

## 5.8 ■ 情報処理技術 — 過去十年そして今後の十年 —

# 暗号技術の動向と課題

辻井 重男 中央大学

### ■ まえがき — 暗号は社会を変える

暗号は攻めの面と守りの面を表裏一体として合わせ持ち、サイバー世界の基盤技術として社会を変革する原動力となっている。

暗号には情報の秘匿という古来からの機能と1970年代以降、認識され始めた認証という機能があり、前者はプライバシーや産業機密を保護することにより、情報社会を守る堀の役割を果たし、後者は主として、デジタル署名などの技術によって電子経済、電子政府、電子医療、電子文化などの展開を可能ならしめる攻めの役割を受け持っている。

また、暗号を方式の視点から大別すれば、共通鍵暗号と公開鍵暗号があり、どちらの方式も、秘匿、認証の両機能を果たし得るが、共通鍵暗号は秘匿に、公開鍵暗号は認証（デジタル署名）に適性を持つといえる。暗号に関する概括的な知識をお持ちでない読者のためにその理由を簡単に述べておこう。

共通鍵暗号は、送信者と受信者の

対ごとに、両者のみが知る秘密の鍵を共有する方式であり、換字・転置を複雑に繰り返す回路構成により、数十メガビット／秒から数百メガビット／秒に及ぶ暗号化・復号処理を実現できる。

一方、公開鍵暗号は、個人対不特定多数という環境に適した方式であり、1人1人が秘密鍵とそれに対応する公開鍵を対として所有し、秘密鍵は自己のみの秘密として保管し、公開鍵は通常、不特定多数に公開する。

公開鍵暗号は、その秘密鍵が公開鍵に数理的構造として内包されており、秘密鍵から公開鍵を計算することは容易であり、逆に公開鍵から秘密鍵を割り出すことは難しいという、いわゆる一方方向性関数の性質を利用している。

公開鍵暗号においては、現在のところ、暗号化・復号処理に大きな数を法とするべき乗計算のような手間のかかる計算が利用される方式が多く、処理速度は共通鍵暗号に比べて2桁以上遅い。このため、長い平文のリアルタイムの秘匿通信などには不

向きであり、秘匿用としては共通鍵暗号の鍵を配送あるいは共有するような利用に適している。

公開鍵暗号の本領は認証において発揮される。サイバースペースは無色透明ともいえる世界であり、その中で、人、モノ、カネ、サービス、情報コンテンツ、ソフトウェア、人々の権利が(正確にはそれらの代理としてのデータの場合が多いが)、自由に飛び交う。これらの真正性を保証することなしに情報社会は構築し得ない<sup>1)</sup>。

銀行などの発行機関の署名のない電子マネーはあり得ない。電子マネーとは、暗号の持つ認証機能によって金額情報が保証された現金である。暗号によって電子マネーの安全性が高められるというより、電子マネーは暗号によって初めて作られるのである。本格的な電子マネーは、その普及は少し先になるだろうが、将来、経済社会に国際的規模で影響を及ぼし国家の輪郭をも崩しかねない威力を秘めているだけに、暗号の安全性に関する責任は著しく重いものがある。

金よりも重いのは人の命である。遠隔医療やカルテの電子化は、医療の進歩や効率化を大いに進めるが、このような医療の電子化も、1つ間違えば、患者の命にかかわるだけに暗号による本人確認や改ざん防止の技術が本質的に重要となる。

政治や行政面では、電子申請・ワンストップサービスによる行政の効率化が進められようとしており、さらに、政治形態にまで影響を及ぼしかねない電子投票も話題を呼んでいる。いずれも本人確認や改ざん防止が基本技術であるが、特に電子選挙については、無記名投票における2重投票などの不正防止とプライバシー保護を両立させる(投票資格を確認するとともに投票者と投票内容の結び付きが選挙管理者に知られないようにすること)ため、暗号技術が

不可欠となる。

その他、ETC (Electronic Toll Collection) による交通渋滞の軽減にもられるような交通や物流の効率化も暗号の認証機能によって実現される。

