NEWS RELEASE

NTT

日本電信電話株式会社

2010年1月8日

# 公開鍵暗号の安全性の根拠である「素因数分解問題」で世界記録を更新

～768ビット合成数を一般数体篩法にて完全分解に成功～

日本電信電話株式会社（以下NTT、本社：東京都千代田区、代表取締役社長：三浦惺）は、スイス連邦工科大学ローザンヌ校（以下、EPFL）、ドイツのボン大学、フランスの国立情報学自動制御研究所（以下、INRIA）、オランダの国立情報工学・数学研究所（以下、CWI）との共同研究により、わずかなビット数でも桁違いの計算量が必要となる素因数分解問題※1において、これまでの世界記録（663ビット、10進200桁）を大きく上回り、768ビット（10進 232桁）の合成数に対して、一般数体篩法※2による素因数分解を達成し、世界記録を更新しました。

**＜研究の背景及び意義＞**

インターネットの本格的な普及に伴い、ネット決済やインターネット銀行などネットワークを活用した便利なサービスが身近な存在となり、インターネット上における機密情報のやり取りが大幅に増加しました。そのため、ネットワークを利用した社会経済活動において、情報セキュリティを十分に確保することが不可欠な状況にあります。

NTT情報流通プラットフォーム研究所（以下、ＮＴＴ研究所）では、情報の安全性を確保するため、新たな暗号技術を研究するとともに既存暗号の安全性の検証に取り組んできました。

現在公開鍵暗号※3として広く用いられているRSA暗号※4は素因数分解の難しさを安全性の根拠としているため、素因数分解可能なビット数の検証はRSA暗号の安全性、強度の有効性をより精密に予測する上で極めて重要なものです。

今回700ビットを大幅に超える素因数分解を達成しましたが、これは近い将来RSA暗号で広く使われている1024ビットの素因数分解も達成される可能性があることを示唆しており、より強度が高く効率的な暗号技術を利用する必要性が高まっています。

**＜研究の内容＞**

今回の素因数分解は、巨大な合成数に対して現段階で最も高速な解法として知ら

れている一般数体篩法により実現しました。一般数体篩法は、多項式選択、篩（ふるい）、filtering、線形代数、平方根の5つのステップからなります。このうち、篩と線形代数が最も計算量を要するステップです。各ステップにおいて、選択すべきパラメータは多数あります。このパラメータの選択によって計算量が大きく変化しますが、その有効な選択方法については多くの場合についてはまだ解明されていません。今回の共同研究ではこのパラメータを適切に選択することにより、高速に計算することに成功しました。以下、今回の分解におけるそれぞれのステップの詳細を示します。

（1）多項式選択

このステップは残りの計算量を決める重要なステップではありますが、どの程度の時間をかけどのように多項式を探せばよいのかについては現在のところ有効な手段は見つかっていません。今回は、2005年夏、ボン大学においてOpteron[※5] 2.2GHzをおよそ20年かけたのと同程度の計算量で探索して得られた多項式を選択しました。その後、2007年はじめにEPFLで、さらによい多項式の探索を試みましたが、Opteron 2.2GHz換算で20年かけたのと同程度の計算量を費やしても、見つかりませんでした。

（2）篩（ふるい）処理

このステップは全体の計算量の大半を占めますが、比較的容易に分散計算可能であることから多数の参加組織により並列に計算を行いました。今回の計算では利用可能計算機のメモリ容量に応じいくつかのパラメータを準備しました。2007年夏から開始し、2009年4月に終了しました。殆んどの処理は2008年春から2009年3月にかけて行なわれました。篩処理は主にNTT研究所、EPFL、ボン大、INRIA、CWIにある多種多様のPCやクラスタを用いました。全体ではおよそOpteron 2.2GHz換算で1500年かけたのと同程度の計算量を要しました。

（3）filtering

このステップを実行することにより、この次の線形代数ステップを桁違いに高速に実行することができるようになります。EPFLにある10TBのハードディスクを備えた8コア計算機とクラスタを利用しました。さまざまなパラメータで何度かやりなおしたことにより不必要になった計算を含みますがCore2[※6] 2.66GHz換算で6カ月以下の計算量でした。

（4）線形代数（連立方程式の解法）

このステップは理論的には最も計算量を要するステップのひとつであり、分散計算[※7]が困難です。今回は、少数のクラスタを利用し、またそれぞれのクラスタの速度や空き時間が異なっていても効率的に計算できる手法を開発・利用しました。NTT研究所及びEPFLのクラスタ、またINRIAはフランスにあるALADDIN-G5K[※8]を効率的に用い、filteringで生成された疎行列からなる連立方程式を解きました。Opteron 2.2GHz換算でおよそ155年の計算量を要しました。その結果、分解に利用

