IMES DISCUSSION PAPER SERIES

公開鍵暗号方式の安全性評価に関する現状と課題

楠田浩二・櫻井幸一

Discussion Paper No. 97-J-11

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒100-91 東京中央郵便局私書箱 203 号

IMES Discussion Paper Series 97-J-11
1997 年 7 月

公開鍵暗号方式の安全性評価に関する現状と課題

楠田浩二*・櫻井幸一**

要　旨

インターネットの爆発的な普及に伴い、電子マネーや電子商取引の実現に対する期待が高まっている。電子マネーや電子商取引は、インターネットのようなオープンなネットワーク上で利用されるため、部外者から情報の機密性を守ることや、取引の真正性を確認することが、従来以上に重要となる。そのための手段として、暗号技術、とりわけ公開鍵暗号技術が注目を集めている。

公開鍵暗号は、従来から利用されてきた共通鍵暗号（DES 暗号等）に比べ、オープンなネットワーク上で利用する場合の利便性が高いと言われている。例えば、事前に鍵を交換しておかなくても秘密通信を行うことができるし、書面における署名・捺印に代わる機能を果たす「ディジタル署名」と呼ばれる機能を実現することもできる。ディジタル署名は、「特定の人しかディジタル署名を作成できないが、誰でもその署名を検証できる」という特徴を持ち、電子マネーや電子商取引を実現する際の鍵となる技術である。

今後、こうした暗号技術を利用していく際には、その安全性について正確な理解を持つことが極めて重要である。これまで暗号研究者の間では、公開鍵暗号の安全性について数多くの研究が蓄積されてきた。しかし、公開鍵暗号の原理が難解なこともあって、暗号を利用する一般の技術者レベルでは、その安全性に関して十分な理解は得られていないように伺われる。

そこで本稿では、代表的な公開鍵暗号の原理を紹介するとともに、その安全性に関するこれまでの研究を概観し、様々な角度から、各方式の安全性を検討・整理した。

キーワード：暗号、安全性評価、公開鍵暗号、情報セキュリティー、ディジタル署名
JEL 分類番号: L86, Z00

*　日本銀行金融研究所研究第２課
**　九州大学大学院システム情報科学研究科(E-mail: sakurai@csce.kyushu-u.ac.jp)

本論文の作成に当たっては、岡本龍明特別研究員（NTT 情報通信研究所）、宮地充子研究員（松下電器産業）、松本勉助教授（横浜国立大学）、岡本栄司教授（北陸先端科学技術大学院大学）から有益なコメントを頂戴した。但し、本論文の内容及び意見は筆者達個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。

目　次

（はじめに）

インターネットの爆発的な普及に伴い、電子マネーや電子商取引の実現に対する期待が高まっている。これまでも銀行は、電子的な決済サービスを提供してきたが、それは銀行内や銀行間のクローズド・ネットワークでの利用を前提とするものであった。しかし、電子マネーや電子商取引は、インターネットのようなオープンなネットワーク上で利用されるため、部外者から情報の機密性を守ることや、取引の真正性を確認することが、従来以上に重要となる。そのための手段として、暗号技術、とりわけ公開鍵暗号技術が注目を集めている。

公開鍵暗号は、特殊な数学演算を行うアルゴリズムを使用し、異なる鍵を用いて暗号化と復号化を行う技術で、暗号化用の鍵（公開鍵）を公開し、復号化用の鍵（秘密鍵）を秘匿して利用される。この結果、「誰でも暗号化ができるが、特定の人にしか復号化ができない」という特徴を持つ暗号が実現できる。

公開鍵暗号は、従来から利用されてきた共通鍵暗号（DES 暗号等）に比べ、オープンなネットワーク上で利用する場合の利便性が高いと言われている。例えば、事前に鍵を交換しておかなくても秘密通信を行うことができるし、書面における署名・捺印に代わる機能を果たす「ディジタル署名」と呼ばれる機能を実現することもできる。ディジタル署名は、「特定の人しかディジタル署名を作成できないが、誰でもその署名を検証できる」という特徴を持ち、電子マネーや電子商取引を実現する際の鍵となる技術である。

今後、こうした暗号技術を利用していく際には、その安全性について正確な理解を持つことが極めて重要である。これまで暗号研究者の間では、公開鍵暗号の安全性について数多くの研究が蓄積されてきた。しかし、公開鍵暗号の原理が難解なこともあって、暗号を利用する一般の技術者レベルでは、その安全性に関して十分な理解は得られていないように伺われる。実際、安全性の面で問題のあることが明らかにされた暗号製品が気付かれないまま利用されている例もあるようである[1]。

そこで本稿では、代表的な公開鍵暗号の原理を紹介するとともに、その安全性に関するこれまでの研究を概観し、様々な角度から、各方式の安全性を検討･整理した。本稿の構成は次の通りである。

まず I で公開鍵暗号の概要、諸機能、強度評価の枠組みについて紹介する。次に II で公開鍵暗号の秘密通信機能、ディジタル署名機能を有する代表的な諸方式の概要、基本的な安全性、利用上の留意事項等について説明する。最後に、III で公開鍵暗号の

[1] 例えば、PGP(Pretty Good Privacy)と呼ばれる暗号通信機能を持つソフトウェアはフリー・ソフトであることもあってインターネット上で相当に普及しているとみられるが、ここで利用されている RSA 暗号の鍵生成プロトコルにおいて簡単に解読される弱い暗号鍵が生成される確率が小さくないことが指摘されている（酒井・石塚・櫻井[1997]）。

安全性の根拠となっている数学の問題の解法を紹介した後、最強の解法を前提に公開鍵暗号の諸方式の現在及び将来の強度を試算する。

I 公開鍵暗号に関する基礎事項

1. 公開鍵暗号の概要

暗号の方式は、暗号化と復号化に共通の鍵が用いられる「共通鍵暗号（common key cryptosystem）」と、暗号化鍵と復号化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な「公開鍵暗号（public key cryptosystem）」に分類できる。公開鍵暗号では、上記性質から何れか一方の鍵を公開することが可能となる。この場合、公開する方の鍵は公開鍵、秘密にしておく方の鍵は秘密鍵と呼ばれる。

公開鍵暗号の概念は 1976 年に米国 Stanford 大学の Diffie and Hellman[1976]によって発表された。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。

・鍵配送の容易さ

共通鍵暗号では、暗号通信の当事者が鍵を共有するため同鍵を秘密裏に入手しなければならない。翻って、公開鍵暗号では、通信相手の公開鍵の正当性を確認する仕組みは必要となるが、秘密裏に入手する必要はなくなるため、この分、鍵配送が容易になる。

・所要鍵数の大幅減少

今、n 人の利用者が互いに暗号通信を行う場合を想定すると、共通鍵暗号では、${}_nC_2$ 種類の鍵が必要となるが、これに対し、公開鍵暗号では、$2n$ 個で済む。こうした特徴を活かして共通鍵暗号の利用に際し公開鍵暗号を利用して鍵を共有する方法がとられる場合が少なくない。

・ディジタル署名の実現

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、共通鍵で作成された文書は同鍵を所有する二人のうち何れが作成したかを特定することができない。一方、公開鍵暗号では、秘密鍵を所有する者が唯一人であるため「（同鍵で作成された）文書は確かに同鍵の所有者が作成したことを確認できる」という意味で証拠性を持ち得る。公開鍵暗号が持つこうした機能は「ディジタル署名」と呼ばれている。

・ 処理速度の低さ

公開鍵暗号は共通鍵暗号に比べ処理に大量の計算を要するため、計算機の能力が等しいとすれば、これは処理速度の低さとなって現われる。実際、共通鍵暗号の処理速度を現時点での最高速の専用 LSI で評価すると数百 Mbps 程度が一般的であるのに対し、大方の公開鍵暗号は高々同数 Mbps 程度となっている。

上記にみられるような各方式の長・短所を反映し、膨大なデータの処理が要求される文書の暗号化には共通鍵暗号が、ディジタル署名や共通鍵暗号に用いられる秘密鍵の配送には公開鍵暗号が利用されるという棲分けがなされているようで

ある。

次に、公開鍵暗号の原理をみてみよう。通信文 M に対して、公開鍵 e を用いた変換を $E(e,M)$とし、秘密鍵 d を用いた変換を $D(d,M)$とすると、公開鍵暗号アルゴリズムは、まず、次の二つの条件を満たす必要がある。

① 公開鍵 e を知っているとき、暗号化 $E(e,M)$の計算は容易。秘密鍵 d を知っているとき復号化 $D(d,M)$の計算は容易。
② 秘密鍵 d を知らなければ、公開鍵 e、変換手順 E、暗号文 $C=E(e,M)$を知っていても、元の平文 M を計算することは「計算量的に困難」[2]。

秘密通信機能を実現するためには、条件①②に加え、次の条件が満たされることが望ましい。

③ 全ての通信文 M に対し、$D(d,E(e,M))=M$ が成立する。

条件①②③に加え、次の条件が成立する場合は、秘密通信機能に加えディジタル署名機能も実現し得る。

④ 全ての通信文 M に対し、$E(e,D(d,M))=M$ が成立する。

ディジタル署名機能のみの方式（ElGamal 署名、ESIGN 署名等）においても、実用性を意味する上記要件①、一方の鍵を公開しても安全性が保たれることを意味する上記要件②と同様の要件は必要となるが、受け手が署名を元の文書に復元する必要はないため上記要件③④は必要とされない。

それでは、次に上記諸条件を満足する関数の構成法について簡単に述べよう。まず、条件①②は「一方向性関数（one way function）」と呼ばれる特殊な関数を利用して実現できる。一方向性関数とは、関数 f の計算は容易であるが逆関数 f^{-1} の計算は困難であるような関数である。但し、一方向性関数自体を暗号化関数とすることはできない。受信者は受け取った暗号文 $C=f(M)$を復号化するための計算 $f^{-1}(C)$ができないからである。そこで、一方向性関数の逆関数に「落し戸（trapdoor）」と呼ばれる同計算を容易にするパラメーターを仕掛けた「落し戸付き一方向性関数（trapdoor one way function）」を構築することが必要となる。この場合、関数 $f(\cdot,e)$

[2] 計算量的に困難とは、理論的には計算可能であるが、実際に計算するのは計算量が莫大であり費用と時間を要し過ぎることから事実上計算不可能なことを指す。

に対応する逆関数 $f^{-1}(\cdot,d)$における d が落し戸となる。パラメーターe からパラメーターd を求めることは計算量的に困難であり、かつこれらのパラメーターを生成することが容易という条件が満たされている場合、公開鍵を e とし秘密鍵を d とすれば公開鍵暗号を実現できるのである。

2. 公開鍵暗号の諸機能

(1)秘密通信

1.で述べた条件①②③を満たす関数は秘密通信機能を持つ。同機能を持つ公開鍵暗号により送信者 A から受信者 B へ平文 M を秘密通信する場合の手順は次の通り。

Step 1： A は B の公開鍵 e_B で平文 M を暗号化し、暗号文 C を B に送る。
Step 2： B は自分の秘密鍵 d_B で C を復号し、元の平文 M を得る。

受信者 B の公開鍵は不特定多数に公開されているため、A に限らず誰もが同じ公開鍵により B への秘密通信が可能となるのである。これがネットワーク全体の鍵を大幅に削減する仕組みであるが、利点ばかりではない。すなわち、共通鍵暗号はデータの守秘に加え、相手確認、データの完全性の機能を併せ持っていたが、これらの機能は鍵が通信当事者である二者の間だけで秘密にされているために実現されているにほかならない。公開鍵暗号の場合、上の例における B の公開鍵を誰もが知っているため、通信路上の B に送信されている暗号文を他人に置き換えられる可能性を否定できないのである。従って、公開鍵暗号の秘密通信方式には相手確認、データの完全性の機能はないものと考えなければならない。加えて、冒頭で述べたように公開鍵暗号は共通鍵暗号に比べ処理速度が格段に劣ることから、多くの場合、通信文書自体の暗号化は共通鍵暗号によって行われており、公開鍵暗号の暗号機能は共通鍵暗号に用いられる秘密鍵の配送等に利用されている。

(2)ディジタル署名

ディジタル署名の具体的方法は「通信文復元法」と「認証子照合法」に大別される。しかし、下記のように、通信文復元法は問題が多いため、現在は一部の用途を除き、認証子照合法が用いられている。

イ．通信文復元法

通信文復元法では、図 1 に示すように、まず送信者が文書に自分の秘密鍵で変換を施し、$D(M)$を受信者に送信する。受信者は送られてきた通信文に

対し送信者の公開鍵で逆変換を施す。復元された文書が「意味のあるもの」ならば、受信者は通信文の送信者及び内容が正当なものであるとみなす。

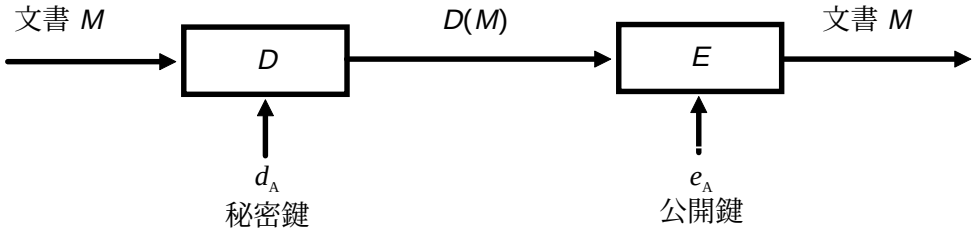

図 1 通信文復元法によるディジタル署名

但し、同方法では、任意のデータ X に対し公開鍵暗号により暗号化を施すと、同データ X は暗号化結果 $E(X)$に対する署名となり、従って存在的偽造が極めて容易に実現可能なほか、上述の「意味のあるもの」かどうかの判定を人間を介さずに、コンピューターにより自動処理することが非常に困難であるといった問題がある。また、RSA 暗号等のように公開鍵暗号が乗法的である、すなわち $E(XY) = E(X)E(Y)$が成立する場合は、同性質を利用した署名偽造法も可能となる（詳細は II 1.(1)にて説明）。

ロ．認証子照合法

認証子照合法は、次に示す手順で行われる（次頁図 2 参照）。

Step 1： 署名作成者 A は文書 M を「ハッシュ関数」と呼ばれる特殊な関数 h により一定長に圧縮、これをディジタル署名方式により自分の秘密鍵 d_Aで変換し、署名 S を生成する。

Step 2： A は署名付き文書(M, S)を署名検証者 B に送信する。

Step 3： B は送信された署名 S をディジタル署名方式により A の公開鍵 e_Aで変換した結果と文書 M をハッシュ関数 h で圧縮した結果 $h(M)$を突合し一致するかどうかを検証する。

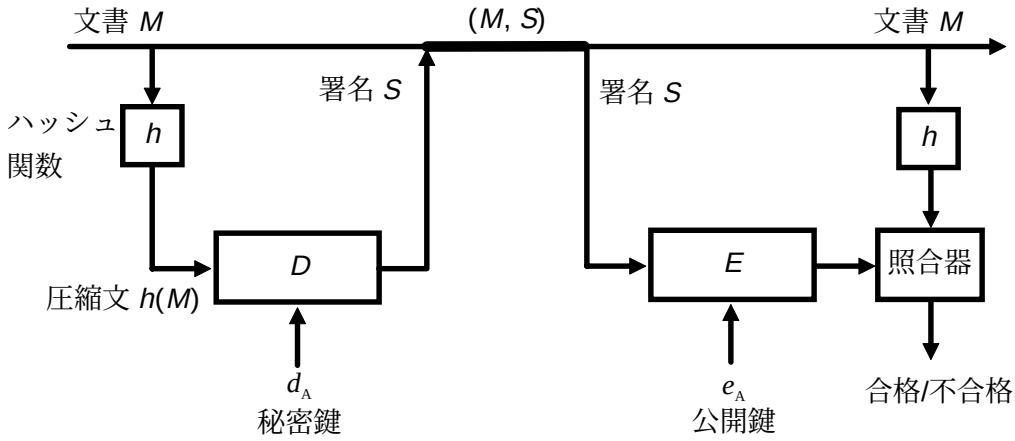

図 2　認証子照合法によるディジタル署名

認証子照合法では、通信文復元法で問題となっていた存在的偽造が不可能となる一方、コンピューターによる自動検証は可能となる。また、一方向性ハッシュ関数は乗法的でないため、乗法性を利用した偽造法も不可能となる。

以下では、認証子照合法によりディジタル署名が実現されているものとして議論を進める。さて、ディジタル署名が署名としての機能を果たすためには次の 2 条件を満たす必要がある。

① 送信者以外は署名付き文書を改竄・偽造できない
② 署名付き文書を送った事実を送信者が後で否定できない

ディジタル署名方式の実現法としては、署名者と署名の検証者の間の通信のみで行われる方式（以下「直接署名方式」）と署名者と検証者以外の第三者を介する方式（以下「調停署名方式」）に大別される。各方式が上記 2 条件を満たすかどうかをみてみる。

まず直接署名では、条件①は満たされるが、条件②が満たされない。すなわち、送信者が以前に送信した署名付き文書に対し、「私はそのような署名付き文書を作成した覚えはない。署名に使われている秘密鍵は当時既に紛失していたので、自分に責任はない」と送信の事実を否認された場合に真実を明らかにすることが困難だからである。

調停署名方式の代表例は、一般に認証機関による認証を利用した方式として知られている（図 3 参照）。

Step 1：　署名者 A は自分の ID（ID_A）と公開鍵 K_{PA} を認証機関に送信す

る。

Step 2： 認証機関は（ID_A ,K_{PA}）に対し自分の秘密鍵 K_Sにより 署名 S_{AC} を施し、A に返信する。

Step 3： A は署名付き文書（M,S_A）に認証機関の証明書（ID_A ,K_{PA},S_{AC}）を添付し、B に送信する。

Step 4： B は証明書（ID_A ,K_{PA},S_{AC}）の真正性を認証機関の公開鍵 K_P により検証した後、A の署名付き文書（M,S_A）の真正性を A の公開鍵 K_{PA}により検証する。

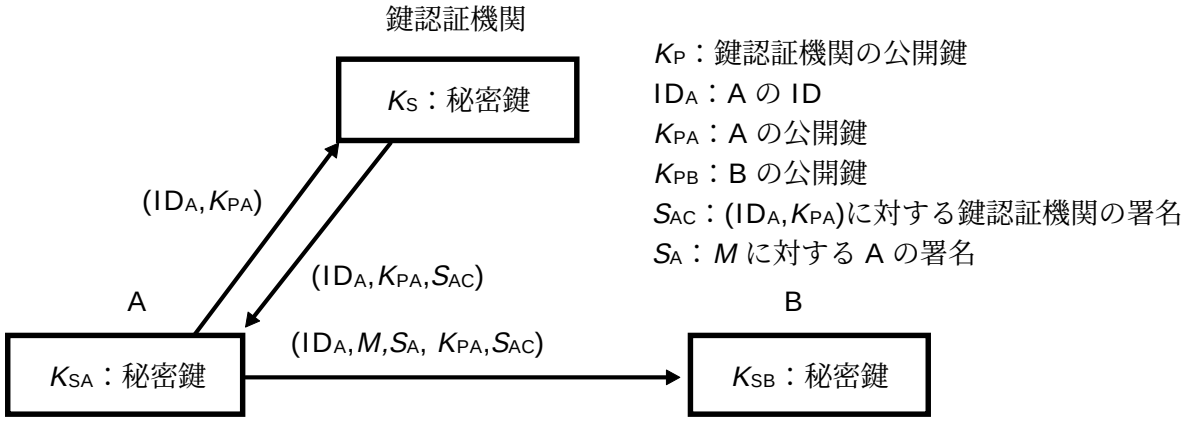

図 3 調停署名方式によるディジタル署名

同方式では、秘密鍵の盗難または紛失があった場合、被害者は鍵認証機関にそれまで利用していた公開鍵の登録を抹消し、新しい公開鍵の登録と同鍵に対する新しい認証子の発行依頼を行うルールとすれば、上記否認のような問題は生じないことになる。

(3)鍵共有・配送

冒頭で述べたように、公開鍵暗号は処理に大量の計算を必要とするため、秘密通信には適していない。このため、秘密通信には共通鍵暗号を用いる事例が多く見受けられるが、この場合、通信当時者間で最初に鍵を共有するための方法、所謂「鍵共有・配送」が問題となる。

最も単純な鍵配送法として、公開鍵暗号の秘密通信機能の利用が考えられる。すなわち、A が B と鍵を共有する場合、A は鍵 k_{AB}を生成し、これを B の公開鍵で暗号化し、B に配送するという方法である。但し、この手順では、B は「送られてきた鍵が確かに A のものであること」を確認する術がない。そこで、A は鍵 k_{AB}にディジタル署名を添付して B に配送することが望まれる。この鍵配送法

は、RSA 暗号のように秘密通信機能とディジタル署名機能を兼備した公開鍵暗号を利用できる状況であれば、同暗号単独で比較的容易に実現できる。

秘密通信機能を持つ公開鍵暗号方式を用いずに実現できる鍵配送法もある。それが Merkle によって考案された「公開鍵配送法（public key distribution system）」と呼ばれる概念である。Diffie-Hellman[1976]は同概念を具現化した「DH 型公開鍵共有法」（以下、DH 法と略記）と呼ばれる手順を示した。 利用者 A と B の間で DH 法により鍵を共有する具体的な手順は下記の通りである。素数 p とその原始根 α が公開鍵となる。

Step 1　A は[0, p-1]の整数 X_A をランダムに選び、

$$Y_A = \alpha^{X_A} \bmod p \quad (1)$$

を計算し、Y_A を B に送信する。

Step 2　同様に B も[0, p-1]の整数 X_B をランダムに選び、

$$Y_B = \alpha^{X_B} \bmod p \quad (2)$$

を計算し Y_B を A に送信する。

Step 3　A は鍵を次のように計算する。

$$K = Y_B^{X_A} \bmod p$$
$$= \alpha^{X_A X_B} \bmod p \quad (3)$$

Step 4　B も同様にして鍵 K を得られる。

上記手順から明らかなように攻撃者は公開鍵情報である p、α のほか、通信路の傍受により Y を入手可能である。ところが、このとき $Y=\alpha^X \bmod p$ の式から X を導き出す問題は「離散対数問題」と呼ばれ、p、α が十分に大きければ同問題を解くことは計算量的に困難とされている（詳細は後述）。すなわち、DH 法は離散対数問題が困難であることに安全性の根拠を置いているのである。

但し、DH 法には離散対数問題を解く以外の攻撃法が存在する。すなわち、DH 法に対しては「中間侵入攻撃（intruder-in-the-middle-attack）」と呼ばれる攻撃が成立することが指摘されている。これは攻撃者 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 $Y_C=\alpha^{X_C} \bmod p$ に置き換えることにより自分と 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 に成り済ますという攻撃である。中間侵入攻撃は通信当事者が相手を相互に確認していないために生じている。DH 鍵共有法に相手を相互確認する仕組みを導入した「Station-To-Station プロトコル」（Diffie-van Oorschot-Wiener[1992]）と呼ばれる方法が提案されている。

このほか、RACE[3] Integrity Primitives Evaluation (RIPE)で開発された Rabin 暗号と零知識対話証明を利用した「COMSET」（Brandt et al.[1990]）、 共通鍵暗号と公開鍵暗号を組合せた「EKE（Encrypted Key Exchange）」（Bellovin and Merritt[1992]）等、様々な方式が提案されている。

さらに、通信相手の ID を入力するのみで鍵を共有できるという「ＩＤに基づく鍵共有方式」が Shamir[1985]により考案されており、代表的な実現方式としては DH 法と RSA 暗号を利用した「岡本方式」（E. Okamoto[1989]）、線形スキームを利用した「KPS（Key Predistribution System）」[4]（Matsumoto-Imai[1988]）、RSA 暗号と DLP を利用した「自己証明公開鍵方式」（Girault[1991]）等が挙げられる。

(4)その他

ここでは、公開鍵暗号のその他の機能として、署名者に文書の内容を知られることなく署名を受けられる「ブラインド署名」、署名文が署名者の許しなく流通するという問題を解決する「否認不可署名」、一組の文書と署名だけからは秘密鍵の特定を不可能にする「故障停止署名」、グループの代表署名において問題が生じた場合にのみ責任の所在を明らかにできる「グループ署名」、秘密鍵の所有者に文書の内容を知られることなく復号化を依頼できる「ブラインド復号化」の各機能について簡単に紹介する。

イ．ブラインド署名 (blind signature)

ブラインド署名とは、署名依頼者が署名者に文書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、電子選挙等に利用される重要な基礎技術となっている。同署名は、署名を受ける文書とカーボン紙を封筒に封入し、その上から署名をして貰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。

Chaum[1982]は RSA 暗号によりブラインド署名を実現する手順を示した。その後、 ElGamal 署名による実現方式（Camenisch et al.[1994]）、「ゼロ知識対話証明（Zero Knowledge Interactive Proof; ZKIP）」（後述）による実現方式（Okamoto and Ohta[1990]）が示されている。

---

[3] RACE(The Research and Development in Advanced Communication Technologies in Europe)計画は EC による IBC(Integrated Broadband Communication)に関連する通信規格及び技術を調査・研究する計画である。

[4] KPS は既にインターネット用の電子メールソフトである Eudora、MS excahnge 等にプラグイン形式で機能追加できる形で製品化されている。

RSA 暗号によるブラインド署名の基本手順を、署名依頼者 A が文書 M に B のブラインド署名を受ける場合を例にとって説明しよう。なお、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。

Step 1　署名依頼者 A は秘密の乱数 r を生成した後、署名者 B の公開鍵(e,n)を用いて

$$X = Mr^e \mod n \tag{4}$$

を計算し、結果 X を B に送信する。

Step 2　B は自分の秘密鍵(d,n)を用いて

$$Y = X^d \mod n$$
$$= M^d r \mod n \tag{5}$$

を計算し、結果 Y を A に送信する。

Step 3　A は受け取った Y に秘密の乱数の逆数 r^{-1} を掛けることにより B の署名 $S = M^d \mod n$ を得る。

Step 4　最後に A は署名 S の正当性を B の公開鍵により検証する。

$$S^e = M \mod n \tag{6}$$

なお、Step 3 の r^{-1} は $r^{-1}r = 1 \bmod n$ となる整数であるが、これは GCD$(r, n) = 1$ から Euclid の互除法により簡単に求められる。

上記手順は「署名依頼者 A が署名者 B の意図せざる文書に署名させるという不正が可能」という点で応用例によっては問題が生じる。Chaum はこのような不正に対する措置として「cut-and-choose-methodology」と呼ばれる手順を上記基本手順に組み込んだ。これは言わば署名者による抜取検査であり、検査回数を増やしていけば署名依頼者による上記不正の検出確率を限りなく 1 に近くすることができる。しかしながら、同技法では取扱うデータ量が膨張する。そこで、ZKIP を利用した「DLP 型制約付きブラインド署名」（Brands[1993]）、「RSA 型部分ブラインド署名」（Abe-Fujisaki[1996]）、「DLP 型部分ブラインド署名」（Abe-Camenisch[1997]）等の cut-and-choose-methodology を用いずに 1 個のデータのみで署名対象文書の正当性を確認する技法が提案されている。