以上のように、あらゆる面で社会の基盤となる現代の暗号技術は、コンピュータの進歩やインターネットの普及に伴って激しい変化を見せている。

本稿では、暗号技術の最近10年を中心とする動向を概観するとともに、21世紀初頭における暗号のあり方と研究方策を探ることとしたい。

## ■ 共通鍵暗号の動向

### ■ 歴史的役割を終えたDES

1977年、米国連邦政府標準暗号として制定された史上初のアルゴリズム公開型共通鍵暗号DES (Data Encryption Standard) は、5年ごとの見直しに3度耐えて20年にわたり、米国のみならず世界的にも金融分野を中心に広く利用されてきた。

しかし、1990年代に入るやBiham, Shamirによる差分解読法(1990年)、松井による線形解読法(1993年)などの解読アルゴリズムの進歩が続いて、DESに対する信頼感が揺らぎ始めた。差分解読法についてはDESの設計者も織り込み済みだったようだが、線形解読法は設計者にも予想外だったという。

よく知られているように、DESは同一の回路が16段繰り返される構成となっており、Bihamらは1990年の段階では7、8段までを解読したに過ぎなかったが、松井は、線形解読法により16段実装のDESを世界で初めて解読した。

もっとも、一言で解読といってもそれにはさまざまなレベルがある。差分解読法に対しては、解読者は「解読に都合よく選択された平文と

それらに対応する暗号文の対を多数知っているという条件下で鍵を推定する」という選択平文攻撃が適用され、線形解読法に対しては、解読者は「平文に注文はつけないが、平文とそれに対応する暗号の多数の対を知っているという条件下で鍵を推定する」という既知平文攻撃が適用される。

「平文が分かっているのなら、鍵を割り出すことに意味があるのか」という疑問を持たれるかもしれないが、同じ鍵が使用され続ける場合には、未知の平文が解読されてしまうことになる。また、既知平文攻撃も選択平文攻撃も膨大な量の平文と暗号文の対を必要とするから、実際の環境での適用は難しいと思われるが、暗号の安全性に関する研究は、一般に解読者に有利な状況、言い換えれば、暗号設計者にとっては厳しい環境を想定して行われている。

したがって、実際の環境の下での有効な解読法は、多くの場合、鍵の総当たり攻撃ということになる。DESの鍵長は56ビットであるから、鍵の総数は $2^{56} \approx 10^{17}$ であり、1マイクロ秒で1つの鍵をチェックできるプロセッサが100万台あれば、等価的に1つの鍵を1ピコ秒でチェックできることになる。そして1日が約 $10^{17}$ ピコ秒であることから、平均半日程度でDESの解読が可能となる。このことはDESが制定された当初から意識されていたのだが、プロセッサの進歩とインターネットの普及によって、最近では現実的解読時間となってしまう。

また、郵政省の認可法人である通信・放送機構で実施されている情報通信セキュリティプロジェクトでは、下田(現富士通)、金子(理科大)により、並列計算機AP3000を用い、線形解読法に代数的手法を加味して、4日間でDESを解読して、最も権威ある国際会議CRYPTO 98に発表し、最も効率的な解読法との折り紙



をつけられた。

このようにDESも歴史的役割を終えつつあることから、米国商務省のNIST (National Institute of Standards and Technology, 米国標準技術局) は、ポストDESとしてAES (Advanced Encryption Standard) を世界各国から公募し、2001年を目途に米国連邦政府標準暗号として制定すべく、現在策定中である。

AESはDESと同じく、平文をブロック化して暗号化するブロック暗号であるが、DESのブロック長が64ビットであるのに対し、AESでは128ビットと拡大され、鍵長も128ビット～256ビットと大幅に増大された。量子コンピュータのような新しいタイプのコンピュータが出現すればともかく、現在のコンピュータを想定する限り、その急速な進歩を考慮に入れても、128ビットあれば、鍵の総当たり法によってAESが解読されることはあり得ないといえる。これは単純計算から分かることであるが、鍵の総当たり法以外のさまざまな解読法に対する安全性を考えておかねばならないことはもちろんである。

