公開鍵暗号の最近の話

2 安全性が証明された新しい公開鍵暗号

岡本 龍明　藤崎 英一郎　内山 成憲
NTT情報流通プラットフォーム研究所

安全性の証明が標準方式の決め手に

前回は，楕円曲線暗号の安全性について解説した[16]．今回は，公開鍵暗号[8]の安全性について前回提示した以下のような問題に答えることを目的としよう．

- 公開鍵暗号が安全である（安全でない）とはどういう意味か？
- 安全であることをどのように定義するか？　また，証明するか？
- 安全であると証明された公開鍵暗号にはどのようなものがあるか？

このような問題を考える上で，まず最近話題になった「事件」を取り上げよう．この事件とは，1998年6月に，現在最も広く使われている公開鍵暗号であるRSA暗号の標準的な利用フォーマットPKCS（Public-Key Cryptography Standards）#1に対する攻撃法がベル研究所の研究者により発表されたことである（以降，この攻撃法の発明者の名前をとり，Bleichenbacher攻撃法という[4]）．この攻撃法の内容は後でもう少し正確に述べるが，PKCS#1を作ったRSAデータセキュリティ社では，この攻撃が発表されると直ちにPKCS#1を改訂した（現在は，古いPKCS#1をPKCS#1バージョン1と呼び，新しいPKCS#1をPKCS#1バージョン2と呼んでいる）．RSAデータセキュリティ社は，このPKCS#1バージョン2としてカリフォルニア州立大学の研究者によりすでに提案されていたOAEP（Optimal Asymmetric Encrytion Padding）というRSA暗号[21]の利用方式を採用した．それでは，なぜOAEPが選ばれたのであろうか？　その理由は，OAEPが最も強力な攻撃法に対してさえも安全であるという（ある種の）証明が付いている，いわゆる安全性の証明付き（provably secure）の方式であったためである．なお，OAEPは，インターネット上での標準的なクレジットカード決済プロトコルであるSET（Secure Electronic Transaction）でも採用されており，RSA暗号の標準的な利用方式としての地位を確保しつつある．つまり，安全性の証明が付いているということが標準的な方式となるための決め手になったわけである．

一方，1998年にNTTはある種の安全性の証明の付いたEPOC暗号を，また同年，IBMとスイス連邦工科大学（ETH）の研究者は別の意味の安全性の証明の付いたCramer-Shoup暗号を発表した．

本稿では，このような公開鍵暗号に関する安全性の証明の意味（上で述べた「ある種の安全性の証明」の意味など）ならびにOAEP, EPOC, Cramer-Shoupなどの暗号の安全性がそれぞれどのような意味で証明されているかについて解説しよう．

公開鍵暗号の安全性

本稿の読者の多くは，暗号を破るとは暗号文（と公開情報）を与えられてから解読作業を行い，平文を読み取ることと考えているだろう．しかし，理論的に暗号の安全性を考えるときは，解読するために行う攻撃の種類や，解読される（秘密が漏れる）度合いを分類・定義する．そして，最も強力な攻撃を前提としても最も強い秘匿性（いかなる部分秘密情報も漏らさないというような性質）を持つような暗号方式が安全であると考えるのである．

したがって，理論的な意味で安全でない（ある種の解読法がある）とされた暗号が，現実的な環境で直ちに危険であるとはいえない．しかしながら，最初に述べたRSA暗号のPKCS#1の攻撃法（Bleichenbacher攻撃法）を例にして，理論的な安全性ならびにその証明が現実においてもそれなりの意味を持つことを説明しよう．

理論的安全性の意義：ケーススタディ

まず，先ほど述べたBleichenbacher攻撃法を説明しよ

う．RSA暗号の実用化を推進しているRSAデータセキュリティ社では，RSA暗号などの公開鍵暗号をさまざまな応用に利用するための標準的な利用フォーマットPKCS（Public-Key Cryptography Standards）を定めている．最も代表的なものが，RSA暗号に基づくデータ暗号（鍵配送）のための利用フォーマットで，PKCS#1と呼ばれるものである．現在RSA暗号を利用する多くのアプリケーションがこのPKCS#1フォーマットを使っているため，利用者は単にRSA暗号を利用していると思っていても，実はPKCS#1フォーマットのRSA暗号を使っている場合が非常に多いのである．1998年6月に発表されたBleichenbacher攻撃法とは，RSA暗号そのものに対する攻撃法ではなく，このPKCS#1フォーマットのRSA暗号に対する攻撃法である．

PKCS#1フォーマットでは，平文の特定部分がフォーマットの識別子として特定の値になっており，受信者は暗号データを受信するとそれを復号し，この特定部分のデータをチェックする．一方，受信データのチェック結果を送信者に通知するのは通信プロトコルとしては常識的な設計である．Bleichenbacher攻撃法は，このような常識的な環境の下で，あるルールにより作った暗号文を受信者（復号者）に送り，受信者がその復号結果を正しいデータであると答えるか間違ったデータであると答えるかの1ビット情報を得ることによって，これを繰り返し行いRSA暗号の解読を行うものである．

この攻撃法のエッセンスは，RSA暗号の復号結果の特定部分（たとえば，先頭1ビット）の情報を攻撃者に繰り返し教えると，RSA暗号全体の解読につながるということである．つまり，RSA暗号はある種の（能動的な）攻撃に対して決して安全でないということが現実的な環境の中で明示されたことになる．