ロ．否認不可署名（undeniable signature）

通常のディジタル署名方式では、署名の対象の選び方によっては、署名文が署名者の許可なく電子的に複製され不正利用されるという所謂「署名の一人歩き」の問題がある。否認不可署名は、こうした署名の一人歩きを防止するため、署名者の同意なくしては署名の正当性を確認できないようにした方式

であり、Chaum and van Antwerpen[1990]によって発案された。同方式の原理の基本手順は次のように示すことができる。

Step 1　署名者 A は B に自分の署名 S_A を提示する。
Step 2　B は乱数 r を生成して、これを A に渡す。
Step 3　A は受け取った r と自分の秘密鍵 d_A を用いて所定の計算を行い、計算結果を B に渡す。
Step 4　B は A の公開鍵 e_A により計算が正しいかどうかを検証する。A が署名 S_A に対応する秘密鍵 d_A を知っているときに限り正しい計算が行われる。

実は上記手順のみでは、署名者 A が過去に作成した署名文を自分のものであると認めたくない場合、作成の事実を否認するために上記手順の過程で故意に計算を誤るおそれがある。そこで、実際のプロトコルにおいては上記手順に加え「否認手順（disapproval protocol）」と呼ばれる前述のブラインド署名における抜取検査と同様の仕組みが用意されている。同手順において検査回数を増やしていけば、上記不正の検出確率を限りなく 1 に近くすることができる。

ハ．故障停止署名（fail-stop signature）

通常のディジタル署名方式では、公開鍵に対応する秘密鍵は一意に定まるため、非常に強力な計算能力を有する解読者が公開鍵の情報のみから秘密鍵を求めるおそれがある。故障停止署名は、このような非常に強力な解読者に対抗するために、Pfitzman and Waidner[1990]が提案した方式であり、鍵は使い捨てられることが想定されている。すなわち、同方式では、一つの公開鍵に対応し、かつ任意の一文書から生成される署名が一致するような秘密鍵が多数存在し、さらに、そうした複数の秘密鍵の一つからは他の秘密鍵を求められない仕組みとなっている。従って、解読者は一組の文書と署名だけから秘密鍵を特定することはいかなる計算能力をもってしても不可能となる。但し、同じ秘密鍵によって作成された二組の文書と署名を解読者が入手した場合には秘密鍵を特定できるようになる。従って、鍵は使い捨ての形で利用されることが望ましいということになる。

ニ．グループ署名（group signature）

Chaum[1991]は次の機能を実現する署名方式を考案し、これを「グループ署名」と名付けた。

・ グループのメンバーだけが当該グループの署名を施すことができる。
・ 署名文の受け手は署名の妥当性を検証できるが、署名者を特定することはできない。
・ 紛争が生じた場合、署名作成者が明らかにされる。

同方式の基本手順を簡単に述べると以下の通りである。

Step 1　調停者は公開鍵・秘密鍵の組を必要なだけ生成し、グループの各メンバーに相異なる秘密鍵のリストを配布する。この際、如何なるリストの鍵も一致しないようにする。

Step 2　調停者はグループの全ての公開鍵のマスター・リストをランダムな順番で発行する。調停者はどの鍵が誰に属するかを記載した記録を保存しておく。

Step 3　グループのメンバーは各自のリストからランダムに選んだ秘密鍵を用いて文書に署名する。

Step 4　署名文の受け手は同署名に用いられた秘密鍵に対応する公開鍵を同グループのマスター・リストから検索し、同署名の正当性を検証する。

Step 5　紛争が生じた場合、調停者は Step 2 で作成した記録から問題の署名文の作成者を特定できる。

上記手順においては調停者は信頼できる者でなければならない。調停者は全員の秘密鍵を知っており、署名を偽造することができるからである。また、全てのメンバーは彼らがどの鍵を使っているかを分析するのに十分な長さの鍵のリストを持っていなければならない。

前出の Chaum[1991]の論文では、調停者が偽造できない方式や調停者自体を必要としない方式などが提案されている。

ホ．ブラインド復号化（blind decryption）

ブラインド復号化とは、例えば、ある暗号文の復号化鍵を持たない者が同鍵を持つ者に復号化を依頼する際、鍵所有者に文書の内容を知られることなく依頼した暗号文の復号化を実現する方式であり、鍵寄託方式において捜査機関の無制限の盗聴を防ぐ方式等への利用が提案されている（Micali[1993]、山根・櫻井[1996]）。

ブラインド復号化の原理はブラインド署名と本質的に同じである。ブラインド署名においては、いわば、依頼者が文書を封筒に入れ封をした上から署名者に署名を施して貰ったのと同様に、ブラインド復号化においては、依頼者

は暗号文を封筒に入れ封をした上から暗号文を復号化して貰うのである。具体的なブラインド復号化方式としては、RSA 暗号による方式（Micali[1993]）や ElGamal 暗号による方式（山根等[1995]）が知られている。

3. 公開鍵暗号の強度評価に関する基礎事項

暗号を解読するための計算量は、一般に解読・偽造に際し攻撃者が利用できる情報の質と量に応じ変化する。すなわち、攻撃者が暗号文しか利用できない場合よりも自分で選んだ暗号文に対応する平文を自由に利用できる場合の方が一般的には解読が容易になるのである。

一方、攻撃の結果としての解読・偽造に関してもいくつか種類があり、それらが与え得る被害の程度は大きく異なる。すなわち、解読の方では秘密鍵を導出するという意味での解読と平文の 1 bit のみを導出するという意味での解読の間には大きな隔たりが在るし、偽造の方でも任意の文書に署名できるという意味での偽造と一応いくつかのデータに署名できるが同データを制御することはできないという意味での偽造にはやはり大きな隔たりが在る。

従って、暗号学では、解読・偽造の前提条件を攻撃者が利用できる情報の程度に応じ、また解読・偽造の種類を解読の程度に応じ、それぞれ分類・整理している。解読・偽造の前提条件と解読・偽造の種類を秘密通信の場合、ディジタル署名の場合の順で説明する。

(1)秘密通信の場合

イ．解読・偽造の前提条件

①**直接攻撃** (direct attack)

公開鍵だけから行う攻撃。

②**選択平文攻撃** (chosen plaintext attack)

攻撃者が予め指定した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。

③**選択暗号文攻撃** (chosen ciphertext attack)

攻撃者が予め指定した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。

④**適応的選択暗号文攻撃** (adaptive chosen ciphertext attack)

選択暗号文攻撃における暗号文の選択を攻撃者が同攻撃により得た平文の情報を参考にしながら決定できる場合の攻撃。

公開鍵暗号が直接攻撃に対し十分な安全性を有していなければならないことは言うまでもない。公開鍵暗号の場合、誰でも公開鍵により任意の平文を

暗号化できることから選択平文攻撃も容易に実現可能である。従って、公開鍵暗号による秘密通信は選択平文攻撃に対し十分な安全性を有することが必須である。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難い攻撃ではあるが、同攻撃に対しても安全であることが現代暗号では望ましいとされている。特に、数個の選択暗号文により解読が可能であれば、同解読は十分に脅威であると考えられる。

攻撃者が攻撃の対象とする暗号装置に自由にアクセスできるような運用がなされている場合には「故障利用暗号攻撃（fault-based attack）」と呼ばれる暗号装置に対する物理的攻撃が脅威と成り得る。これは暗号装置に物理的影響を与えることにより故意に起こした計算誤り等の結果が得られる場合の攻撃である。具体的な誤り例としては、鍵の特定の 1 bit の値を反転させるとか、特定の命令コードをスキップするなどが挙げられる。故障利用暗号攻撃が成立する場合は、暗号技術による対応は難しくなる。例えば、鍵を格納しているメモリがパリティチェック機能を持つ場合に鍵の特定の 1 bit に 1（または 0）を設定できれば、パリティエラーが生じるか否かにより同 bit の値を決定できる（Anderson[1996]）。ここまでできない場合でも、鍵の特定の 1 bit の値を自由に反転させることができれば RSA 暗号等の秘密鍵を求めることができ、乱数を入手できれば ElGamal 系署名の秘密鍵を求めることができる（詳細は後述）。

ロ．解読・偽造の種類

①**全面的解読** (total break)

ある公開鍵に対応する秘密鍵を求めること。

②**一般的解読** (general break)

秘密鍵を求めずに任意の暗号文に対応する平文を求められる効率的なアルゴリズムを導出すること。

③**部分的解読**（partial break）

暗号文より平文の部分情報が求められること。例えば、平文に関するある 1 bit の情報が求められること。ここでの 1 bit の情報とは、平文の最上位 bit 等の特定の位置の 1 bit の場合だけでなく、平文のヤコビ記号の値等の平文の関数値をも指している。

逆に、どのような部分解読も困難なとき、「強秘匿（semantically secure）」と呼ぶ（Goldwasser and Micali[1984]）。

④**改竄** （tampering）

暗号文から元の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元の平文に意図的な変更を加えることができること。すなわち、意図

的な変更を関数 f で表現すると傍受した $C=E(M)$から $M'=f(M)$を満たすような $C'=E(M')$を求められること。

逆に、どのような関係 f に対しても、攻撃者が $C=E(M)$から $M'=f(M)$を満たすような $C'=E(M')$を作成できなければ、このような暗号方式は「頑健（nonmalleable）」であると呼ぶ。

従って、最も安全な暗号方式は「攻撃者に適応的選択暗号文攻撃を許したとしても、強秘匿でかつ頑健性を保持した方式」と考えられる。そのような暗号方式を以下では「安全な」暗号方式と呼ぶ。

公開鍵暗号の諸方式の強度を予め表に整理しておくと概ね次の通り。

	受動的攻撃			能動的攻撃	
	直接攻撃	暗号文 単独攻撃	既知・選択 平文攻撃	選択暗号文攻撃	適応的選択 暗号文攻撃
全面的解読	—	共通法 RSA 暗号（同報通信）	—	Rabin 系暗号	—
一般的解読	ナップザック暗号	共通法 RSA 暗号（同報通信） RSA 暗号（低指数公開鍵）	Rabin 系暗号	—	—
部分的解読	—	—	Goldwasser-Micali 暗号	—	Naor-Yung 暗号 OAEP
改竄	—	RSA 暗号（低指数公開鍵）	—	—	OAEP

：攻撃による解読・改竄が容易な場合

：攻撃による解読・改竄が困難な場合

(2)ディジタル署名の場合

イ．偽造の前提条件

①**直接攻撃**（direct attack）

公開鍵だけから行う攻撃。

②**既知文書攻撃**（known message attack）

ランダムないくつかの文書に対応する署名を入手できる場合の攻撃。

③**選択文書攻撃**（chosen message attack）

攻撃者が予め選んだいくつかの文書に対して真の署名者に署名させた後に、そこで得た情報を用いて第三の文書の署名を偽造する攻撃。

④**適応的選択文書攻撃**（adaptive chosen message attack）

選択文書攻撃では真の署名者に署名させる文書を攻撃開始に先立って全て選択しなければならない。適応的選択文書攻撃は適宜選択した文書の署名を眺めながら次の文書を選択していける攻撃である。

攻撃対象者の署名付き文書を収集すれば既知文書攻撃は可能となる。従って、ディジタル署名は最低限既知文書攻撃に対しては十分に安全でなければならない。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難い攻撃ではあるが、同攻撃に対しても安全であることが望まれる。特に、ブラインド署名のように署名者が必ずしも文書内容を把握できない場合にも署名を施さなければならない状況が存在することを考慮すると、攻撃者が数個の選択文書を入手することを非現実的とみることはできないと思われる。

ロ．偽造の種類

①**全面的偽造**（total forgery）

ある公開鍵に対応する秘密鍵を求めること。

②**一般的偽造**（universal forgery）

秘密鍵を求めずに任意の文書に対する署名を偽造できる効率的なアルゴリズムを求めること。

③**選択的偽造**（selective forgery）

解読者が予め選んだ特定の文書に対応する偽造署名を求めること。

④**存在的偽造**（existential forgery）

少なくとも 1 個の文書に対応する偽造署名を求めること。但し、この場合、解読者は署名を得る文書を制御することはできない。

従って、最も安全なディジタル署名方式は「攻撃者に適応的選択文書攻撃を許したとしても、存在的偽造さえできない方式」と考えられる。以下では、そのようなディジタル署名方式を「安全な」ディジタル署名方式と呼ぶ。

ディジタル署名の代表方式に対する攻撃と偽造可能性の関係を予め整理しておくと概ね次表の通り。

	受動的攻撃		能動的攻撃	
	直接攻撃	既知文書攻撃	選択文書攻撃	適応的選択文書攻撃
全面的偽造	—	—	Rabin 系暗号による署名法	OSS 署名
一般的偽造	OSS 署名	—	ElGamal 署名（特殊な公開鍵）	—
選択的偽造	RSA 暗号による署名法（通信文復元型署名）	—	—	—
存在的偽造	通信文復元型署名 DSA 署名	—	—	Naor-Yung 署名 Bellare-Goldwasser 署名

：攻撃による偽造が容易な場合

：攻撃による偽造が困難な場合

II 公開鍵暗号の諸方式

公開鍵暗号は、秘密通信・ディジタル署名の双方が可能な方式、秘密通信のみが可能な方式、ディジタル署名のみが可能な方式の 3 種類に大別される。各方式の紹介に入る前に簡単に公開鍵暗号の歴史を整理しておこう。Diffie-Hellman が公開鍵暗号の概念を発表した後、最初に公表されたのが RSA 暗号という秘密通信・ディジタル署名の双方が可能な極めて完成度の高い公開鍵暗号である。

RSA 暗号は「素因数分解問題」（Factoring Problem、以下 FP と略記）として古くから知られる有名な数学の問題の困難性に概ね基づいている。ここで概ねとしたのは素因数分解よりも効率的な解読法が存在しないということが証明されていないからであるが、公表後現在に至るまでの 20 年近くもの間、多くの暗号研究者が様々な角度から検討を加えたにも拘らず、素因数分解を上回る効率的な解読法は示されていない。

RSA 暗号の登場後に残された問題としては次の四つを指摘できる。安全性の面では① FP の決定的解法が発見される可能性が小さいながらもあること、②暗号解読が計算量的に困難とされる数学の問題と等価でないこと、が挙げられるほか、機能性の面で③暗号化・復号化処理があまり速くないこと、④ FP の解法の進展に伴い長い鍵が必要となり③の問題を深刻化させつつあること、を指摘し得る。RSA 暗号の発表後はこれらの問題を解決する目的で多くの方式が提案されてきた。

すなわち、①の問題に関しては FP とは異なる問題に基づく有力な方式として、ナップザック問題、誤り訂正符号復元問題、「離散対数問題」（Discrete Log Problem、以下 DLP と略記）等に基づく方式が提案された。しかしながら、前二者の問題に基づく方式は既に解読法が示された。DLP に基づく ElGamal 暗号・署名、改良型 ElGamal 署名（Schnorr 署名、DSA 署名）は有力な方式であるが当初期待されていた DLP は FP より難しいとの予想は、その後 FP に対し発見された高速解法が何れも DLP に対し形を変えて適用し得ることが明らかにされたため、FP に対し決定的な解法が発見された場合に DLP に同様の解法が発見されないとみることはできないとの見方が一般的となっている。

②の問題に対しては、受動的攻撃による解読が素因数分解と等価であることを証明し得る方式として、Rabin 暗号、改良型 Rabin 暗号（Williams 暗号、逆数暗号）が提案されたが、逆にこれらの Rabin 系暗号は能動的攻撃（選択暗号文攻撃）により極めて容易に解読されることが示されている。また、署名方式については、能動的攻撃に対しても存在的偽造すら許さないことを証明し得る方式として Bellare-Goldwasser 署名等が提案されているが、これらの方式は効率が悪く実用的とは言い難いのが実情である。

③の処理速度の問題に対しては、ナップザック暗号、McEliece 暗号、MI 暗号、Ong-Schnorr-Shamir 署名、 ESIGN 署名、Fiat-Shamir 署名が高速暗号・署名として提

案されたが、 ESIGN 署名、Fiat-Shamir 署名を除き、何れも有効な解読法が示された。ESIGN 署名、Fiat-Shamir 署名は有効な解読法が示されておらず有力な公開鍵暗号の一つと思われるが、ESIGN 署名は安全性の根拠となる数学上の問題が新たに一つ加わっており、Fiat-Shamir 署名では署名のサイズが非常に大きくなっている。

ところが 1980 年代後半頃から、これらの問題を解決する方法論ないしは方式が示されはじめた。まず、②の問題に対しては、最近になってであるが仮想的なランダム関数の存在等を仮定した安全かつ効率的な暗号・署名方式の構成法が盛んに研究されるようになっている。すなわち、暗号方式については、仮想的なランダム関数の存在を前提とすれば能動的攻撃に対し強秘匿でありかつ頑健性を保持した実用的な方式（Optimal Asymmetric Encryption Padding、以下「OAEP」と略記）が構成できることが示された。また、同様に仮想的なランダム関数を前提とすれば、FP や DLP が困難であると仮定して Schnorr 署名や ElGamal 署名を若干変形した方式等が安全であることが証明できることも示された。但し、実際には仮想的なランダム関数は実現不可能であり、既存のハッシュ関数等で代用するため、このとき安全性は必ずしも明らかではなくなる。従って、仮想的なランダム関数といった非現実的な前提ではなく、実現可能な前提に基づく安全性証明付きの効率的暗号・署名方式を実現することが期待されている。

また、①③④の問題に対しては、楕円曲線（elliptic curve）により定義された有限可換群上の DLP（以下「EDLP」と呼ぶ）に基づく暗号・署名方式がこれらの問題を解決する方式として現在注目を浴びている。EDLP に対しては DLP に適用される準指数関数時間の高速解法が一般に適用できず、将来的にも準指数関数時間の一般的解法は発見されないとみる研究者が少なくないからである。こうした予想が真実であるならば、EDLP に基づく暗号・署名方式は問題①③④を解決したとみなせるであろう。このとき、EDLP に基づく方式では決定的解法が発見されないことが保証されており、また、FP、DLP に基づく方式に比べ同等の安全性を保ちつつ鍵長を相当程度短くでき、さらに、これに伴い処理速度を高速化し得るからである。もっとも、EDLP に基づく暗号・署名方式に関しては FP や DLP に基づく方式ほど十分な研究がなされているとは言えないのが実情であり、こうした予想が真実であるかどうかを見極めるためには今少し研究の蓄積を待つ必要があろう。

以下では、代表的な公開鍵暗号方式を秘密通信機能とディジタル署名機能を兼備した方式、秘密通信機能に特化した方式、ディジタル署名機能に特化した方式の順に紹介する。

1. 秘密通信・ディジタル署名方式

秘密通信機能とディジタル署名機能の双方を兼ね備えた方式としては、素因数分解問題の困難性に基づく「RSA 暗号」、同暗号を変形し受動的攻撃に対する安

全性を証明できるようにした「Rabin 暗号」のほか、Rabin 暗号の改良版である「Williams 暗号」と「逆数暗号」、Obscure 表現と多変数連立多項式の解法の困難性に基づく「MI 暗号」等が挙げられる。以下、これらの方式の手順と基本的な安全性につき順次紹介する。

(1)RSA 暗号

RSA 暗号は MIT の Rivest, Shamir, and Adleman[1978]によって考案された最初の具体的な公開鍵暗号である。RSA 暗号は、大きな合成数を素因数分解すること、所謂「素因数分解問題（FP）」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。確かに、同問題の解法はここ 20 年ほどの間に長足の進歩を遂げており、従来と同等の安全性を保つためには従来よりも長い鍵を用いることを余儀なくされているが、RSA 暗号の存在自体を脅かすまでには至っていない。また、RSA 暗号に対し素因数分解以外の解読法が存在しないという証明はないものの、発表されてから現在まで 20 年近くもの間世界中の暗号研究者に様々な角度から攻撃に晒されてきたにも拘らずこれまで素因数分解以上に有効な解読法が一つとして報告されていない。こうした歴史的事実を背景に RSA 暗号は最も信頼性の高い公開鍵暗号として、事実上の国際標準暗号と目されるほど世界的に普及している。以下では、RSA 暗号による秘密通信の手順を紹介した後、同暗号の安全性に関する議論を整理する。

【手順】A が B に対し秘密通信を行う手順は次の通りである。

[**鍵生成**] 受信者 B は鍵を次のように生成する。まず、二つの大きな素数 p と q を適当に選び[5]、これらの積 $n=pq$ を計算する。次に、p-1 と q-1 の最少公倍数 l=LCM(p-1,q-1)を計算する。最後に、GCD(e,l)=1 となるような自然数 e を選び、ed=1 (mod l)を満たす d を求める。

秘密鍵：d

公開鍵：(e, n)

[5] 各利用者がこうした方法で鍵を生成するためには大きな素数を高速に生成する方法が必要となる。これは大きな奇数を「ランダムに」発生させた後、同奇数を「素数判定法」と呼ばれる方法で素数かどうかを判定するという手順で実現される。素数判定法は、確率的に素数を判定する「確率的素数判定法」とこれを確定的に行う「確定的素数判定法」とに大別される。汎用的な確率的素数判定法の代表例としては Fermat テスト、Solovay-Strassen テスト（Solovay and Strassen[1977]）、Miller-Rabin テスト（Rabin[1976]）が、汎用的な確定的素数判定法の代表例としては Adleman-Rumely テスト（Adleman et al.[1983]）、Atkin-Morain テスト（Atkin and Morain[1993]）、Goldwasser-Kilian テスト（Goldwassr and Kilian[1986]）、Adleman-Huang テスト（Adleman and Huang[1992]）が挙げられる。

[**暗号化**] 平文 M に対し、暗号文 C は次式で求められる。

$$C = M^e \pmod{n} \tag{7}$$

[**復号化**] 暗号文 C から元の平文 M は次式で求められる。

$$M = C^d \pmod{n} \tag{8}$$

【安全性】

イ．全面的解読に対する安全性

RSA 暗号の全面的解読に対する安全性は n を p と q に素因数分解する難しさに根拠をおいている。これは、素因数分解以外の解読法が存在しないことまでを意味するものではないが、少なくともこれまでのところ、素因数分解を上回る解読法は発見されていない。n を p と q に素因数分解せずに秘密鍵を求める方法としては、

① 既知平文 M と対応する暗号文 C を入手し、復号化関数 $M = C^d \pmod{n}$ から秘密鍵 d を求める。

② n から直接 $\varphi(n) = (p-1)(q-1)$ を計算する。

の二つが挙げられるが、前者（素因数が未知の合成数 n の法での離散対数問題）は合成数 n の素因数分解以上に困難であり、後者は同素因数分解と同程度に困難であることが証明されている（Miller[1976]）。

最近になって、Kocher[1996]は秘密鍵による変換に要する時間に基づいて全面的解読を行う「時間測定攻撃（timing attack）」という攻撃法を発表した。指数の値によりべき乗の計算時間が微妙に異なることを利用する同攻撃法は離散対数問題に基づく方式（Diffie-Hellman 鍵共有法、DSA 署名等）の解読にも適用し得る。しかしながら、同攻撃の前提となる厳密な時間測定は困難であり、Kocher 自身も同攻撃により大きな合成数を実際に素因数分解するという実績を示すには至っていない。このため、時間測定攻撃は現実の脅威足り得ないとみる向きが大勢のようである。また、仮に同攻撃が現実の脅威足り得るとわかれば、その時点で処理の際にランダムなダミー処理を入れ時間測定を不可能にすることにより対処し得るという意味でも時間測定攻撃は公開鍵暗号の脅威ではないと考えられる。

FP の困難性に関しては、同解法はここ 20 年ほどの間に急速な進展を遂げている。現在知られている最速の素因数分解法である数体ふるい法の漸近的な平均計算量 $T(p)$は

$$T(p) = \exp\left((1.901+o(1))(\log p)^{1/3}(\log\log p)^{2/3}\right)$$

と準指数関数時間で評価されている。また、一般的には効率的ではないが素因数 p,q の値如何では容易に素因数分解を実行し得る解法が存在する。

さらに、素数 p,q の値は暗号強度と関連の深い暗号化関数の周期に影響を

与える。従って、鍵生成の際、素数 p,q は、こうした解法を念頭に置いて注意深く選ばなければならない。素因数分解等の暗号解読を容易にさせないための p,q の満たすべき条件としては、次の四条件が挙げられる。

① $|p-q|$を大きくする。

② $(p\pm1)$と$(q\pm1)$は、それぞれ大きな素数 p_+, p_-, q_+, q_-を因数に持つ。

③ $(p_+\pm1)(p_-\pm1)$、及び$(q_+\pm1)$と$(q_-\pm1)$は、それぞれ大きな素因数を持つ。

④ GCD$(p-1,q-1)$は小さい。

上記 4 条件のうち、条件①②はそれぞれ Fermat 法、p-1 法&p+1 法 という素因数分解法の対策である。条件②はまた条件③と共に解読に繋がる短周期の防止策ともなっている。素因数分解の解法については、III 1.で包括的に説明するので、次に短周期の問題について述べよう。

ロ．鍵の値と周期の関係

暗号化関数を $f(x) = x^e \bmod n$ と表記する。このとき、

$$f^m(x) = x \tag{9}$$

を満たす最少の正整数 m を x に対する「周期」と呼ぶ。この周期の値は、e,n,x の値に依存している。次に示すように、周期が短いと一般的解読や全面的解読が可能となる。

① 一般的解読

Simmons and Norris[1977]は、p,q を適切に選ばないと、周期が計算可能なまでに短い場合が生じ、暗号文の解読に繋がることを示した。すなわち、暗号文 C に対し周期 m を求めることができれば、このとき、$y=f^{m-1}(C)$が C に対する平文となるからである。この周期の値は、$n(=pq),e,C$ の値に依存しているが、C は制御不可能なので、p,q,e を巧く設定する必要がある。

Rivest[1978]、Williams and Schmid[1979]は、p,q,e が次の条件を満たせば、上記解読法によって RSA 暗号が解読されるおそれは殆どないことを示した。

(i) $p = a'p' + 1, \quad q = b'q' + 1$

$p' = a''p'' + 1, q' = b''q'' + 1$

p', q', p'', q''はそれぞれ 10^{90}以上の十分大きな素数

(ii) $e^l \equiv 1 \pmod{p'q'}$ならば、l は $p'q'$で割り切れる。

② 全面的解読

Knuth[1979]は全面的解読に繋がる周期関連の問題として、次の点を指摘している。すなわち、

$$\mathrm{Prob}\{x|x^k \equiv 1 \pmod n\} \geqq 10^{-2l} \tag{10}$$

となる k をみつけることができれば、$10^l \log k$ 回程度の法 n の演算で n が素因数分解できる、というものである。

同解読法の対策は、小さな値の l に対し上式を満たす k の最小値が小さくなる確率が無視し得るほど小さくなるように p,q を設定することである。Knuth[1981]によれば、同条件は「p-1 と q-1 がそれぞれ大きな素因数 p',q'($p' \neq q'$)を持つこと」であるが、これは Rivest[1978]の設定条件(i)の一つにほかならない。同条件が上記全面解読の対策足り得る理由は、このように p,q を選んだ場合、任意の x に対し、$x^k = 1 \pmod n$を満たす k の最小値が $p'q'$ より小さくなる確率は $1/p'q'$ 以下となるからである。

