

公開鍵暗号の理論研究における 最近の動向

宇根正志 / 岡本龍明

要 旨

公開鍵暗号は、暗号化と復号に異なる鍵を用いる暗号であり、復号に用いる鍵を秘密にする一方、暗号化に用いる鍵を公開する。公開鍵暗号は、公開する鍵の真正性を確保する仕組みが必要となるものの、事前に通信相手に鍵を配送する必要がない、通信相手確認や受信データの真正性確認等を可能にするデジタル署名を実現できるなどの利点を有することから、インターネット等オープンなネットワークにおける情報セキュリティ技術として幅広く利用されている。

公開鍵暗号の理論研究は、1976年にDiffieとHellmanによって公開鍵暗号のアイデアが提案されて以来、多くの暗号学者によって進められてきた。これまでにRSA暗号やElGamal暗号をはじめとする様々な暗号方式が提案されている。

最近の公開鍵暗号の理論研究において特に注目されているのは、証明可能な安全性と実用性を兼ね備えた暗号方式に関する研究である。現在実用化されている暗号方式の中には、これまでに効率的な解読法が見つからないものの、安全性が証明されていないものが多い。したがって、それらの暗号方式について、効率的な解読法が存在する可能性を否定することはできない。これに対し、最近では、OAEPやEPOC等、既存の方式に改良を加えることによって証明可能な安全性と実用性を両立させる暗号方式が提案されている。OAEP等これらの方式の一部は、既に実用化されている暗号プロトコルの安全性を高める目的から、PKCS#1等いくつかの業界標準で採用されている。

公開鍵暗号の安全性証明に関する研究は、公開鍵暗号を利用した様々なシステムにおける信頼性を高める上で、今後一層重要になると考えられる。本稿では、こうした最近の安全性証明に関する研究の動向を中心に、これまでの主要な公開鍵暗号に関する研究成果について説明する。

キーワード：安全性証明、公開鍵暗号、デジタル署名

本稿は、1998年11月4日に日本銀行で開催された「金融分野における情報セキュリティ技術に関するシンポジウム」への提出論文に加筆・修正を施したものである。

宇根正志 日本銀行金融研究所研究第2課(E-mail: masashi.une@boj.or.jp)

岡本龍明 日本電信電話(株)情報流通プラットフォーム研究所
(E-mail: okamoto@sucaba.isl.ntt.co.jp)

I. はじめに

公開鍵暗号は、復号に用いられる鍵を秘密に管理する必要がある一方、暗号化に用いられる鍵は公開することができる暗号方式である。公開鍵暗号には、公開する鍵の真正性を確保する仕組みが必要となるものの、事前に通信相手に鍵を配送する必要がない、各利用者は自分の秘密鍵と公開鍵のみを管理すればよい、通信相手の確認や受信データの真正性確認等を可能にするデジタル署名を実現できる、などの利点が存在する。このため、インターネット等不特定多数の利用者が参加するオープンなネットワークにおいては、情報セキュリティを確保するための必要不可欠な技術として位置付けられている。

公開鍵暗号の理論研究は、1976年にDiffieとHellmanによって公開鍵暗号のアイデアが提案されて以来、多くの暗号学者によって進められてきた。これまでにRSA暗号やElGamal暗号をはじめとする様々な暗号方式が提案されているほか、各暗号方式の安全性に関する研究成果が数多く発表されている。現在実用化されている公開鍵暗号方式の多くは、これまでに効率的な解読法が見つかっていないものの、安全性が証明されているわけではない。したがって、そのような暗号方式について、効率的な解読法が存在する可能性を否定することはできない。

最近の公開鍵暗号の理論研究において特に注目されているのは、証明可能な安全性と実用性を兼ね備えた暗号方式に関する研究である。RSA暗号等既存の方式に改良を加えることによって、証明可能な安全性と実用性を両立させる暗号方式がいくつか提案されており、データ守秘専用の方式としては、OAEP、EPOC、Cramer-Shoup暗号が挙げられるほか、デジタル署名専用の方式としては、PSS署名、改良ElGamal署名、TSH-ESIGNが挙げられる。これらの方式は、攻撃者が暗号文しか解読に利用できない受動的攻撃だけではなく、より強力な能動的攻撃に対しても、一定の仮定のもとで安全であることが証明されている。

こうした証明可能な安全性を有する暗号方式を業界標準に採用し、既に実用化されている暗号プロトコルのセキュリティ水準を高める動きもみられている。RSA社が開発した暗号通信データ形式の規格PKCS#1 Version 1 (RSA暗号を利用)は、SSL等の暗号プロトコルに組み込まれており、幅広い分野で利用されているが、PKCS#1 Version 1をある一定の条件の下で実装した場合には能動的攻撃によって効率的に解読することが可能となるとの研究が発表された。これを受けて、RSA社は、能動的攻撃に対する安全性が証明されているOAEPを利用してPKCS#1 Version 1に改良を加え、新たにPKCS#1 Version 2を発表している。

公開鍵暗号の安全性証明に関する研究は、公開鍵暗号を利用した様々なシステムにおける信頼性を高める上で、今後一層重要になってくると考えられる。本稿では、こうした公開鍵暗号の安全性証明に関する最近の理論研究の動向を中心に、これまでの主要な公開鍵暗号に関する研究成果について説明する。

II. 公開鍵暗号の概要と機能

公開鍵暗号は、暗号化に利用される鍵と復号に利用される鍵が異なり、一方の鍵から他方の鍵を算出することが計算量的に困難である¹ため、どちらか一方の鍵を公開することが可能となる。通常、暗号化に利用される鍵が公開されることから公開鍵と呼ばれ、復号に利用される鍵が秘匿されることから秘密鍵と呼ばれる。

1. 公開鍵暗号の特徴

公開鍵暗号は、共通鍵暗号と比べて次のような特徴を持っている。

鍵配送が容易である

共通鍵暗号では、送信者は受信者に鍵を安全に配送しなければならない。一方、公開鍵暗号では、送信者の公開鍵の正当性を確認する仕組みが必要となる²ものの、暗号化に利用する鍵を公開することができるため、受信者に鍵を配送する必要はなくなる。

各利用者は自分の秘密鍵・公開鍵のみを管理すればよい

n 人の利用者が互いに暗号通信を行う場合、共通鍵暗号においては、各利用者が $n-1$ 個の鍵を秘密に管理する必要があるため、利用者が増加すると鍵の管理に多大なコストがかかる。これに対して、公開鍵暗号では、各利用者は自分の秘密鍵と公開鍵を管理するだけでよい。このため、利用者が膨大となるオープンなネットワークにおける利便性が高い。ただし、各利用者の公開鍵が正当であることを確認するための仕組み（公開鍵インフラ）が別途必要となる。

デジタル署名に利用できる

小切手や契約書など紙ベースでの署名（サイン）は、その署名特有の形状から署名者を一意に特定することを可能にし、署名が付された文書の作成者等を確定させる役割を有している。公開鍵暗号を利用したデジタル署名では、署名の対象が紙ベースの文書からデジタルデータに置き換わり、(i) 署名者がデータを秘密鍵で変換する署名生成のステップと、(ii) 不特定多数の署名検証者が公開鍵を利用し

- 1 計算量的に困難であるとは、その計算を行うことは理論的には可能であるものの、実際にその計算を実行するには計算量が非常に大量となり、膨大な費用と時間を必要とすることから、事実上不可能であることを意味する。どの程度の計算量が「事実上不可能」であるかは、その時々技術条件等によって左右される。
- 2 一般的には、公開鍵の所有者や有効期限等の属性情報やその真正性は、公開鍵証明書と呼ばれるデータによって確認される仕組みが利用されるケースが多い。公開鍵証明書には、証明の対象となる公開鍵やその所有者・有効期間等の情報のほか、それらの情報の真正性を確保するためのデジタル署名（後述）が含まれる。デジタル署名は、認証機関と呼ばれる信頼できる第三者機関によって生成・発行される。このような公開鍵暗号を実用化するために必要となる仕組みは、公開鍵インフラと呼ばれている。

て署名者固有の変換の正当性を確認する署名検証のステップによって構成される。秘密鍵を所有する者は唯一人であるため、秘密鍵による変換は署名者固有の変換となり、署名検証者は署名者の公開鍵で署名の正当性を検証できる。さらに、署名者はデジタル署名付きデータを作成した事実を後で否定できない（否認防止）。なお、共通鍵暗号では、鍵が通信当事者間で共有されているため、暗号文がその鍵を所有する2人のどちらによって作成されたかを特定することができない。

処理速度が遅い

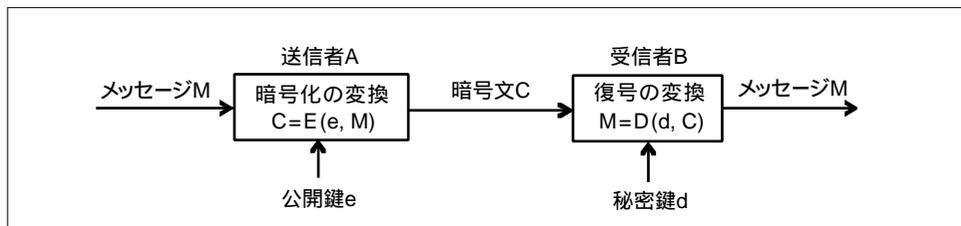
一般的に、公開鍵暗号による暗号化・復号処理には、べき乗剰余演算等計算時間が比較的多く必要となる演算が利用されるケースが多く、加算や乗算など高速処理が可能な演算が主に利用される共通鍵暗号に比べて、処理速度が遅くなる傾向にある。

これらの特徴により、膨大なデータの処理が要求されるデータの暗号化には共通鍵暗号が利用され、デジタル署名や共通鍵暗号に用いられる鍵の配送には公開鍵暗号が利用される場合が一般的である。

2. 公開鍵暗号の原理

データMに対して公開鍵eを用いた公開鍵暗号方式による変換を $E(e, M)$ とし、秘密鍵dを用いた変換を $D(d, M)$ とする（図1参照）と、公開鍵暗号方式は、まず次の3つの条件を満たす必要がある。

図1 公開鍵暗号による暗号通信の一般的な手順



公開鍵eを知っている場合、 $E(e, M)$ の計算は容易である。秘密鍵dを知っている場合には、 $D(d, M)$ の計算は容易である。

秘密鍵dを知らない場合、公開鍵e、変換アルゴリズムE、暗号文 $C = E(e, M)$ を知っていたとしても、秘密鍵dを求めることは計算量的に困難である。

秘密鍵dを知らない場合、公開鍵e、変換アルゴリズムE、暗号文 $C = E(e, M)$ を知っていたとしても、元の平文Mを求めることは計算量的に困難である。

これらの条件を満足する関数を構築するために、「一方向性関数」と呼ばれる関数が利用される。一方向性関数 F においては、関数 F の計算は容易であるが、逆関数 F^{-1} の計算が計算量的に困難となる。この一方向性関数に、逆関数の計算を容易にするためのパラメーター（「落し戸」と呼ばれる）を組み込み、「落し戸付き一方向性関数」と呼ばれる特殊な関数を構築する。上記の例の場合、 $E(e, M)$ に対応する逆関数 $D(d, C) (=E^{-1}(e, C))$ におけるパラメーター d が落し戸となる。このような関数において、公開鍵を e 、秘密鍵を d とすれば、以上の3つの条件が満足され、公開鍵暗号方式を実現させることができる。

3. 公開鍵暗号の機能

公開鍵暗号の主要な機能として、(1)データ守秘、(2)デジタル署名、(3)ブラインド署名、(4)鍵配送が挙げられる。

(1) データ守秘

公開鍵暗号を利用することによって、次のような手順で通信データの守秘を実現することができる（図1参照）。

（ステップ1）データの送信者は、受信者の公開鍵によって平文を暗号化し、受信者に送信する。

（ステップ2）受信者は、暗号文を自分の秘密鍵で復号する。

各受信者の公開鍵は不特定多数に公開されているため、誰もが同じ公開鍵によって暗号通信が可能となる。一方、秘密鍵を所有していない者が暗号文を解読することは計算量的に困難となる。

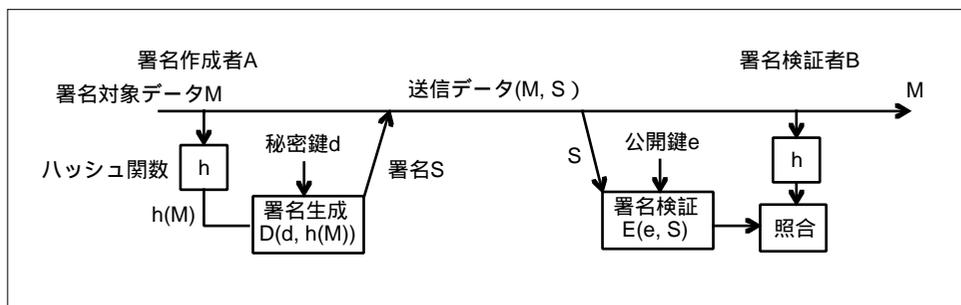
(2) デジタル署名

デジタル署名の方法としては、認証子照合法が利用されるケースが多い³。認証子照合法では、以下の手順によってデジタル署名の生成・検証が行われる（図2参照）。

3 デジタル署名の方法として、データ自身を秘密鍵で変換してデジタル署名を作成する方法（通信文復元法と呼ばれる）も存在する。しかし、この方法では、より多くのデータを処理する必要から計算効率が低下するほか、データ x に対して公開鍵 e で暗号化した場合、データ x が暗号化されたデータ $E(e, x)$ に対するデジタル署名になるという問題がある。これは、 $E(e, x)$ を秘密鍵 d で変換すると、 $D(d, E(e, x)) = E^{-1}(e, E(e, x)) = x$ が成立するためである。さらに、RSA暗号のように、公開鍵暗号が乗法的である場合（ $E(e, xy) = E(e, x)E(e, y)$ が成立）には、 x, y に対する署名 $D(d, x), D(d, y)$ を入手した者は xy に対する署名 $D(d, xy)$ を偽造できるという問題がある。このような問題点が存在するため、認証子照合法が一般的である。

- (ステップ1) 署名作成者は、データMを「ハッシュ関数」と呼ばれる特殊な関数hにより一定長のデータh(M)に圧縮し、これをデジタル署名方式により自分の秘密鍵dで変換してデジタル署名S=D(d, h(M))を生成する。
- (ステップ2) 署名作成者は署名付きデータ(M, S)を署名検証者に送信する。
- (ステップ3) 署名検証者は、署名Sをデジタル署名方式によって署名作成者の公開鍵eで変換した結果E(e, S)と、データMをハッシュ関数hで圧縮した結果h(M)を突合して一致するかどうかを検証する。

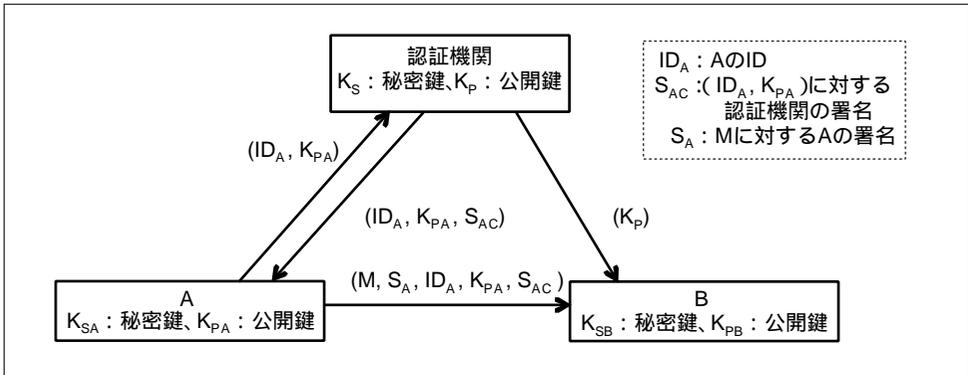
図2 公開鍵暗号によるデジタル署名の一般的な手順



デジタル署名を実現する場合、署名作成者と署名検証者以外の信頼できる第三者を介する「調停署名方式」が利用されるケースが多い。調停署名方式の代表例は、認証機関による公開鍵証明書を利用した方式であり、その手順は以下の通り（図3参照）。

- (ステップ1) 署名作成者Aは自分のID(ID_A)と公開鍵 K_{PA} を認証機関に送信する。
- (ステップ2) 認証機関は、秘密鍵 K_S を利用して(ID_A, K_{PA})に対する署名 S_{AC} を生成して公開鍵証明書とし、Aに返信する。
- (ステップ3) Aは、署名付きデータ(M, S_A)に公開鍵証明書(ID_A, K_{PA}, S_{AC})を添付し、署名検証者Bに送信する。
- (ステップ4) Bは、Aの公開鍵証明書(ID_A, K_{PA}, S_{AC})の真正性を認証機関の公開鍵 K_P で検証した後、Aから送信された署名付きデータ(M, S_A)の真正性をAの公開鍵 K_{PA} によって検証する。

図3 調停署名方式によるデジタル署名



(3) ブラインド署名

ブラインド署名は、署名依頼者が署名者にデータの内容を知られることなく署名を受ける方法で、Chaum [1983] によって提案された。ブラインド署名は、電子現金や電子投票等に利用される技術である。たとえば、署名を受ける文書とカーボン紙を封筒に入れ、その上から署名をしてもらうという紙ベースの方法を電子的に実現する方法といえる。具体的な方法としては、Chaum [1983] によるRSA暗号を利用する方式や、ElGamal署名を利用する方式 (Camenisch et al. [1996]) 等が提案されている。