可能な解が得られました。

（5）平方根（代数的数の平方根の計算及び最小公約数の計算）

このステップは数学的には高度な理論を用いますが計算量はさほど要しません。EPFLに設置された計算機を用い、数時間で以下の解が得られました。

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

=

3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948 9

X

3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

**＜今後の展望＞**

情報通信社会の進展に伴って、情報セキュリティを確保するために暗号技術の重要性はますます高まります。NTT研究所は暗号技術全般の安全性を継続的に評価していくとともに、次世代暗号として楕円曲線上の演算規則を利用した新しい公開鍵暗号方式「楕円曲線暗号※9」の普及にも努めていきたいと考えています。

今後も、暗号理論から社会的影響まで幅広い領域におけるセキュリティ研究を推進し、ネットワーク社会の安心・安全を追求してまいります。

**＜用語解説＞**

※1 素因数分解問題

合成数を素数の積に分解する問題。小さな合成数に対しては、短時間で素因数分解実施可能であるが、大きな数については現実的な時間内に計算を終えることは困難である。ただし、あまり大きくない素因子を持つ場合は、楕円曲線法によりその素因子を求めることができる。

RSA暗号の法に使うような大きな2つの素数の積から構成される合成数の素因数分解法としては、数体篩（ふるい）法が用いられる。現在、RSA暗号の法に使われる合成数に対しては一般数体篩法が最も高速である。

※2 一般数体篩法

Pollardらにより提案され1990年代前半にLenstraらにより完成された素因数分解アルゴリズム。RSA暗号の法に使うような一般的な形の合成数の素因数分解では既知のアルゴリズムで漸近的に最も高速である。2, 3, 5, 7, …と割っていくいわゆる試し割り法の実行時間が指数時間であるのに対し、一般数体篩法は準指数時間で完了すると評価されている。しかし現在知られている実行時間の評価は平均の上限であるので、具体的な数に対する実際の実行時間を精度よく見積もるためには計算機実験の積み重ねが必要である。

※3 公開鍵暗号
　1976年にDiffieとHellmanにより提案された概念。実現方式としてはRSA暗号が有名。従来の暗号方式は暗号化と復号に用いられる鍵と呼ばれる情報は同一であり、秘密に保持しておく必要があったが、公開鍵暗号では暗号化に用いる鍵を公開することができ、復号に用いる鍵のみを秘密に保持しておけば十分である。

※4 RSA暗号
　1978年に公表された公開鍵暗号および電子署名方式で、Rivest、Shamir、Adlemanの3人の開発者の名前の頭文字からRSAの名がついた。電子署名方式として現在最も広く使われている。これまでにさまざまな改良が施され、いくつかのものは電子署名法の指針や電子政府推奨暗号リストに含まれている。RSA暗号の安全性は「法」と呼ばれるがパラメータに依存し、大きいほど安全であるが、処理性能は落ちる。現在、法のサイズとしは1024ビットが広く使われている。

※5 Opteron
　AMDはインテルが開発した32ビットアーキテクチャIA-32を拡張しいわゆる「64ビットCPU」用のアーキテクチャとしてAMD64を発表した。OpteronはAMD64アーキテクチャに基づくCPUである。

※6 Core2
　インテルは64ビットアーキテクチャとしてAMD64互換のEM64Tを発表した。Core2はEM64Tに基づくCPUコア名称である。

※7 分散計算
　大規模な計算を分割して多数の計算機により計算する技術。分割した計算それぞれに依存関係があると分散計算できない。

※8 ALADDIN-G5K
　フランスの9箇所に配置された大規模並列分散システム研究のための基盤。

※9 楕円曲線暗号
　楕円曲線上の点に対して数式によって定義される特殊な加算法に基づいて暗号化・復号を行なう暗号方式。解読の困難さは、楕円曲線上の離散対数問題を解くのと同程度と言われ、効率のよい解読法はまだ発見されていない。
　ＮＴＴ研究所では、「PSEC-KEM」という楕円曲線暗号を開発している。

【本件に関するお問い合わせ】
NTT情報流通基盤総合研究所
（情報流通プラットフォーム研究所）
企画部　広報担当

TEL：0422-59-3663
E-mail：islg-pr@lab.ntt.co.jp

NTT ニュースリリース