勝野[1983]は式(10)が成立する周期 m'を解析し、Rivest[1978]が示した公開鍵の選択法よりも厳しい条件を示している。

ハ．特殊な暗号文に対する安全性

RSA 暗号では、特殊な暗号文に対し次の問題がある。

(a) ある種の暗号文に対しては、p と q が容易に推定できる。

(b) ある種の暗号文は元の平文と等しくなる。

(a)の問題は、暗号文 C が素数 p,q の何れかの倍数に成っている場合に生じる。しかしながら、この問題が生じる確率は、

$$1/p+1/q-1/pq \qquad (11)$$

である。従って、p と q が 10 進数で 100 桁に設定される場合、(a)の問題が生じる確率は、約 $2/10^{100}$ と無視し得るほど小さな値となる。また、こうした特殊な暗号文を合成数 n の素因数を知らずに求めることはできないため同暗号文の導出による解読のおそれも無い。

(b)の問題については、どのような鍵に対しても、少なくとも 9 個の平文は暗号化しても元の平文のままであることが示されているだけであり（Blakley[1978], Blakley and Borosh[1979]）、そのような暗号文が最大何個存在するかは示されていないが、無視し得るほど少ないとの見方が一般的である。また、暗号文が平文と一致した場合、これを機械的に検出することは容易である。

ニ．部分的解読に関する安全性

暗号通信においては、暗号文から平文全体を推測することが困難でなければならないのは勿論であるが、部分的な情報であっても容易に推測されないことが望ましい。RSA 暗号においては、平文の最上位 bit を有意に推測することが平文全体を推測することと同程度に難しいことが証明されている（Chor and Goldreich[1984]）。但し、どのような部分解読も不可能、すなわ

ち強秘匿であるということまでは証明されていない。

ホ．存在的偽造に対する安全性

RSA 暗号等の落し戸に基づく全ての公開鍵暗号は直接攻撃により存在的偽造が可能である。これは、偽造者が選んだ任意のデータに対し公開鍵で変換を行えば、変換により得られた結果が文書、最初に選んだデータが同文書の署名となるからである。この場合、攻撃者は署名を得る文書を制御できない。従って、不正に繋がるような文書が生成される確率が無視し得るほど小さい限りは脅威とならない。一般的には同確率は十分に低いと考えられるため、同偽造は脅威ではないと考えられるが、仮に同確率が十分に低くないと判断される場合であっても、長いチェックサム bit や日時等の付属情報を各平文に含ませ冗長度を高めることにより対処し得る。

ヘ．利用上の留意事項

これまでみてきたように RSA 暗号は少なくとも現時点では基本的な欠陥が示されていない暗号であるが、運用によっては安全性が損なわれる場合がある。すなわち、文書全体を対象に署名が施され、同文書を復元する形で検証が行われる「通信文復元型ディジタル署名」、利用者間で共通の法を用いる「共通法プロトコル」、平文の暗号化及び署名の検証の高速化を図る「低指数公開鍵プロトコル」は利便性の高い利用法である。しかしながら、以下で述べるように何れの利用法も安全性に問題があるため推奨できない。

また、最近になって、暗号化・復号化を行う装置に対し物理的影響により故意に計算誤りを引き起こし、その結果から得られる出力に基づいて解読する故障利用暗号攻撃（Boneh et al.[1996]）と呼ばれる攻撃が発表された。この攻撃は、攻撃者が自由にアクセスできる暗号装置の中に、RSA 暗号の秘密鍵が秘匿されているようなケースにおいて、同装置に物理的影響を与えることによって、その秘密鍵を求めるという方法である。ＩＣカード型電子マネーのように、秘密鍵を求めることが脅威となるような場合、この種の攻撃に注意する必要がある。

ａ．認証子照合型ディジタル署名の推奨

RSA 暗号は暗号化・復号化関数が「乗法的」、すなわち、暗号化・復号化関数の定義域の任意の元 x,y に対し

$$f(xy) = f(x)\, f(y)$$

が成立するため、通信文復元法を採用している場合、他人から署名を不正に得る方法も指摘されている。こうした不正を不可能ならしめるためには認証子照合法を採用することである。一方向性関数は乗法的でないため署

名生成関数も乗法的でなくなるからである。認証子照合法は署名長を文書長に比べ大幅に圧縮し効率化にも寄与するため、同方法の利用が一層強く推奨される[6]。以下では、通信文復元法に対する攻撃について簡単に紹介する。

本来であれば署名を得られないであろうような文書に対し他人から署名を得られることが指摘されている（Davida[1982], Denning[1984], Desmedt and Odlyzko[1985]）。ここでは、ある者が文書 M の署名を不正に得る手段を二通り紹介する。

① ブラインド署名技法を利用した選択的偽造法

攻撃者は署名を得たい文書 M に適当な値 r の e 乗を掛け合わせることにより署名を得られる文書 M' を見つける。

$$M' = r^e M \bmod n \tag{12}$$

攻撃者は文書 M' に対し署名を得る。

$$S' = M'^d \bmod n \tag{13}$$

攻撃者は得られた署名に r の逆数を掛けることにより文書 M に対する署名を得ることができる。

$$S'r^{-1} = M^d \bmod n \tag{14}$$

② 二つの署名を利用した選択的偽造法

攻撃者は署名を得たい文書 M に対し次式を満たし、かつ署名を得られる二つの文書 M_1, M_2 を見つける。

$$M = M_1 M_2 \bmod n \tag{15}$$

攻撃者は両文書に対し署名を得る。

$$S_1 = M_1^d \bmod n \tag{16}$$

$$S_2 = M_2^d \bmod n \tag{17}$$

攻撃者は得られた両署名を掛け合わせることにより文書 M に対する署名を得られる。

$$S_1 S_2 = M^d \bmod n \tag{18}$$

①はブラインド署名と原理的には同じ方法であるが、同方法を成功させるためにはブラインド後の文書が署名者から署名を得られるような文書にしなければならない。このような文書を探し当てることは

[6] 一方向性ハッシュ関数は、関数値から元の値を特定することと関数値が一致する二つの値をみつけることが事実上不可能となるようにデータを圧縮するため、安全性を保ちつつ署名長を短くすることが可能となる。

非常に困難である。

②については、(15)式を満たすような二つの文書をみつけられる確率は無視し得るほど小さいと考えられるため現実の脅威とは成り難いであろう。

しかし、たとえ確率は小さくともこのような不正が存在すること自体嫌みである。これらの不正はディジタル署名として通信文復元法を採用する代わりに認証子照合法を採用すれば不可能にすることができる上、署名長を圧縮し効率化を図ることもできることから、認証子照合法を採用することが推奨される。

b．共通法プロトコルの問題点

RSA 暗号を m 人の参加者から成る通信網で利用する場合、通常は各人がそれぞれ異なる法の値 $n_i = p_i q_i$ と鍵の値 $e_i, d_i (i=1,2,\cdots,m)$ を生成するが、鍵管理機関が一組の素数 p と q を生成した後、この p と q に基づいて m 組の異なる (e_i, d_i) を生成し、各利用者に配送する方式（「共通法プロトコル」）が考えられる。共通法プロトコルでは、法 $n = pq$ は利用者全員で使用することになる。同プロトコルは各利用者が鍵生成を行わなくても良いほか、他者の公開鍵リストを手元に置いておきたい場合、保存対象を (e_i, n) から e_i に削減し得るため効率的なプロトコルといえる。

しかしながら、同方式には三つの解読法が存在するため推奨できない。一つは一般的解読法、残りの二つは全面的解読法である。以下、これら解読法を順番に紹介する。

① 同報通信に対する一般的解読

同一の文書を複数の受信者に送ることを「同報通信」と呼ぶ。RSA 暗号の共通法プロトコルを用いて同報通信を行う場合、暗号文が解読される危険性がある（Simmons[1983]）。例えば、ある電子文書の供給者が同文書を二人の需要者に暗号化して送信しようとする場合、これらの暗号文を入手した第三者は同文書を簡単に復元できるのである。需要者#1 と#2 に送信された同じ文書 M の暗号文を第三者が入手した場合を例にとって説明しよう。この場合、各需要者宛に送信された暗号文はそれぞれ

$$C_1 = M^{e_1} \mod n \tag{19}$$

$$C_2 = M^{e_2} \mod n \tag{20}$$

と表される。このとき、e_1 と e_2 が互いに素ならば、ユークリッドの互除法（「付 1 初等整数論の基礎事項」参照）を用いて次式を

満たす整数 r と s を簡単に算出できる。

$$re_1+se_2 = 1$$

明らかに r ないし s の何れかが負でなければならないので、$r<0$ と仮定する。このとき、次式が示すように元の文書が求められる。

$$(C_1^{-1})^r C_2^{\ s} = M^{re_1+se_2} = M \bmod n \qquad (21)$$

② 全面的解読

共通法プロトコルには同プロトコルの利用者の一人に全面的解読を許す二つの攻撃法が存在する（DeLaurentis[1984]）。全面的解読に成功した利用者は同プロトコルの利用者間で通信される暗号文を解読できるほか、他の任意の利用者の署名を偽造することも可能となる。二つの攻撃法のうち、一つは法 n を素因数分解する確率的アルゴリズムであり、もう一つは法 n の素因数分解を行わずに他の購入者の秘密鍵 d を直接求める決定的アルゴリズムである。ここでは両攻撃法の基本的な発想のみを説明する。

(a) 法 n を素因数分解する確率的アルゴリズム

法 n を素因数分解する基本的な発想は法 n の下での 1 の自明でない平方根、すなわち次の二式を満たすような b を求めることである。

$$b^2 \equiv 1 \mod n \qquad (22)$$

$$b \not\equiv \pm 1 \mod n \qquad (23)$$

もし、こうした値を見つけることができれば、このとき、b+1 ないしは b-1 と法 n の最大公約数をユークリッドの互除法を用いて計算することにより法 n の素因数 p,q を求められる。したがって、このアルゴリズムの成否は法 n の下での自明でない 1 の平方根 b を求められるかどうかにかかっている。詳細は省略するが b を求めるアルゴリズムは次式を満たす正の整数 c,k と奇数 l を求められる場合に限り効率的な探索が可能となる。

$$c\ \phi(n) = 2^k l \qquad (24)$$

但し、$\phi(n)=(p-1)(q-1)$。

利用者は自分の公開鍵 e_1 と秘密鍵 d_1 から、次式が成立するためユークリッドの互除法により上記正整数 c,k と奇数 l を求められる。

$$e_1 d_1 - 1 = c\ \phi(n) = 2^k l \qquad (25)$$

(b) 他の利用者の秘密鍵を求める決定的アルゴリズム

このアルゴリズムでは、共通法プロトコルの利用者は自分の公開鍵と秘密鍵の情報から他の利用者の秘密鍵を多項式時間で求めることができる。厳密に言えば、ある公開鍵・秘密鍵対(e_2,d_2)

の所有者は所与の公開鍵 e_1 に対し、$e_1 d_1 = 1 \bmod \phi(n)$を満たすような整数 d_1 を $\phi(n)$の値を知らずに $O(\log^2 n)$の計算量で求められる。このような d_1 を見つけるためには、e_1 と互いに素で、かつ $\phi(n)$の倍数であるような整数を見つければ良い。これは d と e_1 が互いに素であるかどうかに注意することによって確かめられる。このとき、$rd + se_1 = 1$ を満たす整数 r,s が存在する。もし d が $\phi(n)$の倍数であれば、このとき $se_1 = 1 \bmod \phi(n)$となる。

c．低指数公開鍵プロトコルの問題点

暗号化及び署名検証を高速に行うために公開鍵 e を低次の値に設定するというプロトコルが考えられる。しかし、同プロトコルに対しては暗号文から元の文書を解読する二つの方法が存在することから使用すべきではない。一つは同一の公開鍵を用いた同報通信に適用できる方法であり、もう一つは暗号化される平文の間の関数関係が既知の場合に適用できる暗号文解読法（Coppersmith et al.[1996]）である。以下、これらの方法を順次説明する。

① 同一の公開鍵を用いた同報通信に対する一般的解読

共通法プロトコルの場合、同報通信が危険であることは既に述べた。ところが、たとえ法を変えていても利用者の間で同一の低指数の公開鍵 e が用いられている場合、公開鍵の数値以上の人数の受信者に同報通信を行うと、これらの暗号文を取得した第三者は元の平文 M を復号化し得るという問題が Blum、Liberherr、Williams 等によって指摘されている。あるユーザーが公開鍵を 3 に設定している三人のユーザー#1, #2, #3 に同じ平文 M を暗号送信する場合を例にとって説明しよう。このとき、暗号文はそれぞれ

$$C_1 = M^3 \bmod n_1$$
$$C_2 = M^3 \bmod n_2$$
$$C_3 = M^3 \bmod n_3$$

となる。n_1, n_2, n_3 が互いに素の場合は、中国剰余定理（付 1 定理 1.3 参照）から $M^3 \bmod n_1 n_2 n_3$ を算出することができるが、$M^3 < n_1 n_2 n_3$ であるため算出した $M^3 \bmod n_1 n_2 n_3$ は実は M^3 そのものである。従って、普通に 3 乗根を取ることにより M が求められる。一方、n_1, n_2, n_3 が互いに素でない場合は、前述の共通法プロトコルに対する攻撃が成立する。

② 平文同士が既知の多項式関係を持つ場合の暗号文解読法

Coppersmith et al.[1996]は、平文の間に既知の多項式で表される関係がある場合に暗号文を復号化できることを示した。

解読者が入手する二つの暗号文を(c_1,c_2)、これらに対応する平文を(m_1,m_2)とする。便宜上、m_1とm_2は線形関係、

$$m_2 = am_1+b \tag{26}$$

にあり、公開鍵がe=3の場合を例に採って説明しよう。従って、

$$c_i = m_i^3 \bmod n \quad (i=1,2) \tag{27}$$

である。このとき、次式よりm_1を得ることができる。

$$\frac{b(c_2+2a^3c_1-b^3)}{a(c_2-a^3c_1+2b^3)}$$

$$= \frac{3a^3bm_1^3+3a^2b^2m_1^2+3ab^3m_1}{3a^3bm_1^2+3a^2b^2m_1+3ab^3} \bmod n$$

$$= m_1 \bmod n \tag{28}$$

このように二つの文書m_1,m_2が線形の関係にある場合は、公開鍵eが如何なる値であってもm_1を代数的に導出することが理論的には可能である。しかし、公開鍵eが大きくなるにつれて導出のための計算量は$O(e \log^2 e)$と指数関数的に増加していく。このため、同攻撃が実際に適用できるのはe=32程度までとされている。

m_2がm_1のk次多項式の場合は、同計算量は$O((e+k)^3k^2)$に増大する（Coppersmith et al.[1996]）。

d．故障利用暗号攻撃

故障利用暗号攻撃はBoneh et al.[1996]により発表された暗号装置の計算誤りを利用した全く新しい暗号解読法である。すなわち、暗号装置に放射線を照射したり高電圧を掛けたり瞬間的にクロック周波数を上げたりするなどの物理的影響を与えることにより故意に計算誤りを起こし、それにより得られる誤った計算結果と元の正しい計算結果に基づいて同装置内の耐タンパー装置（tamper resistant device）内部に格納された秘密鍵を求めるという方法である。同攻撃は公開鍵暗号、共通鍵暗号双方に幅広く適用可能な攻撃であるが、RSA暗号に対する攻撃法としてはBao et al.[1996]の解読法が挙げられる。同解読法は鍵のあるbitの値を自由に反転させることができれば同bit値を決定できるという方法である。解読法の概要を簡単に紹介すると以下の通りである。

復号化関数$M=C^d \bmod n$を次のように鍵の各bit値で表現する。まず、暗号文を次のように分解する。

$C_0=C^{a0}$, $C_1=C^{a1}$, $C_2=C^{a2}$, ..., $C_{511}=C^{a511}$

但し、$a_i=2^i$ $(i = 0,1,...,511)$。

このとき、復号化関数は鍵の各 bit 値により次式のように表現される。

$$M = C^{d} \mod n$$
$$= C_{511}^{d511} C_{510}^{d510} \cdots C_{i}^{di} \cdots C_{0}^{d0} \mod n$$

但し、$d = d_{511}|d_{510}|...|d_i.|...|d_0|$。

従って、d_iの 1 bit を反転させ d_i'とすると、

$$M' = C_{511}^{d511} C_{510}^{d510} \cdots C_{i}^{di'} \cdots C_{0}^{d0} \mod n$$

$$\frac{M'}{M} = \frac{C_i^{di'}}{C_i^{di}} \mod n$$

となるため、同式より鍵の i bit 目の値 d_iが決定する。

(2)Rabin 暗号

RSA 暗号の場合、RSA 暗号を全面的に解読する素因数分解よりも効率的な方法が存在しないとの確証がないという点で一抹の不安が残されている。Rabin[1979]は RSA 暗号を変形することによって受動的攻撃による一般的解読が素因数分解と同等の難しさであることを証明し得る公開鍵暗号を発案した。しかし反面、Rabin 暗号は「能動的攻撃（選択暗号文攻撃）により簡単に全面的解読がなされる」という致命的な問題がある。

【手順】A が B に対し秘密通信を行う手順は次の通り。

[**鍵生成**] B は二つの大きな素数 p と q を選び、これらの積 $n=pq$ を計算する。$0 \leqq b < n$ なる b を定める。

秘密鍵：(p, q)

公開鍵：(n, b)

[**暗号化**] 平文 M に対し、暗号文 C は次式で求められる。

$$C = M(M+b) \pmod{n} \quad (29)$$

[**復号化**] 次の連立合同式から平文 M を算出する。なお、2 次合同方程式に対しては、これを確率的多項式時間で解くことができることが示されている。

$$M^2 + Mb - C = 0 \pmod{p} \quad (30)$$
$$M^2 + Mb - C = 0 \pmod{q} \quad (31)$$

【安全性】 Rabin 暗号は RSA 暗号の公開鍵を 2 に限定した方式と解釈することが可能であるが、このような限定を加えることにより、受動的攻撃に対する一般的解読は合成数 n の素因数分解と同等であることが証明される。しかしながら反面、同証明からは選択暗号文攻撃により容易に全面的解読がなされることが示される。制限付き RSA 暗号である Rabin 暗号の鍵の値と周期の関

係は RSA 暗号の場合と同様になる。また、RSA 暗号の場合と同様に解読を容易にする特殊な暗号文が存在するが、これらの発生確率はやはり無視し得るほど小さい。

イ．受動的攻撃による全面的解読に対する安全性

Rabin 暗号の受動的攻撃による一般的解読は法 n を素因数分解することと等価であることが証明されている。法 n を素因数分解できれば解読できることは言うまでもない。逆に、受動的攻撃により一般的解読ができれば素因数分解ができることは次のように証明される。

任意の c,n に対し、

$$x^2 = c \bmod n \tag{32}$$

を満たす x を計算するアルゴリズムがあるとする。すなわち、上式を満たす x は四つ存在するが、同アルゴリズムはこのうちの一つを求められるとする。このとき、適当に選択された y から $c = y^2 \bmod n$ により計算された c に対し同アルゴリズムを適用すると、

$$x^2 = y^2 \bmod n \tag{33}$$

を満たす x が求められるが、1/2 の確率で $x \neq \pm y$ となる。このとき、x-y と n の最大公約数を計算すると、素因数 p ないしは q が求められる。

ロ．能動的攻撃による全面的解読に対する安全性

受動的攻撃による一般的解読が素因数分解と等価であることの上記証明は、逆に能動的攻撃（選択暗号文攻撃）によって簡単に全面的解読ができることを意味している。すなわち、攻撃者が適当に選択した y を 2 乗した値 c (= $y^2 \bmod n$)に対し $x \neq \pm y$ を満たす平文 x を得ることができれば、x-y と n の最大公約数を計算することにより素因数分解できるからである。

【問題点】Rabin 暗号には安全面での問題に加え、機能面でも重要な二つの問題がある。

イ．一意に復号化できない

Rabin 暗号の復号化関数は多価関数なので、平文 M に対する暗号文 C を復号化しても、元の平文 M が一意に定まるとは限らず、一般的には復号化の結果、四つの平文が現れるという問題である。この中から、元の平文 M を機械的に復号化するため、平文の中に機械的に対応し得る秘密情報（例えば、送信者 ID、日付等）を含めることが考えられるが、所詮暫定的措置といった感は否めない。やはり抜本的対策として、同暗号の暗号化・復号化関

数が全単射となるよう再構築することが望まれる。

ロ．一部の文書にしか署名できない

Rabin 暗号によるディジタル署名も原因を同じくする問題がある。すなわち、署名生成関数の性質上、文書が一定の条件を満たしていなければ署名ができないのである。同条件は(30)(31)式が M について解けることであるが、その確率は約 1/4 に過ぎない。

(3)その他

その他の秘密通信・ディジタル署名方式として、「改良型 Rabin 暗号」、「MI 暗号」を紹介する。

イ．改良型 Rabin 暗号

先に指摘したように、Rabin 暗号は機能面で、①暗号文を一意に復号化できない、②任意の文書に署名できない、という二つの問題点を抱えていた。これらの問題は暗号化・復号化関数が全単射でないことに起因している。Williams[1980]は素数 p,q に制限を加えるという工夫を施すことにより、暗号化・復号化関数が全単射の公開鍵暗号を考案した。すなわち、「Williams 暗号」は、受動的攻撃による一般的解読が Rabin 暗号と同様に素因数分解と等価であることが証明されている上、暗号文を一意に復号化でき、任意の文書に署名することもできる。さらに、黒澤等[1987] はこうした Williams 暗号の長所を全て保ちながら同暗号における素数に課される制限を取り払った方式として「逆数暗号」を発表した。

しかしながら、 Williams 暗号、逆数暗号ともに Rabin 暗号の安全面における最も重要な問題、「能動的攻撃（選択暗号文攻撃）により全面的解読がなされる」という問題は克服されていない。

ロ．MI 暗号

Matsumoto and Imai[1983,1988]、松本・今井等[1982,1984,1985]は「個々の関数の逆関数を求めることは容易であっても、それらを合成した関数の逆関数を求めることは個々の関数を知らない限り極めて困難であるように関数を構成する」という「obscure 表現」に安全性の根拠を置く一連の高速公開鍵暗号を提案している。この場合、個々の関数を秘密とし、合成した関数のみを公開すれば、落し戸付き一方向性関数が得られる。初期の 1 変数多項式を用いた方式（Matsumoto-Imai[1983]）は Delsarte et al.[1985]により解読法が示された。そこで、1988 年に多変数多項式系を用いた方式（Matsumoto-Imai[1988]）が提

案されている[7]。

2. 秘密通信方式

秘密通信のみができる代表的方式としては、離散対数問題（DLP）の困難性に基づく「ElGamal 暗号」、 楕円曲線上で定義された有限可換群上の離散対数問題（EDLP）に基づく「DL 楕円暗号」、選択暗号文攻撃に対し強秘匿を満足し、かつ頑健性を保持した「安全な」暗号方式である「OAEP（optimal asymmetric encryption padding）」等が挙げられる。これらの方式について以下順次説明する。

(1)ElGamal 暗号

ElGamal[1984]は、Diffie-Hellman 鍵共有法を変形することにより最初の離散対数問題（DLP）の困難性に基づく公開鍵暗号を構成した。DLP に基づく方式では、FP に基づく方式のように暗号・復号化の過程に自然な形で落し戸を仕掛けることができない。このため、ElGamal は暗号通信の際、秘密の乱数を生成し、同乱数を利用した暗号・復号化の仕組みを実現した。

【手順】A から B へ平文 M を秘密通信する場合の手順を紹介する。

[鍵生成] 受信者 B は次のように鍵を生成する。まず、大きな素数 p と乱数 $x \in_R Z^*_p$ を生成する。次に、p の原始根 α を適当に選んだ後、 $y = \alpha^x \mod p$ を計算する。

秘密鍵：x

公開鍵：(y, p, α)

[暗号化] A は乱数 k を生成した後、B の公開鍵 y を用いて次の二組の暗号文 C_1, C_2 を作成する。

$$C_1 = \alpha^k \mod p \tag{34}$$

$$C_2 = My^k \mod p \tag{35}$$

[復号化] B は自分の秘密鍵 x を用いて次式から元の平文 M を得る。

$$MC_1^{xB} = C_2 \mod p \tag{36}$$

【安全性】

イ．基本的安全性

ElGamal 暗号の基本的な安全性は DLP の困難性に根拠を置いている。公開鍵から秘密鍵を求める問題は DLP である。また、暗号文(C_1, C_2)を入手し

[7] 同方式の一具体例は Patarin[1995]により解読法が示されたが、同方式の枠組み自体は現在でも崩れていない。

た場合、C_1から乱数 k を求めることができれば C_2に y^k の逆数を乗ずることにより平文を復元できるが、C_1から k を求める問題も DLP にほかならない。

ロ．部分情報の安全性

DLP においては、解の最下位 bit は多項式時間で求められることが知られているものの、同最上位 bit を求めることは DLP を解くことと同程度に難しいことが証明されている（Blum and Micali [1982]）。

ハ．利用上の留意事項

ａ．乱数 k 変更の必要性

乱数 k は通信の都度、変えなければならないことに留意したい。これは、同一の k で異なる二つの平文(M_a,M_b)を暗号化した場合、対応する暗号文(C_a,C_b)との間に次の単純な関係が成立するからである。

$$\frac{M_b}{M_a} = \frac{C_b}{C_a} \tag{37}$$

従って、M_aと C_aの組が分かると、C_bから M_bを知ることができる。

ｂ．故障利用暗号攻撃

ElGamal 暗号等の送信者が生成する乱数を秘密情報として利用する公開鍵暗号において、攻撃者が乱数を入手できる場合は Zheng and Matsumoto[1996]が考案した故障利用暗号攻撃が成立する。すなわち、乱数 k が入手できたとすると、暗号文 (C_1,C_2)から次式により平文を算出できる。

$$M = \frac{C_2}{y^k} \mod n$$

(2)EDLP に基づく暗号（DL 楕円暗号）

1985 年に有限体 F で定義された楕円曲線の点のなす有限可換群[8]上の離散対数問題（EDLP）の困難性を安全性の根拠にする公開鍵暗号（以下、DL 楕円暗号と呼ぶ）の概念が発表された（Koblitz[1987], Miller[1986]）。 DLP には準指数関数時間の解法（指数計算法）が存在するのに対し、EDLP にはある種の楕