RSA 暗号によるブラインド署名の手順は以下の通り。署名者BのRSA暗号の公開鍵、秘密鍵はそれぞれ (e, n) 、 d とする。

(ステップ1) 署名依頼者Aは、秘密の乱数 r を生成した後、署名対象データ M 、署名者Bの公開鍵 (e, n) を用いて以下の計算を行い、Bに X を送信する。

$$X = Mr^e \bmod n$$

(ステップ2) Bは、自分の秘密鍵 d を用いて以下の計算を行い、 Y をAに送信する。

$$Y = X^d \bmod n = M^d r \bmod n$$

(ステップ3) Aは、 Y と乱数の逆数 r^{-1} から、署名 $S = M^d \bmod n$ を得る。

(ステップ4) Aは、署名 S の正当性を以下の等式によって検証する。

$$M = S^e \bmod n$$

上記の方法では、AがBにとって都合の悪いデータに署名させることが可能となる。Chaumは、これを防ぐ方法として「cut-and-choose protocol」と呼ばれる手順を組み込んだ方式を提案している。この方式は、署名者が署名対象データの中からいくつかのデータを抜き取り検査し、抜き取ったデータに問題がなければ署名を行うというものである。

(4) 鍵配送

公開鍵暗号は、データの暗号化に利用される共通鍵暗号の暗号鍵を通信相手に配送する手段としても利用される。最も単純な鍵配送の方法は、送信者が共通鍵暗号の暗号鍵を受信者の公開鍵で暗号化し、通信相手に送信するという方法である。ただし、この方法では、受信者は送られてきた鍵が確かに送信者のものであるか否かを確認することはできない。そこで、送信者が暗号鍵にデジタル署名を添付して配送することが必要となる。

幅広く利用されている鍵配送の方法として、Diffie-Hellman法 (Diffie-Hellman [1976]) が挙げられる。Diffie-Hellman法による鍵配送の手順は下記の通り。素数 p とその原始根 α が公開鍵となる。

(ステップ1) A は $p-1$ 以下の自然数 X_A をランダムに選び、

$$Y_A = \alpha^{X_A} \bmod p$$

を計算して Y_A を B に送信する。

(ステップ2) B も、同様に $p-1$ 以下の自然数 X_B をランダムに選び、

$$Y_B = \alpha^{X_B} \bmod p$$

を計算して Y_B を A に送信する。

(ステップ3) A は、共通鍵暗号の暗号鍵 K を次のようにして計算する。

$$K = Y_B^{X_A} \bmod p = \alpha^{X_A \cdot X_B} \bmod p$$

(ステップ4) B も同様にして鍵 K を計算する。

$$K = Y_A^{X_B} \bmod p = \alpha^{X_B \cdot X_A} \bmod p$$

この方式では、攻撃者は p 、 α のほか、通信経路の傍受によって Y を入手できる。ところが、 p 、 α 、 Y から X_A や X_B を入手するためには、「離散対数問題」(詳細は第IV章3(2)で説明)を解く必要がある。 p 、 α が十分に大きい場合、離散対数問題を解くことは計算量的に困難とされている。

一方、Diffie-Hellman法には、離散対数問題を解く以外の攻撃法「中間侵入攻撃」が有効であることが知られている。中間侵入攻撃は、攻撃者 C が通信路上でデータ Y_A 、 Y_B を奪取し、自分が作成したデータ $Y_C = \alpha^{X_C} \bmod p$ に置き換えることで、自分と A 、自分と B の間で鍵を共有し、 A に対しては B に、 B に対しては A に成りすますという攻撃である。この攻撃法は、Diffie-Hellman法において、通信相手を相互に確認する仕組みが存在しないために有効となっていることから、Diffie-Hellman法に相手確認の手段を導入した方式も提案されている(Diffie, Oorschot and Wiener[1992])。

Ⅲ. 主要な公開鍵暗号方式

主要な公開鍵暗号方式は、機能面から、データ守秘・デジタル署名の両方の機能を有する方式、データ守秘専用の方式、デジタル署名専用の方式の3種類に大別されるほか、依拠している数学の問題により、素因数分解問題に基づく方式、有限体上の乗法群における離散対数問題に基づく方式、楕円曲線によって定義された離散対数問題に基づく方式の3つに分類することができる。

また、既存の公開鍵暗号方式を若干改良し、証明可能な安全性を確保する方式も提案されている。データ守秘専用の方式としては、RSA暗号の改良版のOAEP、Uchiyama-Okamoto暗号の改良版のEPOC、ElGamal暗号の改良版のCramer-Shoup暗号が挙げられる。これらの暗号方式は、一定の仮定の下で能動的攻撃に対する安全性が証明されている。また、デジタル署名専用の方式についても、既存のデジタル署名方式に改良を施すことによって安全性が証明可能な方式が提案されており、比較の実用性が高い方式として、RSA暗号の改良版のPSS署名、ElGamal署名の改良版の改良ElGamal署名、ESIGNの改良版のTSH-ESIGN等が挙げられる。これらの主要な公開鍵暗号方式を分類すると、以下の表1の通り。

表1 公開鍵暗号方式の分類

	データ守秘・ デジタル署名	データ守秘専用	デジタル署名専用
素因数分解問題に基づく方式	RSA暗号 Rabin暗号	Okamoto-Uchiyama暗号	ESIGN
改良方式		EPOC OAEP	PSS署名 TSH-ESIGN
有限体上の乗法群における 離散対数問題に基づく方式		ElGamal暗号	ElGamal署名 DSA
改良方式		Cramer-Shoup暗号	改良ElGamal署名
楕円曲線によって定義された 離散対数問題に基づく方式		EC-ElGamal暗号	EC-ElGamal署名 EC-DSA
改良方式		EC-Cramer-Shoup暗号	改良EC-ElGamal署名

1. データ守秘・デジタル署名の両方の機能を有する方式

(1) RSA暗号

RSA暗号は、Rivest, Shamir, and Adleman [1978] によって考案された最初の本格的な公開鍵暗号方式である。RSA暗号は、大きな合成数の素因数を求める問題（素因数分解問題）を解くことが計算量的に困難であることに依拠している。RSA暗号の安全性に関する数学的な証明（たとえば、RSA暗号の安全性と素因数分解問題の困難性との等価性）はこれまで示されていないものの、RSA暗号が発表されてから20年近くもの間、多くの暗号研究者によって様々な角度から研究が進められてきた

結果、素因数分解よりも有効な解読法は報告されていない⁴。このため、RSA暗号は、最も信頼性の高い公開鍵暗号方式として幅広い分野において実用化されており、事実上の標準と目されている⁵。RSA暗号による暗号化・復号および署名生成・検証の手順は以下の通り。

< RSA暗号 >

【鍵生成】最初に2つの大きな素数 p と q を選び、これらの積 $n=pq$ を計算する。次に、 $p-1$ と $q-1$ の最小公倍数 $L = \text{LCM}(p-1, q-1)$ を計算する。最後に、最大公約数 $\text{GCD}(e, L) = 1$ を満足する自然数 e を選び、 $ed = 1 \pmod{L}$ を満たす d を求める。

【秘密鍵】 (d, p, q)

【公開鍵】 (e, n)

(1) データ守秘機能

【暗号化】 $C = M^e \pmod{n}$ (ただし、 M は明文、 C は暗号文)

【復号】 $M = C^d \pmod{n}$

(2) デジタル署名機能 (ハッシュ関数を利用するケース)

【署名生成】明文 M のハッシュ値 $m = H(M)$ を生成した後 (H はハッシュ関数) 以下の計算によって M に対するデジタル署名 S を生成する。

$$S = m^d \pmod{n}$$

【署名検証】 (M, S) を受け取った受信者は、以下の等式が成立するか否かを検証する。

$$H(M) = S^e \pmod{n}$$

4 ただし、最近では、RSA暗号の安全性と素因数分解問題の困難性が等価にはならない可能性があるとの研究成果も発表されている (Boneh and Venkatesan [1998])。

5 RSA暗号は、金融業務における公開鍵暗号を利用した鍵管理の方法に関する標準規格ISO 11166(Banking Key management by means of asymmetric algorithms)の Part 2(Approved algorithms using the RSA cryptosystem)において規定されているほか、公開鍵証明書を利用したデジタル署名の利用方法に関する標準規格案ISO/IEC FDIS 14888-3 (Information technology - Security techniques - Digital signature with appendix - Part 3: Certificate-based mechanism)において、利用可能な公開鍵暗号方式のひとつとして記載されている。また、RSA暗号は、米国の金融業務における国内標準規格ANSI X9.31として標準化されているほか、デジタル署名の米国政府標準規格FIPS 186-1として標準化されている (FIPS 186-1には、RSA暗号のほかにDSAも規定されている)。なお、ISO/IEC FDIS 14888-3に記載されている公開鍵暗号方式は、RSA暗号のほか、ESIGN、DSA、EC-DSA、Pointcheval-Vaudenay方式である。

RSA 暗号は、現時点では安全性に関する大きな欠陥が示されていない暗号であるが、素数 p と q の選び方によっては、素因数分解問題の高速解法が適用可能となるほか、安全性と関連の深い暗号化関数の周期⁶に影響を与える。したがって、鍵生成の際には、素数 p と q を注意深く選ぶ必要がある。素数 p 、 q の満たすべき主な条件として、次の3つが挙げられる。

$|p-q|$ を大きくする。

$(p \pm 1)$ と $(q \pm 1)$ は、それぞれ大きな素因数 p' , p'' , q' , q'' を持つ。

$(p' \pm 1)$ と $(p'' \pm 1)$ 、および $(q' \pm 1)$ と $(q'' \pm 1)$ は、それぞれ大きな素因数を持つ。

上記3条件のうち、条件 1 と 2 はそれぞれFermat法、 $p-1$ 法と $p+1$ 法 という素因数分解の高速解法（第4章3(1)で説明）を適用不可能にするための対策である。条件 3 は解読を比較的容易にする短い周期を防止するための対策である。なお、これらの素数の条件は、RSA暗号に限らず、素因数分解問題の困難性に依拠している暗号方式すべてに当てはまる。

また、RSA暗号の利用方法によっては安全性が損なわれる可能性がある。たとえば、(i)データ全体に対して署名を生成し、そのデータを復元する形で検証が行われる場合（通信文復元型デジタル署名）、(ii)利用者全員が共通の法 n を用いる場合、(iii)平文の暗号化処理やデジタル署名検証の高速化を図るために、公開鍵 e としてサイズの小さな数値を利用する場合には、安全性に問題が生じることが示されている（Simmons [1983]、Coppersmith et al. [1996]）。また、(iv) 能動的攻撃が可能な実装環境においては、素因数分解問題よりも効率的な解読法が存在することが示されている（詳細については後述、Bleichenbacher [1998]）。

(2) Rabin暗号

Rabin暗号は、Rabin [1979] によって提案された方式であり、RSA暗号に改良を加えることによって、「受動的攻撃に対する完全解読（第4章1(1)で説明）の困難性が素因数分解問題の困難性と等価である」ことを証明可能にした方式である。しかし、Rabin暗号には、暗号文を一意に復号することができず、復号によって4通りのデータが生成される、一部のデータに対しては、デジタル署名を生成することができない、能動的攻撃（第4章1(1)で説明）によって完全解読が可能になる、といった問題点がある。Rabin暗号の暗号化・復号および署名生成・検証手順は以下の通り。

6 暗号化関数を $f(x) = x^e \bmod n$ と表す。このとき、 $f^m(x) = x$ を満たす最小の正整数 m が「 x に対する周期」と呼ばれる。周期の値は e, n, x の値に依存している。周期が短いと一般的解読や全面的解読が比較的容易になることが示されている（Williams and Schmid [1979]、勝野 [1983]）。

< Rabin暗号 >

【鍵生成】2つの大きな素数 p と q を選び、これらの積 $n=pq$ を計算する。 $0 < b < n$ を満足する自然数 b を定める。

【秘密鍵】 (p, q)

【公開鍵】 (n, b)

(1) データ守秘機能

【暗号化】 $C = M(M+b) \pmod n$ (ただし、 M は平文、 C は暗号文)

【復号】次の連立合同式を解いて平文 M を算出する。

$$M^2 + Mb - C = 0 \pmod p$$

$$M^2 + Mb - C = 0 \pmod q$$

(2) デジタル署名機能

【署名生成】平文 M のハッシュ値 $m = h(M)$ を利用して以下の連立合同式を満足するデジタル署名 S を生成する(こうしたデジタル署名 S が生成される確率は約 $1/4$)。連立合同式を満足する S は4つ存在するが、そのうちいずれかの値をデジタル署名として M に添付して送信する。

$$S^2 + Sb - m = 0 \pmod p$$

$$S^2 + Sb - m = 0 \pmod q$$

【署名検証】受け取った M と S を用いて、以下の等式が成立するか否かを検証する。

$$h(M) = S(S+b) \pmod n$$

暗号文を一意的に復号できない、任意の文書に署名できないというRabin暗号における問題点は、暗号化・復号関数が全単射でないことに起因している。これに対し、Williams [1980] は、素数 p と q に制限を加えることによって暗号化・復号関数が全単射となる公開鍵暗号方式Williams暗号を考案している。また、黒澤・伊東・竹内 [1987] は、Williams暗号を改良した方式として「逆数暗号」を提案している。しかし、Williams暗号、逆数暗号ともに、Rabin暗号における「能動的攻撃によって解読される」という問題が残されている。

2. データ守秘専用の方式

(1) ElGamal暗号

ElGamal暗号は、ElGamal [1985a] によって発表された有限体上の乗法群における離散対数問題の困難性に基づく公開鍵暗号方式である。有限体上の乗法群における離散対数問題は、次のような数学の問題である。

【有限体上の乗法群における離散対数問題】

素数 p 、 p を法とする乗法群の原始根 a を選び、ある整数 x に対して $b = a^x \bmod p$ を計算する。このとき、 p, a, b を所与として、 $b = a^x \bmod p$ を満足する x を求めよ。

ElGamal暗号の解読困難性と有限体上の乗法群における離散対数問題の困難性との関係については、これまで理論的結果が示されていない。ElGamal暗号では、暗号化の際に秘密の乱数が利用されており、同じ平文を暗号化しても異なる暗号文が生成される。このような性質を有する暗号は確率暗号と呼ばれている⁷。ElGamal暗号の暗号化・復号の手順は以下の通り。

< ElGamal暗号 >

【鍵生成】大きな素数 p と乱数 x を生成し、法 p の乗法群の原始根 α を選ぶ。これらを用いて $y = \alpha^x \bmod p$ を計算する。

【秘密鍵】 x

【公開鍵】 (y, p, α)

【暗号化】送信者は乱数 k を生成し、受信者の公開鍵 y を用いて暗号文 (C_1, C_2) を以下のように作成する。ただし、平文を M とする。

$$C_1 = \alpha^k \bmod p$$

$$C_2 = My^k \bmod p$$

【復号】受信者は以下の等式から M を得る。

$$MC_1^x = C_2 \bmod p$$

ElGamal暗号を利用する場合には、安全性の観点から、通信の都度、乱数 k を生成する必要がある。これは、同一の乱数 k によって異なる2つの平文 (M', M'') を暗号化した場合、対応する暗号文 (C_2', C_2'') との間に、 $M' / M'' = C_2' / C_2''$ という関係が成立し、 M' と C_2' がわかると C_2'' から M'' を知ることができるためである。

(2) Okamoto-Uchiyama暗号

Okamoto-Uchiyama暗号は、Okamoto and Uchiyama [1998] によって提案された公開鍵暗号方式であり、素因数分解問題の困難性に依拠した方式である。Okamoto-Uchiyama暗号は、受動的攻撃に対する一方性 (第IV章 1 (1) で説明) が素因数

7 これに対し、同一の鍵の下で同じ平文を暗号化すると常に同じ暗号文が生成される暗号は、確定暗号と呼ばれている。

分解問題の困難性と等価であることが証明されている、暗号化・復号に必要な計算量がRSA暗号と同程度である、確率暗号である、といった特徴を有している。ただし、能動的攻撃に対しては安全ではないが、Okamoto-Uchiyama暗号に改良を加えた方式EPOCにおいて、能動的攻撃に対する安全性が証明されている。

Okamoto-Uchiyama暗号の暗号化・復号手順は以下の通り。

< Okamoto-Uchiyama暗号 >

【鍵生成】大きな素数 p と q を生成し、 $n = p^2q$ となる自然数 n と、 n を法とする乗法群の原始根 g を選ぶ。

【秘密鍵】 (p, q)

【公開鍵】 (n, g)

【暗号化】送信者は乱数 r ($0 < r < n$) を生成し、次のように平文 m に対応する暗号文 C を生成する。ただし、平文 m のデータは、 $0 < m < p$ を満足する。

$$C = g^{m+nr} \bmod n$$

【復号】受信者は、 $C_p = C^{p-1} \bmod p^2$ と $g_p = g^{p-1} \bmod p^2$ を計算した上で、関数 $L(x) = (x-1)/p$ を利用して以下の計算によって平文 m を復号する。

$$m = \frac{L(C_p)}{L(g_p)} \bmod p$$

なお、Okamoto-Uchiyama暗号は、P部分群問題の困難性を仮定することによって、受動的攻撃に対して強秘匿（第IV章1(1)で説明）であることが証明されている。P部分群問題の概要は以下の通り。

【P部分群問題】

平文 M 、乱数 r の下でのOkamoto-Uchiyama暗号の暗号化関数を $E(M, r)$ とする。2つの乱数 t と s を生成し、以下の計算を行う。

$$E(0, t) = h^t \bmod n, \quad E(1, s) = gh^s \bmod n$$

このとき、 $(h^t \bmod n)$ と $(gh^s \bmod n)$ の値のみを所与として、それぞれが $E(0, t)$ と $E(1, s)$ のどちらの値かを判定せよ。

(3) EC-ElGamal暗号

楕円曲線によって定義された離散対数問題に基づく公開鍵暗号方式は、有限体によって定義された楕円曲線上の点によって構成される有限可換群上での離散対数問題の困難性を安全性の根拠とするもので、Koblitz [1987] とMiller [1986] によって発表された。楕円曲線および楕円曲線によって定義された離散対数問題の概要は以下の通り。

【楕円曲線】

楕円曲線は、3次曲線（関数 $F(x,y)$ の次数が3となる代数方程式 $F(x,y) = 0$ の解の集合）のうち、特異点（ $F(x,y)$ の x および y に関する偏微分係数が0となる (x,y) ）を含まない点の集合である。

