公開鍵暗号（RSA暗号/楕円曲線暗号）の安全性

高木　剛

本稿では，公開鍵暗号の仕組みやその安全性証明に関する解説を行う．最も普及している公開鍵暗号方式としてRSA暗号がある．RSA暗号の安全性は素因数分解の困難性を基にしているため，公開鍵が素因数分解された場合RSA暗号は完全解読される．一方，完全解読ではなく平文の部分情報のみを解読する攻撃も考えられ，暗号が安全である条件は様々な定義が可能である．本稿では，平文ビットの安全性を証明する方法を紹介したあと，Semantic Securityといわれる安全性クラスとRSA暗号を利用した安全性証明可能な構成方法に関して解説する．最後に，RSA暗号と同程度の安全性を，より短い鍵長で構成できる楕円曲線暗号を説明する．

キーワード：公開鍵暗号，RSA暗号，楕円曲線暗号，安全性証明，Semantic Security

1. はじめに

公開鍵暗号は，クレジットカードの番号を暗号化してサーバに送信するなど，インターネットの暗号方式としてすでに広く普及している．公開鍵暗号の構成には，トラップドア付きの一方向関数が必要となる．送信者はサーバの公開鍵のみを利用した一方向関数により平文の暗号化を行い，サーバはトラップドアを作動させる秘密鍵により暗号文を復号化することができる．攻撃者は，秘密鍵の解読を試みるだけでなく，トラップドア付きの一方向関数を破ることも試みる．

本稿では，公開鍵暗号方式として最も普及しているRSA暗号について解説する．2節では，RSA暗号のトラップドアの構成方法および一方向関数の完全解読について解説する．3節では，RSA暗号の平文ビットの安全性に関する証明方法およびランダムパディングによるRSA暗号の方法を紹介する．4節では，平文の部分情報を漏らさないSemantic Securityを解説し，能動的攻撃方法としてBleichenbacherの攻撃法および選択暗号文攻撃に対して安全な（IND-CCA 2）の構成方法を紹介する．5節では，RSA暗号より短い鍵長を持つ楕円曲線暗号について説明する．

2. RSA暗号

RSA暗号は，Rivest, Shamir, Adlemanにより1978年に発表された世界初の公開鍵暗号方式である[16]．

たかぎ　つよし
公立はこだて未来大学 システム情報科学部
〒041-8655 函館市亀田中野町116-2

本章では，RSA暗号の動作原理に関して解説する．

RSA暗号のトラップドア付き一方向関数は，整数の整除に関する基本的な性質を用いて構成される．2個の整数a，bに対して$a=bq+r$，$0\leq r<b$を満たす整数q，rが一意的に存在する．このq，rを，aをbで割った商qと余りrといい，$r=a \bmod b$と書く．2個の整数の公約数が1であるとき互いに素という．整数kの余り全体の集合$\boldsymbol{Z}_k=\{0,1,2,\cdots,k-1\}$は環をなし，$k$を法とする剰余環という．剰余環$\boldsymbol{Z}_k$の元で$k$と互いに素となる全体は群をなし，$k$を法とする乗法群$\boldsymbol{Z}_k^{\times}$という．

RSA暗号の安全性は素因数分解の計算量的困難性を基にしている．そのため，RSA暗号は2個の素数p，qに対して$n=pq$を法とする乗法群$\boldsymbol{Z}_n^{\times}$の上で構成される．ここで，乗法群$\boldsymbol{Z}_n^{\times}$の位数は$(p-1)(q-1)$となり，RSA暗号のトラップドアは，$n$と互いに素な整数$m$に対して$m^{(p-1)(q-1)}=1 \bmod n$を満たす性質（オイラーの定理）を利用する．以下，RSA暗号の構成方法を示す（図1を参照）．

[**鍵生成**] 2個の素数p，qを生成し$n=pq$とする．$ed=1 \bmod (p-1)(q-1)$を満たす整数e，dを生成する．公開鍵を(e,n)，秘密鍵はdとする．公開鍵(e,n)はインターネットにおいて公開し，秘密鍵dはサーバにおいて安全に保存する．