[8] 同有限可換群については「付 3 有限体上の楕円曲線の基礎事項」参照。

円曲線を除いて指数計算法の適用が困難なため、EDLP に基づく暗号・署名方式は従来の方式に比べ鍵長を大幅に短縮できるといわれている。加えて、EDLP に基づく公開鍵暗号の概念自体は特許が取得されていない[9]こともあって、次世代の公開鍵暗号として脚光を浴びている。こうした中、松下電器産業、Certicom（カナダ）、Next（アメリカ）、Siemens（ドイツ）、Thompson（フランス）等、各社において、EDLP に基づく暗号・署名方式を実装化した製品が販売されつつある。

DL 楕円暗号の他の利点として、各利用者が異なる楕円曲線を選べば同一の体 F_q を用いても安全性は保たれることが挙げられる。これは全ての利用者が体 F_q の演算を実行する共通のハードウェアを用いることができることを意味している。

DL 楕円暗号は、有限体上の要素を楕円曲線上の要素に、有限体上の乗法を楕円曲線上の加法に、それぞれ対応させることにより定義される。このとき、有限体の要素の r 乗は楕円曲線の要素の r 倍に対応し、通常有限体の要素の r 乗を計算するのに用いられる高速指数演算法も楕円曲線の要素の r 倍を計算するのに用いることができる。従って、既存の DLP に基づく暗号・署名方式を自然な形で EDLP に基づく方式に変換できるのである。実際、DL 楕円暗号の代表的な具体方式は ElGamal 暗号を上記対応により EDLP に基づく方式に変換した暗号（以下「ECElG 暗号」と呼ぶ）である。従って、ECElG 暗号の手順は次に示すように ElGamal 暗号と本質的に同手順となる。

【手順】 A から B へ文書 m を暗号化して送信する場合を考える。ここで M は m に対応する $E(F_q)$の要素、$P \in E(F_q)$は位数が大きな素数で割れる要素とする。

[鍵生成] 受信者 B は次のように鍵を生成する。まず、正整数 $x \in_R Z^*_p$ を選び、E 上で $Y=xP$ を計算する。

秘密鍵：x

公開鍵：$E(F_q),P,Y$

[暗号化] 送信者 A は乱数 r を選び E 上で

$$C_1 = rP \tag{38}$$

$$C_2 = M+rY \tag{39}$$

を計算し、(C_1, C_2)を B へ送る。

[復号化] B は秘密鍵 x を用いて E 上で

$$C_2-xC_1 = M \tag{40}$$

[9] 但し、EDLP に基づく暗号・ディジタル署名方式は安全性・効率性が具体的な構成法に依存するためこれに関連した特許はいくつか出願・登録されている。

を計算した後、M に対応する文書 m を得る。

上述の文書 m（$0 \leqq m < l$ の整数）から $E(F_q)$上の要素 M への変換と逆変換は暗号化・復号化処理の実行時間に影響を与えるほどのものではない。[10]

【安全性】

イ．基本的安全性

ECElG 暗号等の EDLP に基づく暗号（DL 楕円暗号）の基本的安全性は有限体で定義された楕円曲線の点のなす有限可換群上の離散対数問題（EDLP）の困難性に依存している。同問題は通常の有限体上の離散対数問題（DLP）に対する高速解法である指数計算法が適用不可とされていたが、その後、ある性質を満たす EDLP は DLP に帰着する方法、所謂「MOV 帰着」（Menezes-Okamoto-Vanstone[1991]）が示された。そこで、現在ではこうした帰着法を無効にするような EDLP のいくつかの構成法が提案されている。このとき、楕円曲線 $E(F_q)$に関する EDLP に対する最も高速な解法は Pohlig-Hellman のアルゴリズムで、同アルゴリズムによる概算の平均計算量 $T(q)$は次の通り。

$$T(q) = O\left((\#E(F_q))^{1/2}\right)$$

ロ．プロトコルの安全性

ECElG 暗号の安全性を他の暗号プロトコルとの比較で述べると、楕円曲

---

[10] 平文 m を $E(F_q)$上の要素 M に対応させる方法は以下の通りである。正整数 k を $0 < kl < q$ となるようにとる。$1 \leqq i \leqq k$ なる整数 i に対して $x_{m,i}=mk+i$ とおき、これを p 進展開する。すなわち、

$$x_{m.i} \quad \sum_{i=0}^{r-1} a_i \, p^i \quad (0 \leqq a_i \leqq p-1)$$

この係数 a_i を用いて $x_{m,i}$ を F_q の要素に対応する F_p 上の r-1 次の多項式

$$\sum_{i=0}^{r-1} a_i X^i$$

に対応させる。こうして得られる F_q の要素を $x'_{m,i}$ とする。そこで $f(x'_{m,i})$が F_q の平方数となる最小の i に対して $x_{m,i}=x_m$ とし、,この x_m を用いて平文 m を $E(F_q)$の要素

$$M \quad = \quad (x'_m \, , f(x'_m)^{0.5})$$

に対応させる。なお任意の $1 \leqq i \leqq k$ なる i に対して $f(x'_m)(x_m=mk+i)$が平方数になる確率はほぼ 1/2 であるため、この方法により平文 m が $E(F_q)$の要素に対応できない確率は約$(1/2)^k$となることが分かる。また逆に $E(F_q)$の要素 M の x 座標 x_m に対応する x_m を用いて、

$$m \quad = \quad \left| \frac{x_m - 1}{k} \right|$$

とおくことにより要素の平文 m を得ることができる。

線の要素数が素数の場合、ECElG 暗号の安全性は DH 鍵共有法と等価となることが示されている（Sakurai and Shizuya[1995]）。

ハ．利用上の留意事項

ECElG 暗号は ElGamal 暗号を有限体で定義された楕円曲線の点のなす有限可換群上に置き換えたものに過ぎないため、同暗号のプロトコルの安全性は ElGamal 暗号のプロトコルの安全性に関する議論が基本的に当てはまる。従って、同じ乱数を 2 回以上用いれば 1 対の暗号文・平文から同一乱数の暗号文は全て解読される。また、攻撃者が擬似乱数生成器等に物理的影響を与えることにより乱数を入手できる場合は Zhen and Matsumoto[1996]の故障利用暗号攻撃が成立し、暗号文から容易に平文が算出される。

(3)OAEP（「安全な」暗号方式）

Ⅰ 3.(1)で述べたように適応的選択暗号文攻撃を許したとしても強秘匿でかつ頑健性を保持した方式が最も安全であり、このような公開鍵暗号を「安全な」公開鍵暗号と呼んだ。最近、Bellare and Rogaway[1995]により発表された OAEP（optimal asymmetric encryption padding）は「安全な」公開鍵暗号であるが、同暗号につき説明する前に、このような「安全な」公開鍵暗号の研究経緯を簡単に振り返る。

まず、Goldwasser-Micali[1984]は「素因数分解が困難ならば合成数を法とする平方剰余性の判定が困難である」という仮定を前提に選択平文攻撃に対し強秘匿を満足する暗号（Goldwasser-Micali 暗号）を構成した。しかしながら、Goldwasser-Micali 暗号は選択暗号文攻撃によって容易に解読される。

選択暗号文攻撃に対し強秘匿を満足する暗号の研究は Blum, Feldman, and Micali[1988]により始められた。彼らは同問題の解決に零知識非対話証明（non-interactive zero-knowledge proof、以下 NIZK と略記）が有効なことを示唆した。ここで、零知識証明とは、ある者（証明者）がある知識を有することを当該知識に関する情報を一切漏らすことなく他者（検証者）に証明する方法のことである。零知識非対話証明は、信頼できる第三者の下で証明者から検証者の片方向のみのデータ送信で、零知識証明を実現する方法である[11]。彼らの研究に触発された Naor-Yung[1990]は適応的選択暗号文攻撃に対し部分解読すら許さない暗号を NIZK に基づいて構成した。その後、適応的選択暗号文攻撃に対し強秘匿を満足する Naor-Yung 暗号よりも実用的な暗号方式が Damgard[1992]と Zhen and

[11] これに対し、もう一つの零知識証明である零知識対話証明（zero-knowledge interactive proof、通常 ZKIP と略される）では、証明者・検証者間で双方向の通信が許される。

Seberry[1993]によって提案された。しかしながら、何れにせよこれらの暗号は頑健性を保証する方式ではない。

頑健性を持つ暗号方式は Dolev, Dwork, and Naor[1991]により最初に実現されたが、同方式は非常に非効率的である。

Bellare and Rogaway[1993]は仮想的なランダム関数を前提として適応的選択暗号文攻撃に対し強秘匿及び頑健性を満足する効率的な方式を最初に実現した。その後、同方式を彼らがさらに効率化した方式が OAEP である（Bellare and Rogaway[1995]）。RSA 暗号を利用した OAEP はインターネット上でのクレジットカード決済のプロトコルである SET[12]でも採用されている。

OAEP の暗号化関数は文書 $m \in \{0,1\}^n$ に対し次のように与えられる。

$$f(m0^{k1}) + G(r) \,\|\, r + H(m0^{k1} + G(r))$$

ここで、f は落し戸置換、G は理想的擬似乱数生成器、H は理想的ハッシュ関数、r は乱数、＋は bit 毎の排他的論理和、0^{k1} はパディングである。

Bellare and Rogaway[1995]は OAEP の具体的な構成法として、落し戸置換 f に RSA 暗号を用い、関数 G、H を実在のハッシュ関数 SHA（Secure Hash Algorithm）[13]から構成する方式を提案している。理想的擬似ランダム関数或は理想的ハッシュ関数に課される条件は非常に厳しいため SHA のような実在の関数から構成された関数はこうした条件を満たし得ない。従って、このように具体化された OAEP を「安全な」暗号とみなすことはできないが、効率的かつ「安全な」暗号方式実現に向けての一里塚に到達したとみることはできよう。仮想的なランダム関数といった非現実的な前提を緩めたより現実的な前提に基づく効率的かつ「安全な」暗号方式の研究の動向に注視する必要があると思われる。

(4)その他

秘密通信に特化したその他の代表的な方式としては、ナップザック問題に基づく一連の「ナップザック暗号」、誤り訂正符号の復元問題に基づく「McEliece 暗号」が挙げられる。しかし、これらは既に解読法が示されている。

---

[12] SET(Secure Electronic Transactions)は、VISA と Mastercard が提案し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。SET に準拠したクレジットカード決済実験が世界各地で行われており、de facto standard と目されている。

[13] SHA は米国国防総省の下部機関である NSA（National Security Agency）により開発された米国連邦政府標準ハッシュ関数で、現在ハッシュ関数の主流となっている MD 方式の一つである。

イ．ナップザック暗号

ナップザック暗号とは、Merkle-Hellman[1978]が開発した Merkle-Hellman 暗号を契機に相次いで提案されたナップザック問題に基づく一連の暗号方式の総称であり、代表的なナップザック暗号としては、Merkle-Hellman 暗号のほか、同暗号の改良版である反復 Merkle-Hellman 暗号（Merkle[1978]）、 Graham-Shamir が提案した Graham-Shamir 暗号（Shamir[1980]）、Chor-Rivest 暗号（Chor-Rivest[1984]）等が挙げられる。同問題に基づく署名方式は殆ど無く有名な方式は Shamir[1978]が提案した Shamir 署名程度である。ナップザック問題とは、例えば「長さが知られている n 本の棒があるとする。これらのうちの何本かを用いて、ある定められた長さの細長い箱に隙間が生じないように詰めよ」という問題である。同問題は次のように定式化される。

正整数 c、正整数を要素に持つ n 次元ベクトル（ナップザック・ベクトル）$\boldsymbol{a} = (a_1,a_2,\cdots,a_n)$が与えられたとき、

$$c = \boldsymbol{a}^t\boldsymbol{m} = \sum_i a_i m_i \tag{41}$$

となるような 2 進数ベクトル $\boldsymbol{m} = (m_1,m_2,\cdots,m_n)$を求めよ。

上記問題は解 M を具体的に求めることが要求される探索問題である。与えられたナップザック問題の解が存在するかどうかを判定する問題（判定問題）は問題のサイズ n が大きくなるにつれて解くのが急激に難しくなる「NP 完全問題」である。探索問題は判定問題よりも一般的に難しく、ナップザック探索問題は NP 完全問題よりも一般的に難しい NP 困難問題であることが知られている[14]。

しかしながら、これまで提案されたナップザック暗号は落し戸を仕掛けるためナップザック探索問題に何らかの制約や特徴が付加された形の問題に基づいて構築されている。すなわち、最初に提案された Merkle-Hellman 暗号はナップザック・ベクトルが $a_i > a_1+\cdots+a_{i-1}$ $(i=2,\cdots,n)$を満たす超増加数列という厳しい制約条件が付けられた「やさしい」ナップザック問題[15]を変換することに

---

[14] 通常のアルゴリズムにより問題のサイズ n の多項式時間で解ける問題を「P 問題」、問題を解く過程で現れる分岐を正しく選べる特殊なアルゴリズムを用いれば問題のサイズ n の多項式時間で解ける問題を「NP 問題」と呼ぶ。NP 困難問題とは全ての NP 問題がこれに多項式時間帰着する問題のことである。因みに、「NP 完全問題」とは NP 困難問題のうち特に NP 問題であるものを指す。

[15] 「やさしい」ナップザック問題は問題のサイズ n に比例した計算量で解けることが知られている。

より実現されたものである。Shamir[1982]はナップザック・ベクトルが超増加数列であるという性質を利用し秘密鍵を求めることなく殆ど全ての暗号文を n の多項式時間で解けることを示した。Graham-Shamir 暗号は落し戸を仕掛けるための超増加数列が表に現れないよう巧みに設計されているが、ナップザック・ベクトルの次元数と最大要素の比が小さくなる低密度と呼ばれる特徴があった。ナップザック・ベクトルが低密度の場合、たとえ超増加数列に基づいて生成されていなくとも一般的に解読されることは Lagarias and Odlyzko（Lagarias[1984]）、Brickell [1983]によって明らかにされた。これらの解読法は何れもラティス基底縮小アルゴリズム（LLL アルゴリズム[16]）に基づいている。反復 Merkle-Hellman 暗号の解読（Adleman[1982]、Brickell[1982]）、Shamir 署名の解読（Odlyzko[1984]）においても LLL アルゴリズムが適用されている。Chor-Rivest 暗号は超増加数列に全く基づいていない上、密度も低くならないように構築されていることから、つい最近まで解読法が発見されていなかったが、最近になって Schnorr and Hörner[1995]により有力な解読法が示された。

ここでは紹介できなかったナップザック暗号も数多くあり、中には解読法が示されていない方式も存在すると思われるが、上にみたようにこれまで多くのナップザック暗号が解読されていることを考慮すると、たとえ現在は解読法が示されていない方式であってもナップザック暗号の利用は推奨し難い。

ロ．McEliece 暗号

McEliece[1978]は、Goppa 符号と呼ばれる線形の誤り訂正符号を一般的に復元する問題（NP 完全問題）の難しさに基づく公開鍵暗号（McEliece 暗号）を提案した。McEliece 暗号は、$GF(2)$上の多変数 1 次式タプルの逆関数の計算が、秘密鍵を知っていると容易だが、知らない場合は難しいという事実に基づいている。McEliece 暗号は RSA 暗号よりも数十倍から数百倍高速であるものの、公開鍵が 2^{19} bit（約 500,000bit）と途方もなく長いほか、暗号文長が平文長の 2 倍であるなど、実用的とは到底言い難いものであった。こうした中、同暗号に対する解読法が Norzhik and Turkin[1991]により示された。

上記解読法が決定的とまで言えるほどのものかどうかは議論の余地が残されているようであるが、効率性・安全性の両面から McEliece 暗号の利用は推

[16] Merkle-Hellman 暗号に対する Shamir[1982]の解読法は、変数の数が固定された数理計画法を多項式時間で解く Lenstra[1981]のアルゴリズムに基づいている。しかし、同アルゴリズムを Merkle-Hellman 暗号に適用した場合は変数の個数に対し指数関数時間の計算量となる。LLL アルゴリズムは、Lovasz が Lenstra のアルゴリズムを一部改良し、変数の個数に対し多項式時間で解けるようにしたものである。

奨し難い。

3. ディジタル署名方式

ディジタル署名に特化した代表的な方式としては、離散対数問題（DLP）の困難性に基づく「ElGamal 署名」、同署名の改良版である「Schnorr 署名」と「DSA 署名」、素因数分解問題（FP）と合同多項不等式求解問題の困難性に基づく「ESIGN 署名」、ZKIP を利用した「Fiat-Shamir 署名」、楕円曲線を利用した「EDLP に基づく署名法」が挙げられる。このほか、合同多項式求解問題の困難性に基づいていたが既に解読法が示された「Ong-Schnorr-Shamir 署名」、NIZK を利用した「Bellare-Goldwasse 署名」を紹介する。

Ⅰ 3.(2)において適応的選択文書攻撃を許したとしても存在的偽造が不可能な署名方式を「安全な」ディジタル署名方式と呼んだ。この最も強い意味での安全性が、暗号学的に「理想的な関数」の存在と FP、DLP 等の困難性を前提にすれば、上記諸方式において成立することが示されていることをみておく。但し、前述の OAEP と同様に実際には「理想的な関数」は存在しないため、このことが上記諸方式の安全性を必ずしも保証するものではないことに留意したい。

まず、「仮想的なランダム関数」の存在を前提にすれば RSA 関数や ESIGN 関数の解読が困難であると仮定して RSA 署名や ESIGN 署名が選択暗号文攻撃を許したとしても存在的偽造さえ不可能という意味で「安全で」あることが証明される（Bellare and Rogaway[1996]）。また、同前提の下で FP や DLP が困難であると仮定すれば Schnorr 署名、拡張 Fiat-Shamir 署名、改良 ElGamal 署名が「安全で」あることが証明される（Pointcheval and Stern[1996]）。さらに、仮想的なランダム関数よりも弱い仮定である「無相関一方向性関数（correlation-free one-way hash function）」の存在を前提とすれば FP や DLP が困難であると仮定して Fiat-Shamir 署名が「安全で」あることが証明される（Okamoto[1993]）。

(1)ElGamal 署名

ElGamal 署名（ElGamal[1984]）は最初に発表された離散対数問題（DLP）の困難性に基づく署名方式である。DLP は現時点では FP とほぼ同等の困難性があると評価されている。ElGamal 署名は RSA 暗号による署名方式の場合とは異なり共通法プロトコルを利用できるという利点がある反面、①署名の都度、秘密の乱数を必要とする、②署名長が法の長さの 2 倍となるという問題がある。②の問題は ElGamal 署名の改良版である Schnorr 署名、DSA 署名で解決されている。

①の問題は現時点でも解決されておらず、この点で、ElGamal 系の署名は RSA 暗号を用いた署名よりも劣ると、一般的にはみられている。しかしながら、RSA

暗号では利用者が秘密鍵を生成する際に、弱鍵に留意しなければならないのに対し、ElGamal 系署名では法 p、底 α を利用者共通の値として安全な値に設定しさえすれば、秘密鍵の生成には留意せずとも安全性に問題は生じないとされている[17]。今後、FP、DLP の一般的解法が大きく進歩する可能性はあまり大きくないとしても、素数の性質に依存する特殊な解法は大きく進歩する可能性は小さくないと予想されることを併せ考えると、この点では RSA 暗号を用いた署名よりも ElGamal 系署名の方が優っていると思われる。

【手順】A から B へ文書 M の署名を送信する手順を以下に示す。

[**鍵生成**] 署名者 A は次の手順で鍵を生成する。大きな素数 p と秘密鍵 $x \in_R \boldsymbol{Z}^*_p$ を選び、$y = \alpha^x \bmod p$（但し、α は法 p のもとでの原始根）を計算する。

秘密鍵：x

公開鍵：y, p, α

[**署名**] A は乱数 k を生成し、次の r を計算する。

$$r = \alpha^k \bmod p \tag{42}$$

次に、A は自分の秘密鍵 x と r, k を用いて、次の t を算出する。

$$t = \frac{M - xr}{k} \bmod p\text{-}1 \tag{43}$$

A は B に文書 M と署名 $S = (r, t)$を送る。

[**検証**] B は A の公開鍵 y を用いて、次式が成立するかどうかを検証する。

$$\alpha^M = y^r r^t \bmod p \tag{44}$$

【安全性】ElGamal 署名では、全面的解読に対する安全性のみならず、一般的偽造に対する安全性についても DLP の困難性が根底をなしている。

イ．全面的解読に対する安全性

所与の y, p, α に対し、$y = \alpha^x \bmod p$ を満たす x を求める問題は離散対数問題と呼ばれる。ElGamal 署名の公開鍵(y, p, α)から秘密鍵 x を求めることは離散対数問題を解くことにほかならない。従って、 ElGamal 署名の全面的解読に対する安全性は DLP の困難性に基づいている。DLP は同問題が注目され始めた 10 年ほど前までは素因数分解問題（FP）よりも困難ではないかと思われていたが、その後、解法が急激な進展を遂げた結果、現在では FP

[17] 素因数分解問題では、Fermat 法、p-1 法等の素数に依存した攻撃法が存在するのに対し、離散対数問題では法 p に依存した攻撃法はあっても指数 x に依存した攻撃法は知られていない。

の最高速の解法である数体ふるい法と同速度の解法が示されている。この意味において、現時点では法が同サイズの RSA 系暗号と ElGamal 系暗号の全面的解読に対する安全性は同等となっている。現在 DLP の最速解法とされている Schirokauer[1993]、Adleman[1994]のアルゴリズムの漸近的かつ平均的な計算量 $T(q)$は次式のような準指数関数時間で評価されている。

$$T(q) = \exp((1.922+o(1))(\log q)^{1/3}(\log\log q)^{2/3})$$

ロ．一般的偽造に対する安全性

ElGamal 署名の一般的偽造に対する安全性は全面的解読に対する安全性と同様に DLP の困難性に基づいている。このことを確認するために、ElGamal 署名に対し、A の秘密鍵 x を知らない者が A の署名を偽造する方法を考察してみよう。攻撃法としては、次の四つが考えられる。

① 文書 M と署名の一部 r を適当に選択した上で、これらに対応する t を求める。

② 文書 M と署名の一部 t を適当に選択した上で、これらに対応する r を求める。

③ 署名 $S = (r, t)$を適当に選択した上で、これらに対応する文書 M を求める。

④ 関係式を満たす文書 M と署名 $S = (r, t)$を同時決定する。

攻撃①は離散対数 $t = \log_r \alpha^M y^{-r} \bmod p$ を計算する問題に帰着される。

攻撃②は未知変数 r に関する次の方程式を解く問題に帰着される。

$$y^r r^t = \alpha^M \bmod p \tag{45}$$

同問題は解けないことが証明されている訳ではないが、解けないと予想されている有名な問題である。

攻撃③も離散対数 $M = \log_\alpha y^r r^t \bmod p$ を計算する問題に帰着される。

攻撃④については、次の計算により一応実現できる。

$$r = \alpha^i y^j \bmod p \tag{46}$$

$$t = -rj^{-1} \bmod p\text{-}1 \tag{47}$$

$$M = -r\,i\,j^{-1} \bmod p\text{-}1 \tag{48}$$

但し、$0 \leqq i \leqq p\text{-}2$, $0 \leqq j \leqq p\text{-}2$, $\mathrm{GCD}(j, p\text{-}1)=1$。

しかしながら、同攻撃では文書 M を制御できないので、実際の脅威とは成り得ないと思われる。

以上の考察から、ElGamal 署名の一般的偽造に対する安全性は DLP の困難性に基づいているといえよう。

ハ．利用上の留意事項

ElGamal 署名では、ElGamal 暗号と同様に「乱数 k 変更の必要性」があるほか、「公開鍵 p, α の選び方」に留意しなければならないことが指摘されている。

ａ．乱数 k 変更の必要性

ElGamal 暗号と同様に、乱数 k の取扱いにおいては、次の二つの点に十分に留意する必要がある。

① 乱数 k は、たとえ過去に使用したものであっても、外部に漏らしてはならない。
② 二つの異なる文書に署名する際に同じ k を用いてはならない。

①の点に留意しなければならないのは、ある者が過去に使用された乱数 k に加え、これが用いられたときの署名付き文書 $M, S = (r, t)$を知り得た場合、次式より簡単に秘密鍵 x を計算できるからである。

$$x = \frac{M - k\,t}{r} \mod p\text{-}1 \tag{49}$$

留意点②も、これを守らなければ秘密鍵 x を求められるという意味で極めて重要なものである。ある者が同じ k を用いて作成された二組の文書と署名$(M_1, r, t_1), (M_2, r, t_2)$を偶然に知り得たとしよう。この場合、彼は

$$y^{r} r^{t1} = \alpha^{M1} \bmod p \tag{50}$$

$$y^{r} r^{t2} = \alpha^{M2} \bmod p \tag{51}$$

から、直ちに未知数 k に関する次の方程式を得ることができる。

$$k(t_1 - t_2) = M_1 - M_2 \bmod p\text{-}1 \tag{52}$$

上式から k を求めた後、何れかの署名付き文書を利用して秘密鍵 x を求めることができる。

ｂ．公開鍵 p, α の選び方に関する安全性

つい最近になって、公開鍵である p, α の値如何では秘密鍵の値を知らなくても簡単に一般的偽造がなされることが次の定理により示された（Bleichenbacher[1996]）。

定理（ElGamal 署名の一般的偽造法） $p - 1 = nq$（但し n はスムーズ）とする。もし、$b^{t} = \alpha \pmod p$となるような $b = lq$（但し $0 < l < n$）と整

数 t が知られていれば、このとき任意の文書 M に対し偽造署名(r, t)を求められる。

証明） 定理の条件が満たされている場合、任意の文書 $M \in F_p^*$に対し、$r = b, s = tm \pmod q$と設定できる。このとき、 $\alpha^M y^r r^{-st} = \alpha^M \alpha^{-tM/t} = 1$ に示されるように、(r, s)は文書 M に対する妥当な署名となっている。

所与の F_p と α に対し上記 b をみつけることは一般的には難しいが、ある機関が利用者に F_p と α を提供する場合、同機関は落し戸 b を次のアルゴリズムにより仕掛けることができる。すなわち、まず F_p と p-1 の約数 q を定める。p-1 = qn とする。次に b の次数が q となるような $b = l^q$ ($l \in \{1,\cdots,n\text{-}1\}$)をみつける。最後に、$1 < t < q$-1 に対し基点を $\alpha = b^t \pmod p$と設定する。一般的には n は十分に大きいため同アルゴリズムは巧く機能する。また、明らかに落し戸 b の存在は容易に認識できない。従って、ElGamal 署名では、他者から F_p と α の提供を受けるべきではないと結論付けられよう。

しかし、同偽造法は r が p-1 のある大きな素因数 q を約数として持たない限りは回避できる。署名者がランダムに生成した r が q によって割り切れる確率は極めて小さいため、無作為に生成される署名は殆どの場合偽造のおそれはないが、署名検証者側は同条件が満たされているかどうかを常に検査すべきであろう。