従来，復号鍵（秘密鍵）を持っている人に適当な暗号文を解読してもらうことにより，ある特定の暗号文解読を行うという能動的な攻撃法は理論的な攻撃法であり，そのような攻撃法に対しては復号結果を不用意に相手に渡すようなことをしないように運用で制限すれば防げるため，能動的な攻撃は現実にはあまり深刻な影響はないと考えられてきた．

ところが，Bleichenbacher攻撃法により，能動的攻撃で1ビットの復号情報を相手から得るといったことが現実の環境で可能であり，それがRSA暗号を完全に復号することにつながるということが示されたため，関係者に大きな衝撃を与えた．

この攻撃が可能となった原因は，大きく2つに分類できる．1つは復号データをフォーマットチェックしそれを相手に通知した通信プロトコルの問題である．もう1つの問題は，PKCS#1である．そしてBleichenbacher攻撃法に対する対策も，通信プロトコルを改訂しフォーマットチェック結果を通知しないようにすることと，PKCS#1を改訂することの2つの方法がある．これについては，筆者は以下のような方針で設計すべきであると考える．

- 通信プロトコルは，本来正しく通信が行われているかどうかをチェックする必要があり，フォーマットチェックの結果は原則として送信者に通知すべきである．
- 暗号方式は，いかなる能動的攻撃に対しても安全であるように設計されるべきである．つまり，通信プロトコルがいかなるチェック結果を通知しようが，また受信者が不用意に復号結果を相手に伝えようが，暗号方式そのものが安全性を保証するべきである．

上記の観点に立てば，PKCS#1を安全性が保証されたOAEPに変更した方針は正しいものであったと考える．したがって，今後我々が実用的に用いる暗号は，このような安全性の保証（安全性の証明）の付いたものを極力使うべきであるという結論に達するのである．

どのように安全性を証明するか

それでは，公開鍵暗号の安全性の証明とはどのように行うのであろうか？　ここでは，その基本となる考え方を述べよう．

公開鍵暗号は公開鍵と秘密鍵がある関係を持っているため，十分に大きな計算能力を持つ解読者ならば，公開鍵から秘密鍵を求めることができる．しかし，我々が通常活用できる程度の計算能力ではそのような解読が困難であるという仮定の下で利用されるのが公開鍵暗号である．

それでは，この「我々が通常活用できる程度の計算能力では解読が困難」ということをどのように証明することができるのだろうか？　これに対する現時点での回答は以下のようになる．

- 暗号解読するという問題を考えたとき，その問題を解くために必要な計算時間がその問題のサイズの多項式のオーダとなるならば，「我々が通常活用できる計算能力では解読が可能」と考える．つまり，どのような多項式時間のアルゴリズムを用いても解読できないならば，その方式は安全であると考える．ここで，解読の問題を漸近的に（つまり，問題のサイズを大きくしていったときの計算時間の増え方として）とらえていることに注意されたい．このような問題のとらえ方は，計算量理論を踏襲したものである．
- 現在，たとえば，素因数分解といった非常に基本的な問題ですら，多項式時間で計算できる問題のクラスに属するのかそれとも，どのような多項式時間のアルゴリズムを用いても計算できないクラスに属するのかは分かっていない．このようなことを明らかにすることは，P vs NP問題に代表される計算機科学で最も重要な未解決問題であるが，現時点では解決の糸口すら見つかっていない大変難しい問題である．したがって，上で述べた観点で，ある暗号方式が安全であるかどうかを（現時点では）示す

ことはできない．

そこで，次善の方法として，相対的に安全性を証明することを考える．つまり，あるもっともらしい仮定を前提にすれば，安全であることを示そうということである．たとえば，素因数分解の問題は，数学そのものと同じくらいの歴史を持っているにもかかわらず，いまだに多項式時間のアルゴリズムが発見されていないことより，この問題は困難である（多項式時間のアルゴリズムがない）と仮定する．そのとき，この仮定の下で，いくつかの公開鍵暗号系は，安全であることが証明される．

上記のような立場で，公開鍵暗号方式の安全性を証明する試みが1980年代以降活発に研究されてきた．その結果，現在では安全性の定義や証明の手法に関する標準的な理論が確立しつつある．そこでまず，安全性の定義を紹介しよう．

安全性の定義

暗号は攻撃者（盗聴者）に通信内容を隠して送ることを目的とするため，どの程度通信内容を隠しているかの度合いが重要である．それを本稿では暗号の秘匿性と呼ぶ．さらに，暗号文から平文の内容を知ることはできないが，暗号文を操作することにより，対応する平文に意図的な変更を加えること（たとえば，平文をビット反転させる）などの攻撃があり得る．このようなことが一切できないことを頑強性（non-malleable性）と呼ぶ．このような秘匿性と頑強性をまとめて達成度と呼ぶ．

一方，攻撃者のタイプには単に暗号通信を受信し，それだけから解読を試みる受動的攻撃と，Bleichenbacher攻撃法のように送信者にさまざまな質問をし（暗号文を送り）その回答（その復号結果）をもらうことが許され，そこで得られた情報を利用して目的とする暗号文の解読をするような能動的攻撃がある．