[**暗号化**] 平文mは剰余環$\boldsymbol{Z}_n=\{0,1,2,\cdots,n-1\}$の元とする．公開鍵$(e,n)$をインターネットよりダウンロードして，平文$m$に対して，公開鍵$(e,n)$を利用して，暗号化$c=m^e \bmod n$を計算

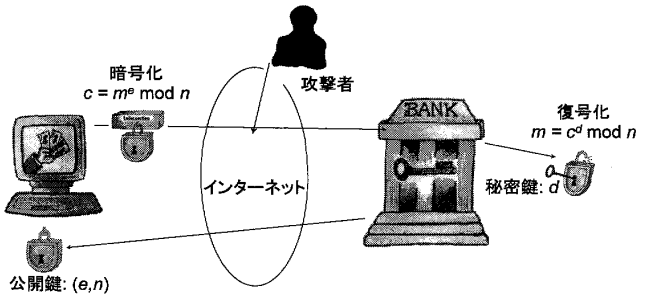

図1　RSA 暗号を利用した公開鍵暗号方式

する．暗号文 c をインターネット経由でサーバに送信する．

［**復号化**］暗号文 c と公開鍵 n に対して，秘密鍵 d を利用して，復号化 $m=c^d \bmod n$ を行う．

ここで，ある整数 h が存在して $ed=1+h(p-1)(q-1)$ となるため，m と n が互いに素である場合は，$c^d=m^{ed}=m^{1+h(p-1)(q-1)}=m \bmod n$ より復号化できる．また，m と n が互いに素ではない場合は，$m=0 \bmod p$，$m=0 \bmod q$，または $m=0$ を満たすが，この場合も同様に復号化可能である．

2.1　RSA 暗号の完全解読

RSA 暗号は素因数分解の困難性を安全性の根拠にしている．もし公開鍵 $n=pq$ が素因数分解された場合，秘密鍵 d は $d=e^{-1} \bmod (p-1)(q-1)$ により求めることが可能であり，RSA 暗号は完全に解読される．現在知られている最も高速な素因数分解アルゴリズムは数体篩法[12]であり，n のビット長に対して準指数時間の計算時間が必要である．この公開鍵 n のサイズが RSA 暗号の鍵長といわれ，2008 年現在のところ 1024 ビットや 2048 ビットが選ばれることが多い．将来的には，素因数分解アルゴリズムの改良や計算機のソフトウェア/ハードウェアの進展により，より長い鍵長を選択する必要がある．RSA 暗号の安全な鍵長に関する見積もりは，CRYPTREC より詳しい報告書が出されている[7]．

次に，一方向性の意味での安全性について説明する．以下，鍵長が ℓ ビットの RSA 暗号における公開鍵全体の集合を RSA_ℓ と書き，RSA 暗号の一方向性を形式的に定義する．自然数全体の集合を $\mathbf{N}$，実数全体の集合を $\mathbf{R}$ と書く．関数 $\epsilon(\ell)$: $\mathbf{N}\to\mathbf{R}$ が negligible とは，任意の整数 $\alpha>0$ に対して，ある整数 $\ell_\alpha>0$ が存在して，$\ell>\ell_\alpha$ を満たすすべての ℓ において $\epsilon(\ell)<1/\ell^\alpha$ となることをいう．RSA_ℓ からランダムに選んだ公開鍵 (e, n) とランダムな暗号文 $c\in\mathbf{Z}_n$ から，平文 m を求めるアルゴリズム $\mathcal{A}$ を考える．入力サイズ ℓ のすべての多項式時間アルゴリズム $\mathcal{A}$ に対して，確率

$$Pr\left[\begin{matrix}(e,n)\leftarrow RSA_\ell,\ m\leftarrow \mathbf{Z}_n,\\ c\leftarrow m^e \bmod n:\ \mathcal{A}(e,n,c)=m\end{matrix}\right]<\epsilon(\ell)$$