ところで、後述する改良型 ElGamal 署名である DSA 署名に適用できるかどうかであるが、同署名の場合は $r = b$ とはならないため、同偽造法を DSA 署名に直接適用することはできない。

c．故障利用暗号攻撃に対する安全性

送信者が生成する乱数を秘密情報として利用する公開鍵暗号において攻撃者が乱数を入手できる場合は Zheng and Matsumoto[1996]が考案した故障利用暗号攻撃により全面的解読が成立する。すなわち、攻撃者が擬似乱数生成器等に物理的影響を与えることにより乱数 k を入手できる場合は、文書 M と署名 $S = (r, t)$から次式により秘密鍵を算出できる。

$$x = \frac{M - kt}{r} \pmod{p\text{-}1}$$

攻撃者が乱数を入手できれば上記解読は容易に実行される。但し、前

述の通り、通常は攻撃者が攻撃の対象とする暗号装置に自由にアクセスできるような運用はなされないため、同攻撃が実際の脅威となることは少ないであろう。

(2)ESIGN 署名

「ESIGN 署名」は NTT の Okamoto[1990]により提案された高速処理を特徴とするディジタル署名方式である[18]。 同方式は、FP 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。なお、ESIGN 署名の楕円曲線上への拡張が Okamoto et al.[1993]により提案されている。

【手順】A が文書 M の署名を生成し B が同署名を検証する手順を以下に示す。

[**鍵生成**] 署名者 A は鍵を次のように生成する。まず、大きな素数 p,q を $p>q$ を満たすように選ぶ。$n=p^2q$, $k>3$ とする。

秘密鍵：(p, q)

公開鍵：(k, n)

[**署名生成**] A は空間 $\boldsymbol{Z}_{pq}^{*}$から乱数 x を生成する。そして、次の計算を行う。

$$w = \frac{h(M)-(x^k \bmod n)}{pq} \tag{53}$$

$$y = \frac{w}{kx^{k-1}} \bmod p \tag{54}$$

$$s = x+ypq \tag{55}$$

A は B に文書 M と署名 s を送る。

[署名検証] B は A の公開鍵 k を用いて、署名の正当性を次式の成否により検証する。

$$h(M) \leqq s^k \bmod n < h(M)+2n^{2/3} \tag{56}$$

【安全性】ESIGN 署名は署名の検証式に不等式を用いるなどやや複雑な構成を採っているため、安全性分析もやや複雑になる。以下では、「受動的攻撃による全面的解読に対する安全性」、「受動的攻撃による一般的偽造に対する

[18] Okamoto[1986,1987]は ESIGN 署名と同様の発想に基づく暗号方式を二つ提案しているが、最初に提案した方式は Shamir に、同方式の修正版は Vallée et al.[1988]により、それぞれ解読法が示されている。

安全性」、「選択文書攻撃に対する安全性」の三つに分類して、同署名方式の安全性を検討する。

イ．受動的攻撃による全面的解読に対する安全性

ESIGN 署名の秘密鍵導出に対する耐性は RSA 暗号と同様に合成数 n を p^2q に素因数分解することの困難さに基づいていると考えられる。素因数分解以外の攻撃法としては、

① 署名 s からの p,q の導出

② 既知文書攻撃により入手した署名等から形成される連立方程式からの p,q の導出

③ 既知文書攻撃により入手した署名集合$\{s_j \mid j=1,\cdots,J\}$或は集合$\{t_j \mid t_j = (s^k \bmod n)\text{-}h(M), j=1,\cdots,J\}$からの p,q の統計的推測

が考えられる。

しかし、攻撃①については、署名 s は乱数 x に依存しているため、p,q は乱数 x の値を知り得ない以上 s から導出することは不可能である。

攻撃②は次の連立方程式を解くことを意味している。

$$n = p^2q \tag{57}$$

$$w_i = \frac{h(m)-(x_j^k \bmod n)}{pq} \qquad (j=1,\cdots,J) \tag{58}$$

$$y_i = \frac{w_i}{kx_j^{k-1}} \bmod p \qquad (j=1,\cdots,J) \tag{59}$$

$$s_j = x_j+y_jpq \qquad (j=1,\cdots,J) \tag{60}$$

上記連立方程式は、未知変数の個数$(3J+2)$が連立方程式の本数$(3J+1)$を上回っているため解けない。

攻撃③についても、まず乱数系列$\{x_j\}$が Z_{pq}^*上で一様に分布しているため$\{s_j\}$は Z_n^*上に一様分布しており$\{s_j\}$から p,q を推測することは不可能となる。他方、$\{t_j\}$は Z_{pq}上の一様分布となるため、系列$\{t_j\}$が十分に長ければ pq は系列$\{t_j\}$の統計的推測値から推測することが一応可能。しかしながら、実際には攻撃者は高々10^{10}程度の$\{t_j\}$しか収集できないであろう。この場合、推測し得る pq のオーダーも 10^{10}程度に過ぎないため、$\{t_j\}$からの統計的推測による攻撃も脅威とはならない。

ESIGN 署名の安全性の根幹となる FP に関しては、RSA 系の暗号とは別の留意点がある。すなわち、RSA 系暗号は合成数 n のサイズに依存する解法

の中で最高速の解法である数体ふるい法のみを警戒していれば事足りるのに対し、ESIGN 署名では合成数が $n=p^2q$ の形をしているため合成数 n のサイズと最少の素因数 q のサイズ如何では最少の素因数 q に依存する解法である楕円曲線法が最高速の解法と成り得ることである。

ロ．受動的攻撃による一般的偽造に対する安全性

受動的攻撃による一般的偽造法としては、所与の文書に対し出鱈目に生成した署名が検証式を満たすかどうかを次々と試していく「盲目攻撃」、署名検証に用いられている合同多項不等式を「合同多項式問題」または「合同多項不等式求解問題」として解くことにより検証式に合格する署名を偽造する方法が挙げられる。

ａ．盲目攻撃

乱数により署名 s を偽造しようとする盲目攻撃の成功確率は僅か $\exp(-(\log n)/3)$ に過ぎないため脅威とは成り得ない。

ｂ．合同多項式求解問題

署名検証に用いられている合同多項不等式は次の合同多項式が解ければ解ける。

$$s^k = h(M) \bmod n \qquad (61)$$

しかし、上記問題は RSA 暗号の暗号文から平文を求める問題と同等か、ないしはそれ以上に難しいように思われる。

ｃ．合同多項不等式求解問題

ESIGN 署名の検証式は未知の素因数の合成数を法とする累乗根の近似値を効率的に求めることができれば同署名が偽造されることを意味しているが、これは $k \geqq 4$ の場合に対しては未解決の問題である。ESIGN 署名が Okamoto and Shiraishi[1985]により最初に提案されたときには、k は 2 に設定されていたが、Brickell and deLaurentis[1986]により直ちに署名偽造法が発表された。同偽造法は $k=3$ の場合にも適用し得る。また、$k=2$ の場合に対しては Shamir も異なる偽造法を示している。現在では、ESIGN 署名の開発者は k,p,q,n の値を安全性の観点から次のように設定することを推奨している。

k: 8,16,32,4,128,256,512,1024

p,q: 192 bits 以上

n: 576 bits 以上

以下では、Shamir の偽造法と k=3 の場合に対する Brickell and deLaurentis[1986]の偽造法を紹介した後、k≧4 の場合（現行 ESIGN 署名）の安全性に関する議論を簡単に纏めておこう。

① k=2 の場合に対する Shamir の署名偽造法

偽造者は所与の $h(M)$に対し $h(M) \leqq s^2 \bmod n < h(M)+2n^{2/3}$ を満たすような署名 s の偽造を目論む。偽造者は、r を適当に選択した上で、次式を満たす x を計算する。

$$2rx-h(M)+r^2 \bmod n \ < 2n^{2/3} \ (1 \leqq x < n^{1/3}) \qquad (62)$$

このような x は、$n^{2/3}$ 個の $h(M) \bmod n$ に対する署名結果が[0, n]区間に一様に分布する場合は殆ど全ての r に対して存在すると期待できる。x が存在するのであれば、それは拡張ユークリッドの互除法と類似の方法を利用して容易に求められる。このとき、$s = r+x$ が偽造署名となる。

② k=3 の場合に対する Brickell and deLaurentis の署名偽造法

偽造者は r = [n/3](i.e., $r = n/3+a$ for $|a| \leqq 1/2$)を満たす r を適当に選択した後、$z = h(M)-r^3 \bmod n$ と $z^{1/3}$ に最も近い 3 で割り切れる整数 x (i.e., $x = z^{1/3}+b$ for $|b| \leqq 1/2$)を計算する。このとき、次式から $s = r+x$ が $h(M)$に対する偽造署名となることが示される。

$$\begin{aligned} s^3 &= r^3+3r^2x+3rx^2+x^3 \bmod n \\ &= r^3+3(n/3+a)^2x+3(n/3+a)x^2+z+3z^{2/3}b+3z^{1/3}b^2+b^3 \bmod n \\ &= h(M)+3a^2x+3ax^2+3z^{2/3}b+3z^{1/3}b^2+b^3 \bmod n \\ &= h(M) \bmod n \ < 2n^{2/3} \end{aligned} \qquad (63)$$

上記偽造法自体は署名の際に n/3 に近い署名をはじくことによって対抗し得るが、同偽造法はこのような対抗策を無効とするような一般化が可能である。

③ k≧4 の場合（現行 ESIGN 署名）の安全性

Brickell and deLaurentis[1986]の署名偽造法は次式

$$([N^{1/k}])^k - N = O(N^{k-1/k})O(\mathrm{N}^{2/3}) \qquad (64)$$

を利用したものと解釈し得る。しかし、上式は k≧4 の場合は検証式を満たさない。ラティス・アルゴリズムに基づく同攻撃を一般化する様々な技法(Vallee et al.[1988a,1988b], Girault et al.[1989])が提案されているが、k≧4 の場合の合同多項不等式を満たす根を導く方法は示されていない。

ハ．選択文書攻撃に対する安全性

最後に、選択文書攻撃による全面的解読と一般的偽造に対する安全性に関する議論を紹介する。以下の議論では、攻撃者が選んだ都合の良いいくつか

の文書 $M_1,M_2,\cdots,M_t$ に対応する署名 $s_1,s_2,\cdots,s_t$ を得られる、とする。

① 全面的解読

選択文書攻撃により得られる署名集合に関し攻撃者にとって最も都合の良い結果は、

$$s_i^k = h(M_i) \bmod n \quad (i=1,\cdots,t) \tag{65}$$

が成立する場合である。これらの情報から法 n を因数分解する問題は RSA 暗号に対し選択文書攻撃により法 n を因数分解する問題と本質的には変わりがないと思われる。この問題は 10 年以上多くの研究者により研究がなされてきたが有効な解法は示されていない。

② 一般的偽造

この場合の一般的偽造は、所与の文書 M_0 に対し得られた署名集合$\{s_i|i=1,\cdots,t\}$から $m_0 \leqq s^k \bmod n < m_0+2n^{2/3}$ を満たすような s を求める問題である。やはり得られる署名集合が $s_i^k \bmod n = m_i$ (但し、$m_i = h(M_i),\ i=1,\cdots,t$) となる RSA 暗号のような場合が最も簡単である。このとき、$m_0,m_1,\cdots,m_t$ の間に適当な既知の代数的関係があれば偽造署名を求める効率的なアルゴリズムは存在するが、こうした代数的関係が存在しない場合は効率的な偽造アルゴリズムは示されていない。他方、選択文書攻撃により得られる署名集合は $m_i \leqq s_i^k \bmod n < m_i+2n^{2/3}$ を満たすに過ぎず、こうした場合はたとえ $m_0,m_1,\cdots,m_t$ の間に適当な既知の代数的関係があったとしても効率的な偽造アルゴリズムは示されていない。

(3)DSA 署名

ElGamal 署名には、署名長が法の長さの 2 倍となるという問題があった。Schnorr[1989]は ElGamal 署名の手順を参考にしつつも「DLP における法 p に対し p-1 の約数 q を法とする有限体上で署名を構成する」という技法により署名長を ElGamal 署名における 2 p から 2 q に短縮した「Schnorr 署名」と呼ばれる方式を発表した。この場合、法 q に対しては DLP の準指数関数時間の解法である指数計算法を適用できないため p よりかなり小さい値に設定しても安全性は損なわれない。

「DSA 署名」も Schnorr 署名と同様に ElGamal 署名の改良方式であり、NIST[19][1992]により提案され 1994 年に米国連邦政府のディジタル署名標準とな

[19] NIST（National Institute of Standards and Technology）は、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 FIPS を制定する権限を有している。但し、米国政府の情報セキュリティ政策を国防長官の管轄と定めた 1980 年の大統領令（Executive Order

っている。同方式は ElGamal 署名と同様の署名生成・検証式に Schnorr 署名の署名短縮技法を持ち込んだ方式と解釈し得る。DSA 署名では署名生成は高速に行われるが、署名検証は RSA 暗号よりもかなり時間を要する。

離散対数問題と乱数を利用して落し戸付き一方向性関数を構成した署名方式としては、このほか Hoster et al.[1995]や Miyaji[1996]が提案した方式等が挙げられる。後者の方式は、メッセージ復元型署名方式であり、同方式を楕円曲線で実現した方式は DSA を楕円曲線上で実現した方式と同等の安全性を持つことが証明されている（Miyaji[1996]）。

【手順】A が文書 M の署名を生成し B が同署名を検証する手順を以下に示す。

[**鍵生成**] A は鍵を次のように生成する。まず、大きな素数 p を選んだ後、, p-1 の約数 q を選ぶ。次に、乱数 $x \in_R Z_q$ を生成後、$y = g^x \bmod p$（g は法 q の下での原始根）を計算する。

秘密鍵：x

公開鍵：y, g, p, q

[**署名生成**] A は、まず乱数 $k \in_R Z_q$ を生成した後、次の r を計算する。

$$r = (g^k \bmod p) \bmod q \tag{66}$$

次に、A は自分の秘密鍵 x と r, k を用いて t を計算する。

$$t = \frac{h(m)+xr}{k} \bmod q \tag{67}$$

A は B に文書 M と署名 $S = (r, t)$を送る。

[**署名検証**] B は A の公開鍵 y を用いて、署名の正当性を次式が成立するかどうかにより検証する。

$$r = (g^{h(m)/t} y^{r/t} \bmod p) \bmod q \tag{68}$$

【安全性】以下では、DSA 署名に対する安全性を「全面的解読に対する安全性」、「一般的偽造に対する安全性」、「利用上の留意事項」の順で検討する。

イ．全面的解読に対する安全性

DSA 署名において公開鍵から秘密鍵を求めるということは、所与の $y \in \langle g \rangle$（g は法 q の下での原始根）に対し、

$$y = g^x \bmod p \tag{69}$$

12333）等により実際の暗号政策の企画立案や標準策定は国防総省の下部機関である NSA（National Security Agency）が強い影響力を持つとされている。

の形の離散対数問題を解くことにほかならない。同問題の解法は、元の群の位数 p に対し準指数関数時間の解法である指数計算法（Gordon のアルゴリズム）を適用する、部分群の位数 q に対し指数関数時間の解法である Pohlig-Hellman のアルゴリズムを適用する、の二つがある。これらの解法に対する強度に関しては III 2.で詳述する。

ロ．一般的偽造に対する安全性

DSA 署名の一般的偽造法は次の四つが考えられる。

① 文書 M に対し署名の一部 r を適当に選択した上で、これらに対応する t を求める。

② 文書 M に対し署名の一部 t を適当に選択した上で、これらに対応する r を求める。

③ 文書 $S = (r, t)$を適当に選択した上で、これらに対応する文書 M を求める。

④ 関係式を満たす文書 M と署名 $S = (r, t)$を同時決定する。

攻撃①は次式から未知変数 t, z を求める問題に帰着される。

$$qz+r = (g^{h(M)}y^{r})^{1/t} \bmod p \tag{70}$$

同問題は明らかに法 p 上の DLP よりも難しい。

攻撃②は未知変数 r, z を次式から求める問題に帰着される。

$$(qz+r)^{t}y^{-r} = g^{h(M)} \bmod p \tag{71}$$

同問題は未知変数 r を次式から求める問題より明らかに難しい。

$$r^{t}y^{-r} = g^{h(M)} \bmod p \tag{72}$$

前述したように上記問題は解けないことが証明されている訳ではないが、解けないと予想されている有名な問題である。

攻撃③は未知変数 M, z を次式から求める問題に帰着される。

$$(qz+r)^{t}y^{-r} = g^{h(M)} \bmod p \tag{73}$$

同問題も法 p 上の DLP よりも明らかに難しい。

攻撃④は、明らかに次式を満たす M,r,t を求める問題より難しい。

$$r = (g^{h(M)}y^{r})^{1/t} \bmod p \tag{74}$$

上記問題自体は解法が存在するが、同解法では文書 M を制御できないので実際の脅威足り得ないことは既に述べた通りである。

ハ．存在的偽造に対する安全性

最近になって、ある特定の文書に対しては不正に繋がるような改竄が可能であることが指摘された（Vaudenay[1996]）。すなわち、同文書に対しては

然るべき改竄を施せば改竄前と同一の署名が得られるとの指摘である。しかし、このような文書は非常に限られているため、実際の脅威とは成り得ないと考えられる。

二．利用上の留意事項

ElGmal 署名と全く同じ理由（秘密鍵を算出させないため）から乱数 k は過去に使用したものであっても外部に漏らしてはならないし、二つの異なる文書に署名する際に同じ乱数 k を用いてはならない。

また、このことから明らかなように、故障利用暗号攻撃により乱数 k を攻撃者に入手させてはいけない。

ただ、ElGamal 署名とは異なり Bleichenbacher[1996]の一般的偽造法は成立しない。

(4)Fiat-Shamir 署名

Fiat-Shamir 署名（Fiat-Shamir[1986]）は素因数分解の困難性及び平方剰余問題の困難性に基づく方式である。同方式は challenge and response から成る基本手順を順次繰り返す Fiat-Shamir 認証（Fiat-Shamir[1986]）において情報をベクトルとして同時に実行するように変形した方式と解釈可能である。Fiat-Shamir 署名は RSA 暗号より 100 倍程度の高速化が可能であるが、このとき署名等のサイズは非常に大きくなるため一長一短といえる。

【手順】

[**鍵生成**] 署名者 A は鍵を次のように生成する。まず、二つの大きな素数 p と q を選び、これらの積 $n=pq$ を計算する。次に、$k\in_R Z$ に対し、 k-bit 出力のランダムハッシュ関数 h を定める。それから、$s\in_R Z_n$ から $v=s^2 \bmod n$ を算出する。

公開鍵：n, f

秘密鍵：s

[**署名生成**] A は k 個の乱数を生成した後、各乱数の平方と $h=(e_1\cdots e_k)=f(m,x_1,\cdots,x_k)$を計算する。これらのデータからAは$y_i=r_i s^{ei} \bmod n$を計算した後、$\sigma_1=(x_1,\cdots,x_k)$と$\sigma_2=(y_1,\cdots,y_k)$を算出する。$(\sigma_1,h,\sigma_2)$が文書 m の署名となる。

[**署名検証**] B は送信されてきた文書 m と署名(σ_1,h,σ_2)から次式が成立するかどうかを検証する。

$$h = f(m,\sigma_1) \tag{75}$$

$$y_i = r_i s^{ei} \bmod n \quad \text{for} \quad \forall i \tag{76}$$

【安全性】Fiat-Shamir 署名は仮想的なランダム関数よりも弱い仮定である「無

相関一方向性関数（correlation-free one-way hash function）」の存在を仮定すれば素因数分解が困難であるとの前提の下で、能動的攻撃に対しても存在的偽造さえ不可能であることが証明されている（Okamoto[1993]）。

(5)EDLP に基づく署名法

EDLP に基づく署名法のうち、代表的なものとしては、「ECElG 署名」、「ECSS 署名」、「ECDSA 署名」が挙げられる。特に、ECSS 署名は IEEE[20]（Institute of Electrical and Electronic Engineers）で、ECDSA 署名は IEEE と ANSI[21] (American National Standards Institute)で標準化作業が進行中である。これらは何れも DLP に基づく有限体の署名法を有限体で定義された楕円曲線の点のなす有限可換群上に置き換えた方式である。すなわち、 ECElG 署名は ElGamal 署名を、ECSS 署名は Schnorr 署名を若干変形した方式を、ECDSA 署名は DSA 署名を、それぞれ同群上に置き換えたものである。前述の通り、EDLP は DLP に適用される高速の解法（指数計算法）がある種の楕円曲線を除けば適用困難なため、FP や DLP に基づく方式に比べ鍵長を大幅に短縮できる方式として注目を集めている。両方式の手順は ECSS 署名及び ECDSA 署名と同様なので、ここでは割愛する。

【安全性】

イ．基本的な安全性

楕円曲線の点のなす有限可換群上の離散対数問題（EDLP）の困難性に依存している。2.(2)で述べたように、同問題は DLP に対する高速解法である指数計算法が適用不可とされていたが、その後、ある性質を満たす EDLP は DLP に帰着する方法、所謂「MOV 帰着」（Menezes-Okamoto-Vanstone[1991]）が示された。そこで、現在ではこうした帰着法を無効にするような EDLP のいくつかの構成法が提案されている。このとき、楕円曲線 $E(F_q)$に関する EDLP に対する最も高速な解法は Pohlig-Hellman のアルゴリズムで、同アルゴリズムによる概算の平均計算量 $T(q)$は次の通り。

$$T(q) = O((\#E(F_q))^{1/2})$$

[20] IEEE は米国の電気・電子工学分野の学会であると同時に、ANSI から信任された国内標準策定機関の一つでもある。IEEE は米国内の標準を策定する機関に過ぎないが、国際標準の実質的内容が IEEE で作成されているという場合も少なからずあるため、同機関における標準化動向が注視される。

[21] ANSI は、1918 年に政府機関及び民間組織によって設立された民間非営利団体であり、米国内での技術の標準化を推進している。ANSI は ISO の米国代表でもある。

ロ．他の方式との比較

ECElG 署名と ECDSA 署名のプロトコルの安全性に関しては、楕円曲線が素数位数でかつ元の個数が#E(F_q)≧q の場合、両署名方式を偽造する問題は等価になることが示されている（Miyaji[1996]）。

ハ．利用上の留意事項

ElGamal 署名、DSA 署名と全く同じ理由（秘密鍵を算出させないため）から乱数 k は過去に使用したものであっても外部に漏らしてはならないし、二つの異なる文書に署名する際に同じ乱数 k を用いてはならない。従って、故障利用暗号攻撃により乱数 k を攻撃者に入手させてはならない。

(6)その他

その他の重要な署名法として、受動的攻撃のみならず能動的攻撃に対しても全面的解読は素因数分解と同程度に難しいことが証明できる「Ong-Schnorr-Shamir 署名」と受動的攻撃のみならず能動的攻撃に対しても存在的偽造すら不可能であることが証明できる「Bellare-Goldwasser 署名」がある。但し、前者は既に直接攻撃で容易に一般的偽造ができることが示されており、後者は非効率的で実用化は困難とされている。

イ．Ong-Schnorr-Shamir 署名

Ong et al.[1984]は、合同多項式の求解問題に基づく一連の高速署名方式を提案した。総称して Ong-Schnorr-Shamir 署名と呼ばれるこれらの方式は受動的攻撃のみならず能動的攻撃に対しても全面的解読は素因数分解と同程度に難しいことが示される。しかしながら、一般的偽造に関する安全性の根拠は同方式の提案後、覆されることとなった。すなわち、最初の提案方式（Ong and Schnorr[1984]）では次の合成数 n を法とする 2 変数 2 次合同式

$$x^2+ky^2 = m \mod n \tag{77}$$

を解くことが計算量的に困難であろうとの予想に基づいていた。しかし、Pollard は上記方程式を多項式時間で解くアルゴリズムを発表、同方式が直接攻撃で容易に一般的偽造ができることを示した。そこで、Ong et al.は 2 次合同式に代えて、3 次合同式、4 次合同式を利用する方式を再提案したが、前者は Pollard[1987]、後者は Estes et al.[1986]によって一般的偽造法が示された。これらの解読法の存在は Ong-Schnorr-Shamir 署名の基本的枠組み自体が安全でないことを意味するものではないが、この種の方式の安全性に対し強い疑惑の念を醸成するものとなったことは間違いない。また、次数を引き上げるなどの暗号化・復号化の計算量の増加に繋がる解読法対抗策は、同暗号の利点で

あった高速性を薄めることになる。こうした点を考慮してか、Ong et al.は 4 次合同式を利用した署名方式が解読されて以来、同署名型の署名方式を提案していない。

ロ．Bellare-Goldwasser 署名

Bellare and Goldwasser[1990]は、既述の零知識非対話証明（NIZK）を利用して、受動的攻撃のみならず能動的攻撃に対しても存在的偽造すら不可能なことがやや特殊な仮定の下で[22]証明できる署名方式を考案した。同方式では、信頼できる第三者が生成した乱数列 R に応じた署名が NIZK を利用して作成されるが、次の三つの問題点が指摘されている。

① 公開検証可能な NIZK が存在しないと任意の検証者が署名の正当性を検証できない。

② 同一の乱数列 R を用いて複数の文書に署名すると偽造ができるようになる。

③ ②を解決するために署名済みの文書に署名が依存するように対策を施すと署名の履歴を記録しておく必要が生じる。

これらの問題は Bellare-Goldwasser 署名の一部を Feige and Shamir [1990]が提案した技法で置き換えることで解決できる。しかしながら、同方式は計算量が依然として多く実用的とは言い難いのが実情である。Dwork and Naor [1994]は、計算量を RSA 方式の 2 倍から 5 倍に抑えることに成功したものの、相当の記憶容量を要する上、署名のサイズは RSA よりも大きくなっている。

[22] Naor and Yung[1989]、 Rompel[1990]は一方向性関数の存在のみを仮定した方式を提案しているが、これらの方式は効率が悪く実用的でない。

III 公開鍵暗号の強度評価

これまでの議論から明らかなように、現在十分に安全性が高く、かつ実用的であるとされている公開鍵暗号は、極く少数の例外を除けば、素因数分解問題（FP）、ないしは離散対数問題（DLP、EDLP）の何れかの問題の困難性に基づいていると言える。すなわち、RSA 暗号、Rabin 系暗号（Rabin 暗号、Williams 暗号、逆数暗号）、ESIGN 署名、Fiat-Shamir 署名は FP の困難性に、ElGamal 暗号・署名、DSA 署名、Schnorr 署名は DLP の困難性に、DL 楕円暗号（ECElG 暗号、ECDSA 署名、ECSS 署名）は EDLP の困難性に依拠している。従って、ユーザーがこれらの公開鍵暗号を利用する際には、計算機のコスト・パフォーマンス（単位費用当り計算速度）と脅威となり得る解法（最小計算量）を把握した上で、各自に必要なセキュリティー水準（仮想攻撃者の解読予算と解読耐久時間）を満たすように利用する暗号の鍵長等を設定しなければならない。本章では、最小計算量を把握するために脅威と成り得る解法を分析した後、現時点の計算機のコスト・パフォーマンス及び同コスト・パフォーマンスの向上を考慮し、現時点及び将来の鍵長、解読費用、解読時間の関係について簡単な試算を行う。