そこで、AESへの応募に限らず、暗号設計者がある共通鍵暗号方式を考案して提案する場合には、差分解読法や線形解読法など既知の解読法については安全であることが証明されている Provably Secure な暗号として発表することが半ばルール化している。これらの解読法に対して安全であるとは、解読に要する手間が、鍵の総当たり法以上となることをいう。

しかし、差分解読法と線形解読法にばかり配慮していると代数的色彩の強い暗号となってしまう、他の解読法、たとえば代数的解読法に完敗してしまうことにもなりかねない。たとえば、KnudsenとNybergによるKN暗号は、そのようなタイプの暗号であったが、盛合、金子(敏信)、下山により、高階差分解読法と呼ばれる代数的手法によって解読され

た。すべての解読法を列挙することは人智の及ばざるところであるが、 $\chi^2$ 検定のような乱数性をさまざまな条件 (たとえば、RC5、RC6というRSA社の暗号に対して、鍵のある部分を固定したという条件) の下でチェックするというような手法も含めて、できる限り多面的に安全性を評価することが望まれる。

もともと、有限の構成と鍵長からなる暗号に、どのような解読法に対しても無限の強度を持たせることは不可能であるから、多様な解読法に対してバランスを保つことが良策であろう。こうした観点から、角尾らによる考え得るすべての解読法に対する耐力を総合して、その強度評価値を3次元グラフ等で視覚表現する評価方法は納得のいくものといえる。このほか、最近、安全性評価方法や評価ツールについては多くの成果が報告されている。

2000年から2030年あたりを視野に入れた鍵長128ビット以上のブロック型共通鍵暗号については、NTTのE2、NECのCIPHERUNICORNあるいは、NTT・三菱のCamelia (椿) 等々日本からも国際競争に耐える方式が提案されつつある。国内では、電子政府のインフラストラクチャとして、標準方式 (1つとは限らないが) を絞ろうという考えもあり、ここ数年は提案、評価、淘汰、標準化などさまざまな変化が予想されるが、奇想天外な解読法が出現しなければその後の10年程度は落ち着いた状態が続くものと思われる。

以上、ブロック型暗号について述べたが、第2次大戦などでも活躍したストリーム暗号についても今後、設計法や安全性評価について理論武装を強めていく必要があろう。

次世代インターネットをはじめ、将来の情報ネットワークはテラビット級の高速性が求められているが、ストリーム暗号には、ブロック暗号以上の高速性が期待できる。カオス

現象を利用したストリーム型暗号などの提案が増えつつあるが、アルゴリズムを公開せず、暗号文のみを見せて鍵と平文を求めるといった類の懸賞問題が新聞紙面を賑わしたりして、暗号研究者の不信感を募らせている。平文が意味のある文章ならともかく、ストリーム型暗号の場合、同じ暗号文に対して鍵と平文の組合せはどのようにでも設計できるから、上のような問題設定は無意味である。他方、DESの制定以来、米国や日本の学会では、ブロック型暗号の研究に精力を注ぎ、ストリーム型暗号の研究は活発でなかったことは否めない。ストリーム型暗号の研究を深め、その安全性に対する評価能力を高めることは21世紀初頭の課題の1つであろう。

## ■公開鍵暗号の動向と課題

公開鍵暗号の分野でもここ数年、注目すべき成果が挙げられている。1つは、実用的なプロトコル環境下で証明可能安全性を有する方式の提案が相次いだこと、他の1つは、楕円曲線などの代数曲線を用いた耐解読性の高い暗号方式に関する研究が理論的にも深められ、実用面でも進展したことである。

## ■証明可能安全性

素因数分解の困難性を利用したRSA暗号は、20年近い耐解読実績を有し、利用者の信頼感を勝ち得て、最近では、インターネットの普及に伴って広く使用されてきた。

1995年、BellareとRogawayによって、データ守秘専用の公開鍵暗号方式OAEP (Optimal Asymmetric Encryption Padding) が提案された<sup>3)</sup>。OAEPはRSA暗号を下の2つの仮定の下に、能動的攻撃に対しても、強秘匿であるように高信頼化したものである。



