【電子・情報通信技術特集】

数学的な進歩による IT セキュリティーの強化（欧州）

サイバー犯罪が急激に増加し、インターネットがテロ攻撃の媒体として使用される可能性が増加しているため、IT セキュリティーは、大きな課題を抱えている。

暗号文は、この課題の中心として、プライバシー、機密性および識別機能を支えていると共に、電子商取引および安全な通信手段を提供している。インターネットの初期以来、暗号文は、広範な RSA [注1]パブリックキーシステムがベースであり、ディジタルサインとプライベートキーの交換に使用され、メッセージ内容を暗号化する。

RSA 暗号システムは、1977 年に Rivest, Shamir および Adlement らにより紹介され、大きな整数を因数分解することの難しさにより安全確保をたもっていた。RSA は、これまでのところ良く機能している。しかし、提供できる保護レベルは、それを破るためのより強力な手法を開発する不断の試みによって、浸食されてきた。

しかしながら、楕円曲線の数学的理論に基づいた異なるアプローチが、より有効な暗号の最有力候補として浮かびあがってきた。これにより、セキュリティーと処理効率の最適な組み合わせを提供することが可能になる。楕円曲線[注2]は、方程式の中に例えば X と Y の二つの変数が含まれていて、X と Y の両方は、2 乗またはそれ以上に掛け合わすことができる。

楕円曲線理論は 1990 年代初期、有名なフェルマー最終定理（Fermat ’s Last Theorem）の解決に重要な役割を演じた。そして皮肉なことに、RSA 暗号学のセキュリティー（の脆弱性）を攻撃するためにも使われた。

楕円曲線、及びその他の現代的な数学手法の潜在的な可能性に関して、ヨーロッパ科学財団（ESF）が近年組織したワークショップで議論が行われ、欧州全体の研究開発の場が用意された。

フランス、マルセーユの Luminy 数学研究所（Institut de Mathematiques de Luminy）出身で、ESF ワークショップ会議議長の David Kohel は次のように述べている。「私の PhD アドバイザーである Hendrik Lenstra が開発した、整数の因数分解のための楕円曲線手法の効果は、暗号研究者に楕円曲線を紹介する役割を果たしてきた。」

確かに、ILuminy 数学研究所において、楕円曲線を数の因数分解、および暗号法に適用することは、ほぼ同時期（1980 年代後半）に起きたことであった。最初は因数分解への応用がより速く進展した。一方、そこに含まれている技術的な困難性により、楕円曲線による暗号化は発展が阻害されていた。しかし、他ならぬ楕円曲線因数分解の成功が、RSA のセキュリティーを弱体化させ始めたのである。それは RSA は、二つの（大きな）素数の積を因数分解することの困難さに依存しているからである。「このことが逆に､近年の楕円曲線暗号処理の開発に刺激を与えた。」と Kohel は述べている。そして、楕円曲線の高度

[注1]Rivest, Shamir および Adlement らの発明者の頭文字をつなげて RSA

[注2]楕円曲線の方程式　$y^2 = x^3 + ax + b$

な数学自体が暗号処理を結果的に助けることになった。

Kohel の指摘によると、楕円曲線暗号の利点は、RSA の強みを浸食してきた特別な攻撃に対する抵抗力があり、少ないキーにより、所定の保護レベルを提供できることである。「現在我々が理解している範囲では、セキュリティーを確保するのに必要な楕円曲線暗号（ECC: elliptic curve cryptography）における基本的なキーサイズは、RSA またはもう１つの代替暗号手法である EIGamal に必要なものより、大変少ない」と Kohel は語る。実際に 160 ビットキーの長さを使用する ECC は、1024 ビットキーの RSA と同じセキュリティーレベルである。

その結果、ECC を実行するために必要なアルゴリズムは、RSA より遙かに複雑であるけれども、コンピュータ処理は、より効率的である。実質的に ECC は、コンピュータに過度の負荷をかけずに、ハッカーよりも一歩先んじることができるであろう。

「一般的に暗号使用者は、暗号解読者（暗号システムを攻撃する人）よりも強みを持つ。なぜなら、もし暗号使用者の誰もが暗号システムへの最適の攻撃方法に関する基本的な同じレベルの知識を持っているという条件であれば、暗号使用者は望ましいセキュリティーレベル（ユーロ（金額）あるいはコンピュータイヤー[注3]といった「コスト」で測定される）に対応したキーサイズを選択できるからである。」と Kohel は指摘している。

重要なことは、RSA の場合でもそうであるが、コンピュータ上では、暗号システムを使用することよりも、破壊することのほうが難しいということである。Kohel が指摘したように、この使用と破壊との差は、ECC の場合はより大きい。

ESF ワークショップは、複雑な暗号のアルゴリズムを実現するのに必要とされる数学者とコンピュータ・スペシャリスト達の専門知識を組み合わせることにより、すばらしい成功を収めた。Kohel の指摘では、通常、先端的な数学を暗号処理に利用するにはタイムラグがある。なぜなら、アルゴリズムの実行に責任を持つ技術者達が、そのアルゴリズムの複雑な技術を把握するのに数年かかるからである。ESF ワークショップの一つの明確な利益は、タイムラグを減らす可能性があることである。

曲線符号理論と暗号学の ESF ワークショップは、2009 年 3 月、フランスのマルセーユで開催された。

[注3] IT 業界の変化の速さを表現するのに、人間の 7 倍の速度で歳をとる犬にたとえて「ドッグイヤー」と呼んだり、さらに 1 年が 18 年分のスピードである「マウスイヤー」という俗語が使われた。ここではこうした表現を computre-years と称している。あるシステムが 1 年後には陳腐化して新しいシステムに取って替わられるものだとしたら、暗号システムのセキュリティーも 1 年間は破られる可能性がない、というレベルに設定すれば十分であるという意味。

会議の議長:
David Kohel
Institut de Mathematiques de Luminy
163 avenue de Luminy Case 907
13288 Marseille
France
Gilles Lachaud
Institut de Mathématiques de Luminy
CNRS
Marseille
France
Christophe Ritzenthaler
Institut de Mathematiques de Luminy Ritzenthaler[at]iml.univ-mrs.fr
CNRS
Marseille
France

翻訳　土橋　誠

出典：
http://www.esf.org/activities/exploratory-workshops/news/ext-news-singleview/article/mathematical-advances-strengthen-it-security-579.html