【有限体上の楕円曲線】

有限体上の楕円曲線は、要素の個数 p ($p > 3$ の素数) である有限素体 F_p において、

$$\{(x,y) \mid y^2 = x^3 + ax + b \pmod{p}\} \quad (4a^3 + 27b^2 \neq 0, a, b \in F_p)$$

を満足する点 (x,y) (x,y は F_p の要素) の集合と定義される。

【楕円曲線によって定義された離散対数問題】

素数 p に対して有限体 F_p 上の楕円曲線に無限遠点 O を加えた集合を $E(F_p)$ とし、 $E(F_p)$ 上の2点間の加法演算を定義すると、 $E(F_p)$ は有限可換群となる（無限遠点 O はこの有限可換群の単位元となる）。有限可換群 $E(F_p)$ における要素の個数は、 $p + 1 - t(-2\sqrt{p} \quad t \quad 2\sqrt{p})$ と表され、 t の値はトレースと呼ばれる。この $E(F_p)$ 上の点 A, B ($A \neq B$) を選び、 A と B がある自然数 x に対して $A = xB$ という関係にある（定義された加法演算によって点 B を x 回加えると、点 A となる）とする。このとき、 $p, E(F_p), A, B$ を所与として、 $A = xB$ を満足する自然数 x を求めよ。

有限体上の乗法群における離散対数問題には、準指数関数時間の解法（指数計算法、詳細については第IV章3(2)で説明）が存在する一方、楕円曲線によって定義された離散対数問題には、ある種の楕円曲線を除いて指数計算法の適用が困難であることから、安全性を維持しつつ、従来の方式に比べて鍵長を短縮できるとされている。楕円曲線によって定義される離散対数問題に基づく暗号方式は、有限体上の乗法群における要素を楕円曲線上の有限可換群の要素に、有限体上の乗法群において定義される乗法を楕円曲線上の有限可換群において定義される加法にそれぞれ対応させることによって構築される。有限体上の乗法群における要素の r 乗は楕円曲線上の有限可換群における要素の r 倍に対応し、通常乗法群における要素の r 乗を計算するのに用いられる高速演算も楕円曲線上の有限可換群における要素の r 倍を計算するのに用いられる。

楕円曲線によって定義される離散対数問題に基づく代表的な暗号方式として、ElGamal暗号を利用した暗号方式（以下、EC-ElGamal暗号とする）が挙げられる。EC-ElGamal暗号の暗号化・復号の手順は以下の通り。

< EC-ElGamal暗号 >

【鍵生成】まず、素数 p に対して有限素体 F_p 上に定義された楕円曲線を $E(F_p)$ とし、 $E(F_p)$ 上の点 G （ベースポイントと呼ばれる）を選ぶ。ただし、 G は、位数 K が大きな素数となるように選ばれる⁸。整数 t を選び、 $Y=tG$ を計算する。

【秘密鍵】 t

【公開鍵】 $(E(F_p), G, Y)$

【暗号化】送信者は、法 K の乗法群から乱数 r を選び、 $E(F_p)$ 上で以下の計算を行い、暗号文 M に対応する暗号文 (C_1, C_3) を生成する。ただし、 $x(C_2)$ は、 C_2 の x 座標の値を指す。

$$C_1 = rG$$

$$C_2 = rY$$

$$C_3 = M \cdot x(C_2) \bmod p$$

【復号】受信者は、秘密鍵 t を利用して $E(F_p)$ 上で以下の計算を行い、平文 M を得る。

$$M = C_3 / x(tC_1) \bmod p$$

EC-ElGamal暗号のプロトコルの安全性については、ElGamal暗号に関する議論がそのまま当てはまる。このため、同じ乱数 r を2回以上用いると、1対の暗号文・平文ペアから同じ乱数の暗号文はすべて解読される。

3. デジタル署名専用の方式

(1) ElGamal署名

ElGamal署名は、ElGamal [1985a] によって提案された署名方式であり、有限体上の乗法群における離散対数問題の困難性に基づく初めての方式である。ElGamal署名には、(i) 署名生成の都度、秘密の乱数を生成する必要がある、(ii) 署名が法のサイズの2倍となる、という問題が存在する。(ii)の問題については、ElGamal署名の改良版であるSchnorr署名やDSAにおいて改善されている。ElGamal署名の署名生成・検証手順は以下の通り。

8 有限可換群 $E(F_p)$ 上で G を K 回加える（換言すると、 $E(F_p)$ 上で定義された加法“+”を K 回行い、 $G + G + \dots + G = KG$ を計算する）という演算を行う。このとき、 $KG = O$ （ O は無有限遠点）となる最小の自然数 K は、 G の位数と呼ばれる。

< ElGamal署名 >

【鍵生成】大きな素数 p と、 p を法とする乗法群の要素 x を選び、 $y = \alpha^x \bmod p$ (α は p を法とする乗法群の原始根)を計算する。

【秘密鍵】 x

【公開鍵】 (y, p, α)

【署名生成】送信者は乱数 k を生成し、以下の計算によって署名 (r, t) を生成する。ただし、平文を M 、ハッシュ関数を h とする。

$$r = \alpha^k \bmod p$$

$$t = (h(M) - xr) / k \bmod (p-1)$$

【署名検証】受信者は、公開鍵 y を利用して、以下の等式が成立するか否かを検証する。

$$\alpha^{h(M)} = y^r r^t \bmod p$$

ElGamal署名を利用する場合には、ElGamal暗号と同様の理由により、毎回異なる乱数 k を利用する必要がある。また、公開鍵である p と α の値がある一定の条件を満足する場合には、秘密鍵を知らなくても容易にデジタル署名の偽造が可能となることが示されており (Bleichenbacher [1996])、他者が生成した公開鍵 p と α を利用すべきではないといわれている。後述するDSAには、この攻撃法は適用できないことが示されている。

(2) DSA

DSAはElGamal署名の改良方式であり、NIST⁹ [1991] によって提案され、1994年に米国連邦政府のデジタル署名標準 (FIPS 186-1) となっている¹⁰。DSAは、Schnorr [1990] によって提案された「法 p に対して $p-1$ の約数 q を法とする有限体上で署名を構成する」という技法を参考にして、ElGamal署名の署名長を $2p$ から $2q$ に短縮することを可能にした。DSAでは、署名生成は高速に実行することができるが、署名検証はRSA暗号よりも時間を要する。

9 NIST(National Institute of Standards and Technology) : 米国商務省の下部組織で、科学技術全般に関する標準を策定する役割を担っているほか、情報通信の分野では、1987年に成立したComputer Security Actにより、米国政府内部における情報通信規格であるFIPS (Federal Information Processing Standard) を制定する権限を有している。

10 DSAは、ISO/IEC FDIS 14888-3において利用可能なデジタル署名方式として記載されているほか、米国の金融分野に利用されるデジタル署名方式の標準規格ANSI X9.30として規定されている。

< DSA >

【鍵生成】大きな素数 p と、 $p-1$ の素因数 q を選ぶ。続いて、 p を法とする乗法群の要素 x を選び、 $y = g^x \bmod p$ (g は q を法とする乗法群の原始根)を計算する。

【秘密鍵】 x

【公開鍵】 (y, g, p, q)

【署名生成】送信者は乱数 k を生成し、以下の計算によって署名 (r, t) を生成する。ただし、 M は平文、 h はハッシュ関数である。

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

$$t = (h(M) + xr) / k \bmod q$$

【署名検証】受信者は、公開鍵 y を利用して、以下の等式が成立するか否かを検証する。

$$r = (g^{h(M)/t} y^{r/t} \bmod p) \bmod q$$

DSAを利用する場合には、ElGamal署名と同様に、毎回異なる乱数 k を利用する必要がある。

(3) ESIGN

ESIGNは、Okamoto [1990] によって提案された高速処理を特徴とするデジタル署名方式である。ESIGNは、素因数分解問題の困難性と合同多項不等式求解問題の困難性に基づいている。

< ESIGN >

【鍵生成】まず、大きな素数 p と q を、 $p > q$ となるように選び、 $n = p^2q$ を計算する。次に、 $k > 3$ となる自然数 k を選ぶ。

【秘密鍵】 (p, q)

【公開鍵】 (k, n) (n は b bitとする)

【署名生成】送信者は、乱数 x (ただし、 $0 < x < pq$) を生成し、以下の計算によって署名 s を生成する。ただし、平文を M 、ハッシュ関数を h とする。

$$Q = (h(M) - (x^k \bmod n)) / pq \quad (Q \text{以上の最小の整数を} w \text{とする})$$

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

$$s = x + ypq$$

【署名検証】受信者は、送信者の公開鍵 k を利用して、以下の不等式が成立するか否かを確認する。ただし、 N は、 $(2b)/3$ 以上の最小の整数とする。

$$h(M) \quad s^k \bmod n < h(M) + 2^N$$

ESIGNの検証式に利用されるべき乗 k について、 $k = 2,3$ に対しては、Brickell and deLaurentis [1986] によって署名の偽造方法が発表されているものの、 $k = 4$ の場合に対しては、現時点では効率的な署名の偽造方法は示されていない。現在では、安全性の観点から、ESIGNのパラメータとして、 k と n は1024 bit程度、 p と q は340 bit程度が推奨されている。

(4) EC-ElGamal署名

EC-ElGamal署名は、ElGamal署名のアルゴリズムを、楕円曲線によって定義された有限可換群上で実現したデジタル署名方式である¹¹。EC-ElGamal暗号と同様に、有限体上の乗法群における離散対数問題に対する高速解法が適用できないことから、安全性を維持しつつ、署名を短縮することが可能となる。この結果、ElGamal署名と比較して、高速処理が可能になるという利点を有している。EC-ElGamal署名の署名生成・検証手順は以下の通り。

< EC-ElGamal署名 >

【鍵生成】まず、素数 p に対して有限素体 F_p 上に定義された楕円曲線を $E(F_p)$ とし、 $E(F_p)$ 上の点 G (ベースポイント) を選ぶ。ただし、 G は、その位数 l が大きな素数となるように選ばれる。整数 t を選び、 $Y=tG$ を計算する。

【秘密鍵】 t

【公開鍵】 $(E(F_p), G, Y)$

【署名生成】送信者は、法1の乗法群から乱数 k を選び、 $E(F_p)$ 上で以下の計算を行い、平文 M に対応するデジタル署名 (R, S) を生成する。ただし、 h はハッシュ関数であり、 $x(R)$ は R の x 座標の値を指す。

$$R = kG$$

$$S = (h(M) - t \cdot x(R)) / k \pmod{l}$$

【署名検証】受信者は、公開鍵 Y を利用して $E(F_p)$ 上で以下の計算を行い、平文 M に対するデジタル署名の正当性を検証する。

$$h(M)G = SR + Y \cdot x(R)$$

11 EC-ElGamal署名は、楕円曲線によって定義された離散対数問題に基づくデジタル署名方式の標準規格案ISO/IEC WD 15946-2 (Information technology Security techniques Cryptographic techniques based on elliptic curves Part 2: Digital signatures) に記載されている方式のひとつである。本標準規格案には、EC-ElGamal署名のほか、EC-DSAやECKCDSA (EC-DSAのアルゴリズムのうち、デジタル署名の生成方法の一部を変更した署名方式) が記載されている。

(5) EC-DSA

EC-DSAは、DSAのアルゴリズムを、楕円曲線によって定義された有限可換群上で実現したデジタル署名方式である¹²。EC-DSAの署名生成・検証方法は以下の通り。

< EC-DSA >

【鍵生成】まず、素数 p に対して有限素体 F_p 上に定義された楕円曲線を $E(F_p)$ とし、 $E(F_p)$ 上の点 G (ベースポイント)を選ぶ。ただし、 G の位数 l は大きな素数となる。整数 t を選び、 $Y=tG$ を計算する。

【秘密鍵】 t

【公開鍵】 $(E(F_p), G, Y)$

【署名生成】送信者は、法 l の乗法群から乱数 k を選び、 $E(F_p)$ 上で以下の計算を行い、平文 M に対応するデジタル署名 (r, S) を生成する。ただし、 h はハッシュ関数、 $x(R)$ は R の x 座標の値を指す。

$$R = kG$$

$$r = x(R) \bmod l$$

$$S = (h(M) + rt) / k \bmod l$$

【署名検証】受信者は、公開鍵 Y を利用して $E(F_p)$ 上で以下の計算を行い、平文 M に対するデジタル署名の正当性を検証する。

$$r = x((h(M)/S)G + (r/S)Y) \bmod l$$

4. 既存の方式に対する改良方式 データ守秘専用方式

(1) OAEP

OAEP (Optimal Asymmetric Encryption Padding) は、Bellare and Rogaway [1995] によって提案されたデータ守秘専用の公開鍵暗号方式である。OAEPは、「入力データに対してランダムなデータを出力する」理想的なランダム関数が利用可能であり(この仮定はランダム・オラクルモデルと呼ばれている)さらに RSA暗号関数が一方向性を有しているならば、能動的攻撃に対して強秘匿であることが証明されている。RSA暗号関数の一方向性については以下の通り。

12 EC-DSAは、ISO/IEC FDIS 14888-2およびISO/IEC WD 15946-2においてデジタル署名方式のひとつとして記載されているほか、現在米国の金融分野におけるデジタル署名の標準案ANSI X9.62として標準化が完了している。

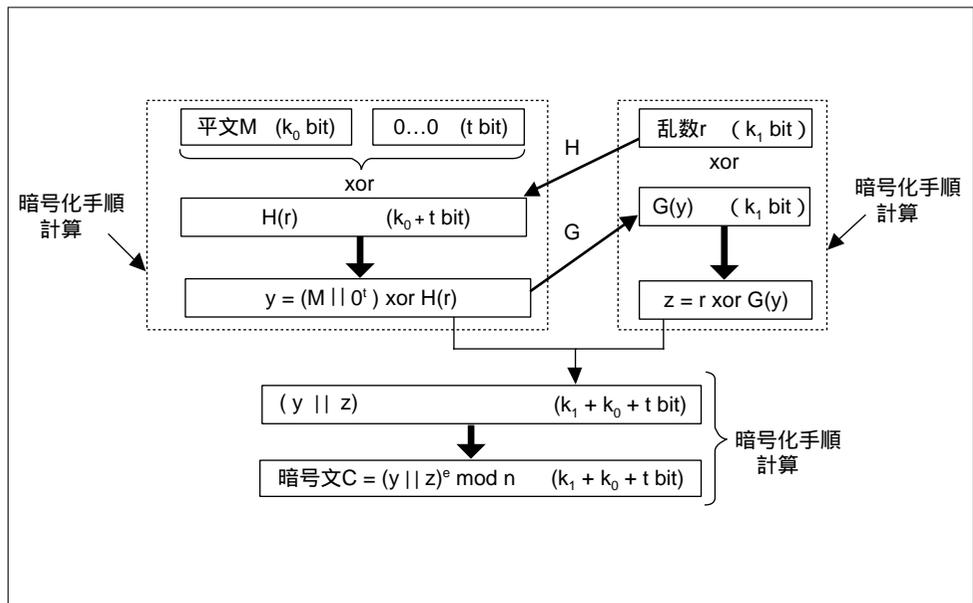
【RSA暗号関数の一方向性】

RSA暗号の公開鍵 (e, n) および $n-1$ 以下の自然数 Y が与えられた場合、以下の等式を満足する x を求めることが計算量的に困難であるとき、「RSA暗号関数は一方向性を有する」と呼ばれる。

$$Y = x^e \pmod n$$

OAEPの暗号化・復号の方法は以下の通り。ハッシュ関数を利用することによって暗号文の冗長性を増し、不正な暗号文ではないか否かを検証することによって、能動的攻撃に対する安全性を確保している点が特徴である。このため、平文よりも暗号文のサイズの方が大きくなる。OAEPは、SET¹³の公開鍵暗号アルゴリズムに採用されているほか、RSA社が開発した公開鍵暗号による暗号通信に関する規格PKCS#1 Version 2にも採用されている。

図4 OAEPの暗号化手順の概念図



13 SET(Secure Electronic Transactions): VISAとMasterCardによって提案されたインターネット上でのクレジットカード決済を実現する技術仕様。現在、世界各国においてSETを利用した実証実験が行われており、日本においてもSmart Collar Club、メディアポート名古屋等の電子商取引実証実験において利用されている。

< OAEP >

【鍵生成】最初に2つの大きな素数 p と q を選び、これらの積 $n=pq$ を計算する。次に、 $p-1$ と $q-1$ の最小公倍数 $L=LCM(p-1, q-1)$ を計算する。さらに、 $GCD(e, L) = 1$ を満足する自然数 e を選び、 $ed = 1 \pmod{L}$ を満たす d を求める（以上は、RSA暗号の鍵生成手順と同じ）。

なお、 H を、 k_1 bitデータの入力に対して、 k_0+t bitの乱数を生成するランダム関数とし、 G を、 k_0+t bitデータの入力に対して、 k_1 bitの乱数を生成するランダム関数とする。さらに、 $[x]^a$ を x の左から a bitのデータとし、 $[x]_a$ を x の右から a bitのデータとする。 \parallel はデータの結合を表す。

【秘密鍵】(d, p, q)

【公開鍵】(e, n)

【暗号化】平文を M とすると、 M は k_0 bitのデータとする（ M が k_0 bit以下の場合にはパディングを行う）。送信者は、 k_1 bitの乱数 r を生成し、以下の計算 ~ によって暗号文 C を生成する（図4参照）。なお、「xor」は排他的論理和を表す。

$$y = (M \parallel 0^t) \text{ xor } H(r), \quad z = r \text{ xor } G(y), \quad C = (y \parallel z)^e \pmod{n}$$

【復号】受信者は、まず以下の計算を行う。

$$X = C^d \pmod{n}, \quad Y = [X]^{k_0+t}, \quad R = [X]_{k_1} \text{ xor } G(y)$$