1. 素因数分解問題（FP）の解法

RSA 暗号、 Rabin 系暗号（Rabin 暗号、Williams 暗号、逆数暗号） 、ESIGN 署名、Fiat-Shamir 署名の基本的な安全性は素因数分解問題（FP）の難しさに根拠をおいている。

(1)研究の経緯

素因数分解のアルゴリズムとして古くから良く知られている試行割算法は、合成数 n を素数で小さい順に割っていく方法である。しかし、これは素因数 p に比例する計算量（$O(p)$と表す）、換言すれば、p の桁数の指数関数時間の計算量を要する。

大きな合成数 n の素因数分解に有効なアルゴリズムは何れも適当な z を求め、n と z の最大公約数 $p=\mathrm{GCD}(n,z)$を計算して n の約数 p を求めることが基本となっている。これは、二つの整数 m, n の最大公約数の計算が、最悪の場合でも $\min(m, n)$の桁数の高々5 倍以内で完了する（Lamé の定理）という極めて効率的なアルゴリズム（Euclid の互除法＜付録 1 参照＞）が存在するからである。問題は z の効率的な求め方であり、様々な手法が提案されている。これらの手法は、計算量が n の素因数 p の性質によって決まる「素因数依存型」と、合成数 n のサイズのみによって決まる「合成数依存型」に大別される。

① 素因数依存型アルゴリズム

素因数依存型アルゴリズムとしては、先述の試行割算法のほか、計算量が

$O(p^{1/2})$の「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]）、楕円曲線の利用により p-1 法の欠点を克服した汎用的な素因数分解法の「楕円曲線法」（Lenstra[1987]考案、Montgomery[1987]改良）が挙げられる。

② 合成数依存型アルゴリズム

合成数依存型の主要なアルゴリズムは 2 次合同式を利用している。すなわち、2 次合同式 $s^2 = t^2 \bmod n$ を満たす s と t を求め、$z=s\pm t$ とおいて最大公約数 GCD(n, z)を計算す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-Brillhart[1975]）、「線形ふるい法」（Schroeppel[1977]）、「2 次ふるい法」（Pomerance[1983]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次の記法を用いる。

$$L_p[a, b]=\exp((b+o(1))(\log p)^a(\log\log p)^{1-a}) \qquad (78)$$

ここで、$o(1)$は極限値が 0 の量。

(2)重要な解法

ここでは、因数分解が容易な「弱い合成数」を示しているという意味で重要な p-1 法、p+1 法、Fermat 法、並列計算に適した 2 次ふるい法、そして最少の素因数 p の次数によっては最高速の解法と成り得る楕円曲線法、現時点で最高速の解法である数体ふるい法の各アルゴリズムを紹介する。

イ．p-1 法&p＋1 法

Pollard[1974]は、n の素因数 p に対し、p-1 が小さな素因数の積になっている場合に有効な p-1 法と呼ばれる素因数分解法を提案した。

n の素因数 p に関して、p-1 が小さな素因数の積になっている、すなわち、ある整数 M に対し、

$$p\text{-}1 = \prod p_i^{ei}, \quad p_i \leqq M \qquad (79)$$

と表されるとき、p-1 は M -smooth であると呼ぶ。

ところで、p は n の素因数であるから、ある a に対し GCD(a, n) = 1 ならば、GCD(a, p) = 1 となる。従って、Fermat の定理（付 1 参照）より

$$a^{p-1} = 1 \mod p \qquad (80)$$

となる。そこで、p-1 の倍数である K に対し、$a^K=1 \bmod p$ となるので、p は a^K-1

と n の最大公約数 GCD(a^K-1, n)を計算して求められる。従って、試行錯誤で p-1 の倍数となるような K を探し当てることにより素因数分解が可能となる。

Pollard[1974]は、p-1 の約数が一つだけ大きい場合でも p-1 法に若干の改良を加えた方法で効率的に素因数分解できることを示している。p-1 が一つだけ大きな約数 q を持つ以外は、小さな約数を持つとき、すなわち、

$$p\text{-}1 = q \prod p_i^{ei}, \quad p_i \leqq M, \quad e_i \leqq m_i, \quad q \leqq M' \tag{81}$$

の場合を考える。このとき、$\prod p_i^{ei}$ の倍数である k に対し $a^k = b$ とおけば、$b^q = 1 \bmod p$ となる。従って、$1 < \mathrm{GCD}(b^j\text{-}1, n) < n$ を満たす j がみつかれば、n の素因数が求められたことになる。

一方、n の素因数 p に関して、p+1 が

$$p+1 = q \prod p_i^{ei}, \quad p_i \leqq M, \quad e_i \leqq m_i, \quad q \leqq M' \tag{82}$$

と表されるときは、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できることを Guy[1975]が示している。

ロ．Fermat 法

基本的な Fermat 法（Fermat's factoring method）は、Fermat が提案したものであるが、同解法が$|p\text{-}q|$が小さい場合に非常に有効であることを再評価したのは Brillhart[1981]であり、彼は自ら同解法の改良法も提案している。素数 p,q の選択指針に$|p\text{-}q|$が大きくなるように選ぶとあるのは Fermat 法の存在を考慮したものにほかならない。ここでは基本的な Fermat 法を紹介しておく。

$n = pq, \quad p \leqq q$ のとき

$$x = (q+p)/2$$

$$y = (q\text{-}p)/2$$

とおくと、

$$x^2\text{-}y^2 = n \tag{83}$$

となる。従って、$(x, y) = ([n], 0)$を初期値とし、(x, y)を少しずつ変化させていき、

$$r = x^2\text{-}y^2\text{-}n \tag{84}$$

が 0 となるような(x, y)をみつけることができれば、このとき、(p, q)が求められたことになる。ところで、$(x+1)^2 = x^2+2x+1$ なので、$A = 2x+1, B = 2y+1$ とおけば、$x \rightarrow x+1$ は $r \rightarrow r+A, A \rightarrow A+2$ となり、$y \rightarrow y+1$ は $r \rightarrow r\text{-}B, B \rightarrow B+2$ となる。すなわち、加減法だけで計算できるのが基本的な Fermat 法の長所である。

ハ．2 次ふるい法

Pomerance[1983]は、2 次合同式 $k^2 = l^2 \bmod n$ を満たす k と l を求める効率的な方法として、2 次ふるい法（quadratic sieve method）を考案した。

Pomerance[1983]が考案した 2 次ふるい法のアルゴリズムを次に紹介する。

2 次ふるい法では、2 次合同式 $k^2 = l^2 \bmod n$ の k と l を探すために、次の関数を導入する。

$$Q(x) = (x+m)^2-n, \qquad m=[n^{1/2}] \tag{85}$$

$x = 0,\pm1,\pm2,\cdots$を $Q(x)$に代入し、$Q(x)$を素因数分解する。このとき、$Q(x)$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。これらの中で「小さな」素因数 p_jのみを持つ $Q(x)$、すなわち、全ての素因数が意図した値 v 以下である $Q(x)$を集める。すなわち、$Q(x)$は

$$Q(x) = p_1^{d1} \cdots p_r^{dr} \mod n \tag{86}$$

と表される。但し $p_1,\cdots,p_r$は v 以下の素因数。

v-smooth な $Q(x)$を集め、その中から次式を満たすような集合 S を探し出す。

$$\prod_S Q(x) = p_1^{a1} \cdots p_r^{ar} \mod n \tag{87}$$

但し a_j (j=1,$\cdots$,r)は偶数。このような集合が見つかれば、

$$k = \prod_S (x+ m) \mod n \tag{88}$$

$$l = \prod_S p_j^{aj/2} \mod n \tag{89}$$

とおくことにより、

$$k^2 = l^2 \mod n$$

が成立する。

もし、GCD($k+l$, n)、または、GCD($k-l$, n)が自明でない n の素因数であれば、アルゴリズムは終了し、そうでなければ、(94)式を満たす別の部分集合を見つけて同じことを繰り返す。

以上が Pomerance[1983]が最初に提案した 2 次ふるい法の概要である。同アルゴリズムの漸近的な平均計算量 $T(n)$は

$$T(n) = L_n[1/2, 1.061]$$

と評価されている。その後、Silverman[1987]は関数 $Q(x)$を改良した「複数多項式 2 次ふるい法」を発表した。これは、$b^2-4ac = kp$（但し、k は小さい整数）を満たす多数の 2 次式 ax^2+bx+c から、上記 k, l を効率的に求めるアルゴリズムである[23]。同アルゴリズムの漸近的な平均計算量 $T_{\text{plural}}(n)$は

$$T_{\text{plural}}(n) = L_n[1/2, 1.020]$$

と評価されている。

[23] 1977 年に Rivest が *Scientific America* 誌上に提出した 129 桁の合成数を素因数する有名な懸賞問題を Lenstra 等が 1994 年に解いたときに用いられた方法がこの複数多項式 2 次ふるい法である。600 台の計算機を動員し 8 ヶ月を要したとされている。

ニ．楕円曲線法

楕円曲線法は、*p*-1 法の欠点を克服し、一般的な合成数の素因数分解を可能とした解法である。*p*-1 法は Z_p*の位数（要素の個数）が *p*-1 であるため、*p*-1|*k* であれば、Z_p*において a^k=1 となるという事実に着目した解法である。楕円曲線法は *p*-1 法における Z_p*を有限体 F_p上で定義された楕円曲線の点のなす可換群 $E(F_p)$で、整数 *a* を同群上の点 $P \in E(F_p)$で置き換えたものと解釈し得る。*p*-1 法と同様に、小さい素数の積から成る整数 *k* をとる。このとき、$E(F_p)$の元が *k* を割り切っているならば、$E(F_p)$において *kP*=*O* となり、*n* の非自明な約数が得られる。従って、$E(F_p)$の位数が小さな素数の積となっていれば素因数分解に成功する。*p*-1 法との違いは、*p*-1 法では *p*-1 が小さな素数の積でない場合は有効に働かなかったが、楕円曲線法の場合、楕円曲線を動かすにつれて位数も相当程度変動するため、位数が小さな素数の積となるような楕円曲線を比較的早期に探し当てることが期待できる。

楕円曲線法により素因数 *p* を求める平均的かつ漸近的な計算量は

$$T(p) = L_p[1/2, 1.414]$$

である。なお、*n*=*pq* かつ *p* と *q* のサイズが同じ場合は、

$$T(n) = L_n[1/2, 1.020]$$

となる。

ホ．数体ふるい法

数体ふるい法は、2 次ふるい法の概念を代数的整数上で実現したものである[24]。

n を合成数、$f \in \boldsymbol{Z}_n[X]$を $\boldsymbol{Z}_n$の要素を係数とする次数 *k* の既約モニック多項式とする。*m* を整数とし、*n*= *f*(*m*)を分解する。 *f*=0 の根の一つを $\alpha \in \boldsymbol{C}$ とする。代数体 *K* を $K = \boldsymbol{Q}(\alpha)$とし、$O_K = \boldsymbol{Z}[\alpha]$を *K* の整数環で一意分解整域とする。

数体ふるい法の原理は、$\varphi : \boldsymbol{Z}[\alpha] \rightarrow \boldsymbol{Z}_n$なる環準同型を

$$f(\alpha) \rightarrow f(m) \bmod n$$

として、次の図式に示すように、二通りの分解の違いを利用している。

$$\begin{array}{ccc} c+d\,\alpha & \rightarrow & O_K\text{での分解} \\ \varphi \downarrow & & \downarrow \varphi \\ c+d\,m & \rightarrow & \boldsymbol{Z}\text{での分解} \end{array}$$

なお、有理整数における smooth という概念を代数的整数にも拡張できる。

---

[24] 以下の説明で用いられる代数的整数論の専門用語及び記号の定義に関しては、例えば小野[1987]を参照。

すなわち、有理整数または代数的整数が smooth であるとは、その素因子が全て因子基底βに含まれることである。因子基底βは、次の二つの集合β_Qとβ_Kから構成されている。

β_Q： ある上限 B より小さい有理素数（代数的整数と区別するために、以下では $\boldsymbol{Q}$ の素数を特に有理素数と呼ぶ）。

β_K： B より小さいノルムを持つ O_K の 1 次の素イデアル、及び O_K の単元（可逆元）の集合。

この場合、$c+d\ \alpha \in \boldsymbol{O}_K$ のノルム $\boldsymbol{N}(c+d\ \alpha)$は

$$\boldsymbol{N}(c+d\ \alpha) = |(-d)^k f(-c/d)|$$

によって計算される。

$(c_i,\ d_i)$を互いに素な有理整数とする。$c_i+d_i m$ は β_Q-smooth であり、かつ $c_i+d_i\ \alpha$ が β_K-smooth とする。$c_i+d_i m$ 及び $c_i+d_i\ \alpha$ が完全に分解されるようなペア(c_i, d_i)を数多く集め、

$$\prod(c_i+d_i m) = s^2$$
$$\prod(c_i+d_i\ \alpha) = t^2$$

なる関係式を求める。そして、GCD$(s^2 \pm t^2, n)$を計算して n の素因数を求める。

2. 離散対数問題（DLP, EDLP）の解法

(1)離散対数問題の概要と研究の経緯

離散対数問題（DLP）とは、有限体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、有限体上での対数の計算は数が大きくなるにつれて飛躍的に難しくなる。

DLP：群 G と $g \in G$ が固定されているとき、所与の $a \in H = \langle g \rangle \subseteq G$ に対して、$g^x = a$ を満たす整数 x を求めよ。

DLP のアルゴリズムは、手法により次の 2 種類に大別される。

① $H = \langle g \rangle \subseteq G$ に対し、H の位数 $\#H$ に依存して $\log_g a$ を求めるアルゴリズム。これまでのところ $\#H$ の最大素因数のサイズ $\log_g \#H$ の指数時間オーダーの実行時間となるアルゴリズムしか知られていない。

② $G = F^*_q (q=p^k)$に対し、$\#G$ に依存して $\log_g a$ を求めるアルゴリズムで、「指数計算法（index calculus method）」と呼ばれている。有限体 F_q のサイズ $\log_g \#F_q$ の準指数時間のオーダーの実行時間となる。

前者に属するものとしては、Shanks[1972]、Pohlig-Hellman[1978]、Pollard[1978]のアルゴリズムが知られている。

指数計算法としては、Adleman[1979]、Coppersmith[1984]、ElGamal[1985]、Coppersmith-Odlyzko-Schroeppel[1986]（Gauss の整数法）、数体ふるい法を DLP に適用した Gordon[1992]とその改良とみられる Schirokauer[1993]、関数体ふるい法（Adleman[1994]）等のアルゴリズムが知られている。

現在、全ての有限体 F_q ($q=p^k$)に対し最高速のアルゴリズムは存在しない。すなわち、$k<(\log p)^{1/2-\varepsilon}$（$\varepsilon$：任意の正整数）に対しては Schirokauer のアルゴリズムが最高速で、その実行時間は $L_p^k[1/3,(64/9)^{1/3}]$と評価されている。一方、その実行時間は $L_p^k[1/3,(64/9)^{1/3}]$と評価されている。これら二つのアルゴリズムの適用領域のギャップ $(\log p)^{1/2-\varepsilon} \leqq k < (\log p)^2$においては $L_p^k[1/2,c]$と評価されるアルゴリズムしか発見されていない（Schirokauer et al.[1996]）。

(2)重要な解法

ここでは、楕円曲線上で定義された離散対数問題（EDLP）や DSA 署名における部分群〈q〉に直接適用でき、また有限群の位数が特殊な形をしている場合には多項式時間で解ける Pohlig-Hellman[1978]のアルゴリズム、有限体 F_q のサイズの準指数関数時間の計算量を実現した指数計算法の一般的アルゴリズム、最後に現在最高速の指数計算法である Gordon[1992]のアルゴリズムを順次紹介する。

イ．Pohlig-Hellman のアルゴリズム

Pohlig-Hellman[1978]のアルゴリズムは、$H=\langle g\rangle \subseteq G$ の位数 n の最大素因数の指数時間オーダーの実行時間を要し効率的な解法とはいえない。同アルゴリズムが強力に働くのは位数 n が $O(\log\ n)$-smooth の場合であり、このときは多項式時間オーダーの実行時間 $O(\log^2 q)$で解けることになる。

$n = \#H = \#\langle g\rangle$ とし、n は y-smooth であるとする。そこで、

$$n = \prod_{i=1}^{k} q_i^{ei}, \qquad q_1 < \cdots < q_k \leqq y \tag{90}$$

という素因数分解が既知であるとする。離散対数 $x = \log_g a$ は明らかに Z_n の元で n の素因数分解が判っているから剰余環の直積環への分解（中国剰余定理）：

$$\boldsymbol{Z}n = \boldsymbol{Z}q_1^{e1} \times \cdots \times \boldsymbol{Z}q_k^{ek} \tag{91}$$

によって、各剰余環における $\log_g a$ の値が求まれば $\log_g a \in Z_n$ が求まる。

以下では、 $\boldsymbol{Z}q_i^{ei}$ における添字 i を省略する。いま、

$$x = \sum_{j=1}^{e-1} b_j q^j, \qquad b_i \in \mathbf{Z}q \tag{92}$$

とおくと、b_j (0≦j≦e-1)が求まれば良い。これらを求めるアルゴリズムは次の通り。

Step 1: $a^{n/q}$ と $\gamma = g^{n/q}$ を計算する。

Step 2: $\gamma^i = g^{n/q}$ となる i を探す。これは、i=0,1,...と次々に試せば良い。発見したら、$b_0 = i$ とする。e＞1 ならば以下を続ける。

Step 3: $a_1 = a\, g^{-b0}$ として、$\gamma^i = a_1^{n/q2}$（但し、$q_2 = q^2$）となる i を探し、$b_1 = i$ とする。

Step 4: $a_2 = a_1 g^{-b1q}$ として、$\gamma^i = a_2^{n/q3}$（但し、$q_3 = q^3$）となる i を探し、$b_2 = i$ とする。

以下、b_{e-1} まで実行。

上記アルゴリズムの実行時間は、群の二項演算の回数で表現すると $O(\Sigma e_i(\log n + q_i))$であり、$n$ の最大素因数のサイズの指数関数オーダーとなる。しかし、n が $O(\log n)$-smooth であるとすれば、$O((\log n)^2)$を得る、換言すれば、群 $H \subseteq G$ の位数 n が $O(\log n)$-smooth の場合、多項式時間で解けることになる。しかし、同条件は $G = H = Z^*_p$ のとき、p-1 が $O(\log p)$程度の小さな素因数のみに分解される場合に相当する。逆にいえば、p-1 が大きな素因数を持てば、Pohlig-Hellman[1978]のアルゴリズムは効率的に働かないことになる。

ロ．指数計算法の一般的アルゴリズム

先ず、指数計算法の基本的なアルゴリズムから説明しよう。指数計算法は、有限体 F_p を有理数体 Q に埋め込むことによって、$H = \langle g \rangle \subseteq G$ から適切に選んだ因子基底の F_p 対数表を作成し、同表から $\log_g a$ を求めるという方法である。

Step 1: 次の写像により F_p の要素を有理数体 Q に埋め込む。

$F_p \rightarrow Q : g^r \bmod p \rightarrow g^r$

Step 2: ある適当な v-smooth な素数の集合$\{p_1, \cdots, p_n \mid 0 < p_i < v\} \subset Q$ に対し、g を底とする F_p 対数表を次のように作成。

① $g^r \bmod p$ が v-smooth となるような r をとる。

$$g^r \bmod p = p_1^{a1} \cdots p_n^{an}$$

② 上式の F_p 対数をとる。

$$r \bmod p\text{-}1 = a_1 \log_g p_1 + \cdots + a_n \log_g p_n$$

n 本の独立な方程式が得られれば$\{\log_g p_i\}$が求められる。

Step 3: $yg^t \bmod p$ が v-smooth となるように $t \in F_p$ をとる。このとき、

$$yg^t \bmod p = p_1^{b1} \cdots p_n^{bn}$$

であり、次式から離散対数が求められる。

$$\log_q y = b_1 \log_q p_1 + \cdots + b_n \log_q p_n \bmod p - t$$

Adleman[1979]は、$G=H=Z^*_p$ の DLP に対して、因子基底βとして $u=L_p[1/2,0]$ 以下の素数の集合を設定するアルゴリズムを示した。すなわち、Step 1 で b_i をランダムに選び、g^{bi} がスムーズになるような b_i だけをふるいに掛けるという手法を示した。このようにβを選ぶと、g^{bi} がスムーズになる確率の評価に若干の仮定が必要となるが、Step 1 と Step 2 を通じた総計算量は $L_p[1/2,c]$(c～0)となる。

指数計算法は DLP を準指数関数時間で解く強力なアルゴリズムであるが、EDLP に対し直接適用することはできないのであろうか。この疑問に対し肯定的な回答は示されていない。なぜならば、有限体 F_p から有理数体 Q への埋込みのような自然な埋込みが $E(F_p) \rightarrow E(Q)$ には存在せず、他に適当な埋込みも見当たらない上、仮にそのような埋込みが発見できたとしても、$E(Q)$ 上では生成元や連立方程式の階数を求める効率的な方法が示されていないからである。研究者の多くはこうした問題を一般的に解決することは困難と予想しているとみられる。

ハ．Gordon のアルゴリズム

$G=H=Z^*_p$ の離散対数問題に対する指数計算法に関しては、Adleman[1979]のアルゴリズム以降は画期的な進展はなかったが、最近になって Gordon[1992]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、従来のものより高速な準指数関数時間アルゴリズムを 2 種類与えた。

一方は一般数体ふるい法に基づくものであり、他方は特殊数体ふるい法に基づくものである。「一般」と「特殊」は、アルゴリズム自体は殆ど同じであるが、その違いは Z_p の標数 p の性質による。すなわち、「一般」の場合は一般の p に対して適用可能であり、「特殊」の場合は次のような性質を持つ p に対してのみ適用可能である。

性質 1： $f \in \boldsymbol{Z}_p[X]$の係数は適当に小さい。

性質 2： ある整数 x,y が存在し、その大きさは何れも $p^{1/k}$ 程度で、$y^k f(x/y)=0 \pmod p$を満たす。

性質 3： $O_K = Z(\alpha)$は一意分解整域。

素体 F_p に対する「特殊」の実行時間 $T_{special}(p)$は、

$$T_{special}(p) = L_p[2/5, 1.005]$$

である。

これに対し、素体 F_p に対する「一般」の実行時間は、

$$T_G(p) = L_p[1/3, 3^{2/3}] = L_p[1/3, 2.080]$$

と評価されている。しかし、素体を含め有限体 F_p^k に対し $k < (\log p)^{1/2-\varepsilon}$（ε：任意の正整数）の場合は Schirokauer[1996]により改良されたアルゴリズムが最高速となっている。その実行時間 $T_S(p^k)$ は、

$$T_S(p^k) = L_p^k[1/3, (64/9)^{1/3}] = L_p^k[1/3, 1.922]$$

と、Adleman-Lenstra 版数体ふるい法と同じ計算量で評価されている。有限体 F_p^k に対し $k \geqq (\log p)^2$ の場合は Adleman[1994]が考案した関数体ふるい法が最高速で Schirokauer のアルゴリズムと同じ実行時間で評価されている。

(3)EDLP に基づく公開鍵暗号の構成法

EDLP に基づく公開鍵暗号が十分安全であるためには、次の二条件を満たすように楕円曲線を構成する必要がある。

条件 1: 楕円曲線のベースポイントの位数が大きな素数で割り切れる。

条件 2: MOV 帰着により楕円曲線 $E(F_q)$上の EDLP が変換される DLP が F_qの小さい拡大体上では定義されない。

条件 1 は EDLP に直接適用される Pohlig-Hellman[1978]のアルゴリズムや Pollard[1978]のアルゴリズムに対し十分な強度を保持するための条件である。同条件は「楕円曲線の要素の個数は大きな素数で割り切れる」ということに他ならないが、このためにはまず楕円曲線の要素の個数を知らなければならない。楕円曲線の要素の個数を求めるアルゴリズムとしては、Schoof[1985]のアルゴリズム[25]が知られているが、残念ながらこれはあまり効率的ではない。そこで、同

[25] Schoof[1985]によって示された有限体上の楕円曲線の要素の数を計算する決定的多項式時間アルゴリズムのこと。しかしながら、多項式時間とはいうものの、問題のサイズの 8 乗のオーダーとなる。通常効率的とされているアルゴリズムは同 3 乗程度以下であり、8 乗のオーダーというのは楕円曲線暗号等の暗号理論の応用分野で利用するサイズのデータに対して実際に計算機で計算できるぎりぎりのところであり、効率的なアルゴリズムとは言い難い。ただ、最近になって Schoof のアルゴリズムの改良版がいくつか提案されており、中には実行時間が問題のサイズの 6 乗となるものも出てきている(Charlap-Coley-Robbins [1991])。従って、さらに改良が進めば同アルゴリズムを用いて楕円曲線を構成する方法が実用に資するようになる可能性

アルゴリズムを用いずに条件 1 を満たす楕円曲線の構成法の研究が行われてきた。代表的な構成法としては次の二つが挙げられる。

表 1　従来の構成法

提案者	構成法の概要	備　　考
Menezes-Vanstone[1990]	F_2 上の超特異楕円曲線を利用した構成法	F_2 上の超特異楕円曲線は 2 倍点の計算が容易なため、高速な暗号化・復号化が可能。
Morain[1991]	F_p 上の楕円曲線で巡回群となるような構成法	巡回群としての構成により素体のサイズの縮小化を実現。

ところが 1991 年になって、Menezes-Okamoto-Vanstone[1991]により「MOV 帰着 （MOV-reduction）」と呼ばれる EDLP を DLP に変換する新しい解法が提案された。MOV 帰着は楕円曲線上の加群を「Weil 対（Weil pairing）」と呼ばれる特殊な単射準同型写像を用いて有限体上の乗法群と同一視することを可能にする方法である。同帰着により、超特異楕円曲線は定義体の高々6 次の拡大体上の DLP に変換されてしまうため、上記 Menezes-Vanstone[1990]の構成法は、定義体を大きくしなければならず実用的でなくなる。これが上記条件 2 が必要とされる理由である。条件 1 に加え条件 2 を満たす代表的な構成法としては、例えば次の二つが挙げられる。

表 2　安全な構成法

提案者	構成法の概要	備　　考
Beth-Schaefer[1991]	F_2 上の超特異でない楕円曲線を利用した構成法	MOV 帰着により楕円曲線 $E(F_a)$上の EDLP が十分大きな F_aの拡大体上の DLP に変換。
Miyaji[1993]	要素の個数が p となる F_p 上の楕円曲線を利用した構成法[26]	EDLP が MOV 帰着のみならずどのような単射同型写像によっても DLP に変換不可能。