図-1 共通鍵暗号・公開鍵暗号の発展

(宮内宏氏 (NEC) が共通鍵暗号について作成された図を参考にして、筆者が新たに作成したものである)

- ①入力データに対して、ランダムなデータを出力するような理想的なランダム関数が利用可能である (ランダムオラクルモデルの仮定)。
- ②RSA 暗号関数は一方向性を有している。RSA 暗号の公開鍵  $(n, e)$  と自然数  $y \leq n-1$  が与えられたとき  $y = x^e \bmod n$  を満たす  $x$  を求めることが計算量的に困難である。
- ここで強秘匿とは、暗号文に対応する平文全体でなく、その一部すらも解読することが困難であることをいう。

一方、現実のプロトコル環境の下で、OAEPを援用する必要性が生じている。1998年6月、Bleichenbacherによって、RSA 暗号が組み込まれたRSA社の暗号通信データ形式の規格PKCS#1 Version 1を、ある特定の双方向通信環境において実装した場合、適応的選択暗号文攻撃によって、任意の暗号文に対する平文を効率的に解読する方法が発表された<sup>3)</sup>。

Bleichenbacherは上記の攻撃に必要な選択暗号文の数を約 $2^{20}$ 個 (百万個) と試算している。

このような攻撃法が、インターネットにおける暗号プロトコルとして利用されているSSL Version 3に対して適用し得る可能性が示されたことから (実際に解読されたという事例が報告されたわけではないが)、RSA社はSSL Ver.3に規定していたPKCS #1を改良し、OAEPを採用入れたPKCS#1 Version 2を発表している。

また、岡本 (龍明)、内山、藤崎によるEPOCやCramer Shoupの暗号など、いくつかの仮定の下で安全性の証明された公開鍵暗号が相次いで提案されている<sup>3)</sup>。

#### ■代数曲線を利用した暗号

1980年代中頃に提案された楕円暗号は、1990年代初頭までは、暗号研究者の中でも、それを専門とする

クローズドなグループによって研究されてきたが、インターネットの普及に伴うコンピューティングパワーの爆発的かつ持続的増大によって、一般の注目を集めるようになった<sup>2)</sup>。というのは素因数分解に依拠するRSA型の暗号は、解読計算量が準指数時間であることから、その安全性を保証するために、合成数 $n$ の桁数を5年、10年の単位で増大していく必要があるのに対して、楕円暗号の場合は、特殊な場合を除いて解読計算量は指数時間であり、コンピューティングパワーの今後の20～30年の増大に十分抵抗できると考えられる。

しかし、暗号研究者は、“そんなはずはなかったのだが”という事象を備えておく責務も負っている。そのような事態には2つのケースが考えられる。

1つは、楕円暗号の解読計算量が指数関数的時間より小さいアルゴリズム

ムが発見された場合であり、他の1つは、量子コンピュータの開発が、「実用化されるとしても21世紀中頃であろう」という予想を超えて、急速に進んだ場合である。

前者に対しては、その特性がかなり知られた楕円曲線ではなく、超楕円曲線あるいはより一般的な代数曲線を利用した暗号方式の探求が続けられている。しかし、これらの代数曲線上(のヤコビ多様体)の離散対数問題も指数時間の計算量であることに変わりはない。量子コンピュータの進展も合わせ考えると、NP-hardより困難な問題を数論的代数幾何学の鉅脈に深く分け入って探すこと、あるいは数論以外の分野から、安全な落し戸付方向性関数を見出すことも大きな課題であろう。

もっとも、量子コンピュータなどの新型コンピュータが、仮に実用的レベルに達したとしても、鍵サイズの増大によって対応できるとも予想されるから、未だ見ぬ影に不安を抱く段階ではないと思われる。

## ■むすびー今後の課題

暗号に関しては、さまざまな技術的、政策的課題があり、本稿では、技術の動向とその課題の一端を示したにすぎない。以下に、共通鍵暗号、公開鍵暗号を含む暗号全般についての課題を定性的に示しておくこととする。

(1) 1970年代以降、計算量的安全性を大きな基盤としてきたが、今後のコンピューティングパワーの増大に備えて、情報量的安全性を持つ実用的方式の研究の比重を高めることが必要であろう。