このように，暗号の強度は，「達成度」と「攻撃法」との組として分類することができる．

以上の観点より，公開鍵暗号の安全性を次のように分類する．

達成度
- 秘匿性
  - 完全解読困難（一方向性）（**one-way: OW**）：暗号文より平文を完全に求めることが困難なこと．暗号関数の一方向性ともいう．
  - 部分解読困難：暗号文より平文の部分情報が求めることが困難なこと．たとえば，平文のある1ビットを求めることが困難であるなどである．ここで，解読の対象となる1ビットは，平文の最上位ビットなどの特定の位置の1ビットの場合だけでなく，平文のヤコビ記号の値などの関数値の1ビットである場合もある．
    また，平文が限定された場合（たとえば，0か1かの1ビットである場合）に暗号文から平文を求めることが困難であることもこの部分解読困難に含めることができる．
  - 強秘匿（**semantically secure / indistinguishable: IND**）：どのような部分情報も部分解読困難なこと[12]．
- 頑強性（**non-malleability: NM**）：どのような関係f（平文のサイズのような自明な関係を除く）に対しても，攻撃者が$c = E(m)$から$m' = f(m)$を満足するような$c' = E(m')$を作成できなければ，頑強（non-malleable）であると呼ぶ（ここで，Eは公開の暗号化関数である）．

攻撃法
- 受動的攻撃
  - 暗号文攻撃（**ciphertext-only attack**）：暗号文だけを利用する攻撃（受動的攻撃）．
  - 選択平文攻撃（**chosen-plaintext attack: CPA**）：平文を選択し，暗号化関数をオラクルとして用いて対応する暗号文を知り得る状況下で，攻撃対象の暗号文を解読しようとする攻撃，公開鍵暗号では，暗号鍵が公開されているので常にこの攻撃は実行可能であるため，選択平文攻撃は，暗号文だけを利用する攻撃（受動的攻撃）と等価である．
- 能動的攻撃：選択暗号文攻撃（**chosen-ciphertext attack: CCA**）：解読者が任意に選んだ暗号文を真の受信者（復号オラクル）に復号させた後に，そこで得た情報と公開情報を用いて，攻撃対象の暗号文を復号する攻撃．当然，攻撃対象の暗号文を復号オラクルに復号してもらうことはできないが，それ以外ならば何を復号してもらってもよい．
  攻撃対象の暗号文を知る以前にしか復号オラクルに聞けない場合を第1種の選択暗号文攻撃（CCA1）といい，いつでも自由に復号オラクルに聞ける場合を第2種の選択暗号文攻撃（CCA2）という．当然，CCA2はCCA1よりも強力な攻撃法である．第1種の選択暗号文攻撃は，歴史的にランチタイム攻撃，非適応的選択暗号文攻撃（non-adaptive chosen-ciphertext attack）などともいわれ，また，第2種の選択暗号文攻撃は，適応的選択暗号文攻撃（adaptive chosen-ciphertext attack）とも呼ばれる．

以上の定義により，暗号の安全性としては，達成度の観点でOW, IND, NMなどの種類があり，攻撃法でCPA, CCA1, CCA2などの種類がある．したがって，たとえば（OW, IND, NM）と（CPA, CCA1, CCA2）を組み合わせて$3 \times 3 = 9$通りの安全性が定義できる．つまり，受動的な攻撃に対して完全解読困難（OW-CPA），受動的な攻撃に対して強秘匿（IND-CPA），受動的な攻撃に対して頑強（NM-CPA），能動的な攻撃に対して完全解読困難（OW-CCA1, OW-CCA2），能動的な攻撃に対して強秘匿（IND-CCA1, IND-CCA2），能動的な攻撃に対して頑強（NM-CCA1, NM-CCA2）などが定義できる．

上記の達成度と攻撃法の分類において，それぞれ下の項目の方がより強い安全性を保証する．したがって，最も安全な公開鍵暗号とは，攻撃者に第2種の選択暗号文攻撃を許したとしても，頑強性を保持する方式である．

なお，本稿ではこれらのフォーマルな定義については示さないので，興味ある方は文献1）を参照されたい．

安全性証明理論の歴史

まず，暗号の安全性を証明するという方向付けをした歴史的に意義のある結果が1979年にRabinにより与えられた．彼は，素因数分解の困難さを仮定して，彼の公開鍵暗号法（Rabin法）が受動的攻撃に対して完全解読困難（OW-CPA）であることを証明した[19]．

1980年代に入ると，GoldwasserとMicaliにより，暗号の安全性をフォーマルに定式化し証明するという研究が強力に押し進められた．まず，1982年に彼らは強秘匿性の概念を初めて導入し定式化するとともに，ある整数論的な仮定（平方剰余仮定）の下で受動的攻撃に対して強秘匿（IND-CPA）であるような暗号（Goldwasser-Micali暗号）を示した[12]．

1985年に，GoldwasserとMicaliは，Rackoffの協力を得てゼロ知識証明の理論を発表した[13]．この理論はさまざまな応用を持つ大変重要な成果であり，安全性の証明の付いた公開鍵暗号を実現する上でも重要な役割を果たすことになる．

1990年には，NaorとYungにより，能動的攻撃（第1種の選択暗号文攻撃）に対して強秘匿（IND-CCA1）である公開鍵暗号方式が初めて示された[14]．しかし，この実現には一般的な（非対話型）ゼロ知識証明が使われており，決して効率的な方式とはいえない．

1991年に，RackoffとSimonは，NaorとYungにより定義された能動的攻撃（第1種の選択暗号文攻撃）の概念を拡張し，第2種の選択暗号文攻撃（CCA2）を導入した[20]．