が negligible になる場合に，RSA 暗号は一方向性の意味で安全であるという．

RSA 暗号の一方向性を破るには，公開鍵 (e, n) と暗号文 c から対応する e 乗根 $m=c^{1/e} \bmod n$ を求めることができればよい．公開鍵 n を素因数分解することなく，RSA 暗号の一方向性を解読することができるかは現在のところ不明である[5]．

3.　平文ビットの安全性

RSA 暗号の平文空間 $\mathbf{Z}_n$ の位数は，1024 ビット以上の大きさを有している．2 節では平文 m を破る一方向性に関して議論したが，平文 m の部分情報（例えば 1 ビット）を破ることは可能ではないか？　という疑問が生じる．そのため，平文ビットの解読の難易度を調べる研究が行われている．3 節では，平文の最下位ビットを解読することが，平文全体の解読と同等の困難性を有していることを証明する方法を紹介する[10]．

証明方針は，平文の下位ビットを求めるアルゴリズムの存在を仮定した場合に，そのアルゴリズムを用いて平文全体が解読できる方法を示すことにある．つまり，RSA 暗号が一方向性の意味で安全となる場合，平文の最下位ビットも安全となる．

公開鍵 n を ℓ ビットとし，平文 m のバイナリ表現を $m=m_{\ell-1}2^{\ell-1}+\cdots+m_1 2^1+m_0 (m_i\in\{0,1\},\ i=0,1,\cdots,\ell-1)$ とする．平文 m の最下位ビットは m_0 であり，$m_0=0$ の場合 m は偶数，$m_0=1$ の場合は m は奇数となる．与えられた公開鍵 (e, n) と暗号文 c から，平文 m の最下位ビット m_0 を求めるアルゴリズムを $\mathcal{A}_{LSB}$ とする．アルゴリズム $\mathcal{A}_{LSB}$ は，入力 e，n，c に対して 1 ビットの情報 m_0 を出力する関数である．ここで，平文の最下位ビット m_0 と $m2^{-1} \bmod n$ の大きさには，次の関係式が成り立つ．

$$\begin{cases}0\le m2^{-1} \bmod n<n/2\\ n/2<m2^{-1} \bmod n<n\end{cases}\iff\begin{cases}m_0=0,\\ m_0=1.\end{cases}$$

言い換えると，平文空間 $[0, n]$ において，平文 m が領域 $[0, n/2]$ に属するための必要十分条件は $2m \bmod n$ の最下位ビットが 0 となることである．また，

Algorithm 1：帰着アルゴリズム LSB-RSA

Input: 公開鍵 (e, n), 暗号文 c, n のビット長 ℓ
Output: 平文 m s.t. $c = m^e \bmod n$
1. **for** $j = 0$ **to** $\ell - 1$ **do**
   $y_j \leftarrow \mathcal{A}_{LSB}(c2^e)$; $c \leftarrow c2^e \bmod n$;
2. $a \leftarrow 0$; $b \leftarrow n$;
   for $j = 0$ **to** $\ell - 1$ **do**
   $d \leftarrow (a + b)/2$;
   if $y_i = 1$ **then** $a = d$;
   else $b = d$;
3. **return** $[d]$;

RSA暗号の準同型性から関係式 $c2^e = (2m)^e \bmod n$ を満たす．よって，平文 m の暗号文と公開鍵 (e, n) の情報より，平文 $2m \bmod n$ の暗号文である $c2^e \bmod n$ を生成できる．以上より，平文 m が領域 $[0, n/2]$ に属するための必要十分条件は $\mathcal{A}_{LSB}(c2^e \bmod n) = 0$ となる．以上より，アルゴリズム $\mathcal{A}$ を1回動かすことにより平文検索空間が半分の大きさになるため，Algorithm 1の平文 m に関する2分検索が可能となる．Algorithm 1において，アルゴリズム $\mathcal{A}_{LSB}$ は ℓ 回動作し，他のステップもサイズ ℓ の多項式時間である．このAlgorithm 1は，平文の最下位ビットの安全性を，RSA暗号の一方向性の困難性に帰着するアルゴリズムとみなせる．