また、量子暗号のような物理学的安全性に基づく暗号の開発にもこれまで以上に力を注ぐべきであろう。

広田修は筆者への私信の中で計算量的、情報量的、物理量的の3つの側

面を総合した暗号科学の重要性を強調している。

(2) 最近の朝日新聞(2000年3月2日夕刊)に黒崎政男(哲学者)により「ネットワークの不安定さ—文字信仰裏切る非物質性」と題する一文が寄せられている。暗号研究者が主張する数学的論理だけでは一般の人々は納得しない。筆者らは最近、DNAや指紋等の情報を秘密鍵に埋め込んだ公開鍵暗号方式を提案したが、この例に見られるような証拠性の強さを実感できる暗号方式も考えておく必要があるであろう。

(3) 情報セキュリティは、アルゴリズムのみで強化されるものではなく、ICカードの耐リバースエンジニアリング性や難読ソフトウェア等により耐タンパー性を高めることも忘れてはならない。逆に、実装上、どのような不正な仕掛けが製品に施されているかは、社会安全上、深刻な課題となっている。また、危機管理の観点から万一、暗号が破られた場合に備えて、2重化等の対応をとっておくことも必要であろう。

...

現在、暗号メーカ各社は、ISOの暗号標準制度に対応すべく次世代共通鍵暗号の提案に余念がない。また、次世代の移動通信システム(IMT-2000)に三菱電機のKASUMI(霞)と呼ばれる共通鍵暗号が標準暗号として採用されたことなどから分かる通り、暗号研究者たちは、少数精鋭ながらよく頑張って日本の暗号技術を世界のトップレベルに押し上げてきた。問題はそれを活かすコンピュータ(特にOS)技術・産業力、制度・組織力、政治力等が弱いことであろう。

公開鍵も共通鍵もその安全性、つまり解読攻撃に対して十分な強度を持つことが必須である。したがって、安全性評価がきわめて重要であり、米国はもちろん、欧州の主要国は、暗号の評価や標準化のための国家的・第三者の組織を持っている。

これに対し、我が国は第2次大戦の敗者であったことによる歴史的経緯や行政組織のあり方と安全性に関して感度の鈍い国民性が相まって、暗号に関する国としてのポリシーもなく、暗号評価標準化組織もなかったが、安全な基盤の上にサイバー世界を築いて国際社会を生き抜いていくために、こうした組織を設置することが強く望まれる。

このような機関を持たなければ、我が国は諸外国から主権国家として、鼎の軽重を問われることにもなりかねない。

また、暗号の輸出管理について言えば、その国際協約であるワッセナー・アレジメントは暗号技術の急速な進歩と完全に不整合を生じている。米国は本年1月、ワッセナー・アレジメントを無視する格好で輸出規制を大幅に緩和し、ヨーロッパ諸国のひんしゅくを買っている。我が国としては国際の場で意味のない規制を緩めるよう働きかけて、国際的整合を図りつつ、暗号の輸出についての自主的ポリシーとルールを確立し、我が国の暗号製品が海外でも広く活用されるよう努めるべきであろう。

米国と比べると、暗号を含め暗号と情報セキュリティに関する国家の予算は2桁程度低い。企業と同様に、国としてもトップの強いリーダーシップの下に、国民の意識を高め、予算を増やし、優れた人材を育成することから始めなければならない。

情報系諸学会は協調して、国としての情報セキュリティに関するポリシーの確立と安全性評価機関の設置を政策提言していくべきであろう。

## 参考文献

- 1) 辻井重男: 暗号と情報社会, 文春新書(Dec. 1999).
- 2) 辻井重男, 趙 晋輝: 楕円暗号へのガイドライン, 電子情報通信学会論文誌, Vol.J82-A, No.8, pp.1200-1211 (Aug. 1999).
- 3) 宇根正志, 岡本龍明: 公開鍵暗号の理論研究における最近の動向, Discussion Paper No.98-J-28, 日本銀行金融研究所(98-11).

(平成12年3月21日受付)