1991年に，Dolev，Dwork，Naorは頑健性の概念を導入し，能動的攻撃に対して頑健（NM-CCA2）であるような暗号方式を初めて示した[7]．この実現においてもゼロ知識証明が有効に使われているが，非効率であり実用的な方式ではない．しかし彼らの結果により，「理論的には」最も安全な方式（NM-CCA2）が実現できることが示されたことになる．これ以降，最も安全な方式（NM-CCA2）が「(単に）実現できるかどうか」から「効率的に実現できるかどうか」に興味の対象が移ることになる．

安全性が証明された方式を「効率的に」実現するために，1993年以降，BellareとRogawayは新たなアプローチを開拓した[2]．それは，ランダムオラクルモデルと呼ばれるもので，理想的なランダム関数を仮定することにより安全性の証明を行う．ランダム関数の仮定そのものは非現実的であるため，実際にはランダム関数を実用的な一方向性関数で置き換えることに実用的な暗号を構成する．このとき，実用的な一方向性関数を用いた暗号方式は安全性が証明されたものではなくなるが，安全性が証明された暗号方式の近似版であるため，ある種の安全性の保証があるものと考える．

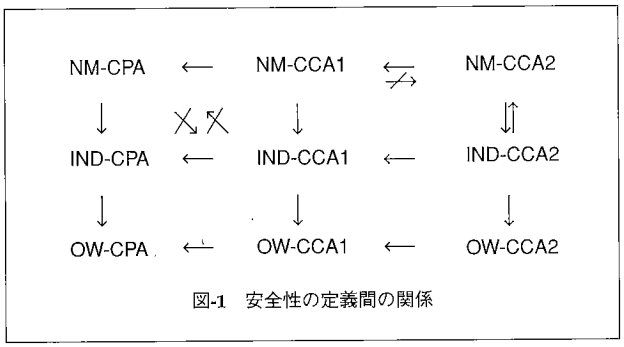

図-1　安全性の定義間の関係

1994年に，Bellare, Rogawayは，ランダムオラクルモデルとRSA暗号（落とし戸付き一方向性置換）に基づき，最も安全な方式（NM-CCA2）をきわめて効率よく構成する方法を示している[3]．これが，OAEP（Optimal Asymmetric Encryption Padding）と呼ばれている方式であり，前に述べたようにRSA暗号の標準的利用方法であるPKCS#1バージョン2となっている．

安全性の定義間の関係

暗号の安全性が，達成度と攻撃法の組により分類されることは前章で述べた．そこで，第1種の選択暗号文攻撃（CCA1）に対して，頑強性（NM）を保持する暗号を，NM-CCA1，第2種の選択暗号文攻撃（CCA2）に対して，強秘匿（IND）である暗号をIND-CCA2などと表すことにする．

1998年，上で述べた安全性の定義間の（いくつかの）関係が，Bellare, Desai, Pointcheval, Rogawayにより明確化された[1]．

以下に，その関係を**図-1**に示す．その一部の関係はすでに知られていたが，彼らは安全性の定義を，過去の定義を包括しながら，見通しよく再定義し直し，さらにいくつか新たな関係を証明した．以下，A→Bは，ある暗号方式がAならばBであることを意味する．A ↛ Bはその否定である．

彼らの結果の中で，重要なものは以下である．

1. ある方式がNM-CPAであっても，必ずしもIND-CCA1とは限らない．
2. ある方式がIND-CCA1であっても，必ずしもNM-CPAとは限らない．
3. ある方式がNM-CCA2であることとIND-CCA2であることは同値である．

特に最後に述べた関係は，最強の安全性（NM-CCA2であること）を示すためには，IND-CCA2を示すだけで十分であることを意味する．

OAEP暗号とその安全性

OAEP暗号とは

すでに述べたようにOAEP（Optimal Asymmetric Encryption Padding）は，RSA暗号などをより安全な暗号方式に変換する方式であり，現在RSA暗号を利用する際の標準的な利用方式PKCS#1に採用されている．この変換方式は，暗号関数とランダム関数を巧みに組み合わせることで実現され，その安全性（IND-CCA2）の証明は，ランダムオラクルモデル（理想的なランダム関数）に基づいている．

OAEPの意義については前に述べたように，RSA暗号そのものが能動的な攻撃に対して安全でないため，能動的な攻撃に対しても安全であるような暗号方式に（効率的に）変換して利用する方法が求められたためである．

前で述べたBleichenbacher攻撃法はPKCS#1バージョン1というRSA暗号関数そのものよりも高度な方式に対する攻撃であった．RSA関数そのものならばもっと簡単に選択暗号文攻撃に弱いことを示すことができる．いま，(n, e)をRSAの公開鍵，dを秘密鍵とする（以下，mod nを省略）．第2種の選択暗号文攻撃（CCA2）を許された攻撃者は，解読対象の暗号文yと乱数rから，$y' = y \cdot r^e$を作り，y'を復号してもらう（つまり，$x = y'^d$をもらう）．そこで，$z = x/r$を計算すればこれが求める答え，つまり$z = y^d$となる（なぜならば，$z = (y \cdot r^e)^d / r = (y^d \cdot r)/r = y^d$であるから）．この攻撃法の本質は，RSA暗号関数の持つ数学的構造（準同型性）にある．PKCS#1バージョン1はこのようにRSA暗号関数の持つ準同型性を崩すようなデータフォーマットを導入することにより，このような攻撃法を無効にすることを狙ったものであった．しかし，前で述べたように，PKCS#1バージョン1のようにアドホックな方法では，ある種の攻撃は防げても，あらゆる能動的攻撃に対して安全であるなどということは保証されないのである．