以上の証明ではオラクルの回答が完全な（100%正しい）場合を考察した．一方，オラクルが1/2よりnon-negligibleで大きな確率において正しい回答を与える場合でも，多数決原理，ランダム抽出方法，Chebyshev不等式などを利用して，同様の安全性結果を得ることができる[1]．また，最下位ビット以外の安全性については，下位 $\log(\log n)$ ビットに関しても同様の証明が得られることが知られている[1]．

3.1 乱数パディングによるRSA暗号化

RSA暗号の暗号化 $c = m^e \bmod n$ は決定的関数である．そのため平文 m が小さな空間（例えば4桁の暗証番号）から選択された場合，その空間に含まれる元の総当たりにより平文 m を解読することが可能である．実際，1回の暗号化演算 $c = m^e \bmod n$ が汎用PCにおいて1ミリ秒必要（実際はより高速）とすると，4桁の暗号暗証番号の空間は10,000通りであるため10秒程度で総当たり攻撃が可能である．

この場合，上位ビットにランダムなビット列 r をパディングすること $c = (r|m)^e$ により暗号化する方法が考えられる．3節で述べたように，平文 m のサイズが $\log(\log n)$ ビット程度の場合は，RSA暗号の一方向性の意味で安全であることが証明できる．

4. Semantic Security

GoldwasserとMicaliは，公開鍵と暗号文から対応する平文に関する情報を一切漏らさないSemantic Securityという公開鍵暗号の安全性を定式化した[9]．

以下，Semantic Securityを定義するため，アルゴリズム $A_{SS} = (A^1_{SS}, A^2_{SS})$ を説明する．アルゴリズム A^1_{SS} は，公開鍵 (e, n) から，2個の平文 $m_0, m_1 \in \mathbf{Z}_n$ を生成する．$b \in \{0, 1\}$ をランダムに選び，一方の平文 m_b の暗号化 $c = m_b^e \bmod n$ を行う．アルゴリズム A^2_{SS} は，入力 m_0, m_1, c に対して，ビット b を推測する関数とする．RSA暗号がSemantic Securityを満たすとは，入力サイズ ℓ の任意の多項式時間アルゴリズム $A_{SS} = (A^1_{SS}, A^2_{SS})$ が以下を満たすことをいう．

$$\left| Pr\left[\begin{array}{c} (e, n) \leftarrow RSA_\ell, \\ m_0, m_1 \leftarrow \mathcal{A}^1_{SS}(e, n), \\ b \leftarrow \{0, 1\}, c \leftarrow m_b^e \bmod n : \\ \mathcal{A}^2_{SS}(e, n, m_0, m_1, c) = b \end{array} \right] - \frac{1}{2} \right| < \epsilon(\ell)$$

ここで，$\epsilon(\ell)$ は2.1節で述べたnegligibleな関数とする．アルゴリズム $\mathcal{A}_{SS}$ がランダムなビットを出力すると，丁度確率1/2で b を当てることができる．そのため，アルゴリズム $\mathcal{A}_{SS}$ の正解確率から1/2が引かれた値が，ビット情報 b を推測できる成功確率となる．

4.1 RSA暗号を利用した構成方法

BellareとRogawayは，RSA暗号を利用してSemantic Securityの意味で安全な公開鍵暗号の構成方法を提案した[2]（図2参照）．

[**鍵生成**] ℓ ビットのRSA暗号の鍵集合 RSA_ℓ から，公開鍵 (e, n) と秘密鍵 d を選択する．ℓ ビット入力に対して $\ell_0 (< \ell)$ ビットを出力するランダム関数 $g: \{0, 1\}^\ell \rightarrow \{0, 1\}^{\ell_0}$ も公開する．

[**暗号化**] 平文 m を ℓ_0 ビットのビット列とする．ℓ ビットの乱数 r を生成し，公開鍵 (e, n) とランダム関数 g により，平文 m を暗号化

$$(c_0, c_1) = (r^e \bmod n, g(r) \oplus m)$$

する（$\oplus$ はビット毎の排他的論理和とする）．

[**復号化**] 暗号文 (c_0, c_1) に対して，秘密鍵 d を利用して復号化 $r = c_0^d \bmod n$ および $m = g(r) \oplus c_1$ を行う．