ここで、以下の等式が成立するか否かを確認する。

$$[Y \text{ xor } H(R)]_t = 0^t$$

上記等式が成立する場合には、以下の計算によって平文 M を復号する。等式が成立しない場合には、不正な暗号文とみなして受け付けない。

$$M = [Y \text{ xor } H(R)]^{k_0}$$

(2) EPOC

EPOCは、Okamoto-Uchiyama暗号に改良を加えた暗号方式である (Okamoto, Uchiyama and Fujisaki [1998])。EPOCには2種類の使用方法があり、Okamoto-Uchiyama暗号のアルゴリズムにハッシュ関数演算が組み込まれているEPOC-1と、ハッシュ関数のほかに共通鍵暗号方式 (任意) が組み込まれているEPOC-2が提案されている。まずEPOC-1の安全性については、ランダム・オラクルモデルと、P部分群問題の困難性を仮定することによって、能動的攻撃に対して強秘匿であることが証明されている。EPOC-1の暗号化・復号の手順は以下の通り。

< EPOC-1 >

【鍵生成】 大きな素数 p と q (いずれもサイズは k bit) を生成し、 $n = p^2q$ を計算する。法 n の乗法群の要素 g を選ぶ。ただし、 $g_p (= g^{p-1} \bmod p^2)$ の位数が p となるように g を選ぶ。また、 $h = g^n \bmod n$ とする。 H を、 k bit データ ($k = k_0 + k_1$ 、 k_0 は平文 m のサイズであり、 k_1 は乱数 r のサイズ) から $3k$ bit のサイズの乱数を発生させるランダム関数とする。

【秘密鍵】 (p, q)

【公開鍵】 (n, g, h)

【暗号化】 送信者は乱数 r (サイズは k_1) を生成し、平文 m に対応する暗号文 C を以下の計算によって生成する。

$$C = (g^{m||r})(h^{H(m||r)}) \bmod n$$

【復号】 受信者は、関数 $L(x) = (x-1)/p$ を利用して以下の計算を行う。

$$C_p = C^{p-1} \bmod p^2, X = L(C_p)/L(g_p) \bmod p$$

これらの計算結果を利用して、以下の等式が成立するか否かを確認する。

$$C = (g^X)(h^{H(X)}) \bmod n$$

等式が成立した場合には、以下の計算によって平文 m を復号する。成立しない場合には、不正な暗号文とみなして受け付けない。

$$m = [X]^{k_0}$$

EPOC-1は、Okamoto-Uchiyama暗号の暗号化・復号処理に1回のハッシュ関数演算を追加するのみであり、Okamoto-Uchiyama暗号とほぼ同程度の処理時間で実現可能とみられている。

一方、EPOC-2の安全性については、ランダム・オラクルモデルと、素因数分解問題の困難性を仮定することによって、能動的攻撃に対して強秘匿であることが証明されている。EPOC-2の暗号化・復号の手順は以下の通り。

< EPOC-2 >

【鍵生成】大きな素数 p と q (いずれもサイズは k bit) を生成し、 $n = p^2q$ を計算する。法 n の乗法群の要素 g を選ぶ。ただし、 $g_p (= g^{p-1} \bmod p^2)$ の位数が p となるように g を選ぶ。また、 $h = g^n \bmod n$ とする。 H を、 k bitデータ ($k=k_0 + k_1$ 、 k_0 は平文 m のサイズであり、 k_1 は乱数 r のサイズ) から $3k$ bitのサイズの乱数を発生させるランダム関数、 G を k_1 bitデータから k_2 bitデータ (k_2 bitは共通鍵暗号のセッション鍵のサイズ) を発生させるランダム関数とする。なお、 $\text{SymEnc}(a,b)$ は、共通鍵暗号方式を利用して平文 b をセッション鍵 a で暗号化する演算を表し、 $\text{SymDec}(a,b)$ は、暗号文 b をセッション鍵 a で復号する演算を表す。

【秘密鍵】(p, q)

【公開鍵】(n, g, h)

【暗号化】送信者は乱数 r (サイズは k_1) を生成し、平文 m に対応する暗号文 (C_1, C_2) を以下の計算によって生成する。

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

【復号】受信者は、関数 $L(x) = (x-1)/p$ を利用して以下の計算を行う。

$$C_p = C_1^{p-1} \bmod p^2, \quad X = L(C_p)/L(g_p) \bmod p, \quad m' = \text{SymDec}(G(X), C_2)$$

これらの計算結果を利用して、以下の等式が成立するか否かを確認する。

$$C_1 = (g^X)(h^{H(m'||r)}) \bmod n$$

等式が成立した場合には、 m' が正しい平文であることが判明する。等式が成立しない場合には、不正な暗号文とみなして受け付けない。

EPOC-2で利用される共通鍵暗号方式の代わりに、セッション鍵と平文の排他的論理和を利用することができる。この場合、 C_2 の計算を非常に高速で実現することができることから、EPOC-2はEPOC-1とほぼ同程度の処理時間で実現可能であるとみられている。

(3) Cramer-Shoup暗号

Cramer-Shoup暗号は、Cramer and Shoup [1998] によって提案されたデータ守秘専用の公開鍵暗号方式である。Cramer-Shoup暗号は、ElGamal暗号に一部改良を加えた方式であり、Diffie-Hellman判定問題の困難性と、汎用一方向性ハッシュ関数 (任意の x に対して $H(x)=H(y)$ を満足する y ($x \neq y$)を見つけることが困難なハッシュ関数 H) を仮定することによって、能動的攻撃に対して強秘匿であることが証明されている。なお、Cramer-Shoup暗号は、有限体上の乗法群における離散対数問題に基づいているが、楕円曲線によって定義された離散対数問題に基づく方式としても利用可能である。

【Diffie-Hellman判定問題】

素数 p を法とする乗法群 G の原始根 g と3つの要素 x, y, z を任意に選ぶ。これらを利用して、 $g^x \bmod p, g^y \bmod p, g^z \bmod p$ を計算する。このとき、 $(g^x \bmod p, g^y \bmod p, g^z \bmod p)$ のみを所与として、 $xy = z \bmod p$ が成立するか否かを判定せよ。

Cramer-Shoup暗号の暗号化・復号の方法は以下の通り。

< Cramer-Shoup暗号 >

【鍵生成】 大きな素数 p, q を生成する (ただし、 q は $p-1$ の素因数とする)。次に、 p を法とする乗法群の要素 g_1 と g_2 を選ぶ (ただし、 $1 = g_1^{q-1} \bmod p, 1 = g_2^{q-1} \bmod p$ を満足する)。 p を法とする加法群の要素 x_1, x_2, y_1, y_2, z を選ぶ。これらを用いて、 $c = g_1^{x_1} g_2^{x_2} \bmod p, d = g_1^{y_1} g_2^{y_2} \bmod p, h = g_1^z \bmod p$ を計算する。 H をハッシュ関数とする。

【秘密鍵】 (x_1, x_2, y_1, y_2, z)

【公開鍵】 $(p, q, g_1, g_2, c, d, h)$

【暗号化】 送信者は乱数 r を生成し、受信者の公開鍵を用いて以下の計算を行う。ただし、平文を M とする。このとき、暗号文は (u_1, u_2, e, v) となる。

$$u_1 = g_1^r \bmod p, u_2 = g_2^r \bmod p, e = h^r M \bmod p, \alpha = H(u_1, u_2, e), \\ v = (c d^\alpha)^r \bmod p$$

【復号】 受信者は、受け取った暗号文に対して以下の等式が成立することを確認する。

$$(u_1^{x_1 + \alpha y_1})(u_2^{x_2 + \alpha y_2}) = v \pmod{p}$$

上記等式が成立する場合には、以下の計算から平文 M を得る。成立しない場合には、不正な暗号文とみなして受け付けない。

$$M = e / u_1^z \bmod p$$

5. 既存の方式に対する改良方式 デジタル署名専用方式

(1) PSS署名

PSS (Probabilistic Signature Scheme) 署名は、Bellare and Rogaway [1996] によって提案されたデジタル署名専用の方式である。PSS署名は、RSA署名を改良した方式であり、ランダム・オラクルモデルと、RSA暗号関数の一方向性を仮定することにより、能動的攻撃における存在的偽造(第4章1(2)で説明)が不可能となることが証明されている。PSS署名では、署名生成の際に乱数が利用されており、同一の文書に同一の鍵で署名を生成しても、毎回異なる乱数を利用すればそれぞれ異なる署名が生成される。

なお、Bellare and Rogaway [1996] は、Rabin暗号を同様の方法によって改良することで、能動的攻撃に対する安全性が素因数分解問題と等価になることが証明可能なPRab (Probabilistic Rabin Scheme) 署名を同時に発表している。もっとも、PRab署名の場合、署名生成の際に乱数を利用して合成数 n の平方剰余を計算する必要があり、計算量が比較的多くなるという短所がある。PSS署名の署名生成・検証方法は以下の通り (図5参照)。

< PSS署名 >

【鍵生成】最初に2つの大きな素数 p と q を選び、これらの積 $n = pq$ を計算する。次に、 $p-1$ と $q-1$ の最小公倍数 $L = \text{LCM}(p-1, q-1)$ を計算する。最後に、 $\text{GCD}(e, L) = 1$ を満足する自然数 e を選び、 $ed = 1 \pmod{L}$ を満たす d を求める (以上は、RSA暗号の鍵生成手順と同じ)。

【秘密鍵】(d, p, q)

【公開鍵】(e, n)

【署名生成】乱数を出力するハッシュ関数 h (ハッシュ値は k_1 bit)とデータ拡張関数 g (k_1 bit ($k-k_1-1$) bit)を用意する。なお、 g 関数で利用するデータサイズ k ($k > k_1$)を予め設定する。

さらに、 g 関数の拡張変換に加えて、出力データの左 k_0 bitを出力する関数 g_1 と、左($k-k_0-k_1-1$) bitを出力する関数 g_2 を用意する。平文を M とし、 k_0 bitの乱数 r を生成して以下の計算 ~ を行い、デジタル署名 S を生成する。

$$w = h(M\|r), \quad R = g_1(w) \text{ xor } r,$$

$$S = X^d \pmod{n} \quad (\text{ただし、} X = (0\|w\|R\|g_2(w)))$$

【署名検証】平文とデジタル署名(M, S)を受け取った受信者は、 $X = S^e \pmod{n}$ を計算し、 X の最初の1 bitを b 、次の k_1 bitを y 、次の k_0 bitを z 、残りのbitを α とする。すなわち、 $X = (b\|y\|z\|\alpha)$ とする。

次に、 $R' = g_1(y) \text{ xor } z$ を計算する。

このとき、以下の3つの等式が成立するか否かを検証する。

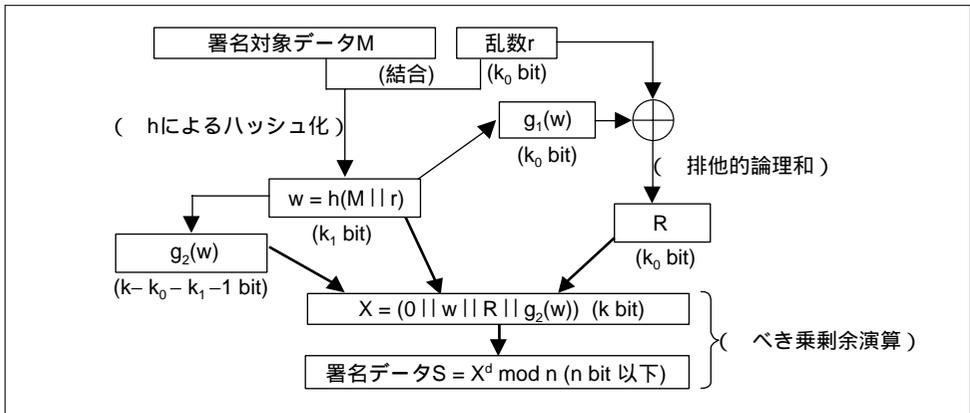
$$h(M\|R') = y, \quad g_2(y) = \alpha, \quad b = 0$$

3つの等式がすべて成立すれば、 S が真正であることが確認される。

1つでも等式が成立しない場合、 S を受け付けない。

PSS署名の署名生成・検証に必要な計算量は、署名生成・検証のいずれの場合も、RSA署名の計算量に、1回のハッシュ関数演算と2回のデータ拡張関数演算が追加されるのみであり、実用性が高いとみられている。しかし、ランダム関数である h や g に通常ハッシュ関数を利用すると、ランダム・オラクルモデルの仮定が満足されず、安全性の証明が成立しなくなる。

図5 PSS署名の署名生成手順の概念図



(2) 改良ElGamal署名

改良ElGamal署名は、Pointcheval and Stern [1996] によって提案された方式であり、ElGamal署名のアルゴリズムをベースにして開発された。改良ElGamal署名は、ElGamal署名で利用されているハッシュ関数に一部変更を加えた方式である。安全性については、ランダム・オラクルモデルと、離散対数問題の困難性を仮定することによって、能動的攻撃における存在的偽造が不可能となることが証明されている。改良ElGamal署名は、有限体上の乗法群における離散対数問題に基づいているが、楕円曲線によって定義された離散対数問題に基づく方式としても利用可能である。

なお、Schnorr署名に対しても同様の改良を施すことによって、能動的攻撃に対する安全性を証明可能とすることもできることが示されている。改良ElGamal署名の署名生成・検証手順は以下の通り。

< 改良ElGamal署名 >

【鍵生成】大きな素数 p と、 p を法とする乗法群の要素 x を選び、 $y = \alpha^x \bmod p$ (α は p を法とする乗法群の原始根)を計算する。

【秘密鍵】 x

【公開鍵】(y, p, α)

【署名生成】まず、ハッシュ関数 h を用意するとともに、乱数 k を生成する。その上で、以下の計算によってデジタル署名 (r, t) を生成する。ただし、 M は平文である。

$$r = \alpha^k \bmod p$$

$$t = (h(M, r) - xr) / k \bmod (p-1)$$

【署名検証】受信者は、公開鍵 y を利用して、以下の等式が成立するか否かを検証する。

$$\alpha^{h(M,r)} = y^r r^t \bmod p$$

改良ElGamal署名は、ElGamal署名で利用されているハッシュ関数 $h(M)$ を $h(M,r)$ に変更するという比較的マイナーな改良によって証明付きの安全性を実現していることから、改良ElGamal署名の処理速度はElGamal署名とほぼ同程度とみられている。しかし、ハッシュ関数 h がランダム関数であるという仮定を外すと、安全性の証明が成立しなくなる。このため、既存のハッシュ関数を利用して実用化した場合には、安全性の証明という長所は失われることとなる。

(3) TSH-ESIGN

TSH-ESIGN (Trisection-Size-Hash ESIGN) は、ESIGNを改良したデジタル署名方式である (Okamoto, Fujisaki and Morita [1998])。TSH-ESIGNでは、ランダム・オラクルモデルと、 e 乗根近似問題の困難性を仮定すると、能動的攻撃における存在的偽造が不可能であることが証明されている。 e 乗根近似問題の困難性については、以下の通り。

【 e 乗根近似問題】

TSH-ESIGNの公開鍵を (e, n) とし、 $n = p^2q$ のサイズを $3k$ とする (p と q のサイズを共に k とする)。さらに、サイズが $k-1$ の自然数 y が与えられた場合、以下の不等式を満足する x を求めよ。ただし、 $[A]^k$ は、 A の左 k bit 分のデータを表す。

$$0 \parallel y = [x^e \bmod n]^k$$

TSH-ESIGNの署名生成・検証手順は以下の通り。

< TSH-ESIGN >

【鍵生成】まず、大きな素数 p と q を選び、 $n = p^2q$ を計算する。ただし、 p と q のサイズはいずれも k とする。次に、 $e > 4$ となる自然数 e を選ぶ。

【秘密鍵】 (p, q)

【公開鍵】 (e, n) (n は $3k$ bit)

【署名生成】送信者は、乱数 x (ただし、 $0 < x < pq$) を生成し、以下の計算によって署名 s を生成する。ただし、 M を平文、 h をハッシュ関数とし、 h のハッシュ値のサイズは $k-1$ とする。また、 \parallel は、データの結合を表す。

$$Z = (0 \parallel h(M) \parallel 0^{2k}), \quad \alpha = (Z - x^e) \bmod n$$

$$Q = \alpha / pq \quad (Q \text{ 以上の最小の整数を } W_0 \text{ とする})$$

$$W_1 = pqW_0 - \alpha \quad (W_1 \text{ が } 2^{2k-1} \text{ の場合には、乱数 } x \text{ を選び直す})$$

$$t = W_0 / (ex^{e-1}) \bmod p,$$

$$s = (x + tpq) \bmod n$$

【署名検証】受信者は、送信者の公開鍵 e を利用して、以下の等式が成立するかどうかを確認する。ただし、 $[Y]^k$ は Y の左 k bit 分のデータを表す。

$$[s^e \bmod n]^k = 0 \parallel h(M)$$

IV. 公開鍵暗号の安全性評価に関する研究

公開鍵暗号の安全性評価は、攻撃や解読のタイプを分類した上で、公開鍵暗号方式の安全性と、その暗号方式において利用されている数学の問題の困難性との関連を評価する（相対評価）、利用されている数学の問題における困難性を評価する（絶対評価）という2つのステップによって構成される。この結果、各暗号方式に対して、「どのようなタイプの攻撃に対して、どの程度の解読がどれだけ困難なのか」を評価することが可能となる。

1. 安全性評価のための概念整理

公開鍵暗号の安全性評価を行う場合、まず、攻撃および解読のタイプを分類しておく必要がある。本節では、公開鍵暗号をデータ守秘およびデジタル署名にそれぞれ利用する場合において、攻撃のタイプと解読・偽造のタイプを整理する。

(1) 公開鍵暗号方式をデータ守秘に利用する場合

攻撃のタイプ

公開鍵暗号方式をデータ守秘に利用する場合に、攻撃のタイプは4つに分類される（表2参照）。

表2 データ守秘に利用する暗号方式への攻撃のタイプ

攻撃方法		内容
受動的 攻撃	直接攻撃	公開鍵のみを利用して行う攻撃
	選択平文攻撃 (CPA)	攻撃者が予め指定したいいくつかの平文に対応する暗号文を入手できる場合の攻撃
能動的 攻撃	選択暗号文攻撃 (CCA1)	攻撃者が予め指定したいいくつかの暗号文に対応する平文を入手できる場合の攻撃（ただし、攻撃者は、攻撃前に予め入手する暗号文と平文のペアをすべて選択しなければならない）
	適応的選択暗号 文攻撃(CCA2)	選択暗号文攻撃における暗号文の選択を、それまでに入手した暗号文・平文ペアに関する情報を参考にしながら決定できる場合の攻撃