いま，ある落し戸付き一方向性置換（trap-door one-way permutation）fを仮定する．落し戸付き一方向性置換とは，$f(\cdot)$を計算するのは容易で，（秘密の落し戸の鍵を知らない者にとって）$f^{-1}(\cdot)$を計算するのが難しい全単射関数のことをいう．このような関数の代表例が，RSA（またはRabin）関数である．

1994年に，BellareとRogawayは，上記のようなfに対して，理想的なランダム関数を利用することにより最強の暗号（IND-CCA2, NM-CCA2）を作ることができることを示した．

fをRSA関数とした場合について，本稿の最後（付録）にOAEP暗号方式を示しているので参照されたい．

OAEP暗号の安全性

まず，fをRSA関数とした場合の安全性の結果を示そう．

定理1

ランダムオラクルモデル（ランダム関数G, Hが理想的にランダム）の下で，RSA問題が難しい（RSA関数が完全解読困難：一方向性関数：OW-CPA）と仮定すると，OAEP暗号は第2種の選択暗号文攻撃に対して強秘匿（IND-CCA2）である[3]（すなわち，NM-CCA2でもある）．

OAEPが選択暗号文攻撃に対して強秘匿（IND-CCA2）であることの証明は，大きく2つに分けられる．1つはOAEPが受動的攻撃（選択平文攻撃）に対して強秘匿（IND-CPA）であることを示すことであり，もう1つは，OAEPが平文知覚性（plaintext awareness: PA）と呼ぶ性質を持つことである☆1．Bellareらの最近の結果[1]により，ある方式が受動的攻撃（選択平文攻撃）に対して強秘匿（IND-CPA）でありかつ平文知覚性（PA）を持つとき，その方式は最強の安全性（IND-CCA2）を持つ．

平文知覚性とは，直感的には，正しい暗号文（OAEP暗号の復号手順で，チェックに合格し，復号結果としてmを出力する場合）を作れる人は，その平文を知っているはずであるというような性質を定式化したものである．

暗号方式が平文知覚性を保持する場合，能動的攻撃（選択暗号文攻撃）を行っても，正しい暗号文に対してしか復号結果を得られない．そして，平文知覚性より，このとき得られる復号結果は攻撃者自身がすでに知っているはずのものであるため，結局，攻撃者は選択暗号文攻撃によって有効な情報を得ることはできないことになる．これが，受動的攻撃に対して強秘匿（IND-CPA）でありかつ平文知覚性（PA）を持てば，能動的攻撃に対して強秘匿（IND-CCA2）となる直感的理由である．

さて，OAEP暗号が平文知覚性を持つことをどのように証明するかを簡単に説明しよう．ここでは，ランダム関数の関数値を求めるには，ランダムオラクルという仮想的なデータベースに問い合わせると想定し，問い合わせた内容はすべて記録されているものとする．このとき，暗号文作成者がランダムオラクルに問い合わせた内容と暗号文を付き合わせることにより，暗号文が正しい暗号文かどうか，さらに正しい暗号文ならばその平文が何であるかを効率的に（多項式時間で）出力することができる．このような手順でOAEP暗号が平文知覚性を持つことを示すことができる[1]．

☆1 平文知覚性の文献3）での定義は不十分であり，ここでは文献1）により与えられた定義を意味するものとする．

EPOC暗号とその安全性

EPOC暗号は，新しい公開鍵暗号関数（OU暗号関数）[15]と最強の安全性（IND-CCA2）を持つ暗号への新しい変換方法[10),11)]に基づき構成された暗号方式である[17)] ☆2．本章では，まずこの暗号関数の紹介を行い，その暗号関数を用いて構成したEPOC暗号とその安全性について述べる．

新しい公開鍵暗号関数

前回述べたように，公開鍵暗号を実現する仕掛けとして現在実用に使われているものは（驚くべきことに）本質的に2つしかなく，いずれも公開鍵暗号が発見された直後の1970年代に提案されたものである．それは，RSA-Rabin手法とDiffie-Hellman-ElGamal手法である．さらに，その安全性（OW-CPA）がその基本問題（素因数分解問題もしくは離散対数問題）の困難性と等価であることが証明されている手法は，Rabin法だけである．

1998年になり，岡本と内山はそれらとまったく別の仕掛けによる新しい実用的な公開鍵暗号関数を発表した[15)]．しかもこの暗号関数は，素因数分解と等価に安全であることが証明されたのである．

この新しい暗号関数の発見は，楕円曲線暗号と密接に結びついている．1997年10月に，anomalous曲線と呼ばれる楕円曲線を利用した楕円暗号に対する攻撃法（SSSAアルゴリズム）が発表されたことは前回述べた．anomalous曲線上の離散対数問題へのアルゴリズムは，Fermat商☆3と呼ばれるものの楕円曲線上への類似物を考えることによって自然に得られたものであるが，新しい暗号関数でも，このFermat商が本質的に使われており，SSSAアルゴリズムに対応する（離散対数問題を解く）アルゴリズムがこの暗号関数の復号処理に用いられる．

