授賞業績

先導的暗号研究による情報セキュリティへの貢献

アディ・シャミア博士

1952年7月6日生まれ(64歳　イスラエル)
ワイツマン科学研究所　教授

概　要

インターネットなどのオープンなデジタルネットワークを利用して、私たちは便利な生活を営んでいます。その快適さの背景には、重要な情報が盗まれたり改ざんされたりすることなく、安全性が保たれているということがあります。その根幹となる種々の提案を行い、実現する方法を次々と開発してきたのが、アディ・シャミア博士です。
デジタルネットワークでの情報は2進数に置き換えられています。シャミア博士は、数学的な方法論を駆使して、画期的な暗号法「RSA暗号」、安全に情報を保管できる「秘密分散法」、秘匿する情報に触れることなく個人を特定できる「個人識別法」、多くの共通鍵暗号を解読できる汎用的な「差分解読法」など数多くの発明、提案を行いました。
また、暗号を処理するコンピュータなどの消費電力や雑音から暗号を読み解くサイドチャネル攻撃についても、大きな研究成果をあげています。

MITの2人の研究者と共同で公開鍵暗号方式を初めて実現

暗号は人間の生活に重要な役割を果たすものですが、長らく国や軍などの特定の集団の中だけで使われ、暗号化する鍵と復号(暗号を元に戻す)する鍵は同じもので、集団の中でも特定の人々だけが秘かに共有していました。ところがオープンなデジタルネットワークが登場し、不特定多数の人が情報をやり取りするようになると、どう鍵を配り、どう共有すれば安全なのかが大きな問題になり、新しい暗号方式が求められます。

1976年にスタンフォード大学の2人の研究者により、「公開鍵暗号」というまったく新しい方式が提案されました。暗号化鍵と復号鍵の2種類を用意し、暗号化鍵を公開して、復号鍵を手元に置くというものです。この方式では、不特定多数の人が秘匿したい情報を公開鍵で暗号化して送れば、受け取る人だけがそれを復号できるので、クレジットカードを使ったインターネットでの買い物などが安全に行えます。

これを最初に実現したのが「RSA暗号」で、1977年にマサチューセッツ工科大学(MIT)の3人の若手研究者、ロナルド・リベスト博士とアディ・シャミア博士とレオナルド・エイドルマン博士の共同研究で開発されました。公開鍵方式の提案に興味をもったリベスト(R)博士とシャミア(S)博士が、さまざまな数学的手法を駆使して暗号化をはかり、途中から共同研究に参加したエイドルマン博士(A)がその不備を突いて解読するということを繰り返し、43回目の提案として成功したのがRSA暗号です。3人の名前の頭文字をとって、RSA暗号と名付けられました。

この暗号の要は、大きな数(2つの素数の積)の素因数分解の困難さにあります。暗号化鍵として2つの素数の積が公開されますが、復号鍵を求めるには、それを素因数分解して2つの素数を見いださねばなりません。現在のRSA暗号に使用されているその積は、2進数で表すと2^{2048}から2^{4096}で、銀河の原子数という天文学的数字2^{223}よりも圧倒的に大きく、スーパーコンピュータを使って1万年かけても解けるようなものではありません。また、RSA暗号は署名法としても利用されています。復号鍵で暗号化したものは、逆に暗号化鍵で復号できるので、誰にでも署名した人が確かに復号鍵を持っている人だと分かるのです。

災害から情報を守る秘密分散法を発明

重要なデータを安全に保管するためには、分散することが重要です。1979年にシャミア博士は、どのように分散すればどの程度分散情報が漏れても安全なのかを保証する「秘密分散法」を最初に提案し、多項式を使って実現しました。

直線は1次多項式、放物線は2次多項式ですが、秘密情報をこのような多項式上の点として表現し、秘密情報以外の多項式上の点を分散して保管します。すると、1次多項式なら分散した情報を2個、2次多項式なら3個集めれば秘密情報が復元できます。直線は2点が分かれば正確に引くことができるし、放物線は3点が分かれば正確に描くことができるからです。同様にk次多項式ならば、分散した情報をk+1個集めると秘密情報を復元できます。つまり、k+1個以上に分散しておけば、k個までは盗まれても相手には復元できないし、何個か壊れてもk+1個が無事ならば復元できるということになります。これを利用すれば、目的に応じて重要なデータの分散化をはかることができます。例えば地震対策なら、国内の離れた3箇所に分散しておき、地震で1箇所の情報が壊れても残り2箇所の情報で復元することなどが考えられます。

またシャミア博士は、「視覚型秘密分散法」も発明しています。元の絵を2枚以上の砂嵐画像のようなパターンに分散し、重ねると元の絵が分かるというものです。分散画像は明暗のドットで表現されており、重ねることにより、明と明、明と暗、暗と暗それぞれが重なる部分ができ、その結果、元の絵が浮かび上がります。

「秘密分散法」はシャミア博士の提案後、多くの研究者によっていろいろなバリエーションが研究され、実際への応用だけでなく、他の暗号技術へも適用され、暗号技術研究の大きな発展につながりました。