公開鍵暗号の場合、攻撃者は公開鍵を用いて任意の平文を暗号化できるため、選択平文攻撃が容易に実現可能となる。したがって、少なくとも、選択平文攻撃に対して十分な安全性を有することが必要である。また、選択暗号文攻撃、適応的選択暗号文攻撃は一般的には成立しがたい攻撃であるとみられているものの、実際に適応的選択暗号文攻撃が可能となるケースも存在することが示されている（PKCS#1 Version 1における攻撃、詳細は本章2.(2)）ことから、これらの攻撃に対しても安全であることが望ましいとされている。適応的選択暗号文攻撃が最も強力な攻撃方法である。

直接攻撃や選択平文攻撃(Chosen Plaintext Attack、以下CPA)は受動的攻撃と呼ばれており、選択暗号文攻撃(Chosen Ciphertext Attack、以下CCA1)や適応的選択暗号文攻撃(Adaptive Chosen Ciphertext Attack、以下CCA2)は能動的攻撃と呼ばれている。

解読のタイプ 強秘匿性と頑健性

解読のタイプとして、2つのタイプに分類できる(表3参照)。

表3 データ守秘に利用する暗号方式の解読のタイプ

解読のタイプ	内容
完全解読	暗号文に対応する平文全体を求める
部分解読	暗号文に対応する平文の一部や、平文に関連する情報を求める

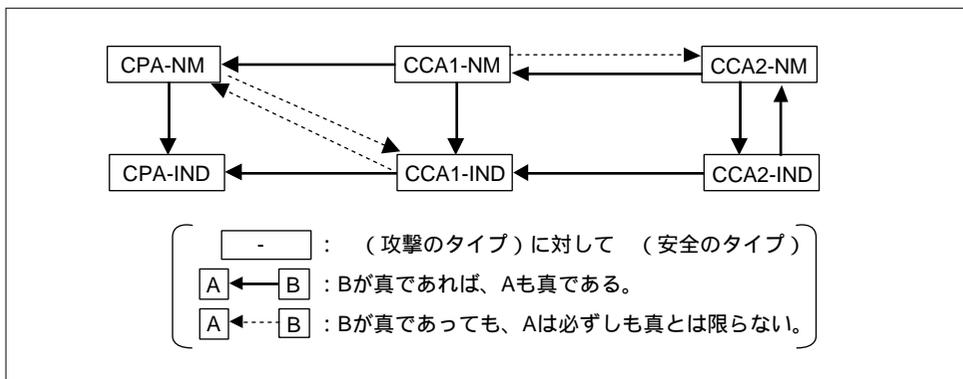
完全解読が困難である場合、その暗号方式は「一方向性 (one-way)」を有していると呼ばれており、いかなる部分解読も困難である場合、その暗号方式は「強秘匿性 (indistinguishability of encryption、以下INDとする)」を有していると呼ばれている (Goldwasser and Micali [1984])。

また、任意の平文Mに対する暗号文を $C=E(M)$ とする場合、どのような関数Fに対しても、Cを用いて $M' = F(M)$ を満足するような $C' = E(M')$ を求めることができないとき、その公開鍵暗号方式は「頑健性 (non-malleability、以下NMとする)」を有していると呼ばれている (Dolev, Dwork and Naor [1991])。

各安全性のレベルに関する分類と関係

3つの攻撃のタイプ(CPA、CCA1、CCA2)と2つの安全性のタイプ(IND、NM)から、6つの安全性のレベルが定義される。各安全性レベルの相互関係に関する研究成果が発表されており(Bellare et al.[1998])、図示すると以下の通り(図3参照)。

図3 安全レベルの相互関係



このように、「適応的選択暗号文攻撃に対して強秘匿 (CCA2-IND)」となる方式は、「適応的選択暗号文攻撃に対して頑健 (CCA2-NM)」であることが証明されており、さらに選択暗号文攻撃等の攻撃に対しても強秘匿および頑健となることから、最も安全性の高い暗号方式であるといえる。

(2) 公開鍵暗号方式をデジタル署名に利用する場合

攻撃のタイプ

公開鍵暗号方式をデジタル署名に利用する場合、攻撃のタイプは以下の4つに分類できる(表4参照)。

表4 デジタル署名に利用する暗号方式への攻撃のタイプ

攻撃方法		内容
受動的 攻撃	直接攻撃	公開鍵のみを利用して行う攻撃
	既知文書攻撃	いくつかのランダムなデータに対応するデジタル署名を入手できる場合の攻撃
能動的 攻撃	選択文書攻撃	攻撃者が予め指定したいくつかの署名に対応する署名対象データを入手できる場合の攻撃(ただし、署名者に署名させるデータを攻撃に先立ってすべて選択しなければならない)
	適応的 選択文書攻撃	選択文書攻撃における署名の選択を、それまでに入手した署名とそれに対応する署名対象データに関する情報を参考にしながら決定することができる場合の攻撃

デジタル署名は、署名付きデータを収集することで既知文書攻撃が可能となるため、少なくとも既知文書攻撃に対して十分な安全性を有する必要がある。また、選択文書攻撃、適応的選択文書攻撃は、一般的には成立しがたい攻撃ではあるが、これらの攻撃に対しても安全であることが望まれる。

偽造のタイプ

デジタル署名の偽造は、以下の3つのタイプに分類することができる(表5参照)。このように、最も安全なデジタル署名方式は、「適応的選択文書攻撃に対して、存在的偽造が不可能な方式」といえる。

表5 デジタル署名に利用する暗号方式の偽造のタイプ

偽造のタイプ	内容
一般的偽造	任意のデータに対してデジタル署名を偽造できる
選択的偽造	攻撃者が予め選んだいくつかのデータに対し、デジタル署名を偽造できる
存在的偽造	少なくともある特定のデータに対して、デジタル署名を偽造できる

2. 安全性の証明に関する研究

公開鍵暗号の安全性評価の第1ステップは、評価の対象である公開鍵暗号方式の安全性と、その暗号方式に利用されている数学の問題の困難性との関連を分析・評価することである。最近では、非現実的と考えられてきた適応的選択暗号文攻撃が、実際に利用可能な場合も存在することを示す研究成果も発表されており、能動的攻撃に対して安全性の証明が付いている公開鍵暗号方式が目玉されている。

(1) これまでの研究の経緯

データ守秘専用の方式

安全性の証明に関する研究は、まず受動的攻撃に対する安全性から始められた。受動的攻撃に対して安全性が証明されている公開鍵暗号方式として最初に提案されたのが、Rabin暗号である。Rabin暗号は、素因数分解問題の困難性を仮定すると、受動的攻撃に対して一方向性を有することが証明されている。しかし、受動的攻撃に対する強秘匿性や頑健性については証明されていないほか、能動的攻撃に対して容易に完全解読されてしまうことが示されている。

その後、Goldwasser and Micali [1984] が強秘匿の概念を初めて提案し、データ守秘専用の方式として、Goldwasser-Micali暗号を発表した。Goldwasser-Micali暗号は、平方剰余判定問題¹⁴の困難性を仮定すれば、受動的攻撃に対して強秘匿性が証明されるものの、能動的攻撃に対しては完全解読が可能となることが示されている。

能動的攻撃に対しては、Naor and Yung [1990] によって、安全性が証明可能な暗号方式の構成法が初めて提案された。NaorとYungは、受動的攻撃に対して強秘匿である暗号方式（たとえば、Goldwasser-Micali暗号）と非対話型ゼロ知識証明¹⁵を組み合わせることによって、適応的選択暗号文攻撃に対しても強秘匿となる暗号方式を構成できることを示した。しかし、NaorとYungが提案した構成方法は、計算量が非常に多くなること等から、実用的とはいえない。また、Dolev, Dwork, and Naor [1991] は頑健性の概念を初めて提案し、適応的選択暗号文攻撃に対して頑健性を有する暗号方式を提案したが、この方式も計算量が多いことから実用的な方式とはいえない。

こうした中、適応的選択暗号文攻撃に対して強秘匿性と頑健性を満足し、さらに暗号化・復号に必要な計算量の面から実用的といえる暗号方式が、Bellare and Rogaway [1993] によって最初に提案された。その後改良が加えられ、1995年にBellare and Rogawayによって再び提案された方式が、RSA暗号をベースにしたOAEPである。OAEPは、ランダム・オラクルモデルとRSA暗号関数の一方向性の仮定を置くことにより、適応的選択暗号文攻撃に対して強秘匿性かつ頑健性を有することが証明されている。もっとも、実際に利用する場合には、ランダム関数の代わりにハッシュ関数が利用されていることから、厳密には安全性の証明に必要な条件が満たされていない。したがって、実用化されているOAEPを「厳密に安全性が証明された暗号」とみなすことはできないが、「実用性と安全性の高い暗号」の実現に向けての重要な研究成果と位置付けられている。

14 自然数 n と互いに素な自然数 a ($a < n$) に対して、 $x^2 = a \pmod{n}$ を満足する x が存在するとき、 a を n に関する平方剰余という。平方剰余判定問題は、「任意の自然数 a が、 n に関して平方剰余となるかどうかを判定せよ」という問題である。

15 ゼロ知識証明は、自分がある情報を知っているという事実を、その情報の内容を一切漏らすことなく他者に対して証明する方法のことである。非対話型ゼロ知識証明は、信頼できる第三者を介して、1回だけ相手に必要な情報を送るだけでゼロ知識証明を実現する方式である。

また、1998年には、Okamoto and Uchiyama [1998] によって、Okamoto-Uchiyama暗号が提案されている。Okamoto-Uchiyama暗号は、最も実現性が高い受動的攻撃に対する一方向性が素因数分解問題の困難性と等価であることが証明されているほか、暗号化・復号に必要な計算量もRSA暗号と同程度とされており、証明可能な安全性と実用性を兼ね備えている。このOkamoto-Uchiyama暗号の改良版であるEPOCは、一定の仮定の下で適応的選択暗号文攻撃に対して強秘匿であることが証明されている。EPOCには2種類のバージョンが存在し、EPOC-1の安全性証明には、ランダム・オラクルモデルとP部分群問題の困難性の仮定が必要となる。一方、EPOC-2の場合には、ランダム・オラクルモデルと素因数分解問題の困難性の仮定が必要となる。さらに、Cramer and Shoup [1998] は、ランダム・オラクルモデルよりも緩い仮定とみられている (i) Diffie-Hellman 判定問題の困難性と (ii) 汎用一方向性ハッシュ関数の仮定を置くことによって、適応的選択暗号文攻撃に対する強秘匿性が証明可能なCramer-Shoup暗号を提案している。Cramer-Shoup暗号は、ElGamal暗号をベースにした方式であり、実用性も高いといわれている。

デジタル署名専用の方式

「最も安全なデジタル署名方式」すなわち「能動的攻撃において存在的解読が不可能なデジタル署名方式」の概念は、1984年にGoldwasser, Micali and Rivestによって定義され、その後、最も安全なデジタル署名方式として、Goldwasser-Micali-Rivest署名が提案された (Goldwasser, Micali and Rivest [1988])。Goldwasser-Micali-Rivest署名は、素因数分解問題が困難であるとの仮定の下で、能動的攻撃における存在的偽造が不可能であることが証明されている。しかし、アルゴリズムが複雑であり、署名生成・検証に必要な計算量が多くなるため、実用的な方式とはいえない。

その後、Naor and Yung [1989] は、汎用一方向性ハッシュ関数を利用することによって、能動的攻撃における存在的偽造が不可能な署名方式を提案した。また、Rompel [1990] は、Naor and Yung [1989] の考え方を拡張して、より緩い仮定である一方向性関数の利用可能性を仮定すれば、能動的攻撃における存在的偽造が不可能となる署名方式を構築できることを示した。しかし、Naor and YungおよびRompelが提案した署名方式は、莫大な計算量が必要となるため、実用性は低い。

こうした中、証明可能な安全性と比較的高い実用性を有する署名方式が、Bellare and Rogaway [1996] やPointcheval and Stern [1996] によって提案されている。Bellare and Rogawayは、ランダム・オラクルモデルとRSA暗号関数の一方向性を仮定すれば、能動的攻撃における存在的偽造が不可能であることが証明可能なPSS署名を提案した。PSS署名の署名生成・検証の計算量は、RSA暗号の計算量に3回のランダム関数計算量を加えたものに等しくなっており、それまでに提案されてきた証明可能な安全性を有している署名方式に比べて実用性が高い。一方、Pointcheval and Sternは、ElGamal署名のアルゴリズムを基に、ランダム・オラクルモデルと離散対数問題の困難性を仮定すれば、能動的攻撃における存在的偽造が不可能となる

改良ElGamal署名を提案している。改良ElGamal署名は、ElGamal署名に利用されているハッシュ関数を一部変更した方式であり、署名生成・検証に必要となる計算量はElGamal署名の計算量とほぼ同程度となっている。

このように、一定の仮定のもとで最も安全なデジタル署名がいくつか提案されている。しかし、これらの方式を実用化するには、ランダム・オラクルモデルにおいて仮定されている「理想的なランダム関数」を利用することが不可能であるため、安全性の証明は成立しなくなるという問題が残されている。

(2) 能動的攻撃の適用可能性 - PKCS#1への攻撃 -

近年、能動的攻撃に対して証明可能な安全性と実用性を兼ね備えた方式がいくつか提案されているが、これまでは能動的攻撃が実際にどれだけ適用可能なのかについて疑問視する見方が少なくなかった。しかし、1998年6月に、RSA社によって開発された公開鍵暗号を利用した暗号通信データ形式の規格PKCS#1 Version 1をある特定の双方向通信環境において実装した場合、適応的選択暗号文攻撃によって任意の暗号文に対する平文を効率的に解読する方法が、Bleichenbacher [1998] によって発表された。

PKCS#1 Version 1の概要を簡単に説明すると、以下の通り。

PKCS#1 Version 1において利用されるRSA暗号の公開鍵を (e, n) (n は k byteとする)、秘密鍵を d 、平文を M 、パディングデータを PS とすると、暗号化の対象となるデータ ED (ED は k byte)の形式は以下のように規定されている。

$$ED = 00\ 02 \parallel PS \parallel 00 \parallel M$$

ED の最初の2 byteはそれぞれ00と02であり、 PS と M は1 byteのデータ00によって区切られる。 M が m byteであった場合、 PS は $k-m-3$ byteとなる。送信者は、この ED を受信者の公開鍵を用いて以下の計算によって暗号文 C に変換し、送付する。

$$C = ED^e \pmod n$$

受信者は、自分の秘密鍵 d で暗号化データ C を復号して ED を入手し、 ED が規定通りの形式のデータになっていることを確認して M を平文として入手する。

PKCS#1 Version 1に対する攻撃が有効となるのは、たとえば、共通鍵暗号の鍵配送等に利用される双方向通信において、「受信者が受け取った暗号化データを復号したときに、復号データの最初の2 byteが“00 02”となっていない等規定の形式とは異なっていた場合に、何らかのエラーメッセージを送信者に送る」等の手続きが組み込まれており、攻撃者が不当な暗号文を送信した場合、そのデータを復号アルゴリズムによって変換した値が上記フォーマットと適合しているか否かを確認することができる、さらに「特定の送信者から送信された暗号化データにおいて一定回数エラーが発生した場合、その送信者からのデータ受信をストップする」といった、攻撃者が繰り返し不当な暗号文を送信できないようにする対策が講じら

れていない、というケースである。こうした実装環境であれば、攻撃者は、自分の選択した暗号化データがエラーとなるか否かを何度でも検証することが可能となり、エラーとならない場合には、その時送信した暗号化データに対応する復号データが“00 02”で始まることがわかる。

上記の実装環境における適応的選択暗号文攻撃の概要は以下の通り。ただし、攻撃対象者（暗号文の受信者）の秘密鍵を (d, p, q) 、公開鍵を (e, n) とし、攻撃者がある暗号文 C に対する平文 M を入手しようとする場合を想定する。

(ステップ1) 攻撃者は、次のようなデータ系列 $C_i (i = 1, 2, \dots)$ を作成する。

$$C_i = C \cdot r_i^e \pmod n$$

ただし、 $r_i (i = 1, 2, \dots)$ は $0 < r_i < n-1$ を満足する整数であり、攻撃者は、それまでに送付した C_1, \dots, C_{i-1} に対する攻撃対象者からの反応を確認しながら r_i を決めることができる。

(ステップ2) 攻撃者は、攻撃対象者に $C_i (i = 1, 2, \dots)$ を送付し、攻撃対象者の反応を観察する。復号データがPKCS#1 Version 1に規定されているデータ形式と異なる場合にはエラーメッセージが送信され、規定のデータ形式（上記のEDの形式）に適合している場合にはエラーメッセージは送信されない。

(ステップ3) 攻撃対象者からエラーメッセージが送信されない場合、攻撃者は、 C_i に対する平文 $M_i (= C_i^d \pmod n = M r_i \pmod n)$ の特定のbitに関する情報を入手することができる。

(ステップ4) 攻撃者は、平文 M_i の特定のbitに関する情報を集めて平文 M を求める。

Bleichenbacher [1998] は、鍵長が1024 bitの場合、上記の攻撃に必要な選択暗号文数を約 2^{20} 個と試算している。本攻撃法が有効なのは、特定の条件を満たす実装環境においてのみであるが、インターネット上での暗号・認証プロトコルとして広く利用されているSSL Version 3¹⁶に対して本攻撃が適用できる可能性が指摘されたことから、インターネット技術者の間で大きな注目を集めた。これまでのところ、実際に本攻撃を利用してSSL Version 3の暗号文を解読したという事例は報告されていないが、本攻撃はインターネットのセキュリティに対する潜在的な脅威と認識されている。

なお、RSA社は、この発表を受けてPKCS#1 Version 1を改良し、OAEPを利用した平文の事前処理やパディングを実行するPKCS#1 Version 2を発表している。