この暗号関数は，以下のような考え方により，素因数分解との安全性の等価性が証明できる．証明の大筋は，なにがしかの解読装置が存在すると仮定すれば，それを用いて素因数分解ができてしまうことを示すのである．いま，ある数以上の平文mを暗号化する．それをこの解読装置に入力すると，その復号化結果を出力してくれる．それを，m'としよう．実は，この暗号関数は，平文はある数よりも小さいことを前提としているので，復号結果m'は，その数よりも小さいのである．つまり，$m \neq m'$となり，さらに$m - m'$は秘密鍵（素因数）の情報を含むため，公開鍵の素因数分解ができる．

定理2

素因数分解が難しいという仮定の下で，OU暗号関数は，受動的攻撃に対する完全解読に関して安全（OW-CPA）である．

ここで，注意すべきことは，この暗号関数は能動的攻撃に関しては安全でないことである．つまり，上で示したような安全性の証明そのものが能動的な攻撃に対する脆弱性を意味している．したがって，暗号方式として利用する場合には，この暗号関数を能動的攻撃に強い（安全性が証明できる）方式に変換する必要がある．以下，そのような方式としてEPOC暗号を紹介しよう．なお，EPOC暗号の方式を本稿の最後（付録）に示す．

EPOC暗号の安全性

前の章で，BellareとRogawayにより，RSA暗号関数のような落し戸付き一方向性置換を最強の安全性（IND-CCA2）を持つ暗号へ変換する方法としてOAEP暗号が提案されたことを説明した．

ところが，彼らの方法を一般的な（確率的な）落し戸付き一方向性関数に適用することはできないのである．たとえば，RSA-Rabin暗号関数と並んで代表的な落し戸付き一方向性関数は，Diffie-Hellman-ElGamal系の方式であるが，OAEPの手法をこれらの方式に適用することはできない．同様に上で述べたOU暗号関数にもOAEPの手法を適用することはできない．

1998年，藤崎と岡本は，これら一般的な（確率的な）落し戸付き一方向性関数を最強の安全性（IND-CCA2）を持つ暗号へ変換する方法を初めて提案した[10),11)]．この方法を，OU暗号関数に適用した方式がEPOC暗号である．

まず，EPOC暗号の安全性の結果を示そう．

定理3

ランダムオラクルモデル（ランダム関数G, Hが理想的にランダム）の下で，素因数分解が難しいと仮定すると，EPOC暗号は第2種の選択暗号文攻撃に対して強秘匿（IND-CCA2）である[17)]（すなわち，NM-CCA2でもある）．

OAEP暗号と同様に，EPOC暗号が選択暗号文攻撃に対して強秘匿（IND-CCA2）であることの証明は，受動的攻撃に対して強秘匿（IND-CPA）であることを示すことと，平文知覚性（PA）を示すことから構成される．

☆2 ここでEPOCとして紹介する方式は，文献17）でEPOC-2と呼ばれている方式の特別な場合である．

☆3 素数p，pと素な整数aに対して，$q(a) = \frac{a^{p-1}-1}{p}$ をaのpを底とするFermat商と呼ぶ．実は，この値がpで割れるかどうか，すなわち，$q(a) \equiv 0 \pmod{p}$となるかどうかが，Fermatの最終定理と関係していることも知られている[22)]．

方式	安全性 (IND-CCA2の観点で)	数論的 仮定	ランダム関数 仮定
PKCS#1 Ver.1	解読可	−	−
OAEP (PKCS#1 Ver.2)	安全 (IND-CCA2)	RSA	理想的ランダム関数
EPOC	安全 (IND-CCA2)	素因数分解	理想的ランダム関数
Cramer-Shoup	安全 (IND-CCA2)	DDH	汎用一方向性ハッシュ関数

表-1 各方式の比較

Cramer-Shoup暗号とその安全性

Cramer-Shoup暗号の特徴：標準モデルでの安全性証明

これまで紹介したOAEP暗号，EPOC暗号のいずれもランダムオラクルモデルの下で，最強の安全性（IND-CCA2）を持つことが証明できた．それでは，標準モデル（理想的なランダム関数を仮定しないモデル）の下で，実用的で最強の安全性（IND-CCA2）を持つ暗号は構成可能であろうか？ 従来，標準モデルの下では，IND-CCA2であることが証明できてもきわめて効率の悪い方式（たとえば，Dolev-Dwork-Naorの暗号方式）しか提案されていなかった．

1998年，CramerとShoupは，標準モデルの下で実用的でかつIND-CCA2であることが証明できる暗号方式を初めて構成することに成功した[6]．この方式では，理想的なランダム関数という仮定の代わりに，現実的な汎用一方向性ハッシュ関数（universal one-way hash function: UOWHF）[18]という仮定を用いる．この方式の紹介は，やはり本稿の最後（付録）に示す．

Cramer-Shoup暗号の安全性

Cramer-Shoup暗号では落とし戸付き一方向関数としてDiffie-Hellman-ElGamal手法[9]を用いている．つまり，Diffie-Hellman-ElGamalの落とし戸付き一方向関数をこの方式特有の手法で最強の安全性を持つ暗号方式に変形したものがCramer-Shoup暗号である．

定理4

汎用一方向性ハッシュ関数が存在するという仮定の下で，Diffie-Hellman決定（DDH）問題が難しいと仮定すると，Cramer-Shoup暗号は第2種の選択暗号文攻撃に対して強秘匿（IND-CCA2）である[6]（すなわち，NM-CCA2でもある）．

