年松下電器産業(株)に入社. 現在, 通信システム研究所に勤務. 入社以来, 暗号と情報セキュリティの研究に従事. 電子情報通信学会会員.