16 SSL(Secure Socket Layer)Version 3: Netscape社が提唱する暗号通信、認証等のセキュリティ機能が付加されたHTTPプロトコル。SSL Version 3で利用されるデータ形式等について、PKCS#1を採用することが規定されている。

(3) 証明付きの安全性のレベル比較

データ守秘専用の方式

これまで提案されているデータ守秘専用の方式の中で、証明付きの安全性と実用性を兼ね備えた主要な方式として、OAEP、EPOC、Cramer-Shoup暗号が挙げられる。各暗号方式の適応的選択暗号文攻撃に対する安全性を比較すると、以下の表6の通り。

表6 各データ秘匿専用方式の適応的選択暗号文攻撃に対する安全性

	証明されている安全性	安全性の証明に必要となる前提	利用されている数学の問題
OAEP	強秘匿	・ランダム・オラクルモデル ・RSA暗号関数の一方向性	素因数分解問題
EPOC-1	強秘匿	・ランダム・オラクルモデル ・P部分群問題の困難性	素因数分解問題
EPOC-2	強秘匿	・ランダム・オラクルモデル ・素因数分解問題の困難性	素因数分解問題
Cramer-Shoup暗号	強秘匿	・汎用一方向性ハッシュ関数 ・Diffie-Hellman判定問題の困難性	離散対数問題

安全性の証明に利用されている問題の困難性については、長年の研究の中で準指数関数時間の計算量による解法しか示されていない素因数分解問題や離散対数問題の困難性が、最も高い信頼を得ている。したがって、これらの問題の困難性を前提条件として安全性が証明されている暗号方式が望ましい。一方、RSA暗号関数の一方向性、Diffie-Hellman判定問題、P部分群問題の困難性については、素因数分解問題や離散対数問題ほど研究が進んでいるわけではなく、素因数分解問題等との関連性に関する厳密な証明も示されていないことから、素因数分解問題や離散対数問題ほど困難性に対する信頼性は高くない。なお、ランダム・オラクルモデルの仮定は、汎用一方向性ハッシュ関数の仮定よりも緩い仮定であるとみられている。

3つの暗号方式の適応的暗号文選択攻撃に対する安全性のレベルを比較すると、いずれも強秘匿であることが証明されているが、Cramer-Shoup暗号が、他の2つの方式(ランダム・オラクルモデル)と比較して緩い仮定(汎用一方向性ハッシュ関数)の下で証明されていることから、Cramer-Shoup暗号が比較的高い安全性を有していると考えられる。

デジタル署名専用の方式

これまで提案されているデジタル署名専用の方式の中で、証明付きの安全性と実用性を兼ね備えた主要な方式として、PSS署名、改良ElGamal署名、TSH-ESIGNが挙げられる。各方式の適応的選択文書攻撃に対する安全性を比較すると、以下の表7の通り。

いずれの方式も、適応的選択文書攻撃に対して最も高いレベルの安全性を有している。しかし、どの方式も証明の仮定としてランダム・オラクルモデルが必要となっており、実用化の際にランダム関数をハッシュ関数で置き換える場合には、この仮定が満足されなくなり、安全性の証明は成立しなくなる。なお、ランダム・オラクルモデルを仮定した場合、3つの方式の中でも、離散対数問題の困難性を前提としている改良ElGamal署名の安全性が比較的高いと考えられる。

表7 各デジタル署名専用方式の適応的選択文書攻撃に対する安全性

	証明されている 安全性	安全性の証明に必要な前提	利用されている 数学の問題
PSS署名	存在的偽造不可能	・ランダム・オラクルモデル ・RSA暗号関数の一方性	素因数分解問題
改良ElGamal署名	存在的偽造不可能	・ランダム・オラクルモデル ・離散対数問題の困難性	離散対数問題
TSH-ESIGN	存在的偽造不可能	・ランダム・オラクルモデル ・e乗根近似問題の困難性	素因数分解問題

3. 主要な数学問題の解法に関する研究

各公開鍵暗号方式の安全性の証明可能性に関する評価に加え、その安全性が依拠している数学の問題がどの程度困難であるかを評価する必要がある。これまで様々な数学の問題の解法に関する研究が進められているが、最も研究が進んでおり、多くの実用的な暗号方式に利用されているものが、素因数分解問題と有限体上の乗法群における離散対数問題である。また、最近では、楕円曲線によって定義された離散対数問題を利用した暗号方式がいくつか提案されており、楕円曲線によって定義された離散対数問題の解法に関する研究も盛んに行われている。以下では、上記3つの数学の問題に対する解法について説明する。

(1) 主な素因数分解問題の解法

これまでに提案されてきた素因数分解に有効なアルゴリズムの多くは、「まず適当な整数 z を求め、 n と z の最大公約数 $p = \text{GCD}(n, z)$ を計算することによって n の約数 p を求める」という手法が基本となっている。これは、2つの整数 m と n の最大公約数を計算する極めて効率的なアルゴリズム(Euclidの互除法¹⁷)が存在するためである。したがって、問題は「どのようにして初期値 z を効率的に求めるか」であり、これまでに様々な手法が提案されている。これらの手法は、計算量が素因数 p の性質によって決定する「素因数依存型」と、合成数 n の大きさのみによって決定する「合成数依存型」に大別される。

素因数依存型アルゴリズムとしては、「モンテカルロ法」(Pollard [1975])、 $p-1$ が小さな素数の積になっている場合に有効な「 $p-1$ 法」(Pollard [1974])、 $p+1$ が小さな素数の積になっている場合に有効な「 $p+1$ 法」(Guy [1975])、 $p-q$ が小さい場合に有効な「Fermat法」(Brillhart [1981])、楕円曲線を利用する「楕円曲線法」(Lenstra [1987] 考案、Montgomery [1987] 改良)等が挙げられる。

一方、合成数依存型の主要なアルゴリズムは、2次合同式 $s^2 = t^2 \pmod{n}$ を満たす s と t を求め、 $z = s \pm t$ において最大公約数 $\text{GCD}(n, z)$ を計算して素因数を見つけるという手法である。具体的なアルゴリズムとしては、「連分数法」(Morrison and Brillhart [1975])、「2次ふるい法」(Pomerance [1985] 考案、Silverman [1987] 改良)そして、現時点で最高速の素因数分解アルゴリズムである「数体ふるい法」(Lenstra et al. [1990])が挙げられる。

なお、以下では、計算量の評価の際には一般的に次の記法が用いられる。

$L_p [a, b] = \exp((b+o(1))(\log p)^a (\log \log p)^{1-a})$ (ただし、 p のときに、 $o(1) \rightarrow 0$)
 $L_p [a, b]$ の値が小さいほど計算量が少ないことを意味する。

$p-1$ 法と $p+1$ 法

まず、 $p-1$ 法は、Pollard [1974]によって提案された解法であり、その計算量は、合成数 n の素因数 p に対して $p-1$ の最大素因数のサイズに依存する。このため、 $p-1$ が小さな素数の積になっている場合、すなわち、「ある整数 M に対し、 $p-1 = \prod p_i^{e_i}$ ($p_i \leq M$)と表される場合」(このような $p-1$ は、 M -smoothと呼ばれる)に $p-1$ 法が有効となる。 $p-1$ 法による素因数分解の考え方は以下の通り。

17 Euclidの互除法：2つの整数の最大公約数を求めるアルゴリズムのひとつ。たとえば、210と18の最大公約数を求める場合、次のような手順となる。210を18で割って余り12を得る、18を12で割って余り6を得る、12を6で割ると余りは0となる、割り切れたときの割る数6が最大公約数となる。このように、最初に2つの数のうち大きい方の数を小さい方の数で割り、もし余りが0でなければ割る数を余りで割る。この計算を余りが0となるまで繰り返し、余りが0となったときの割る数が求める最大公約数となる。この手順を用いれば、計算の対象となる数が大きくなっても、効率的に最大公約数が計算できることが知られている。

< p-1法 >

pをnの素因数とする。このとき、nと互いに素な自然数aが存在して、

$$\text{GCD}(a, n) = 1 \text{ ならば、 } \text{GCD}(a, p) = 1$$

となる。したがって、Fermatの小定理¹⁸から、

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

となり、p-1の倍数 Kに対して、 $a^K = 1 \pmod{p}$ が成立する。素因数pは $a^K - 1$ とnの最大公約数 $\text{GCD}(a^K - 1, n)$ を計算することによって求めることができるため、試行錯誤によってp-1の倍数となるようなKを探し当てる必要がある。試行錯誤によってp-1の倍数となるようなKを探し当てる必要がある。

ただし、Kを効率的に見つけることができるのは、p-1の最大素因数が比較的小さな自然数 M以下の場合に限定される。このとき、必要となる計算量はMのサイズに依存する。

一方、nの素因数 pに関して、p+1が比較的小さな素数の積で表される場合には、p-1法を若干変形したp+1法と呼ばれる方法によって効率的に素因数分解を実行することができる。その際の必要な計算量はp+1の最大素因数のサイズに依存することが示されており、p-1およびp+1がM-smoothの場合には、 $O(M(\log n)/(\log M))$ となる (Guy [1975])

Fermat法

基本的なFermat法は、Fermatによって提案されているが、この手法が $|p-q|$ が小さい場合に非常に有効であることを評価したのは、Brillhart [1981] である。このFermat法による解法を避けるためには、素数 pとqを $|p-q|$ が大きくなるように選ぶことが必要となる。Fermat法による素因数分解の考え方は以下の通り。

< Fermat法 >

$n = pq, p < q$ の場合、 $x = (q+p)/2, y = (q-p)/2$ とおくと、 $x^2 - y^2 = n$ となる。そこで、 $(x, y) = (K, 0)$ (K は $n^{1/2}$ 以下で最大の整数)を初期値として、 (x, y) を少しずつ変化させ、 $r = x^2 - y^2 - n$ が0となるような (x, y) を見つける。この (x, y) を利用して連立方程式を解くことによって、 (p, q) を求めることができる。

18 Fermatの小定理は、「素数pと、0でない任意の整数m($< p$)に対して、 $m^{p-1} \pmod{p} = 1$ が成立する」という定理である。

なお、 $(x+1)^2 = x^2 + 2x + 1$ なので、 $A = 2x+1$ 、 $B = 2y+1$ とおけば、 $x = r-A$ となり、 $y = y+1 = r-B$ となる。このように、加減法だけで計算できるのが本手法の長所である。Fermat法が適用できる場合、その処理量は $0.5 \exp(\log(n+1)) - \exp(0.5 \log n)$ と評価されている。

2次ふるい法

2次ふるい法 (quadratic sieve method) は、2次合同式 $k^2 = l^2 \pmod n$ を満たす k と l ($k \equiv \pm l \pmod n$) を求める解法であり、Pomerance [1985] によって考案された。2次ふるい法による素因数分解の考え方は以下の通り。

<2次ふるい法>

2次合同式 $k^2 = l^2 \pmod n$ の k と l を探するために、次の関数を導入する。

$$Q(x) = (x+m)^2 - n \quad (\text{ただし、} m \text{ は } n^{1/2} \text{ 以下の最大の整数})$$

$Q(x)$ に $x = 0, \pm 1, \pm 2, \dots$ を代入し、 $Q(x)$ を素因数分解する。 $Q(x)$ は比較的小さな値となるので、小さな素因数を持つ可能性が高い。そこで、小さな素因数 p_j のみを持つ $Q(x)$ 、言い換えると、すべての素因数が比較的小さな自然数 v 以下となるような $Q(x)$ をたくさん集める (このような $Q(x)$ は、 v -smooth と呼ばれる)。このとき、 $Q(x)$ は、

$$Q(x) = p_1^{d_1} \dots p_r^{d_r} \pmod n$$

と表される (ただし、 p_1, \dots, p_r は v 以下の素因数)。

次に、 $Q(x)$ の集合の中から、次式を満たすような部分集合 S を探し出す (ただし a_j ($j=1, \dots, r$) は偶数)。

$$\prod_{Q(x) \in S} Q(x) = \prod_S p_j^{a_j} \pmod n$$

このような部分集合 S が見つければ、

$$k = \prod_S (x+m) \pmod n, \quad l = \prod_S p_j^{(a_j/2)} \pmod n$$

とおくことにより、 $k^2 = l^2 \pmod n$ が成立する。 $\text{GCD}(k+l, n)$ 、または $\text{GCD}(k-l, n)$ が n の素因数であれば、アルゴリズムは終了する。そうでなければ、別の部分集合 S を見つけて同じ手順を繰り返す。

このアルゴリズムの漸近的な平均計算量は、 $L_n[1/2, 1.020]$ と準指数関数時間の計算量で評価されている。

楕円曲線法

楕円曲線法は、 $p-1$ 法において利用されている法 p の乗法群を、有限体 F_p 上で定義された楕円曲線の点によって構成される有限可換群 $E(F_p)$ で置き換えるとともに、整数 a を $E(F_p)$ 上の点で置き換えた解法であり、Lenstra [1987] によって考案された。楕円曲線法による素因数分解の考え方は以下の通り。

<楕円曲線法>

素因数分解の対象となる合成数を n として、楕円曲線 $E_n : y^2 = x^3 + ax + b \pmod{n}$ を選び、 E_n 上の点 $M = (x, y)$ を適当に選ぶ。

次に、 $p-1$ 法と同様に、小さい素数の積からなる合成数 k を生成し、楕円曲線 E_n 上で定義された加法によって、 kM を計算する（点 M を k 回加える）。ここで、 n の未知な素因数のひとつを p とすると、法 p による特殊な写像により、 E_n 上の点は、有限体 F_p 上での楕円曲線 $E(F_p) : y^2 = x^3 + a'x + b' \pmod{p}$ に移される。この $E(F_p)$ の要素の個数が k の約数となっていたとすると（つまり、 $E(F_p)$ の要素の個数が小さな素数の合成数であったと仮定する）。このとき、 $E(F_p)$ 上において $kM = O \pmod{p}$ （ O は無限遠点）が成立し、 E_n 上における kM の x 、 y 座標の分母の値と n は互いに素ではなくなり、1よりも大きな公約数を有する。

したがって、 $E(F_p)$ の要素の個数が k の約数となっていたとすれば、 E_n 上の点 kM を $(c_1 / d_1, c_2 / d_2)$ とすると、 $\text{GCD}(d_1, n)$ と $\text{GCD}(d_2, n)$ を計算することによって n の素因数を見つけることができる。そこで、有限体 F_p 上での楕円曲線 $E(F_p)$ における要素の個数が小さな素数の積となるように試行錯誤を行い、さらに適当な k を見つけることができれば、 n の素因数分解が可能となる。

前述の $p-1$ 法では、合成数 n の素因数 p に対して、 $p-1$ が小さな素因数のみによって構成される場合に有効となるのに対し、楕円曲線法では、こうした素因数 p に関する制約が存在しない。さらに、利用する楕円曲線 E を適宜変えることによって楕円曲線の要素の個数を変えることが可能であり、要素の個数が小さな素数の積となるような楕円曲線を比較的早く探し当てることのできる点が特徴である。

楕円曲線法の計算量は最大素因数 p のサイズに依存しており、 $L_p[1/2, 1.414]$ となる。したがって、最大素因数 p のサイズが小さければ高速な計算が可能となる。なお、 $n = pq$ の形の合成数 n において p と q が同一のサイズとなっている場合には、必要な計算量は $L_n[1/2, 1.020]$ となる。

数体ふるい法

数体ふるい法は、2次ふるい法概念を代数的整数上で実現した解法である。数体ふるい法は、素因数分解の対象となる合成数を2種類の異なる代数体上で表現し、その表現の相違を利用して、 $k^2 = l^2 \pmod{n}$ を満たす k と $l(k \not\equiv l \pmod{n})$ を求める方法である。

数体ふるい法による素因数分解の考え方は以下の通り。

<数体ふるい法>

n を合成数、 f を次数 k の既約多項式（多項式の係数は Z_n (n を法とする加法群)の要素)とする。ただし、 f における k 次（最高次）の係数は1とする。 m を $f(m) = 0 \pmod{n}$ を満足する整数とし、 α を $f(\alpha) = 0$ を満足する数とする。さらに、この α を要素とする特殊な集合 O_K (代数体 $K = Q(\alpha)$ の整数環)を用意するとともに、特殊な準同型写像 ϕ を以下のように定義する。

$$\phi : \alpha \rightarrow m \pmod{n}$$

以上の前提の下で、整数のペア (c_j, d_j) を適当に選んで $(c_j + d_j m)$ と $(c_j + d_j \alpha)$ を計算し、それぞれ小さな素因数の積になるような (c_j, d_j) のペアを大量に集める。

$$c_j + d_j m = \prod_{p_i \in F} p_i^{e_i}, \quad c_j + d_j \alpha = \prod_{q_i \in G} q_i^{e_i'} \prod_{r_i \in U} r_i^{e_i''}$$

ただし、 F をある値以下の素数の集合、 G を集合 O_K におけるある値以下の素数の集合、 U を集合 O_K におけるある特殊な基底の集合とする。

集めた (c_j, d_j) のペアを適当に組み合わせて、以下の等式が成り立つようにする。

$$\prod (c_j + d_j m) = \left(\prod_{p_i \in F} p_i^{e_i} \right)^2 \tag{1}$$

$$\prod (c_j + d_j \alpha) = \left(\prod_{q_i \in G} q_i^{e_i'} \prod_{r_i \in U} r_i^{e_i''} \right)^2 \tag{2}$$

ここで、上記の等式(2)を ϕ を用いて変換し、以下の等式を導出する。

$$\prod (c_j + d_j m) = \phi \left(\prod_{q_i \in G} q_i^{e_i'} \prod_{r_i \in U} r_i^{e_i''} \right)^2 \pmod{n} = \left(\prod_{q_i \in G} \phi(q_i)^{e_i'} \prod_{r_i \in U} \phi(r_i)^{e_i''} \right)^2 \pmod{n} \tag{3}$$

等式(1)と(3)より、

$$\left(\prod_{p_i \in F} p_i^{e_i} \right)^2 = \left(\prod_{q_i \in G} \phi(q_i)^{e_i'} \prod_{r_i \in U} \phi(r_i)^{e_i''} \right)^2 \pmod{n} \tag{4}$$