Diffie-Hellman決定問題とは，$D = (g, g^a \bmod p, g^b \bmod p, g^{ab} \bmod p)$ と $R = (g, g^a \bmod p, g^b \bmod p, g^c \bmod p)$（$c$：ランダムに選ぶ）のいずれかが与えられたとき，それがDであるかRであるかを決定する問題である．また，汎用一方向性ハッシュ関数Hとは，xが与えられて，$H(x) = H(y)$となるようなyを見つけることが（多項式時間限定の攻撃者には）難しいような関数である[18]．

安全性の証明のエッセンスは，以下である．Cramer-Shoup暗号を（IND-CCA2の意味で）破る攻撃者Advが存在すると仮定する．そのとき，このAdvをブラックボックスとして使って，DDH問題を解くアルゴリズムMを構成するのである．これは，DDH問題が難しいという仮定に反するので，そのようなAdvは存在しないことが示せる．つまりCramer-Shoup暗号は（IND-CCA2の意味で）安全であることが証明される．

アルゴリズムMを構成するときポイントとなるのは，DDH問題が与えられたとき，それに基づくCramer-Shoup暗号の秘密鍵をM自身が決めることができることである．これにより，Advの選択暗号文攻撃に対してM自身が自由に復号結果を返すことができる（復号オラクルをシミュレーションできる）．また，M自身が問題となる暗号文を作ってAdvに与えるため，Advが最終的に正しい答え（暗号解読）を出したかどうかを判定することができる．

一方，汎用一方向性ハッシュ関数の仮定と方程式の解の情報理論的な考察より，DDH問題の入力がRの場合には，Advから見える情報は（暗号化された）平文情報と独立であることが示せる（つまり，与えられた暗号文がどの平文を暗号化したものかの情報をAdvに漏らさない）．このことより，もしAdvが何らかの有効な判断をするとしたらDDH問題の入力がDのときであることが分かる．したがって，Advが正しい答え（暗号解読）を出したならばDと判断し，さもなければRと判定する．

このアルゴリズムにより，もしAdvが無視できない確率でIND-CCA2の意味での暗号解読に成功するならば，そのAdvを使ってMはDDH問題を無視できない確率で正しく判定できることになる．

まとめ

以上紹介した各方式を**表-1**で比較する．

Cramer-Shoup暗号は，ランダム関数に対する仮定が現実的な汎用一方向性ハッシュ関数である点で他の2つの方式よりも優れている．反面，数論的な仮定では（基本的な離散対数仮定よりも強い仮定である）Diffie-Hell-

man仮定よりもさらに強いDDH仮定に基づいている点が欠点であろう．一方，EPOC暗号は，理想的なランダム関数に基づいているものの，数論的な仮定では基本的な素因数分解仮定に基づいている点で優れている．

今後の重要な課題の1つは，ランダムオラクルモデルの安全性と標準モデルでの安全性のギャップもしくは実質的な等価性を示すことであろう[5]．

また，本文で述べたように，公開鍵暗号の安全性の証明については，現状ではあくまで相対的な安全性を示すことしかできないが，計算量理論の進展により何らかの下界を示す理論ができれば，暗号においても絶対的な安全性を示すことが可能となろう．

参考文献

1) Bellare, M., Desai, A., Pointcheval, D. and Rogaway, P.: Relations Among Notions of Security for Public-Key Encryption Schemes, Proc. of Crypto'98, LNCS 1462, Springer-Verlag, pp.26-45 (1998).
2) Bellare, M. and Rogaway, P.: Random Oracles are Practical: A Paradigm for Designing Efficient Protocols, Proc. of the First ACM Conference on Computer and Communications Security, pp.62-73 (1993).
3) Bellare, M. and Rogaway, P. : Optimal Asymmetric Encryption, Proc. of Eurocrypt'94, LNCS 950, Springer-Verlag, pp.92-111 (1995).
4) Bleichenbacher, D.: Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1, Proc. of Crypto'98, LNCS 1462, Springer-Verlag, pp.1-12 (1998).
5) Canetti, R., Goldreich, O. and Halevi, S.: The Random Oracle Methodology, Revisited, Proc. of STOC, ACM Press, pp.209-218 (1998).
6) Cramer, R. and Shoup, V.: A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Message Attack, Proc. of Crypto'98, LNCS 1462, Springer-Verlag, pp.13-25 (1998).
7) Dolev, D., Dwork, C. and Naor, M.: Non-Malleable Cryptography, Proc. of STOC, ACM Press, pp.542-552 (1991).
8) Diffie, W. and Hellman, M.: New Directions in Cryptography, IEEE Trans. on Information Theory, IT-22, 6, pp.644-654 (1976).
9) ElGamal, T.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. on Information Theory, IT-31, 4, pp.469-472 (1985).
10) Fujisaki, E. and Okamoto, T.: How to Enhance the Security of Public-Key Encryption at Minimum Cost, to appear in Proc. of PKC'99, LNCS, Springer-Verlag.
11) Fujisaki, E. and Okamoto, T.: Provably Secure Integration of Asymmetric and Symmetric Encryption Schemes, manuscript (Nov. 1998).
12) Goldwasser, S. and Micali, S.: Probabilistic Encryption, JCSS, 28, 2, pp.270-299 (1984).
13) Goldwasser, S., Micali, S. and Rackoff, C.: The Knowledge Complexity of Interactive Proof Systems, SIAM J. Comput., 18, 1, pp.186-208 (1989).
14) Naor, M. and Yung, M.: Public-Key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks, Proc. of STOC, ACM Press, pp.427-437 (1990).
15) Okamoto, T. and Uchiyama, S.: A New Public-Key Cryptosystem as Secure as Factoring, Proc. of Eurocrypto'98, LNCS 1403, Springer-Verlag, pp.308-318 (1998).
16) 岡本龍明, 内山成憲: 公開鍵暗号の最近の話(1)楕円曲線暗号の安全性について, 情報処理, Vol.39, No.12, pp.1252-1257 (Dec. 1998).
17) Okamoto, T., Uchiyama, S. and Fujisaki, E.: EPOC: Efficient Probabilistic Public-Key Encryption, Submission to IEEE P1363a (Nov. 1998).
18) 岡本龍明, 山本博資: 現代暗号, 産業図書 (1997).
19) Rabin, M.O.: Digital Signatures and Public-Key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCS/TR-212 (1979).
20) Rackoff, C. and Simon, D.: Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack, Proc. of Crypto'91, LNCS 576, Springer-Verlag (1991).
21) 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 (1978).
22) 和田秀男: コンピュータと素因数分解, 遊星社 (1997).