以下，上記の暗号方式が，RSA暗号が一方向性を満たすとしてSemantic Securityであることを証明す

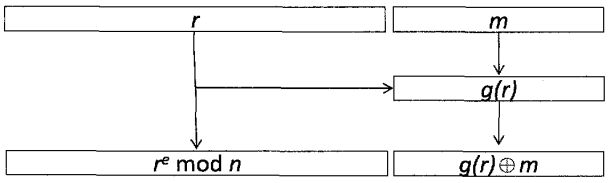

図2　Semantic Security を満たす RSA 暗号

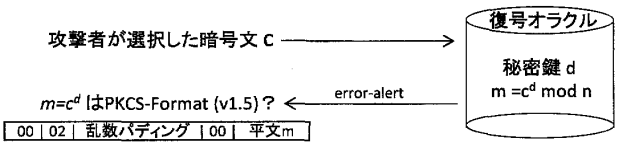

図3　Bleichenbacher による PKCS#1 v1.5 への攻撃

る．証明テクニックとして，Semantic Security を non-negligible な確率（$>\epsilon(\ell)$）で解読するアルゴリズム $\mathcal{A}$ の存在を仮定して，RSA 暗号の一方向性を破る敵として振舞うシミュレータ S を作成できることを示す．

最初に，S には n を法とする RSA 暗号のランダムな暗号文 y^* および ℓ_0 ビットのランダム値 h^* が与えられる．また，S はランダム関数 g の入出力 $(r, g(r))$ のリスト $L(g)$ を管理する．g に新しいクエリ r があった場合，ℓ_0 ビットの乱数 r_ℓ を生成して (r, r_ℓ) を $L(g)$ に加える．r がすでに $L(g)$ に属している場合は，$(r, g(r))\in L(g)$ の $g(r)$ を出力する．次に，S はアルゴリズム $\mathcal{A}_{SS}^1$ により 2 個の平文 m_0，m_1 を得る．S は $b\leftarrow\{0,1\}$ をランダムに選び，m_b の暗号文として (y^*, h^*) を出力する．S はアルゴリズム $\mathcal{A}_{SS}^2(m_0, m_1, (y^*, h^*))$ により b を得る．S は最終的に，ランダム関数 g のリストの中から $y^*=(x^*)^e \bmod n$ を満たす x^* を出力する．

ここで，x^* が $L(g)$ に含まれる確率が，non-negligible（$>\epsilon(\ell)$）であることを示す．もし，x^* が $L(g)$ に含まれない場合は，b をランダムより高い確率で推測できないため次の関係式を満たす．

$$Pr[A_{SS}^2(m_0, m_1, (y^*, h^*))=b|x^*\notin L(g)]=\frac{1}{2}$$

以下，$A_{SS}^2(m_0, m_1, (y^*, h^*))=A$ と表記し，$Pr[A=b]$ を求める成功確率を $Adv(\mathcal{A})$ と書く．確率の基本的な性質より次の変形ができる．

$$\begin{aligned}\frac{1}{2}+Adv(\mathcal{A})&=Pr[A=b]\\&=Pr[A=b\wedge x^*\in L(g)]\\&\quad+Pr[A=b\wedge x^*\notin L(g)]\\&=Pr[A=b|x^*\in L(g)]Pr[x^*\\&\quad\in L(g)]+Pr[A=b\wedge x^*\notin L(g)]\\&\leq Pr[x^*\in L(g)]+\frac{1}{2}\end{aligned}$$

ゆえに，$Pr[x^*\in Lg)]\geq Adv(\mathcal{A})$ を得た．Semantic Security が解読できる仮定より，アルゴリズム $\mathcal{A}$ は non-negligible な確率（$Adv(\mathcal{A})>\epsilon(\ell)$）で正しいビット b を得る．以上より，$Pr[x^*\in L(g)]>\epsilon(\ell)$ を満たし，non-negligible な確率で $x^*=(y^*)^{1/e} \bmod n$ を求める（RSA 暗号の一方向性を破る）ことができた．