が成立することから、 $y = \prod_{p_i \in F} p_i^{e_i}$ 、 $x = \prod_{q_i \in G} \phi(q_i)^{e_i'} \prod_{r_i \in U} \phi(r_i)^{e_i''}$ とおけば、以下の

合同式が得られる。

$$x^2 = y^2 \pmod{n}$$

このような (x, y) のペアをいくつか集めることによって、 $\text{GCD}(x-y, n)$ を計算して n の素因数を求めることが可能となる。

以上のように、数体ふるい法では、 Z_n と O_K という2つの異なる集合を利用することによって、合成数 n を2通りに分解する点がポイントである。AdlemanとLenstraらによって改良された数体ふるい法による計算量は合成数 n のサイズに依存し、準指数関数時間の計算量 $L_n [1/3, 1.922]$ と評価されている (Adleman [1991], Lenstra et al. [1990])。現時点では、このAdleman-Lenstra版数体ふるい法が最高速の素因数分解アルゴリズムとなっている¹⁹。

主な解法のまとめ

これまでに提案されている主要な素因数分解問題の解法をまとめると、以下の表8の通り。表8は、合成数 N が2つの素数 P と Q の積になっている場合に、どの解法を利用するとどの程度の計算量が必要になるのかを整理したものである。 P と Q が同一のサイズであり、 P と Q に特殊な性質が存在しない場合には、現時点ではAdleman-Lenstra版の数体ふるい法が最高速の解法となっている。

表8 素因数分解問題のタイプと主な解法

合成数 $N(=P \times Q)$ の性質	解法	計算量
$P \pm 1$ もしくは $Q \pm 1$ が小さな素数の積となる場合	$P + 1$ 法、 $P - 1$ 法	$P \pm 1$ もしくは $Q \pm 1$ の最大素因数を M とすると、 $O(M(\log n)/(\log M))$
$ P - Q $ が小さな素数の積となる場合	Fermat法	$0.5 \exp(\log(n+1)) - \exp(0.5 \log n)$
上記のいずれの条件も満足せず、かつ P と Q のサイズが同一の場合	2次ふるい法	$L_n [1/2, 1.020]$
	楕円曲線法	$L_n [1/2, 1.020]$
	Adleman-Lenstra版数体ふるい法	$L_n [1/3, 1.922]$

(注) $L_n [a, b] = \exp((b+o(1))(\log n)^a (\log \log n)^{1-a})$

19 RSA社は、サイズが等しい2つの素数の積となっている合成数の素因数分解にどれだけ短時間で成功するかを競うコンテストを実施しており、1999年2月には、数体ふるい法によって465 bitの合成数の素因数分解が約2か月で成功している (300MHzのパソコンに換算して約60台を使用、計算量は約2000 MIPS年*)。こうしたことから、現時点では、デジタル署名方式に関する国際標準 (ISO/IEC 14888-3 [1998]) や金融機関において利用される情報セキュリティ技術に関するガイドライン (ISO/TR 13569 [1998]) 等において、RSA暗号等素因数分解問題を利用する公開鍵暗号方式には、1024 bit以上の鍵長を利用することが推奨されている。

*MIPS年: 1 MIPSは1秒間に100万回の命令を実行できる計算能力を表しており、2000 MIPS年は、1 MIPSの計算能力を有する計算機によって2000年間かけて実行される計算量を表す。

(2) 有限体上の乗法群における離散対数問題の主な解法

有限体上の乗法群における離散対数問題は、有限体上において対数を計算する問題のことである。実数体上で対数を計算することは大きな数であっても容易であるが、有限体上で対数の計算は数が大きくなるにつれて指数関数的に難しくなることが知られている。素因数分解問題の困難性と理論的に厳密な比較は示されていないものの、最高速の解法における必要計算量によってほぼ同程度の困難度とみられている。

これまでに提案されている離散対数問題の解を求めるアルゴリズムは、(i) 素数 p を法とする乗法群上での離散対数の計算量が、 $p-1$ の最大素因数のサイズに依存するアルゴリズムと (ii) 素数 p を法とする乗法群上での離散対数の計算量が、 p のサイズに依存するアルゴリズムに大別できる。計算量が $p-1$ の最大素因数のサイズに依存する代表的なアルゴリズムとしては、Shanks [1972] や Pohlig and Hellman [1978] のアルゴリズムが挙げられる。これらのアルゴリズムの計算量は、 $p-1$ における最大素因数のサイズの指数関数時間となる。

一方、計算量が p のサイズに依存するアルゴリズムとして、「指数計算法」が提案されている。指数計算法にはこれまで様々な改良法が発表されており、代表的な解法としては、Adleman [1979]、Coppersmith [1984]、ElGamal [1985b]、Coppersmith、Odlyzko and Schroepel [1986] (Gaussの整数法) のアルゴリズムや、数体ふるい法を利用した Gordon [1993] のアルゴリズム、その改良法の Schirokauer [1993] のアルゴリズム、Adleman [1994] の関数体ふるい法等が挙げられる。これらのアルゴリズムの計算量は、 p のサイズに対する準指数関数時間となる。

以下では、離散対数問題の主要な解法として、楕円曲線上で定義された離散対数問題や、DSAにおける q を法とする有限体上での離散対数問題に直接適用できるとともに、有限群の要素の個数が特殊な場合には多項式時間の計算量で解くことができる Pohlig-Hellman のアルゴリズム、有限体における要素の個数に対する準指数関数時間の計算量によって解くことができる指数計算法の一般的なアルゴリズムとその改良アルゴリズムについて説明する。

Pohlig-Hellmanのアルゴリズム

Pohlig and Hellman [1978] のアルゴリズムは、素数 p を法とする乗法群に対して、要素の個数 $p-1$ における最大素因数のサイズに対する指数関数時間の計算量を要する。Pohlig-Hellman のアルゴリズムが最も有効となるのは、 $p-1$ の最大素因数がある一定の値 (p のサイズ) 以下となる場合である。このときの計算量は、多項式時間の計算量 $O((\log p)^2)$ となることが示されている。

Pohlig-Hellman のアルゴリズムの考え方は以下の通り。

< Pohlig-Hellmanのアルゴリズム >

p を法とする乗法群 G の原始根を g 、 $g^x \bmod p = a$ とし、所与の a 、 g 、 p の下で離散対数 x を求めるケースを考える。このとき、乗法群 G における要素の個数は $p-1$ となる。ただし、 $p-1$ は、以下のような合成数となっていることがわかっている。

$$p-1 = \prod_{i=1}^k q_i^{e_i} (q_1 < \dots < q_k \text{ log } p)$$

離散対数 x に対して $x \bmod q_i^{e_i} (1 \leq i \leq k)$ をすべて求めることができれば、中国人剰余定理²⁰によって、以下のように x を求めることができる。

$$x \bmod \prod_{i=1}^k q_i^{e_i} = x \bmod p-1 = x \quad (x < p-1)$$

そこで、以下の等式を満たす $b_{i,j} (1 \leq i \leq k, 0 \leq j \leq e_i-1)$ を求める。

$$x \bmod q_i^{e_i} = \prod_{j=1}^{e_i-1} b_{i,j} q_i^j \quad (0 \leq b_{i,j} \leq q_i-1)$$

$b_{i,j}$ は、以下のような手順によって見つけることができる。

(ステップ1) $a^{(p-1)/q_i}$ と $\gamma = g^{(p-1)/q_i} \bmod p$ を計算する。

(ステップ2) $\gamma^i = a^{(p-1)/q_i} \pmod{p}$ を満足する i を、 $i = 0, 1, \dots$ と次々に試して見つける。 i が見つかったら、 $b_{i,0} = i$ とする。

(ステップ3) $a_1 = a g^{-b_{i,0}}$ として、 $\gamma^i = a_1^{(p-1)/q_i^2} \pmod{p}$ となる i を探し、 $b_{i,1} = i$ とする。

(ステップ4) $a_2 = a_1 g^{-q b_{i,1}}$ として、 $\gamma^i = a_2^{(p-1)/q_i^3} \pmod{p}$ となる i を探し、 $b_{i,2} = i$ とする。

以上の手順を b_{k,e_k-1} まで実行し、 $b_{i,j}$ を利用して $x \bmod q_i^{e_i} (1 \leq i \leq k)$ を求め、

$x \bmod \prod_{i=1}^k q_i^{e_i}$ から x を求める。

指数計算法

(i) 指数計算法の一般的アルゴリズム

指数計算法の一般的アルゴリズムは、最初に有限体 F_p 上での対数表を作成し、その表を利用して離散対数を計算するという方法である。

指数計算法の一般的アルゴリズムの考え方は以下の通り。

20 中国人剰余定理は、「 m_1, m_2, \dots, m_k が互いに素であるとし、 $M = m_1 \times \dots \times m_k$ とする。このとき、連立合同式 $X = d_i \pmod{m_i} (i = 1, \dots, k)$ の解 X は、法 M の下で一意に存在する」という定理である。

< 指数計算法の一般的アルゴリズム >

まず、最大の素数が v 以下となる素数の集合 $\{p_1, \dots, p_n \mid 0 < p_i < v\}$ に対し、 g を底とする有限体 F_p 上での対数表を以下の要領で作成する。

$g^{r \bmod p}$ の最大素因数が v 以下となるように、有限体 F_p の要素 r を選ぶ。このとき、 $0 < p_i < v$ を満足する素数 $p_i (i = 1, \dots, n)$ が存在して、以下の等式が成立する。

$$g^{r \bmod p} = p_1^{a_1} \dots p_n^{a_n}$$

上記等式を満足する (a_1, \dots, a_n) を求める。

の等式の両辺について、 g を底とする対数をとる。

$$r \bmod p - 1 = a_1 \log_g p_1 + \dots + a_n \log_g p_n \dots \quad (1)$$

適当に選んだ n 個の r に対して上記 ~ の手順を繰り返すことによって、 n 本の独立な方程式(1)を得ることが可能となり、連立方程式を解いて $(\log_g p_1, \dots, \log_g p_n)$ を得る。これらを記録して対数表を作成する。

$y = g^x \bmod p$ の離散対数 x を計算する場合を考える。 $yg^t \bmod p$ の最大素因数が v 以下となり、さらに以下の等式が成立するような $t \in F_p$ を選ぶ。

$$yg^t \bmod p = p_1^{b_1} \dots p_n^{b_n} \quad (2)$$

両辺の対数を計算して次式を得る。

$$x = \log_g y = (b_1 \log_g p_1 + \dots + b_n \log_g p_n) - t$$

上記の式を基に、対数表の値 $(\log_g p_1, \dots, \log_g p_n)$ を利用することで、離散対数 x を求めることができる $(b_i (i = 1, \dots, n))$ は、(2)式の計算過程で既知。

後述するように、この一般的アルゴリズムに様々な改良を加えることによって、準指数関数時間の計算量による解法がいくつか提案されている。

(ii) 数体ふるい法と関数体ふるい法

指数計算法の一般的アルゴリズムに対して、Gordon [1993] は、素因数分解のために開発された数体ふるい法の概念を応用し、従来の手法よりも高速である準指数関数時間の計算量のアルゴリズムを2種類提案した。ひとつは一般数体ふるい法に基づくものであり、もうひとつは特殊数体ふるい法に基づくものである。「一般」と「特殊」については、アルゴリズム自体はほとんど同じであるが、適用可能な乗法群 Z_p における要素の個数 p の性質に差異が存在する。「一般」の場合は、すべてのタイプの p に対して適用可能である一方、「特殊」の場合は、以下のような性質を有する p に対してのみ適用可能である。

(3) 楕円曲線によって定義された離散対数問題の主な解法

楕円曲線によって定義された離散対数問題には、通常の有限体上の離散対数問題における準指数関数時間の計算量となる高速解法（指数計算法）が適用できないと考えられている。しかし、楕円曲線の中でも (i) MOV帰着やFR帰着によって、拡大次数が小さい拡大体への埋め込みが可能となる楕円曲線（たとえば、トレース0および2の楕円曲線）や、(ii)トレース1のAnomalous曲線については、それぞれ準指数関数時間および多項式時間での解法が適用できることが示されている。このように、楕円曲線の種類によって利用可能な解法が異なってくる。トレース0の楕円曲線は超特異楕円曲線と呼ばれている。超特異楕円曲線やAnomalous曲線については以下の通り。

【超特異楕円曲線】

有限素体 F_p の楕円曲線 $E(F_p)$ において、楕円曲線上の点 (x,y) 座標の値がいずれも F_p の要素となる点の個数を X とする。このとき、 $X = p + 1$ となる（トレースが0となる）楕円曲線 $E(F_p)$ が、超特異楕円曲線と呼ばれている。

【Anomalous曲線】

有限素体 F_p の楕円曲線 $E(F_p)$ において、楕円曲線上の点 (x,y) 座標の値がいずれも F_p の要素となる点の個数を X とする。このとき、 $X = p$ となる（トレースが1となる）楕円曲線 $E(F_p)$ が、Anomalous曲線と呼ばれている。

拡大次数が小さい拡大体への埋め込みが可能な楕円曲線

楕円曲線のなす有限可換群 $E(F_p)$ は、Menezes、Okamoto and Vanstone [1991] によって提案された「MOV帰着（MOV-reduction）」、Frey and Rück [1994] によって提案された「FR帰着（FR-reduction）」、内山・齋藤 [1998] によって提案されたFR帰着の改良アルゴリズム「USアルゴリズム」と呼ばれる手法により、多項式時間の計算量によって拡大体 F_{p^k} に埋め込むことが可能となる。しかし、 F_{p^k} の拡大次数 k が大きき場合には、数体ふるい法や関数体ふるい法等、有限体上の離散対数問題の高速解法を利用しても現実的な時間内に解を求めることは不可能となる。これらの手法が有効となるのは、拡大次数が小さい場合（ $k < \log p$ が必要十分条件とされている（内山・齋藤 [1998]））に限定される。このような条件を満足する楕円曲線としては、これまでトレース0の超特異楕円曲線やトレース2の楕円曲線が知られている。

もっとも、要素の個数が素数となるような任意の楕円曲線に対してこれらの手法が有効となる確率は、 $O((\log p)^9 (\log \log p)^2 / p)$ 以下となり、非常に小さいことが示されている（Balasubramanian and Koblitiz [1998]）。

(i) 超特異楕円曲線

超特異楕円曲線 $E(F_p)$ に対しては、MOV帰着あるいはFR帰着（USアルゴリズム）を利用することで、多項式時間によって、 k が高々6程度となる拡大体 F_p^k に埋め込むことが可能となることが知られている（Menezes, Okamoto and Vanstone [1991]）。このため、有限体上の離散対数問題に適用可能な解法によって、準指数関数時間の計算量で解を求めることができる。

(ii) トレース 2 の楕円曲線

トレース 2 の楕円曲線（要素の個数が $p-1$ ） $E(F_p)$ によって定義された離散対数問題に対しては、FR帰着（USアルゴリズム）が有効となる（内山・齋藤 [1998]）。このタイプの楕円曲線にFR帰着（USアルゴリズム）を適用することで、楕円曲線上の離散対数問題を確率的多項式時間によって F_p （拡大次数 k が1）に帰着させることが可能となり、準指数関数時間の計算量の解法が適用可能となることが示されている。一方、MOV帰着を適用した場合には、拡大次数 k が大きくなるため、準指数関数時間の計算量の解法が適用できなくなる。

Anomalous曲線

Anomalous曲線によって定義された離散対数問題は、フェルマー商と呼ばれる関数を利用することによって、楕円曲線上の有限可換群 $E(F_p)$ を同じ要素の個数をもつ加法群に埋め込むことにより、多項式時間の計算量（ $(\log p)^3$ に比例する計算量）で解を求めることが可能となる。この解法は、Smart [1997]、Semaev [1998]、Satoh and Araki [1998] によって発表されたことから、「SSSAアルゴリズム」と呼ばれている。

ただし、任意に選んだ楕円曲線がAnomalous曲線となる確率は非常に小さいとみられており、十分大きな素数 p の下での確率は $O((\log p)(\log \log p) / p)$ 程度と見積もられている（McKee [1997]）。また、ランダムに選んだ楕円曲線がAnomalous曲線であるかどうかは容易に検査できるので、Anomalous曲線が実際に用いられてしまうことを完全に排除することが可能である。

主な解法のまとめ

以上の解法をまとめると、以下の表10の通り。上記、以外の楕円曲線によって定義された離散対数問題を解くためには、現時点では、指数関数時間の計算量が必要になるとみられている。最高速の解法であるPohlig-Hellmanのアルゴリズムにおける計算量は $\exp(0.5 \log p)$ 程度と見積もられている。

表10 各楕円曲線に基づく離散対数問題のタイプと主な解法

楕円曲線のタイプ	適用可能な解法	必要計算量	ランダムに楕円曲線を選んだ場合に各曲線が生成される確率
拡大次数が小さい拡大体への埋め込みが可能な楕円曲線	MOV帰着、FR帰着(USアルゴリズム)	準指数関数時間	$O((\log p)^9(\log \log p)^2/p)$
超特異楕円曲線(トレース0)	MOV帰着、FR帰着(USアルゴリズム)		
トレース2の楕円曲線	FR帰着(USアルゴリズム)		
Anomalous曲線(トレース1)	SSSAアルゴリズム	多項式時間	$O((\log p)(\log \log p)/p)$
上記以外の楕円曲線	Pohlig-Hellmanのアルゴリズム	指数関数時間	

(4) 各数学問題の必要計算量の比較

上記3種類の数学の問題を解くために必要な計算量を試算・比較する。比較対象とする各数学問題の解法には、現時点で最高速といわれている解法を適用する。素因数分解問題にはAdleman-Lenstra版の数体ふるい法、有限体上の乗法群における離散対数問題にはSchirokauer版数体ふるい法(あるいはAdlemanの関数体ふるい法)、楕円曲線によって定義された離散対数問題にはPohlig-Hellmanのアルゴリズムを利用する。各アルゴリズムの必要計算量は、以下の表11の通り。