はある。

[26] 同構成法では、与えられた要素の個数を持つ楕円曲線を生成する必要があるが、これについては Deuring[1941]により幅広く研究されている。

ところが楕円曲線の場合、楕円曲線上の 1 回の加算に 12～13 回の乗算を要求する。このため、定義体の大きさが小さくなってもあまり処理速度が速くならない。そこで MOV 帰着を避けると共に処理速度を速くするための研究が進められている。任意の楕円曲線の利用を可能とする構成法は前述の Schoof[1995]のアルゴリズムを実用化することであり同方面の研究が盛んになされている[27]。一方、楕円曲線に制約を設けることにより安全性と効率性を実現しようとする方式も数多く提案されている。それらから代表的な方式を挙げると次表の通りである。

表 3　楕円曲線に制約を設けることにより
安全性と効率性を実現する構成法

方式分類	提案者	構成法の概要	備　　考
楕円曲線固有の性質を利用する方式	Koblitz[1991] Meier-Staffelbach[1993]	GF(2^l)上の超特異でない変則楕円曲線(anomalous elliptic curve)を利用した構成法	Frobenius 写像を利用して P の m 倍点の計算を高速化。
	Miyaji[1994]	#E(F_p)=p となる楕円曲線のうち P の x 座標が 0 となる楕円曲線を利用した構成法	P との加算に必要な定義体上の乗算の量を削減。
	Miyaji[1994]	F_p 上の楕円曲線のうち P の x,y 座標の絶対値が共に小さくなるような楕円曲線を利用した構成法	P との加算に必要な計算量とメモリ量を削減。
減法を利用する方式	Koyama-Tsuruoka[1992]	#E(F_p)が適当な大きさの素因数を持つ楕円曲線を利用した構成法	P の m 倍の計算を高速化。

3. 公開鍵暗号の計量的強度評価

最後に、FP、DLP、EDLP に基づく公開鍵暗号の「強度」を計量的に評価する。なお、ここでは「強度」を「利用者側が既存の解読法に対し最善の備えを行っているとの前提の下で、所与の鍵長の公開鍵暗号に対し攻撃者側が現時点で最善とされている方法で全面的解読を行うための平均計算量」と定義する。さらに、同計算量を実際の脅威度として実感するために、いくつかの前提をおいた上で、解

[27] Lercier and Morain[1995]は同方面の研究に関する優れたサーベイを与えている。

読に要する費用と時間に換算する。評価対象は現時点及び先行き 10 年後、20 年後の強度とする。試算の前提となる条件は以下の通りである。

まず、利用者側は既存の解読法を十分に考慮して鍵等の設定、日々の運用を行っていると仮定する。すなわち、利用者側は故障利用暗号攻撃を被らないような措置を講じるなど II で述べた個々の方式における利用上の留意事項を守った上で、FP に基づく公開鍵暗号を利用する場合には *p*-1 法、Fermat 法、特殊数体ふるい法等により、また DLP、EDLP に基づく公開鍵暗号を利用する場合には Pohlig-Hellman のアルゴリズム、指数計算法（特に DLP の場合は特殊版 Gordon のアルゴリズム、EDLP の場合は MOV 帰着）等により容易に解読されないように鍵を生成していると仮定する。このとき、攻撃者側の最善の全面的解読法は、FP に基づく公開鍵暗号に対しては一般数体ふるい法、DLP に基づく公開鍵暗号に対しては Schirokauer 版 Gordon のアルゴリズムないしは関数体ふるい法、EDLP に対しては Pohlig-Hellman のアルゴリズムとなるであろう。なお、一般数体ふるい法の平均計算量評価としては Coppersmith 版が理論的には最速であるものの実装が非常に困難とされているため、ここでは Adleman-Lenstra 版を取り上げた。

次に、Rivest の試算[28]を参考に上記平均計算量を解読費用と時間の積に換算するための前提を示そう。まず、1 計算量を計算機の処理速度を図る指標である MIPS[29]における 1 命令と換算した。次に、現時点（1997 年 6 月）の MIPS 単価を次のように試算した。現在では 250MIPS 相当の PC が約 20 万円とみられる。従って、200,000÷250 = 800（円／MIPS）となる。なお、解読装置である上記 PC の耐用年数は Rivest と同様に 5 年とする。また、技術進歩に伴う MIPS 単価の年間下落率予測については、これも Rivest と同様に、最小値で 20%、平均値で 33%、最大値で 45%と三つのシナリオを用意した。以下では、これらシナリオをそれぞれ最善シナリオ、標準シナリオ、最悪シナリオと呼ぶこととする[30]。

最後に、攻撃者が解読のために投資する資源（時間及び費用）の上限値を Type I、

---

[28] 同試算については Garfinkel[1995]を参照のこと。

[29] 1MIPS は対象となる計算機が一秒間に百万回の命令を実行する計算能力を持つことを示す。

[30] 本稿では解法自体に大きな進歩はないことを前提として試算している。これは解法が二つの技術パラメーターを持つ関数のためこれまでの通算 10 回弱の解法の進歩からこれらのパラメーターを有意に予測することが統計的に不可能な上、同進歩が安定的なトレンドを持つとは直観的にも考え難いからである。但し、技術進歩に伴う MIPS 単価の年間下落率予測における最悪シナリオの値は相当高目の値であるため、同予測により解法の進歩は部分的に織込まれるものと思われる。なお、解法の進歩を織込んだ予測としては Odlyzko [1995]が挙げられるが、そこでの解法の進歩に関する予測は統計的な手法を用いたものではなく予測精度が高いとは思われない。

Type II、Type III の 3 種類の攻撃者を想定して設定する。解読費用の上限値については、Type I が 1 千万円、Type II が 10 億円、Type III が 1,000 億円とする。試算を単純化するため、解読時間の上限値は何れのタイプの攻撃者も装置の耐用年数である 5 年とする。このように単純化することによって、解読途中の更新費用を考慮しないで済む上、攻撃者のタイプの違いを解読費用の違いのみで表せるからである。

以上に述べた強度評価に関する前提条件を纏めると表 4 の通り。

表 4　強度評価に関する前提条件

平均計算量	FP	解法：Adleman-Lenstra 版一般数体ふるい法 平均計算量：$L_p[1/3,1.922]=\exp(1.922(\log p)^{1/3}(\log\log p)^{2/3})$
	DLP	解法：Schirokauer 版 Gordon のアルゴリズムないしは関数体ふるい法 平均計算量：$L_p^k[1/3,1.922]=\exp(1.922(\log p^k)^{1/3}(\log\log p^k)^{2/3})$
	EDLP	解法：Pohlig-Hellman のアルゴリズム 平均計算量：$\exp(0.5\log p)$
単位計算速度当り費用	現在	MIPS 単価：800 円／MIPS
	将来	最善シナリオ：MIPS 単価の年間下落率 20% 標準シナリオ：同 33% 最悪シナリオ：同 45%
攻撃者の解読資源	解読時間	5 年間
	解読費用	Type I　：1 千万円 Type II：10 億円 Type III：1,000 億円

まず、各問題に関する鍵長と所要平均計算量（単位：MIPS YEAR＜以下、MYと略記＞）の関係を示すと表5の通り。

表5　鍵長と所要平均計算量の関係

[単位：MY]

鍵長	所要平均計算量	
	FP & DLP	EDLP
160	—	3.8E+10
200	—	4.0E+16
240	—	4.2E+22
280	—	4.4E+28
512	5.4E+05	—
1,024	4.0E+12	—
1,536	4.0E+17	—
2,048	4.7E+21	—

表5からは、FP・DLPに基づく方式の鍵長1,024 bit版がEDLPに基づく方式の同176 bit版に概ね相当し、FP・DLPに基づく方式の鍵長2,048 bit版がEDLPの同232 bit版に概ね相当することがみてとれる[31]。

[31] この辺りの結果は試算における前提の置き方により若干開きが生じる。例えば、一部の研究者の間ではFPに基づく方式の鍵長1,024 bit版がEDLPの同160 bit版に相当し、FPの同2,048 bit版がEDLPの同224 bit版に相当するとみられている。

次に、現時点で解読を 5 年間掛けて行う場合の鍵長と解読費用の関係は表 6 の通りである。なお、以下に掲載する表では、網掛けを次のように定義する。

：攻撃者 Type III により解読可能

：攻撃者 Type II により解読可能

表 6　5 年間で解読を行う場合の鍵長と解読費用の関係

[単位：億円]

鍵長	解読費用	
	FP & DLP	EDLP
160	―	6.1E+04
200	―	6.4E+10
240	―	6.7E+16
280	―	7.1E+22
512	8.7E-01	―
1,024	6.5E+06	―
1,536	6.4E+11	―
2,048	7.5E+15	―

FP・DLP に基づく方式の場合、現在よく利用されている鍵長 512 bit 版（以下、FP-512、DLP-512 と略記、他の暗号も同様に略記）は攻撃者 Type III のみならず攻撃者 Type II も解読可能となっており、これらは既に十分な安全性が保たれなくなっていることが示唆されている。反面、EDLP-160 は攻撃者 Type III でさえ解読困難であることを示唆する結果が示されている。

解読時間を 5 年間とした場合に、鍵長と解読費用の将来の関係を標準シナリオに基づいて試算すると表 7-1 に示す通りである。

表 7-1　鍵長と解読費用の関係の将来予測（標準シナリオ）

[単位：億円]

		解読費用			
問題		FP & DLP		EDLP	
解読開始時		10 年後	20 年後	10 年後	20 年後
鍵長	160	—	—	1.1E+03	1.8E+01
	200	—	—	1.1E+09	1.9E+07
	240	—	—	1.2E+15	2.0E+13
	280	—	—	1.2E+21	2.1E+19
	512	1.5E-02	2.6E-04	—	—
	1,024	1.1E+05	2.0E+03	—	—
	1,536	1.1E+10	1.9E+08	—	—
	2,048	1.3E+14	2.2E+18	—	—

FP-512、DLP-512 は 10 年後には攻撃者 Type I にさえ解読可能となるとの予測が示されている。FP-1024、DLP-1024 は 20 年後に攻撃者 Type III に解読される危険性が出てくることが示されている。EDLP-160 は 20 年後には攻撃者 Type III に解読可能となるが、EDLP-200 は 20 年後も解読困難との予測が示されている。

解読時間を 5 年間とした場合に、鍵長と解読費用の将来の関係を最悪シナリオに基づいて試算すると表 7-2 の通りである。

表 7-2　鍵長と解読費用の関係の将来予測（最悪シナリオ）

[単位：億円]

		解読費用			
問題		FP & DLP		EDLP	
解読開始時		10 年後	20 年後	10 年後	20 年後
鍵長	160	—	—	1.6E+02	3.9E-01
	200	—	—	1.6E+08	4.1E+05
	240	—	—	1.7E+14	4.3E+11
	280	—	—	1.8E+20	4.5E+17
	512	2.2E-03	5.6E-06	—	—
	1,024	1.6E+04	4.2E+01	—	—
	1,536	1.6E+09	4.1E+06	—	—
	2,048	1.9E+13	4.8E+10	—	—

FP-1024、DLP-1024 が 20 年後に攻撃者 Type III により解読可能となると予測されている。EDLP-160 は 10 年後に攻撃者 Type II に解読されるようになるが、EDLP-200 は 20 年後も解読困難との予測が示されている。

同様に、鍵長と解読費用の将来の関係を最善シナリオに基づいて試算すると表 7-3 の通りである。

表 7-3　鍵長と解読費用の関係の将来予測（最善シナリオ）

[単位：億円]

		解読費用			
問題		FP & DLP		EDLP	
解読開始時		10 年後	20 年後	10 年後	20 年後
鍵長	160	—	—	6.6E+03	7.1E+02
	200	—	—	6.9E+09	7.4E+08
	240	—	—	7.2E+15	7.8E+14
	280	—	—	7.6E+21	8.2E+20
	512	9.4E-02	1.0E-02	—	—
	1,024	7.0E+05	7.5E+04	—	—
	1,536	6.9E+10	7.4E+09	—	—
	2,048	8.0E+14	8.6E+13	—	—

以上の結果を総合すると、解法には殆ど進展がないとの前提の下では次のようなことが言えるであろう。すなわち、たとえ最悪の場合（最悪シナリオ）でも 20 年後に十分な強度を確保できるような方式を利用者が望むのであれば、FP、DLP に基づく方式の場合、鍵長は 1,536 bit 以上のものが推奨されるのに対し、EDLP に基づく方式の場合、鍵長は 200 bit 以上のものが推奨される。

実際には解法の進歩が起こり得ることを考慮すると、解法の進歩がないことを前提とした上記結論よりも最低限一段階は高い水準の方式、FP、DLP に基づく方式では鍵長が 2,048 bit 以上のもの、EDLP に基づく方式では同 240 bit 以上のものを採用することが推奨される。特に、EDLP では準指数関数時間の解法が一般的に存在しないとの予想は未だ確固としたものではなく、同問題に対し信頼のできる解答を得るまでには今後少なくとも 5 年間程度の研究の蓄積を待つ必要があるとの見方が一般的である。従って、現時点で EDLP に基づく方式を導入するのであれば、何時でも迅速に鍵長を切り替えられるような仕組みを確保しておく必要があると思われる。

（おわりに）

本稿では、公開鍵暗号の安全性に関するこれまでの研究を概観し、様々な角度から、各方式の安全性を検討・整理した。その結果、現在十分な強度を持つとされている方式は、秘密通信方式、ディジタル署名方式の何れも FP、DLP、EDLP の何れかの問題の困難性に基づいていることが示された。また、具体的な方式には同方式固有のいくつかの利用上の留意事項があることが示された。特に、暗号装置に物理的影響を与えることにより暗号化の計算途上で誤りを発生させ、その結果を解読に利用する故障利用暗号攻撃は非常に強力な攻撃であるため、同攻撃が運用上脅威と成り得る場合には同攻撃に対する備えが必要とされることが明らかにされた。最後に、FP、DLP、EDLP に基づく公開鍵暗号の強度を計量的に評価した。その結果、解法に画期的な進展がもたらされないとの前提の下では、解読に 1,000 億円を投資できるような非常に強力な仮想攻撃者に対して今後 20 年間十分な強度を保つためには FP、DLP に基づく方式の場合、鍵長は 2,048 bit 以上のものが推奨され、EDLP に基づく方式の場合、鍵長は 240 bit 以上のものが推奨されるとの結果が示された。EDLP は FP や DLP ほど研究されていないため、将来、画期的な解法が発見される可能性がないとは言い切れない。しかし、たとえ画期的な解法が示されるとしても、同解法が FP や DLP の解法よりも高速な解法に成るとは想定し難いことを考慮すると、近い将来、公開鍵暗号を新規に導入するのであれば、何時でも迅速に鍵長を切り替えられるような備えを施した上で、鍵長 240 bit 以上の EDLP に基づく方式を採用することは現時点における有力な選択肢の一つであると思われる。

但し、解法もコンピューターの処理性能も予測できないほど急激に進歩する場合がある。極端な例を挙げると、FP や DLP が多項式時間で解けるような画期的な解法が考案されるとか、超並列処理が可能な DNA コンピューターが実現するといった可能性も完全に否定することはできない。従って、絶対的なセキュリティが要求される環境で暗号技術が利用されている場合、解法やコンピューターの処理性能等の暗号解読技術の進歩を常に注視しておく必要があると思われる。

以　上

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

今井秀樹、『暗号のおはなし』、日本規格協会、1993 年

太田和夫・藤岡　淳、「ゼロ知識証明の応用」、岡本・太田（共編）、『暗号・ゼロ知識証明・数論』、共立出版、1995 年

岡本龍明・櫻井幸一、「代数幾何学的アルゴリズム」、岡本龍明・太田和夫（編）、『暗号・ゼロ知識証明・数論』、共立出版、1995 年

————・櫻井幸一、『現代暗号』、産業図書、1997 年

小野　孝、『数論序説』、裳華房、1987 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

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、A、Vol. J70-A、No. 11、pp. 1632-1636、1987 年 11 月

————・藤岡　淳・宮地充子、「暗号理論への応用」、岡本龍明・太田和夫（編）、『暗号・ゼロ知識証明・数論』、共立出版、1995 年

小山謙二・静谷啓樹、「素因数分解と離散対数問題アルゴリズム」、岡本龍明・太田和夫（編）、『暗号・ゼロ知識証明・数論』、共立出版、1995 年

————・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

酒井康行・石塚裕一・櫻井幸一、「RSA 暗号鍵の安全性と生成効率に関する実験と解析」、1997 年暗号と情報セキュリティ・シンポジウム、 SCIS’97-15C、1997 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・今井秀樹・原島・宮川、「公開鍵暗号系の新しいアルゴリズム」、電子情報通信学会技術研究報告、IT82-24、1982 年

————・————・————・————、「有限体 *GF*(2)上の多変数多項式を公開鍵とする非対称全射暗号系」、電子情報通信学会技術研究報告、IT83-47、1984 年

————・————・————・————、「Obscure 表現による高速非対称暗号系」、電子情報通信学会技術研究報告、IT84-50、1985 年

————・————、「署名機能と機密保持機能を効率良く実現する多変数多項式タプル非対称暗号系の構成」、電子情報通信学会論文誌(A)、Vol. J71-A、No. 7、pp. 1441-1452、1988 年 7 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、SCIS’97-7B、1997 年

盛合志帆、「故障利用暗号攻撃によるブロック暗号の解読」、1997 年暗号と情報セキュリティシンポジウム、SCIS’97-6A、1997 年

山根義則・古屋聡一、櫻井幸一、「エルガマル暗号によるブラインド復号化方式」、電気関係学会九州支部連合大会講演論文集、1167、pp. 723、1995 年 9 月

————・櫻井幸一、「無制限な盗聴を防ぐ鍵寄託方式」、1996 年暗号と情報セキュリティシンポジウム、SCIS’96-7C、1996 年

Abe, M. and E. Fujisaki, “How to date blind signatures,” Advances in Cryptology — Proceedings of ASIACRYPT ’96, Lecture Notes in Computer Science, Vol. 1163, pp. 244-251, Springer-Verlag, 1996.

Adleman, L. M., “A subexponential algorithm for the discrete logarithm problem with applications to cryptography,” Proceedings of FOCS, ,pp. 55-60, 1979.

———— and R. L. Rivest, “How to break the Lu-Lee (COMSAT) public-key cryptosystem,” MIT Laboratory for Computer Sience, July 1979.

————, C. Pomerance, and R. S. Rumely, “On distinguish prime numbers from composite numbers,” *Ann. of Math.*, Vol. 117, pp.173-206, 1983.

———— and M. A. Huang, *Primarity testing and abelian varieties over finite fields*, Lecture Notes in Math., Vol. 1512, Springer-Verlag, 1992.

————, “The function field sieve,” Algorithmic Number Theory, Lecture Notes in Computer Science, Vol. 877, pp. 108-121, Springer-Verlag, 1994.

Alex, W., B. Chor, O. Goldreich, and C. P. Schnorr, “RSA/Rabin bits are 1/2+1/poly(log *N*) secure,” Proceedings of the IEEE 25th Symposium on the Foundations of Computer Science, pp. 449-457, 1984.

Anderson, R., “A serious weakness of DES,” November 1996. news:CMM.0.90.1.847310320.risko@chirom.cs1.sri.com

Atkin, A. O. L. and F. Morain, “Elliptic curves and primality proving,” *Math. Comp.*, Vol. 61, pp. 29-68, 1993.

Bao, F., R. Deng, Y. Hang, A. Jeng, T. H. Nagir, and D. Narashimaharu, “A new attack to RSA on tamerproof devices,” October 1996, email:<9610240229.AA01599@aquarius.iss.nus.sg>

Bellare, M., 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.

Bellovin, S. M. and M. Merritt, “Encrypted key exchange: Password-based protocols secure against dictionary attacks,” Proceedings of the 1992 IEEE Computer Society Conference on Research in Security and Privacy, pp. 72-84, 1992.

Beth, T. and F. Schaefer, “Nonsupersingular elliptic curves for public key cryptosystems,” Advances in Cryptology — Proceedings of EUROCRYPT ’91, Lecture Notes in Computer Science, Vol. 547, pp. 316-327, Springer-Verlag, 1991.

Blakley, B. and G. R. Blakley,“Security of number theoretic public key cryptosystems against random attack (Part I),” Cryptologia, Vol. 2, No. 4, pp. 305-321, 1978a.

———— and ————, “Security of number theoretic public key cryptosystems against random attack (Part II),” Cryptologia, Vol. 3, No. 1, pp. 29-42, 1978b.

———— and ————, “Security of number theoretic public key cryptosystems against random attack (Part III),” Cryptologia, Vol. 3, No. 2, pp. 105-118, 1979a.

————, “Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages,” Computers and Mathematics with Applications, Vol. 5, pp. 169-178, 1979b.

————, “Safeguarding cryptographic keys,” Proceedings of the National Computer Conference, Vol. 48, pp. 242-268, American Federation of Information Processing Societies, 1979c.

Blaze, M., W. Diffie, R. L. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Wiener, “Minimal key lengths for symmetric ciphers to provide adequate commercial security,” A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, January 1996.

Bleichenbacher, D., “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.

Blum, M. and S. Micali, “How to generate cryptographically strong sequences of pseudo random bis,” Proceedings of FOCS, pp. 112-117, 1982.

————, P. Feldman, and S. Micali, “Non-interactive zero-knowledge proof systems and applications,” Proceedings of the 20-th Annual ACM Symposium on Theory of Comupting, pp. 103-112, 1988.

Boneh, D., R. A. DeMillo, and R. J. Lipton, “A new breed of crypto attack on “Tamperproof” tokens cracks even the strongest RSA Code,” September 1996, available at

http://www.bellcore.vom/PRESS/ADVSRY96/smrtcrd.html

Brands S., “An efficient off-line electronic cash system based on the representation problem,” Texcnical Report, CS-R9323, CWI, April 1993.

Brandt, J., I. B. Damgard, P. Landrock, and, T. Pederson, “Zero-knowledge authentication scheme with secret key excahnge,” Advances in Cryptology — Proceedings of CRYPTO ’88, Lecture Notes in Computer Science, Vol. 403, pp. 583-588, Springer-Verlag, 1990.

Brickell E. F. 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.

———— and A. M. Odlyzko, “Cryptanalysis: A survey of recent results,” in G. J. Simmons, ed., *CONTEMPORARY CRYPTOLOGY — The Science of Information Integrity*, IEEE Press, 1992.

Brillhart, J., D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., “Factorizations of $b^n \pm 1$ up to high powers,” Contemporary Mathematics, Vol. 22, American Mathematical Society, Providence, 1983.

Charlap, L. S., R. Coley, and D. P. Robbins, “Enumeration of rational points on elliptic curves over finite fields,” Manuscript, 1991.

Chaum, D., “Blind signatures for untraceable payments,”Advances in Cryptology — Proceedings of Crypto 82, pp. 199-203, Plenum Press, 1983.

————, “Security without identification: transaction system to make big brother obsolete,” *Communications of the ACM*, Vol. 28, No. 10, pp. 1030-1044, 1985.

————, “Zero-knowledge undeniable signatures,”Advances in Cryptology — Proceedings of EUROCRYPT ’90, Lecture Notes in Computer Science, Vol. 473, pp. 458-464, Springer-Verlag, 1991a.

————, “Group signatures,” Advances in Cryptology — Proceedings of EUROCRYPT ’91, Lecture Notes in Computer Science, Vol. 547, pp. 257-265, Springer Verlag, 1991b.

Coppersmith, D. “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. Schroeppel “Discrete logarithms in *GF*(*p*),” *Algorithmica*, Vol. 1, pp. 1-15, 1986.

————, M. Franklin, J. Patarin, 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, Springer-Verlag,

1996.

Damgard, I., “Towards practical public key cryptosystems secure against chosen ciphertext attacks,”Advances in Cryptology — Proceedings of CRYPTO ’91, Lecture Notes in Computer Science, Vol. 576, pp. 445-456, Springer-Verlag, 1991.

Davida, G. I., “Chosen signature cryptanalysis of the RSA(MIT) public key cryptosystem,” *Technology Report TR-82-2*, Univ. of Wisconsin Department of Electrical Engineering and Computer Science, October 1982.

DeLaurentis, J.M., “A further weakness in the common modulus protocol for the RSA cryptosystem,” *Cryptologia*, Vol. 8, No. 3, pp. 253-259, 1984.

Delsarte, P., Y. Desmedt, A. Odlyzko, and P. Pret, “Fast cryptanalysis of the Matsumoto-Imai public key scheme,” Advances in Cryptology — Proceedings of EUROCRYPT ’84, Lecture Notes in Computer Science, Vol. 209, pp. 142-149, Springer-Verlag, 1985.

Denning, D. E., “Digital signatures with RSA and other public key protocols,” *Commun. ACM*, Vol. 27, pp. 388-392, 1984.

Deuring, M., “Die typen der multiplikatorenringe elliptischer funktionenkorper, ” *Abh. Math. Sem. Hamburg*, Vol. 14, pp. 199-272, 1941.

Diffie, W. 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,” *Designes, Codes and Cryptography*, Vol.2, pp.107-125, 1992.

Dwork, C. 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.

ElGamal, T. E., “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, 1985.

————, “A subexponential-time algorithm for computing discrete logarithms over $GF(p^2)$,” *IEEE Transactions in information Theory*, Vol. IT-31, pp. 473-481, 1985.

Estes, D., L.M. Adleman, K. Konpella, K.S. McCurley, and G.L. Miller, “Breaking the Ong-Schnorr-Shamir signature schemes for quadratic number fields,” Advances in Cryptology — Proceedings of CRYPTO ’85, Lecture Notes in Computer Science, Vol. 218, pp. 3-13, Springer-Verlag, 1986.

Feige, U. and A. Shamir, “Witness indistinguishable and witness hiding protocols, ”

Proceedings of STOC, pp. 416-426, 1990.

Fiat, A. and A. Shamir, “How to prove yourself: practical solutions to identification and signature problems,” Advances in Cryptology — Proceedings of CRYPTO ’86, Lecture Notes in Computer Science, Vol. 263, pp. 186-194, Springer-Verlag, 1986.

Garfinkel, S., *PGP: Pretty Good Privacy*, O’Reilly & Associates, Inc. , 1995.

Girault, M., “Self-certified public keys,” Advances in Cryptology — Proceedings of EUROCRYPT ’91, Lecture Notes in Computer Science, Vol. 547, pp. 490-497, Springer-Verlag, 1991.

Goethals, J. M. and C. Couvreur, “A cryptanalytic attack on the Lu-Lee public-key cryptosystem,” Philips J. Res., Vol. 35, pp. 301-306, 1980.

Goldwasser, S. and S. Micali, “Probabilistic encryption,” *Journal of Computer and System Sciences*, Vol. 28, No. 2, pp. 270-299, 1984.

———— and J. Kilian, “Almost all primes can be quickly certified,” Proceedings of STOC, pp. 316-329, 1986.

————, S., S. Micali, and R. Rivest, “A digital signature scheme against adaptive chosen message attack,” *SIAM J. Comput.*, Vol. 17, No. 2, pp. 281-308, 1988.

Gordon, D. M., “Strong primes are easy to find,” Advances in Cryptology — Proceedings of EUROCRYPT ’84, Lecture Notes in Computer Science, Vol. 209,pp. 216-223, Springer-Verlag, 1985.