(平成10年11月27日受付)

付録：各方式の記述

OAEP暗号

[公開鍵] (e, n)

[秘密鍵] d

p と q は素数で $n=pq$. $ed \equiv 1 \pmod{\phi(n)}$, ここで $\phi(n) = \mathrm{lcm}(p-1, q-1)$, $\gcd(e, \phi(n)) = 1$. $|n| = k_0 + k_1 + l$.

$G: \{0,1\}^{k_1} \to \{0,1\}^{k_0+l}$ と $H: \{0,1\}^{k_0+l} \to \{0,1\}^{k_1}$ がランダム関数.

$\|$ は結合, $[X]^t$ は X の上位 t ビット, $[X]_t$ は X の下位 t ビット

[暗号化] m ($|m| = k_0$)：平文, r ($|r| = k_1$)：乱数.

$y = (m \| 0^l) \oplus G(r)$, $z = r \oplus H(y)$, $C = (y \| z)^e \bmod n$.

C：暗号文.

[復号化]

$X = C^d \bmod n$, $Y = [X]^{k_0+l}$, $R = [X]_{k_1} \oplus H(Y)$.

$[Y \oplus G(R)]_l = 0^l$ が満足されるかどうかをチェック.

チェックに合格すれば以下を出力.

$m = [Y \oplus H(R)]^{k_0}$.

さもなければ, “不正” を出力.

EPOC暗号

[公開鍵] (n, g, h)

[秘密鍵] (p, q)

p と q ($|p| = |q| = k$) は素数で $n=p^2q$. $g \in (\mathbf{Z}/n\mathbf{Z})^*$ であり $g_p = g^{p-1} \bmod p^2$ の位数が p. また $h = h_0^n \bmod n$ ($h_0 \in (\mathbf{Z}/n\,\mathbf{Z})^*$).

$H: \{0,1\}^* \to \{0,1\}^{2k+c}$, と $G: \{0,1\}^* \to \{0,1\}^l$ がランダム関数 ($c > 0$: 定数).

[暗号化] m ($|m| = l$)：平文. r ($|r| = k-1$)：乱数.

$C_1 = g^r h^{H(m \| r)} \bmod n$, $C_2 = m \oplus G(r)$.

(C_1, C_2)：暗号文.

[復号化]

$$C_p = C_1^{p-1} \bmod p^2,\ r = \frac{L(C_p)}{L(g_p)} \bmod p,\quad m = C_2 \oplus G(r),$$

ここで $L(x) = \frac{x-1}{p}$.

$C_1 = g^r h^{H(m \| r)} \bmod n$ が満足されるかどうかをチェック.

チェックに合格すれば m を出力. さもなければ, “不正” を出力.

Cramer-Shoup暗号

[公開鍵] $(p, q, g_1, g_2, c, d, h)$

[秘密鍵] (x_1, x_2, y_1, y_2, z)

p と q は $q \mid p-1$ を満たす素数. g_1 と g_2 $(\mathbf{Z}/p\mathbf{Z})^*$ の要素で位数が q. x_1, x_2, y_1, y_2, z を $(\mathbf{Z}/q\mathbf{Z})$からランダムに選ぶ.

$c = g_1^{x_1} g_2^{x_2} \bmod p$, $d = g_1^{y_1} g_2^{y_2} \bmod p$, $h = g_1^z \bmod p$.

H は汎用一方向性ハッシュ関数 (UOWHF).

[暗号化] $m (0 < m < q)$：平文. $r \in \mathbf{Z}/q\mathbf{Z}$：乱数.

$u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $e = h^r m \bmod p$,

$\alpha = H(u_1, u_2, e)$, $v = c^r d^{r\alpha} \bmod p$.

(u_1, u_2, e, v)：暗号文.

[復号化]

$u_1^{x1+y1\alpha} u_2^{x2+y2\alpha} \equiv v \pmod{p}$ が満足されるかどうかをチェック. チェックに合格すれば以下を出力.

$m = e/u_1^z \bmod p$.

さもなければ, “不正” を出力.