表11 各数学の問題における高速解法と必要計算量

	高速解法	必要計算量
素因数分解問題	Adleman-Lenstra版数体ふるい法	$L_n[1/3, 1.922]$
有限体上の乗法群における離散対数問題	Schirokauer版数体ふるい法(Adlemanの関数体ふるい法)	$L_p[1/3, 1.922]$
楕円曲線によって定義された離散対数問題	Pohlig-Hellmanのアルゴリズム	$\exp(0.5(\log p))$

(注) $L_n[a, b] = \exp((b+o(1))(\log n)^a(\log \log n)^{1-a})$ 、 $L_p[a, b] = \exp((b+o(1))(\log p)^a(\log \log p)^{1-a})$

素因数分解問題の困難性と離散対数問題の困難性との関係は、理論的に厳密な研究成果は現時点では示されていないものの、必要計算量で比較するとほぼ同程度とみられている。

問題のサイズによってこれらの計算量を比較すると、以下の表12の通り。問題のサイズには、素因数分解問題であれば素数pのサイズ、離散対数問題であれば法pのサイズ、楕円曲線によって定義された離散対数問題であれば有限体における要素の個数pのサイズが対応する。

表12 問題のサイズと解を求めるために必要な計算量の関係

問題の サイズ(bit)	必要計算量		
	素因数分解問題	離散対数問題	楕円曲線によって定義された離散対数問題
160			2^{80}
174			2^{87}
200			2^{100}
234			2^{117}
240			2^{120}
280			2^{140}
512	1.86×2^{63}		2^{256}
768	1.39×2^{76}		2^{384}
1024	1.65×2^{86}		2^{512}
1536	1.25×2^{103}		2^{768}
2048	1.77×2^{116}		2^{1024}

このように、素因数分解問題および離散対数問題における問題のサイズが1024 bit、2048 bitの場合の必要計算量は、それぞれ楕円曲線によって定義された離散対数問題における問題のサイズの174 bit、234 bitの必要計算量とほぼ同等となるとみられる。

V. おわりに

従来から、公開鍵暗号方式における安全性の証明に関する研究が盛んに行われ、安全性が証明可能な様々な暗号方式が提案されてきたが、いずれの方式も計算量が多い等の理由から実用化には至らなかった。これに対し、最近では、安全性と実用性を両立させる暗号方式が提案され、OAEP等一部の方式は既に実用化されている。こうした公開鍵暗号における安全性証明に関する研究は、公開鍵暗号に対する一層の信頼性向上に繋がるほか、オープンなネットワークにおける情報セキュリティの向上に資するものである。今後とも、公開鍵暗号の研究動向を注視する必要がある。

また、最近の公開鍵暗号における理論研究により、暗号システムのセキュリティを確保するためには、利用されている暗号方式単体の安全性を確保するだけでは不十分であるとの認識が一層強まっている。Bleichenbacherによって発表されたPKCS#1 Version 1に対する攻撃法は、利用されているRSA暗号を直接攻撃するものではなく、攻撃者が送信したデータに対する攻撃対象者の返信データから、対応する平文の情報を入手するというものである。したがって、Bleichenbacherの攻撃を防ぐためには、少なくとも、攻撃者が送信したデータに対して不用意に平文に関する情報を返信しないような実装が必要となる。このように、情報セキュリティ技術を「総合技術」として位置付け、実装方法を含めて「どのようなセキュリティ技術を採用するか」を検討することが重要である。今後も、PKCS#1の安全性に関する研究のように、実際に利用されている具体的な実装方法の安全性に関する研究についても注視していく必要がある。

参考文献

- 池野信一・小山謙二、『現代暗号理論』、電子情報通信学会、1986年
- 岩下直行・谷田部充子、「金融分野における情報セキュリティ技術の国際標準化動向」、『金融研究』第18巻第2号、日本銀行金融研究所、1999年4月
- 内山成憲・齋藤泰一、「トレース2の楕円曲線上の離散対数問題について」、『電子情報通信学会技術報告ISEC98-27』、pp. 51-57、1998年
- 宇根正志、「公開鍵暗号方式EPOCについて」、『日本銀行金融研究所ディスカッションペーパーシリーズ』、No. 97-J-19、1998年7月
- 岡本龍明・太田和夫（編著）、『暗号・ゼロ知識証明・数論』、共立出版、1995年
- ・藤岡 淳・岩田雅彦、「高速デジタル署名方式ESIGN」、『NTT R&D』、Vol. 40、No. 5、1991年
- 岡本龍明・山本博資、『現代暗号』、産業図書、1997年
- 勝野裕文、「RSA暗号解読への一対策」、『電子情報通信学会論文誌(D)』、Vol. J66-D、No. 8、pp. 963-969、1983年
- 楠田浩二・櫻井幸一、「公開鍵暗号方式の安全性評価に関する現状と課題」、『日本銀行金融研究所ディスカッションペーパーシリーズ』、No. 97-J-11、1997年7月
- 黒澤 馨・伊東利哉・竹内正士、「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』、Vol. J70-A、No. 11、pp. 1632-1636、1987年
- 小山謙二・桑門秀典・鶴岡行雄、「3次曲線に基づく公開鍵暗号」、『NTT R&D』、Vol. 44、No. 10、1995年
- 辻井重男・笠原正雄（編著）、『暗号と情報セキュリティ』、昭晃堂、1990年
- 松本 勉・岩下直行、「金融分野における情報セキュリティ技術の現状と課題」、『金融研究』第18巻第2号、日本銀行金融研究所、1999年4月
- 宮地充子、「ElGamal型楕円曲線暗号の設計と標準化及び実装化動向」、『1997年暗号と情報セキュリティシンポジウム予稿集SCIS'97-7B』、1997年
- L. M. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography" Proceedings of FOCS, pp. 55-60, 1979.
- ・, "Factoring Numbers Using Singular Integers," Proceedings of ACM Annual Symposium on Theory of Computing, pp. 64-71, Springer-Verlag, 1991.
- ・, "The function field sieve," Algorithmic Number Theory, Lecture Notes in Computer Science, Vol. 877, pp. 108-121, Springer-Verlag, 1994.
- American National Standards Institute, "X9.30 Part 1: Public Key Cryptography Using Irreversible Algorithm (DSA)" 1997.
- ・, "Working Draft: X9.31 Digital Signatures Using Reversible Public Key Cryptography For The Financial Service Industry (rDSA)," 1998.
- ・, "Working Draft: X9.62 Public Key Cryptography For The Financial Service Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)," 1998.

- K. Araki, T. Satoh and S. Miura, "Extended Abstract of Overview of Elliptic Curve Cryptography," Proceedings of 1998 International Workshop on Practice and Theory in Public Key Cryptography, 1998.
- R. Balasubramanian and N. Koblitz, "The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm," Journal of Cryptology, Vol. 11, No. 2, pp.141-145, 1998.
- M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations Among Notions of Security for Public-Key Encryption Schemes," Advances in Cryptology Proceedings of CRYPTO '98, Lecture Notes in Computer Science, Vol. 1462, pp. 26-35, Springer-Verlag, 1998.
- and S. Goldwasser, "New paradigms for digital signatures and message authentication based on non-interactive zero knowledge proofs," Advances in Cryptology Proceedings of CRYPTO '89, Lecture Notes in Computer Science, Vol. 435, pp.194-211, Springer-Verlag, 1990.
- and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," Proceedings of the First Annual Conference on Computer and Communications Security, ACM, 1993.
- and , "Optimal asymmetric encryption," Advances in Cryptology Proceedings of EUROCRYPT '94, Lecture Notes in Computer Science, Vol. 950, pp. 92-111, Springer-Verlag, 1995.
- and , "The Exact Security of Digital Signatures How to Sign with RSA and Rabin," Advances in Cryptology Proceedings of EUROCRYPT '96, Lecture Notes in Computer Science, Vol. 1070, pp. 399-416, Springer-Verlag, 1996.
- D. Bleichenbacher, "Generating ElGamal signatures without knowing the secret key," Advances in Cryptology Proceedings of EUROCRYPT '96, Lecture Notes in Computer Science, Vol. 1070, pp. 10-18, Springer-Verlag, 1996.
- , "Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1," Advances in Cryptology Proceedings of CRYPTO '98, Lecture Notes in Computer Science, Vol. 1462, pp. 1-12, Springer-Verlag, 1998.
- D. Boneh and R. Venkatesan, "Breaking RSA May Not Be Equivalent to Factoring," Advances in Cryptology Proceedings of EUROCRYPT '98, Lecture Notes in Computer Science, Vol. 1403, pp. 59-71, Springer-Verlag, 1998.
- E. F. Brickell and J. DeLaurentis, "An attack on a signature scheme proposed by Okamoto and Shiraishi," Advances in Cryptology Proceedings of CRYPTO '85, Lecture Notes in Computer Science, Vol. 218, pp. 28-32, Springer-Verlag, 1986.
- J. Brillhart, "Fermat's factoring method and its variants," Congressus Numerantium, Vol. 32, pp.29-48, 1981.
- J. Camenisch, U. Maurer, and M. Stadler, "Digital payment systems with passive anonymity-revoking trustees," Computer Security Proceedings of ESORICS '86, Lecture Notes in Computer Science, Vol. 1146, pp. 33-43, Springer-Verlag, 1996.
- R. Canetti, O. Goldreich, and S. Halevi, "The Random Oracle Methodology, Revisited (preliminary version)," March 31, 1998. (<http://theory.lcs.mit.edu/~cis/rom/rom.html>)

- D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology* Proceedings of CRYPTO '82, pp. 199-203, Plenum Press, 1983.
- D. Coppersmith, "Fast evaluation of logarithms in fields of characteristic two," *IEEE Transactions on Information Theory*, Vol. IT-30, pp. 587-594, 1984.
- , A.M. Odlyzko, and R. Schroepfel, "Discrete logarithms in GF (p)," *Algorithmica*, Vol. 1, pp. 1-15, 1986.
- , M. Franklin, J. Patarin, and M. Reiter, "Low-exponent RSA with related messages," *Advances in Cryptology* Proceedings of EUROCRYPT '96, *Lecture Notes in Computer Science*, Vol. 1070, pp. 1-9, 1996.
- R. Cramer and V. Shoup, "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack," *Advances in Cryptology* Proceedings of CRYPTO '98, *Lecture Notes in Computer Science*, Vol. 1462, pp. 13-25, Springer-Verlag, 1998.
- W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, pp. 644-654, November 1976.
- , P. C. van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Designs, Codes and Cryptography*, Vol. 2, pp. 107-125, 1992.
- D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography," *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pp. 542-552, 1991.
- C. Dwork and M. Naor, "An efficient existentially unforgeable signature scheme and its applications," *Advances in Cryptology* Proceedings of CRYPTO '94, *Lecture Notes in Computer Science*, Vol. 839, pp. 234-246, Springer-Verlag, 1994.
- T. E. ElGamal, "A public key cryptosystems and a signature scheme based on discrete logarithm," *Advances in Cryptology* Proceedings of CRYPTO '84, *Lecture Notes in Computer Science*, Vol. 197, pp. 10-18, Springer-Verlag, 1985a.
- , "A subexponential-time algorithm for computing discrete logarithms over GF (p²)," *IEEE Transactions in Information Theory*, Vol. IT-31, pp. 473-481, 1985b.
- G. Frey and H. G. Rück, "A Remark Concerning m-divisibility and The Discrete Logarithm in The Divisor Class Group of Curve," *Math. Comp.*, Vol. 62, No. 206, pp. 865-874, 1994.
- S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, Vol. 28, No. 2, pp. 270-299, 1984.
- , S. Micali, and R. Rivest, "A digital signature scheme against adaptive chosen message attack," *SIAM J. Comp.*, Vol. 17, No. 2, pp. 281-308, 1988.
- D. M. Gordon, "Discrete logarithm field in GF (p) using the Number Field Sieve," *SIAM Journal on Discrete Math.*, Vol. 6, pp. 124-138, 1993.
- R. K. Guy, "How to factor a number," *Proceedings of 5th Manitoba Conference on Numerical Mathematics*, pp. 49-89, 1975.
- International Organization for Standardization, "ISO 11166-2 Banking Key Management by means of asymmetric algorithms Part 2: Approved algorithms using the RSA cryptosystem," 1994.

- , "ISO/TR 13569 Banking and related financial services Information security guidelines," 1998.
- and International Electrotechnical Commission, "ISO/IEC 14888-3 Information technology Security techniques Digital signature with appendix Part 3: Certificate-based mechanism," 1998.
- N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, Vol.48, pp.203-209, 1987.
- , *A Course in Number Theory and Cryptography*, Springer-Verlag, 1997. (N. Koblitz著、櫻井幸一訳、『数論アルゴリズムと楕円暗号理論入門』、シュプリンガー・フェアラーク、1997年)
- A. K. Lenstra, H. W. Jr. Lenstra, M.S. Manasse, and J.M. Pollard, "The number field sieve," *Proceedings of ACM Annual Symposium on Theory of Computing*, pp. 564-572, 1990.
- H. W. Jr. Lenstra, "Factoring Integers with elliptic Curves," *Annals of Mathematics*, Vol. 126, pp. 649-673, 1987.
- J. McKee, "Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field," to appear in *J. London Math. Soc.*, 1997.
- A. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *Proceedings of STOC*, pp. 80-89, 1991.
- , P. C. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
- V. S. Miller, "Use of elliptic curves in cryptography," *Advances in Cryptology Proceedings of CRYPTO '85, Lecture Notes in Computer Science*, Vol. 218, pp. 417-426, Springer-Verlag, 1986.
- P. L. Montgomery, "Speeding the Pollard and elliptic curve methods of factorization," *Math. Comp.*, pp. 243-264, 1987.
- M. A. Morrison and J. Brillhart, "A method of factoring and the factorization of F_7 ," *Mathematics of Computation*, Vol. 29, pp. 183-205, 1975.
- M. Naor and M. Yung, "Universal one-way hash functions and their chosen ciphertext attacks," *Proceedings of STOC*, pp. 33-43, 1989.
- and , "Public-key cryptosystems provably secure against chosen ciphertext attacks," *Proceedings of STOC*, pp. 427-437, 1990.
- National Institute for Standards and Technology, "Specifications for a digital signature standard," *Federal Information Processing Standard Publication 186-1*, 1998.
- T. Okamoto, "A fast signature scheme based on congruential polynomial operations," *IEEE Transactions on Information Theory*, Vol. 36, No. 1, pp. 47-53, 1990.
- , E. Fujisaki, and H. Morita, "TSH-ESIGN: Efficient Digital Signature Scheme Using Trisection Size Hash," *Submission to IEEE P1363a*, November 1998.
- and S. Uchiyama, "A New Public-Key Cryptosystem as Secure as Factoring," *Advances in Cryptology Proceedings of EUROCRYPT '98, Lecture Notes in Computer Science*, Vol. 1403, pp. 308-318, Springer-Verlag, 1998.

- , S. Uchiyama, and E. Fujisaki, "EPOC: Efficient Probabilistic Public-Key Encryption," Submission to IEEE P1363a, November 1998.
- S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over GF (p) and its cryptographic significance," *IEEE Transactions on Information Theory*, Vol. 24, pp. 106-110, 1978.
- D. Pointcheval and J. Stern, "Security proofs for signature schemes," *Advances in Cryptology Proceedings of EUROCRYPT '96, Lecture Notes in Computer Science*, Vol. 1070, pp. 387-398, Springer-Verlag, 1996.
- J. M. Pollard, "Theorems on factorization and primality testing," *Proceedings of Camb. Phil. Soc.*, Vol. 76, pp.521-528, 1974.
- "A Monte Carlo method for factorization," *BIT*, Vol. 15, pp. 331-334, 1975.
- C. Pomerance, "The quadratic sieve algorithm," *Lecture Notes in Computer Science*, Springer-Verlag, Vol. 209, pp.169-182, 1985.
- M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," M.I.T. Laboratory for Computer Science, Technical Report MIT/LCS/TR-212, 1979.
- R. L. Rivest, A. Shamir, and L. Adleman, "A method of obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, pp.120-126, 1978.
- J. Rompel, "One-way functions are sufficient for secure signatures," *Proceedings of STOC*, pp. 387-394, 1990.
- T. Satoh and K. Araki, "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves," *Commentarii Math, Univ. Sancti Pauli*, 1998.
- B. Schneier, *APPLIED CRYPTOGRAPHY*, John Wiley & Sons, Inc., 1993.
- O. Schirokauer, "Discrete Logarithms and Local Units," *Phil. Trans. R. Soc. Lond., A* 345, pp.409-423, 1993.
- , D. Weber, and T. Denny, "Discrete Logarithms: The Effectiveness of the Index Calculus Method," *Algorithmic Number Theory, Lecture Notes in Computer Science*, Vol. 1122, Springer-Verlag, pp. 335-361, 1996.
- C. P. Schnorr, "Efficient signature generation for smart cards," *Advances in Cryptology Proceedings of CRYPTO '89, Lecture Notes in Computer Science*, Vol. 435, pp.239-252, Springer-Verlag, 1990.
- I. A. Semaev, "Evaluation of Discrete Logarithms in a Group of p-torsion Points of an Elliptic Curve in Characteristic p," *Math. Comp.*, Vol. 67, No. 221, pp. 353-356, 1998.
- D. Shanks, "Class number, a theory of factorization, and Genera," *Proceedings of Syposium Pure Mathematics*, AMS, 1972.
- R. D. Silverman, "The multiple polynomial quadratic sieve," *Math. Comp.*, Vol. 48, pp. 243-264, 1987.
- G. J. Simmons, "A 'weak' privacy protocol using the RSA crypto algorithm," *Cryptologia*, Vol.7, No.2, pp.180-182, April 1983.
- N. P. Smart, "The discrete logarithm problem on elliptic curves of trace one," preprint, 1997.

H. C. Williams, "A modification of the RSA public-key encryption procedure," IEEE Transactions on Information theory, Vol. IT-26, pp. 726-729, 1980.

and B.K. Schmid, "Some remarks concerning the MIT public-key cryptosystem," BIT, Vol. 19, pp. 525-538, 1979.