4.2　適応的選択暗号文攻撃に対する安全性（IND-CCA2）

公開鍵暗号はクレジットカードを暗号化してサーバに送信する暗号化通信 SSL などに利用される．暗号文はサーバで復号化され，平文に対する乱数パディングのチェックなどの検査が行われる．例えば，SSL において平文に対する乱数パディングが正当でない場合は，送信者に error alert のサインが返信される．Bleichenbacher は，国際会議 CRYPTO'98 において RSA 暗号の乱数パディング方式（PKCS#1 v1.5 [14]）に対して能動的攻撃が可能であることを示した [4]．PKCS#1 v1.5 の上位バイトは |00|02| という固定値を取っている．攻撃者は任意に選んだ暗号文 c に対して，error alert より c の平文 m の上位バイトが |00|02| であるかの情報を得る（図 3 参照）．

実際，攻撃対象となる暗号文 $c=m^e \bmod n$ に対して，選択した $s\in\boldsymbol{Z}_n$ に対する暗号文 $c'=cs^e \bmod n$ を生成し，サーバの復号化から error alert を得る．この問合せを複数の s に対して行い，得られた答えにより平文 m が解読できる．このように復号化関数へアクセスするタイプの攻撃は，適応的選択暗号文攻撃といわれる．

現在では，適応的選択暗号文攻撃に対して Semantic Security を満たすこと（IND-CCA 2）が公開鍵暗号の標準的な安全性基準となっている．RSA 暗号の一方向性仮定の下で IND-CCA 2 を満たす公開鍵暗号として RSA-OAEP がある [8]．RSA 暗号の世界標準としては，RSA-OAEP を使用した PKCS#1 v2.1 が利用されている．

5.　楕円曲線暗号

公開鍵暗号を構成するには，トラップドア付き一方向関数が必要となる．5 節では，素因数分解問題とは異なる構造として，有限体上の楕円曲線の離散対数問

題を基にした楕円曲線暗号を紹介する．楕円曲線暗号は，1985年にMiller[13]とKoblitz[11]に独立に発表された．以下に楕円曲線暗号に関して説明を行う．

$p>3$の素数に対して，$\boldsymbol{Z}_p$上の楕円曲線

$$E(p)=\{(x, y)\in \boldsymbol{Z}_p^2 | y^2=x^3+ax+b\}\cup\{\infty\},$$

を考える．ここで，$a, b\in\boldsymbol{Z}_p$は$4a^3+27b^2\neq 0$を満たす．楕円曲線$E(p)$は無限遠点∞を零元として加法群をなし，点$P=(x, y)$の逆元は$-P=(x, -y)$で与えられる．

通常の楕円曲線暗号では，部分群を利用した攻撃を避けるために曲線の位数が素数となる楕円曲線を生成する必要がある．Hasseの定理$|\#E(p)-p-1|\leq 2\sqrt{p}$より，$p$のビット長が楕円曲線の鍵長となる．また，楕円曲線暗号では1個の曲線をシステムパラメータとして多くユーザが共有して利用することが可能である．現在までに知られている攻撃を考慮した上で，安全な曲線としてSECG (http://www.secg.org/) などから推奨曲線が与えられている．

[**鍵生成**] 素数位数の楕円曲線$E(p)$を生成して，その生成元をGとする．システムパラメータとしてE，Gをユーザ全体で共有する．秘密鍵$s\in\{0, 1, 2, \cdots, \#E(p)-1\}$に対して，$Q=sG$を公開鍵とする．

[**暗号化**] 楕円曲線$E(a, b, p)$上の点Mを平文とする．システムパラメータG，乱数$r\in\{0, 1, 2, \cdots, \#E(p)-1\}$，公開鍵$Q$を利用して，暗号化$C_1=rG$，$C_2=rQ+M$を行い，$(C_1, C_2)$を暗号文とする．