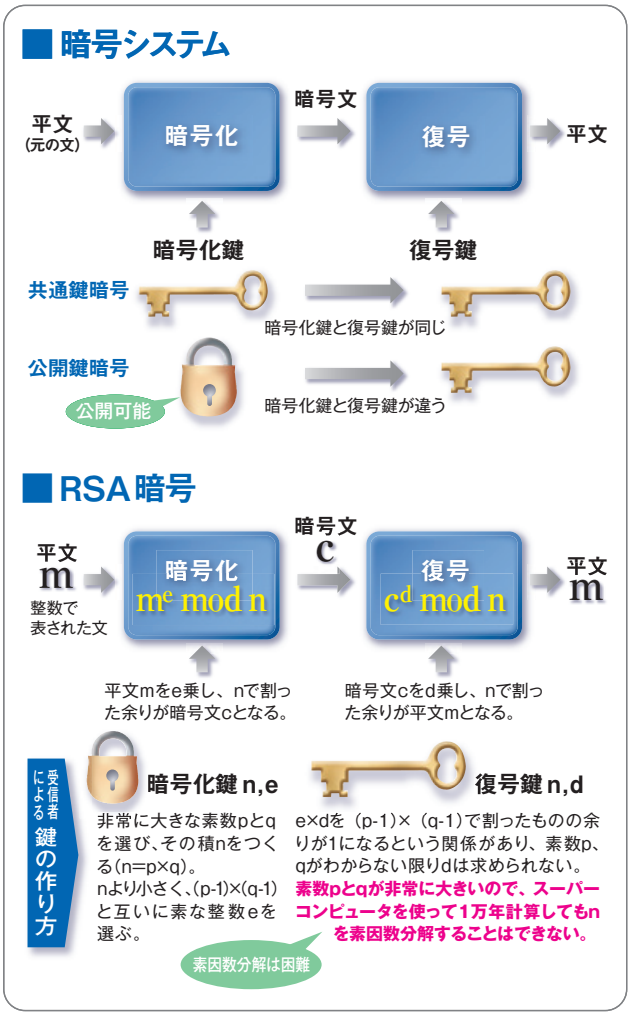
秘密情報をまったく漏らすことなく、自分であることを証明する方法

現実の世界では自分であることを示すために免許証の提示などが求められますが、デジタルネットワークを利用する場合には、パスワードなどの秘密情報を示すと盗まれて他者になりすましを許す可能性があります。1986年にシャミア博士は、自分のもつ秘密情報そのものを漏らすことなく、相手とのやりとりの中で、確かに自分がその秘密情報をもっていることを納得させることができる「個人識別法」の手法を開発しています。平方剰余という数学の考え方を使った方法で、学術的にきわめて優れた成果であると同時に、現実世界でも、衛星放送会社によって利用者の正当性を担保し課金するシステムに採用されました。

共通鍵暗号を解読する汎用的な方法を提示

暗号技術の発展には、優れた暗号技術を新規に開発することはもちろんのこと、既存の暗号技術の不備を見つけ出すことも必要です。シャミア博士たちのRSA暗号もエイドルマン博士の解読に耐えるものを目標に発明されました。シャミア博士自身も解読の可能性についての研究を行い、重要な示唆を行っています。

1990年にシャミア博士は、多くの共通鍵暗号では、2つの暗号文の差分をとっていくと、暗号化処理の一部が相殺され、差分値の統計的な隔たりなどを利用することで解読できることを示しました。共通鍵暗号では簡単な処理を何回も繰り返すことで暗号化することが多く、そのような暗号に適用できる解読法です。そして、実際に米国商務省標準局(NBS、現在のNIST)が1977年に世界初の商取引の標準暗号として採用したDES(Data Encryption Standard)暗号も、8回程度の繰り返し処理だけでは解読されてしまうことを示しました。DES暗号は、同じ処理を16回繰り返していたので、現実には破られることはありませんでしたが、これがより安全な暗号開発の契機になり、NISTは2000年に新たな暗号を採用することになったのです。



パソコンのそばに置いたスマートフォンから暗号を解読

コンピュータの電力消費の増減、発生する雑音といった物理的な情報の変化から、暗号化·復号プログラムの動きを解析して暗号解読を行うことを、サイドチャネル攻撃といいます。シャミア博士はこのサイドチャネル攻撃にも早くから着目し、数々の成果をあげてきました。

2014年には、パソコンの横にスマートフォンを置いて、パソコンの発生する雑音を拾い、その解析から自分たちの考えたRSA暗号を破ることも不可能ではないことを示しました。このような研究は、機器を含めて安全なシステムをどう設計すべきかの重要な拠り所になります。

このようにシャミア博士は40年にわたる研究の中で、ごく一部の人たちのものであった「暗号」を「暗号学」という学問にまで高めました。そして、オープンなデジタルネットワークの発達で世界中のたくさんの人々が自由に情報のやり取りを行う中、常に情報セキュリティ研究の最前線で地平を切り拓き、新しい研究の流れをつくってきました。次には、どのような流れを生み出すのでしょうか。AIなどコンピュータの知能の深化が話題になる昨今、シャミア博士の研究から目が離せません。