————, “Designing and detecting trapdoors for discrete log cryptosystems,” Advances in Cryptology — Proceedings of CRYPTO’92, Lecture Notes in Computer Science, Vol. 740,pp. 66-75, Springer-Verlag, 1993.

————, “Discrete logarithm field in GF(p) using the number field sieve,” to appear in *SIAM Jounal on Discrete Math*.

Guy, R. K., “How to factor a number,” Proceedings of 5th Manitoba Conference on Numerical Mathematics, pp. 49-89, 1975.

Harper, G., A. Menezes, and S. Vanstone, “Public-key cryptosystem with very small key length,” Advances in Cryptology — Proceedings of EUROCRYPT ’92, Lecture Notes in Computer Science, Vol. 658, pp. 163-173, Springer-Verlag, 1993.

Hastad, J., “On using RSA with low exponent in a public-key,” Advances in Cryptology — Proceedings of CRYPTO ’85, Lecture Notes in Computer Science, Vol. 218, pp. 403-408, Springer-Verlag, 1986.

Horster, P., H. Petersen, and M. Michels, “Meta-ElGamal signature schemes based on the

discrete logarithm problem and their applications," Advances in Cryptology — Proceedings of ASIACRYPT '94, Lecture Notes in Computer Science, Vol. 917, pp. 224-237, Springer-Verlag, 1995.

Knuth, D., *The art of computer programming*, Vol. 2, (seminumerical algorithms), Addison-Wesley, 1981.

Koblitz, N., "Elliptic curve cryptosystems," *Mathematcs of Comuptation*, Vol.48, pp.203-209, 1987.

————, "Cm-curves with good cryptographic properties," Advances in Cryptology — Proceedings of CRYPTO '91, Lecture Notes in Computer Science, Vol. 576, pp. 279-287, Springer-Verlag, 1992.

Korzhik, V. I. and A. I. Turkin, "Cryptanalysis of McEliece's public-key cryptosystem," Advances in Cryptology — Proceedings of EUROCRYPT '91, Lecture Notes in Computer Science, Vol. 547, pp.68-70, Springer-Verlag, 1991.

Koyama, K. and Y. Tsuruoka, "Speeding up elliptic cryptosystems by using a signed bunary window method," Advances in Cryptology — Proceedings of CRYPTO '92, Lecture Notes in Computer Science, Vol. 740, pp.345-357, Springer-Verlag, 1992.

Lenstra, A. K., H. W. Jr. Lenstra, M.S. Manasse, and J.M. Pollard, "The number field sieve," *Annals of Mathematics*, Vol. 126, pp. 649-673, 1987.

Lenstra, H. W. Jr., "Integer programming with a fixed number of variables," Univ. of Amsterdam Tech. Report, Vol. 81-03, April 1981.

————, "Factoring Integers with elliptic Curves," *Annals of Mathematics*, Vol. 126, pp. 649-673, 1987.

Lercier, R. and F. Morain, "Counting the number of point on elliptic curves over finite fields: starategies and performances," Advances in Cryptology — Proceedings of EUROCRYPT '95, Lecture Notes in Computer Science, Vol. 921, pp. 79-94, Springer-Verlag, 1995.

Matsumoto, T. and H. Imai, "A class of asymmetric cryptosystems based on polynomials over finite rings," Proceedings of IEEE International Symposium on Information Theory, pp. 131-132, September 1983.

———— and ————, "On the key distribution system: A practical solution to the key distribution problem," Advances in Cryptology — Proceedings of CRYPTO '87, Lecture Notes in Computer Science, Vol. 293, pp. 185-193, Springer-Verlag, 1988.

———— and ————, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption,"

McEliece, R. J., “A public-key cryptosystem based on algebraic coding theory,” Deep Space Network Progress Report, pp. 42-44, Jet Propulsion Laboratory, 1978.

Meier, W. and O. Staffelbach, “Efficient multiplication on certain nonsupersingular elliptic curves,” Advances in Cryptology — Proceedings of CRYPTO ’92, Lecture Notes in Computer Science, Vol. 740, pp. 333-344, Springer-Verlag, 1993.

Menezes, A. and S. Vanstone, “The implementation of elliptic curve cryptosystems,” Advances in Cryptology — Proceedings of AUSCRYPT ’90, Lecture Notes in Computer Science, Vol. 453, pp. 2-13, Springer-Verlag, 1990.

————, T. Okamoto, and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field,” Proceedings of STOC, pp. 80-89, 1991.

Merkle, R. C. and M. E. Hellman, “Hiding information and signatures in trapdoor knapsacks,” *IEEE Transactions on Information Theory*, Vol.IT-24, No.5, pp.525-530, September 1978.

Micali, S., “Fair public key cryptosystems,” Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, Mass.; MIT/LCS/TR-579.b; November 1993.

Miller, V. S., “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.

Miyaji, A., “Elliptic curve cryptosystems immune to any reduction into the discrete logarithm problem,” *IEICE Transactions on Fundamentals*, Vol.E76-A, No. 1, pp. 50-54, 1993.

————, “Elliptic curves suitable for cryptosystems,” *IEICE Transactions on Fundamentals*, Vol.E77-A, No. 1, pp. 98-105, 1994.

————, “A message recovery key signature scheme equivalent to DSA over elliptic curves,” Advances in Cryptology — Proceedings of ASIACRYPT ’96, Lecture Notes in Computer Science, Vol. 1163, pp. 1-14, Springer-Verlag, 1996.

Montgomery, P. L., “Speeding the Pollard and elliptic curve methods of factorization,” *Math., Comp.*, pp. 243-264, 1987.

Moore, J. H., “Protocol failures in cryptosystems,” in G. J. Simmons, ed., *CONTEMPORARY CRYPTOLOGY — The Science of Information Integrity*, IEEE Press, 1992.

Morain, F., “Building cyclic elliptic curves modulo large primes,” Advances in Cryptology — Proceedings of EUROCRYPT ’91, Lecture Notes in Computer Science, Vol. 547, pp. 328-336, Springer-Verlag, 1991.

Naor, M. 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, 1991.

————, "The digital signature standard," Com. of the ACM, Vol.35, No.7, pp.36-40, 1992.

Odlyzko, M., "The future of integer factorization," Proceedings of Multimedia and Information Security, JAIST, pp. 139-151, 1995.

Ohta, K. and T. Okamoto, "A modification of the Fiat-Shamir scheme," Advances in Cryptology — Proceedings of CRYPTO '88, Lecture Notes in Computer Science, Vol. 403, pp. 232-243, Springer-Verlag, 1993.

Okamoto, E. and K. Tanaka, "Keu distribution based in identification information," *Electronics Letters*, Vol.7, No.4, pp. 481-485, May 1989.

Okamoto, T. and A. Shiraishi, "A fast signature scheme based on quadratic inequalities," Proceedings of the 1985 Symposium on Security and Privacy, IEEE, pp. 123-132, April 1985.

————, "Fast public-key cryptosystems using congruent polynomial equations," *Electronics Letters*, Vol. 22, No. 11, pp. 581-582, 1986.

————, "A fast signature scheme based on congruential polynomial operations," *IEEE Transactions on Information Theory*, Vol. 36, No. 1, pp. 47-53, 1990.

———— and K. Ohta, "Divertible zero-knowledge interactive proofs and commutative random self-reducibility," Advances in Cryptology — Proceedings of EUROCRYPT '89, Lecture Notes in Computer Science, Vol. 434, pp. 134-149, Springer-Verlag, 1990.

————, "Provably secure and practical identification schemes and corresponding signature schemes," Advances in Cryptology — Proceedings of CRYPTO '92, Lecture Notes in Computer Science, Vol. 547, pp. 31-53, Springer-Verlag, 1993.

————, A. Fujioka, and E. Fujisaki, "An efficient digital siganture scheme based on an elliptic curve over the Ring Zn," Advances in Cryptology — Proceedings of CRYPTO '92, Lecture Notes in Computer Science, Vol. 547, pp. 54-65, Springer-Verlag, 1993.

———— and K. Ohta, "Survey of digital signatures," Proceedings of the Third Symposium on: State and Progress of Research in Cryptography, pp. 17-29, Fondazone Ugo Bordoni, 1993.

Ong, H. and C.P. Schnorr, "Signatures through approximate representations by quadratic forms," Advances in Cryptology — Proceedings of Crypto '83, Plenum

Press, 1984.

————, ————, and A. Shamir, “An efficient signature scheme based on polynomial equations,” Proceedings of the 16th Annual Symposium on the Theory Computing, pp. 208-216, 1984.

Phitzmann, M. and M. Waidner, “Formal aspects of fail-stop signature,” Fakultät für Informatic, University Karlsruhe, Deutschland, Report 22/29, 1990.

Pohlig, S. 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.

Pointcheval, D. 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.

Pollard, J.M., “Theorems on factorization and primality testing,” Proceedings of Camb. Philos. Soc., Vol. 76, pp. 521-528, 1974.

————, “A Monte Carlo method for factorization,” *BIT*, Vol. 15, pp. 331-334, 1975.

———— and C. P. Schnorr, “An efficient solution of the congruence $x^2+ky^2=m$ (mod n),” *IEEE Transactions on Information Theory*, Vol. IT-33, No.5, pp. 702-709, September 1987.

Pomerance, C., *The quadratic sieve algorithm*, Lecture Notes in Computer Science, Vol. 209, pp. 169-182, 1985.

Rabin, M. O., “Probabilistic algorithms,” Algorithms and complexity-new directions and recent results, Academic Press, 1976.

————, “Digitalized signatures and public-key functions as intractable as factorization,” M.I.T. Laboratory for Computer Science, Technical Report MIT/LCS/TR-212, 1979.

Rivest, R. L., A. Shamir, and L. Adleman, “A metohd of obtaining digital signatures and public key cryptosystems,” *Communications of the ACM*, Vol. 21, No. 2, pp.120-126, 1978a.

————, “Remarks on a proposed cryptanalytic attack on the MIT public-key cryptosystem,” *Cyrptologia*, pp.62-65, 1978b.

Rompel, J., “One-way functions are sufficient for secure signatures,” Proceedings of STOC, pp. 387-394, 1990.

Sakurai, K. and H. Shzuya, “Relationships among the computational powers of breaking discrete log systems,” Advances in Cryptology — Proceedings of EUROCRYPT ’95, Lecture Notes in Computer Science, Vol. 921, pp. 341-355, Springer-Verlag, 1995.

Schneier, B., *APPLIED CRYPTOGRAPHY*, John Wiley & Sons, Inc., 1993.

Schirokauer, O., 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.

Schnorr, C. P., "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.

———— and H. H. Hörner, "Attacking the Chor-Rivest cryptosystem by improved lattice reduction," Advances in Cryptology — Proceedings of EUROCRYPTO '95, Lecture Notes in Computer Science, Vol. 921, pp. 1-12, Springer-Verlag, 1995.

Schoof, R., "Elliptic curves over finite fields and the computation of square roots mod *p*," *Mathematics of Computation*, Vol. 44, pp. 483-494, 1985.

Shamir, A. and R. E. Zippel, "On the security of the Merkle-Hellman cryptographic scheme," *IEEE Transactions on Information Theory*, Vol. IT-26, No.3, pp.339-340, May 1980.

————, "Identity-based cryptosystems and signature schemes," Advances in Cryptology — Proceedings of CRYPTO '84, Lecture Notes in Computer Science, Vol. 196, pp. 47-53, Springer-Verlag, 1985.

Shanks, D., "Class number, a theory of factorization, and Genera," Proceedings of Syposium Pure Mathematics, AMS, 1972.

Silverman, R. D., "The multiple polynomial quadratic sieve," *Math, Comp.*, Vol. 48, pp. 243-264, 1987.

Simmons, G. J. and M. J. Norris, "Preliminary comments on the MIT public-key cryptosystem," *Cryptologia*, Vol. ,No. , pp.406-414, October 1977.

————, "A 'weak' privacy protocol using the RSA crypto algorithm," *Cryptologia*, Vol.7,No.2, pp.180-182, April 1983.

Stinson, D. R., *CRYPTOGRAPHY — Theory and Practice*, CRC Press, 1995.（櫻井幸一監訳、『暗号理論の基礎』、共立出版、1996 年）

Solovay, R. and V. Strassen, "A fast Mote-Carlo test for primarity," *SIAM J. Comp.*, Vol. 6, pp. 84-85, 1977.

Vallée, B., M. Girault, and P. Toffin, "How to break Okamoto's cryptosystem by reducing lattice values," Advances in Cryptology — Proceedings of EUROCRYPT '88, Lecture Notes in Computer Science, Vol. , pp. 83-88, Springer-Verlag, 1996.

van Oorschot, P.C., "A comparison of practical public key cryptosystems based on integer

factorization and discrete logarithms," in G.J. Simmons, ed., *CONTEMPORARY CRYPTOLOGY — The Science of Information Integrity*, IEEE Press, 1992.

Vaudenay, S., "Hidden collisions on DSS," Advances in Cryptology — Proceedings of CRYPTO '96, Lecture Notes in Computer Science, Vol. 1109, pp. 281-291, Springer-Verlag, 1988.

Von zur Gathen, J., D. Kozen, and S. Landau, "Functional decomposition of polynomials," Proceedings of the 28th IEEE Symposium on the Foundations of Computer Science, pp. 127-131, IEEE Press, 1987.

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

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

————, "Some public-key crypto-functions as intractable as factorization," Advances in Cryptology — Proceedings of CRYPTO '84, Lecture Notes in Computer Science, Vol. 196, pp. 66-70, Springer-Verlag, 1985.

Wiener, M.J., "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information theory*, Vol. IT-36, No. 3, pp. 553-558, 1990.

Zheng, Y. and J. Seberry, "Practical approaches to attaining security against adaptively chosen ciphertext attacks,"Advances in Cryptology — Proceedings of CRYPTO '92, Lecture Notes in Computer Science, Vol. 740, pp. 292-304, Springer-Verlag, 1993.

———— and T. Matsumoto, "Breaking smart card based ElGamal signature and its variants," presented at the rump session in ASIACRYPT'96, available at http://pscit-www.fcit.monash.edu.au/～yuliang/pubs/a96-rump.ps.Z

付 1 初等整数論の基礎事項

以下では、公開鍵暗号の根底をなす初等整数論につき簡単に紹介する。

定義 1.1（剰余定理）任意の二つの整数 a,b に対して、$b \neq 0$ ならば、

$$a = qb+r \quad (0 \leqq r < |b|)$$

を満たす q, r が一意に定まる。

r を法 b に関する a の**剰余**（residue）と呼ぶ。$r=0$ の場合、a を b の**倍数**、b を a の**約数**または**因数**といい、このとき a は b で**割り切れる**といって $b|a$ で表す。二つの整数 $a,\ b$ の共通な倍数を**公倍数**といい、そのうち正で最小のものを**最小公倍数**といって、LCM(a, b)で表す。同様に、二つの整数 a, b の共通な約数を**公約数**といい、そのうち正で最大のものを**最大公約数**といって、GCD(a, b)で表す。

$n|(a-b)$のとき、$a \equiv b \pmod{n}$と記し、a と b は n を**法**として**合同**（congruent）という。また、上式を**合同式**（congruence）と呼ぶ。以下では、合同式を表現する場合にも、記号「≡」の代りに「=」を用いることとする。

1 でない自然数 p で、1 と p 以外に約数を持たないものを**素数**（prime number）といい、1 でも素数でもない自然数を**合成数**という。合成数 n は素因数の積に分解される。この分解は本質的に一通りである。

二つの整数の最大公約数は、**Euclid の互除法**により容易に計算できる。

【Euclid 互助法】

Step 1: 与えられた整数 m,n に対し、$n_0:=m;\quad n_1:=n$ とおく。

Step 2: 除法 $n_{i-1}:=q_{i-}\times n_i+ n_{i+1}$、$0 \leqq n_{i+1} < |n_i|$を実行する(1,2,...)。

Step 3: $n_{i+1}=0$ ならば $d:=n_i$ で完了、そうでなければ次の i について Step 2 に戻る。

定義 1.2（剰余類）正の整数 p を法とする剰余の集合 $R_p=\{0,\ 1,\ \cdots,\ p\text{-}1\}$を**剰余類**（residue class）と呼ぶ。剰余類 R_n の中で GCD(a_i, p) = 1 を満たす元の集合を**既約剰余類**（reduced residue class）という。

剰余類 R_p の中で、p と互いに素であるものの個数を$\phi(p)$で表し、**Euler の関数**（Euler's function）という。従って、既約剰余類の場合、$\phi(p) = p\text{-}1$ となる。

定理 1.1（Euler の定理）GCD(a, q) = 1 であるとき、

$$a^{\phi(q)} = 1 \bmod q$$

が成立する。

Euler の定理から次の **Fermat の小定理**が直ちに導かれる。

定理 1.2（Fermat の小定理） GCD(a, p) = 1 であり、p が素数である場合、

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

が成立する。

法が相異なる連立一次合同式の解の存在と一意性、そして具体的な解法は、次の**中国人剰余定理**（Chinese remainder theorem）で与えられる。

定理 1.3（中国人剰余定理） $m_1, m_2, \cdots, m_k$ が互いに素で、$M=m_1m_2\cdots m_k$ とする。このとき、次の連立合同式

$$\begin{aligned} x &= d_1 \bmod m_1 \\ x &= d_2 \bmod m_2 \\ &\cdots \\ x &= d_k \bmod m_k \end{aligned}$$

の解は $\boldsymbol{Z}_M$ 上で一意に存在し、帰納的に計算できる。

定義 1.3（平方剰余） 2 次合同式 $x^2 = a \pmod p$ が整数解をもつとき、a を p を法とした**平方剰余**（quadratic residue）という。一方、同合同式が整数解をもたないとき、a を p を法とした**平方非剰余**（quadratic non-residue）という。

p が素数のとき、a が p の平方剰余か否かを、$(a|p) = +1$ または -1 で表す（**Legendre 記号**）。p が奇素数のとき、$(a|p) = a^{(p-1)/2} \pmod p$ である。$(a|p)$ は次の諸公式で容易に計算できる。

$(ab|p) = (a|p)(b|p)$

$a = b \pmod p$ ならば $(a|p) = (b|p)$

p, q が奇素数ならば $(p|q)(q|p) = (-1)^{(p-1)(q-1)/4}$　（平方剰余の相互法則）

$(-1|p) = (-1)^{(p-1)/2}$　（第 1 補充法則）

$(2|p) = (-1)^{(p+1)(p-1)/8}$　（第 2 補充法則）

付 2 有限体理論の基礎事項

ある集合 G が G 上で定義されるある演算に関して閉じている、すなわち、$a,b \in G$ ならば $a \cdot b \in G$ であるとき、G と演算・の組$(G,\cdot)$を**代数系**という。

定義 2.1（群）代数系$(G,\cdot)$が次の性質を満たすとき、$(G,\cdot)$は**群**（group）であるという。

① 任意の $a,b,c \in G$ に対して、**結合法則**$(a\cdot b)\cdot c = a\cdot(b\cdot c)$が成り立つ。

② ある元 $e \in G$ が存在して、任意の元 $a \in G$ に対して $e\cdot a = a\cdot e = a$ が成り立つ。e を**単位元**と呼ぶ。

③ 任意の元 $a \in G$ に対して、$a\cdot b = b\cdot a = e$ となるような元 b が存在する。b を a の**逆元**と呼ぶ。

群 G の任意の 2 元 a,b に対して、**交換法則** $a\cdot b = b\cdot a$ が成立するとき、G を**可換群**（Abelian group）という。可換群では、便宜上演算・を+と表記し、**加法群**（additive group）と呼ぶ。これに対し、演算・が必ずしも可換でない場合、**乗法群**（multiplicative group）と呼び、単位元を 1、a の逆元を a^{-1} と表現することが多い。

群の元の個数が無限である群を**無限群**（infinite group）、有限である群を**有限群**（finite group）と呼ぶ。群 G に属する元の個数を G の**位数**（order）という。群 G の部分集合 S が同じ演算・のもとに群であるとき、S を G の**部分群**（subgroup）という。

定義 2.2（環）二つの 2 項演算子+,・を持つ代数系$(R,+,\cdot)$が次の条件を満たすとき**環**（ring）という。

① $(R,+)$は可換群である。

② $(R \setminus \{0\},\cdot)$は逆元の存在を除く乗法群の定義を満たす。

③ 任意の $x,y,z \in G$ に対して、$x\cdot(y+z) = x\cdot y+x\cdot z$ かつ$(y+z)\cdot x = y\cdot x+z\cdot x$ が成り立つ（分配法則）。

乗法について可換な環は**可換環**（Abelian ring）と呼ばれる。+,・を通常の足し算、掛け算と考えれば、整数集合 $\boldsymbol{Z}$、有理数集合 $\boldsymbol{Q}$、実数集合 $\boldsymbol{R}$、複素数集合 $\boldsymbol{C}$ は全て可換環である。また、正整数 n を法とする剰余類 $\boldsymbol{Z}_n$ には自然に加法、乗法が定義されて可換環になる。逆に、可換環ではない身近な例としては、$\boldsymbol{Z},\boldsymbol{Q},\boldsymbol{R},\boldsymbol{C}$ 等の可換環の要素を要素とする任意の正方行列に通常の加法と乗法を定義した集合が挙げられる。

定義 2.3（零因子）可換環 R の要素 $a \neq 0$ に対し、$a\cdot b = 0$ となるような $b \neq 0$ が R

に存在する場合、a を**零因子**（zero divisor）と呼ぶ。

定義 2.4（整域）零因子を持たない可換環 R を**整域**（integral domain）と呼ぶ。

$\boldsymbol{Z,Q,R,C}$ は全て整域である。一方、既約剰余類 $\boldsymbol{Z}_n$ は n が素数であれば整域となるが、n が合成数の場合は同合成数の因数が零因子となるため整域とはならない。

定義 2.5（可逆元）可換環 R の要素 $a \neq 0$ に対し、$a \cdot b = 1$ となるような $b \in R$ が存在するとき、a を**可逆元**という。

定義 2.6（体）代数系$(F,+,\cdot)$が次の性質を満たすとき**体**（field）という。

① $(F,+,\cdot)$は可換環である。

② 任意の $x \in (F \setminus \{0\},\cdot)$ $(x \neq 0)$に対し、可逆元 x^{-1} が存在する。

$\boldsymbol{Q,R,C}$ は体であるが、$\boldsymbol{Z}$ は 1 以外には可逆元が存在しないので体ではない。 p が素数の場合の剰余類 $\boldsymbol{Z}_p$ は体であり**素体**と呼ばれる。F が有限集合で、かつ$(F,+,\cdot)$が体となるとき、$(F,+,\cdot)$を**有限体**（finite field）、または **Galois 体**（Galois field）と呼ぶ。また、有限体 F の元の数を位数と呼ぶ。素体は有限体であるが、任意の有限体は位数が $q(=p^n)$の有限体となることが知られている。同位数 $q(=p^n)$の有限体 F,G に対して、F と G の各要素を必ず一対一に対応付けられることも知られている。このような意味において、位数が $q(=p^n)$の有限体は一般的に $GF(q)$または F_q と表記される。

付 3 有限体上の楕円曲線の基礎事項

定義 3.1（楕円曲線）3 次曲線（i.e., $f(x,y)$の次数が 3 であるような代数方程式 $f(x,y)=0$ の解の集合）のうち特異点($\partial f/\partial x=0$ かつ $\partial f/\partial y=0$)のないものを**楕円曲線**（elliptic curve）と呼ぶ。

定義 3.2（有限体上の楕円曲線）標数 p（p は素数）が 3 より大きな体 F_q($q = p^r$)上において

$$\{(x,y)|\ y^2 = x^3+ax+b \pmod q\}\quad (a, b\in F_q)$$

但し、$4a^3+27b^2\neq 0$（特異点が存在しないための必要十分条件）、に無限遠点 $\boldsymbol{O}$ を付け加えた点の集合を有限体 F_q上の楕円曲線という。また上式を満たす(x, y)の組を楕円曲線上の点と言う。

定義 3.3（有限体上の楕円曲線における加法）有限体 F_q上の楕円曲線上の任意の 2 点 $\boldsymbol{P}=(x_1, y_1)$及び点 $\boldsymbol{Q}=(x_2, y_2)$の和 $\boldsymbol{P}+\boldsymbol{Q}=(x_3, y_3)$は以下の加算公式により与えられる。

(a) $\boldsymbol{Q}$ が無限遠点 $\boldsymbol{O}$ の場合、

$$\boldsymbol{P} + \boldsymbol{Q} = \boldsymbol{Q} + \boldsymbol{P} = \boldsymbol{P}$$

(b) $\boldsymbol{Q} = -\boldsymbol{P}$、すなわち $x_2=x_1 \pmod q$かつ $y_2=-y_1 \pmod q$の場合、

$$\boldsymbol{P} + \boldsymbol{Q} = \boldsymbol{Q} + \boldsymbol{P} = \boldsymbol{O}$$

(c) $\boldsymbol{Q}\neq -\boldsymbol{P}$ の場合、

$$x_3 = \{(y_2 - y_1)/(x_2 - x_1)\}^2 - x_1 - x_2 \pmod q$$
$$y_3 = \{(y_2 - y_1)(x_1 - x_3)\}/(x_2 - x_1) - y_1 \pmod q$$

(d) $\boldsymbol{Q} =\boldsymbol{P}$ の場合、

$$x_3 = \{(3x_1^{\,2}+a)/(2y_1)\}^2 - 2x_1 \pmod q$$
$$y_3 = \{(3x_1^{\,2}+a)(x_1 - x_3)\}/2y_1 - y_1 \pmod q$$

mod q でなく実数で考えると、同加法の幾何学的意味が明確になる。すなわち、このとき点 $\boldsymbol{P}$ と点 $\boldsymbol{Q}$ の和はこれらの 2 点を結ぶ直線と楕円曲線の交点を取り、これと x 軸に対し線対称な点として得られる。

楕円曲線上の点の集合は上記加法に関し有限可換群となることが知られている。以下では、有限体 F_q 上の楕円曲線において上記加法公式により構成される群を$E(F_q)$と表記する。有限体上の楕円曲線 $E(F_q)$の位数、すなわち要素の個数$\#\ E(F_q)$については、Hasse により上下限が与えられている。

定理 3.1（Hasse の定理）有限体上の楕円曲線 $E(F_q)$の位数$\#\ E(F_q)$は次式のように評

価される。

$$q-2q^{1/2}+1 \leqq \#E(F_q) \leqq q+2q^{1/2}+1$$

有限体上の楕円曲線 $E(F_q)$は、一般に二つの巡回群の直積となり、それぞれの巡回群の位数を n_1,n_2 $(n_1 > n_2)$としたとき、$E(F_q)$の群構造を(n_1,n_2)と表記する。このとき、n_2は n_1の約数であり、かつ q-1 の約数でもある。従って、$E(F_q)$の位数は$\#E(F_q)=n_1n_2$であり、$E(F_q)$の要素の最大位数は n_1である。