NEWS RELEASE
NTT
日本電信電話株式会社

2007年5月21日

暗号方式の安全性検証に有効とされる「素因数分解」において世界記録を更新

～1000ビット超の特殊な型の合成数に対する素因数分解の達成により暗号鍵の安全性検証に貢献！～

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：和田紀夫）は、ドイツのボン大学、スイスのスイス連邦工科大学ローザンヌ校（以下、EPFL）との共同研究により、公開鍵暗号※1のデファクトスタンダードRSA※2暗号の安全性・強度を把握する手段として世界的にチャレンジが展開されている、大きな数の素因数分解実験において、世界で初めて1000ビットを超える特殊な型の合成数に対して、特殊数体篩(ふるい)法※3による素因数分解を達成しました。

このたびの実験結果は、わずかなビット数の差でも桁違いの計算量が必要となる素因数分解問題※4において、特殊数体篩法でのこれまでの世界記録（911ビット）を大きく上回り、1000ビットを超える1017ビットの合成数に対する素因数分解を達成するという画期的な世界記録です。

本実験は、「(2^1039-1)/5080711」という特殊な型をした合成数に対する素因数分解です。分解対象は1017ビットであり、これは一般の合成数を対象とした一般数体篩(ふるい)法※5でも約700ビットの難しさに相当すると期待されています。

このたびの世界記録樹立は、「素因数分解問題の難しさが、安全性の根拠」といわれ、現在では1024ビットの暗号鍵が主流となっているRSA暗号に関し、安全性・強度の有効性をより精密に予測するうえで極めて重要な意味を持つものです。

＜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、電子商店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ています。

暗号技術は情報セキュリティを確保するためのコア技術です。現在、電子署名※6の実現法の1つであるRSA暗号が事実上の標準規格となっており、ほとんどのウエブ閲覧ソフトに組み込まれている暗号通信プロトコルSSL※7において

も、このRSA暗号が採用されています。
　RSA暗号の安全性が高く評価されているのは、「『素因数分解問題の難しさ』を『安全性の根拠』」としている暗号だからです。つまり、「素因数分解の効率の良い解法はまだ見つかっておらず、大きな数を素因数分解するには、いかなる高性能なコンピュータを使っても莫大な時間がかかる」という数学的な根拠に基づいて設計されているわけです。
　現在の素因数分解技術と計算機能力で、どれくらいの大きさの合成数まで素因数分解が可能であるかを予測することで、暗号解読の可能性を精密に見積もることが可能となり、その結果からRSA暗号鍵長の更新時期を適切に設定し、将来に渡り安全かつ強度な暗号システムの構築に貢献することができます。

＜研究の内容＞

（1）分解候補の選定

　ＮＴＴの情報流通プラットフォーム研究所※8（以下、ＮＴＴ研究所）により、分解対象に小さな因子がないかどうかを楕円曲線法による分解を試みることにより確認しました。その結果65桁以下因子を見逃している確率は3.4%以下、70桁以下因子を見逃している確率は53.2%以下となりました。確認にはAMD社のOpteron248※9を127.5年程度稼動させたものと同程度の計算量を要しました。

（2）篩(ふるい)処理

　ボン大が作成した篩プログラムにより行いました。ＮＴＴ研究所が84.1%、EPFLが8.3%、ボン大が7.6%の計算資源を提供し、Pentium D [3GHz]換算で95年稼動させたものと同程度の計算量を要しました。

（3）行列

　ＮＴＴ研究所及びEPFLに設置されたそれぞれ110台と36台からなるPCクラスタを並列に2ヶ月強用い計算しました。これにより約7千万×約7千万といった巨大疎行列からなる連立方程式の非自明解を47個得ることができました。

（4）平方根

　ボン大のPCクラスタを数時間動かすことにより下記のとおり素因数分解が完了しました。

（80桁と227桁に分解）

(2^1039-1)/5080711

=

5585366661993629126074920465831594496864652701848863764801005234631985328837475370359469516293970800739520988120838703792729090324679382343143884144834882534053344769112223028158321

X

20758181946442382764570481370359469516293970800739520988120838703792729090324679382343143884144834882534053344769112223028158321

7696525376091410189105241993899334109711624358962065972167481161749004803659735573409253205425523689

＜今後の展望＞

情報セキュリティ産業は、21世紀に大きく成長すると期待されています。ＮＴＴ研究所は本実験の成果を利用し、現在デファクトであるRSAの安全性を継続的に評価していくとともに、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ていきます。

＜用語解説＞

※1　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。

※2　RSA

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。

※3　特殊数体篩法

a^b±1といった形の合成数に有効に働く素因数分解アルゴリズム。1980年代後半にPollardにより原型が示され、Lenstraらにより完成された。その後、一般的な形の合成数でも分解可能となる一般数体篩法に拡張された。

※4　素因数分解問題

合成数を素数の積に書き下す問題。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不可能である。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。

※5　一般数体篩法

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。

※6　電子署名

ハンコや署名の機能を電子的に実現する技術。わが国では2001年に、いわゆる電子署名法が制定され、法的効力を持たせることができる。

※7　SSL（Secure Socket Layer）

ウエブ閲覧時などの安全な暗号通信を実現するための技術。現在使われている多くのウエブ閲覧ソフトに組み込まれている。SSLを実現するための暗号要素技術として、RSA暗号も使われている。

※8　情報流通プラットフォーム研究所

情報流通プラットフォーム研究所では、お客様に安心・安全・便利にサービスをご利用頂くため、世界トップクラスの暗号技術をはじめ、セキュリティ、FMC、インターネット・IP通信、ならびにコンピュータアーキテクチャ等の情報処理基盤技術をベースにブロードバンド＆ユビキタス時代のプラットフォームの研究開発を推進しています。

※9　Opteron248

AMD社が開発した64ビットアーキテクチャAMD64に基づくCPU。Opteron248は動作周波数2.2GHzであるOpteronファミリの一員である。Intel社もAMD64互換アーキテクチャとしてEM64Tを発表し、Pentium DやCore2DuoなどのCPUを発表している。

【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 遅塚（ちづか）、山形
TEL：0422-59-3663
E-mail：islg-pr@lab.ntt.co.jp

NTT ニュースリリース