[**復号化**] 暗号文(C_1, C_2)に対して，秘密鍵sを利用して，復号化$M=C_2-sC_1$を行う．

ここで，$C_2-sC_1=(rQ+M)-s(rG)=rsG+M-rsG=M$が成り立つため，平文$M$は一意的に復号可能である．

楕円曲線暗号の安全性は楕円曲線$E(a, b, p)$の離散対数問題の困難性を基にしている．もし公開鍵QとシステムパラメータGから，離散対数問題$Q=sG$が解けたとすると，秘密鍵sが完全解読可能となる．楕円曲線$E(a, b, p)$の離散対数問題は，RSA暗号とは異なり鍵長に対して準指数時間の解読アルゴリズムは知られていない．楕円曲線上の離散対数問題を解く現在知られている最も高速なアルゴリズムはPollardのρ法であり，その計算量は$O(\sqrt{p})$である．1024ビットのRSA暗号と同等レベルの安全性を有する楕円曲線暗号の鍵長は160ビットと見積もられている．このようにRSA暗号と比較して短くなっているため，楕円曲線暗号はメモリの制限された組み込みシステム用ディバイスでの実装に向いているといわれている．

5.1 安全性証明可能な楕円曲線暗号

楕円曲線暗号に対してもSemantic Securityとできる構成方法が幾つか知られている．NTTが開発したPSEC-KEMは，離散対数問題の困難性の仮定の下で安全 (IND-CCA2) であることが証明されている[15]．また，Cramer-Shoup暗号は，Diffie-Hellman判定問題の困難性のもとで標準モデルにおいてIND-CCA2であることが知られている[6]．

参考文献

[1] W. Alexi, B. Chor, O. Goldreich and C. Schnorr, "RSA and Rabin functions: Certain Parts are as Hard as the Whole," SIAM Journal on Computing, Vol. 17, No. 2, pp. 194-209, 1998.

[2] M. Bellare and P. Rogaway, "Random Oracles are Practical, A Paradigm for Designing Efficient Protocols," The first ACM Conference on Computer and Communications Security, pp. 62-73, 1993.

[3] M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption-How to Encrypt with RSA," Eurocrypt'94, LNCS 950, pp. 92-111, 1995.

[4] D. Bleichenbacher, "Chosen Ciphertext Attacks against Protocols based on the RSA Encryption Standard PKCS#1," CRYPTO'98, LNCS 1462, pp. 1-12, Springer, 1998.

[5] D. Boneh and R. Venkatesan, "Breaking RSA May not be Equivalent to Factoring," EUROCRYPT'98, LNCS 1233, pp. 59-71, Springer, 1998.

[6] R. Cramer and V. Shoup, "A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack," CRYPTO'98, LNCS 1462, pp. 13-25, 1998.

[7] Cryptography Research and Evaluation Committees, http://www.cryptrec.jp/.

[8] E. Fujisaki, T. Okamoto, D. Pointcheval and J. Stern, "RSA-OAEP Is Secure under the RSA Assumption," Journal of Cryptology, Vol. 17, No. 2, pp. 81-104, 2004.

[9] S. Goldwasser and S. Micali, "Probabilistic Encryp-

tion," Journal of Computer and System Sciences, Vol. 28, pp. 270-299, 1984.

[10] S. Goldwasser, S. Micali and P. Tong, "Why and How to Establish a Private Code on a Public Network," The 23rd Annual Symposium on Foundations of Computer Science, FOCS'82, pp. 134-144, 1982.

[11] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, Vol. 48, pp. 203-209, 1987.

[12] A. K. Lenstra and H. W. Lenstra, Jr. (eds.), *The Development of the Number Field Sieve*, Lecture Notes in Mathematics 1554, Springer, 1993.

[13] V. Miller, "Use of Elliptic Curves in Cryptography," CRYPTO'85, LNCS 218, pp. 417-426, 1985.

[14] PKCS#1 : RSA Cryptography Standard, RSA Laboratories, http://www.rsa.com/rsalabs/.

[15] PSEC-KEM, Provably Secure Elliptic Curve encryption with Key Encapsulation Mechanism, http://info.isl.ntt.co.jp/crypt/psec/.

[16] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of ACM, Vol. 21, No. 2, pp. 120-126, 1978.