報道発表

本件に関する9月1日付けプレスリリース資料の中に、2箇所の記述誤りがありました。正しい表記（赤色文字および太文字下線）に修正したものを、あらためて本日付け(9/4)で掲載いたします。

尚、今度の記述誤りは研究成果をリリース資料に転記する際の単純ミスによって生じたもので、研究成果そのものの誤りではございません。
ご指摘頂きました方に感謝申し上げますとともに、ご迷惑をお掛けしました皆様方に深くお詫び申し上げます。

- **世界初、専用ハードウェアによる素因数分解実験に成功**
  ～暗号の安全性向上に向けてソフト・ハード技術を融合～

- **平成18年9月1日**

独立行政法人 情報通信研究機構（理事長：長尾 真。以下、NICT）および、富士通株式会社（代表取締役社長：黒川 博昭、本社：東京都港区、以下　富士通）、株式会社富士通研究所（代表取締役社長：村野　和雄、本社：神奈川県川崎市、以下　富士通研究所）は、専用ハードウェアを用いて、暗号に用いられる素因数分解問題*1を解く実験に世界で初めて成功しました。
素因数分解問題は、インターネットの暗号通信などで広く用いられるRSA暗号*2の安全性の根拠となっています。本実験は専用ハードウェアによる暗号解読の可能性を検証する第一歩であり、将来の暗号の安全性を高める上で重要な成果となります。

本実験は、平成16年に開始したNICTの委託研究制度「高度通信・放送研究開発に係る委託先公募」を基に、NICTが富士通との間で進めてきた委託研究「素因数分解の困難性に基づく暗号の技術的評価に関する研究開発」の枠組みの中で行われたものです。また、本実験にあたっては富士通研究所が富士通と独自開発した計算処理ソフトウェアも利用しました。

【開発の背景】
インターネットの本格的な普及に伴い、ネットショッピング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になる一方、秘密情報が漏れないように情報セキュリティを確保することが重要な課題となっています。

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。特にRSA暗号は、ウェブの暗号通信プロトコルSSL*3などでも採用されており、インターネットで最もよく使われる暗号アルゴリズムとなっています。

RSA暗号は、素因数分解問題を解ければ解読できるため、RSA暗号の安全性を保証するには素因数分解問題がいかに難しいかを検証することが重要です。これまで、ソフトウェアによる素因数分解実験は数多く行われてきましたが、専用ハードウェアによる分解実験は行われていませんでした。

【開発した技術】
今回、世界で初めて専用ハードウェアによる素因数分解実験システムを開発しました。その特長は以下の通りです。

1. 最も効率的な素因数分解アルゴリズムとして知られている、一般数体篩(ふるい)法*4をベースとし、最大768ビットの数まで入力可能としました。ボトルネックとなる篩処理を行う専用ハードウェアを開発し、篩処理以外の線型代数処理および平方根計算処理はソフトウェアにより実現し、それらを組み合わせることにより実験システムを構成しました。

2. メモリアクセス回路の最適化および新たなデータ格納法の採用により、メモリ利用効率ならびにメモリアクセス処理の並列数を最大限まで引き上げました。

3. FPGA*5ならびにリコンフィギュラブルプロセッサDAPDNA-2*6を用いて、コア計算処理部を分離することにより、回路配置を最適化し、開発期間を短縮しました。

本システムを用いた分解実験の対象とした数は、Cunningham Project*7から未分解の423ビット(10進128桁)の数を選びました。本システムを約1ヶ月間動かすことで、下記の通り素因数分解が完了しました(62桁と66桁の素因数に分解)。

1100292287249685340593831918273088033131374251433916869047585356090
653266276431398241062784801654937155714269698644175648895865 7
＝
4549363729281646485206701473657133979231541985978421807687584 1 ×
2418563018313384375377878980960626923598195433036198640744103829 77

この実験結果を分析することにより、専用ハードウェアによる暗号解読の可能性を精密に見積ることができ、その結果を考慮してRSA暗号鍵長の更新時期を適切に設定し、将来の安全な暗号システムに貢献することができます。

【今後】
今回の実験では、現実に用いられているRSA暗号の鍵(一般には1024ビット)よりも小さい合成数の分解実験を行ったため、現実のRSA暗号が直ちに解読できることを示すものではありません。アルゴリズムの改良により、更なる高速化を行った場合の暗号解読の可能性を分析することが今後の課題となります。今後、より精密なRSA暗号の安全性・強度評価をすすめるとともに、情報デジタル社会の基盤を支える暗号技術全般に関して、研究開発活動を推進していきます。

《 NICTの委託研究制度 》

NICTがテーマを指定して公募し、研究開発を民間等に委託する制度。民間企業等の研究設備や研究者の研究開発能力の活用により、より一層効果的な研究開発を図るため、NICTが評価委員会の審査を経て決定した研究開発課題を指定して公募し、評価委員会の審査後、プロジェクトの採択を行い、提案した民間企業や大学等に研究開発を委託している。

NICT問合せ先

＜問い合わせ先＞
独立行政法人情報通信研究機構
総合企画部広報室
栗原則幸、大野由樹子
TEL:042-327-6923、FAX:042-327-7587

＜委託研究に関するお問合せ先＞
独立行政法人情報通信研究機構 連携研究部門
委託研究グループ 庄司 真語
Tel: 042-327-7197、FAX: 042-327-5604

富士通問合せ先

＜研究開発に関するお問合せ先＞
株式会社富士通研究所
ITコア研究所 セキュアコンピューティング研究部
Tel: 044-754-2681(直通)

【 用語解説 】

＊1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と考えられている。

＊2RSA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。公開鍵暗号・電子署名方式として、現在最も広く使われている。RSA暗号は、鍵が長くなるにしたがって安全性は増すが、処理性能は落ちる。鍵と同程度の大きさの合成数の素因数分解問題が解ければ、RSA暗号も解読される。

＊3SSL（Secure Sockets Layer）
ウェブ閲覧時などに安全に暗号通信するための技術。現在使われている多くのウェブブラウザ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。

＊4一般数体篩法（いっぱんすうたいふるいほう）
素因数分解の分解方式の一つ。現在最も高速である。

＊5FPGA(Field Programmable Gate Array)
論理回路をユーザーがプログラムできるLSI。一般的に少量生産の場合、カスタムチップ(ASIC)に比べて実装コストを抑えることができる等、ハードウェアの試作段階に適している。

＊6DAPDNA-2
アイピーフレックス社と富士通が開発したダイナミックリコンフィギュラブル(動的再構成)プロセッサ。内部にDAP （Digital Application Processor)と呼ばれるRISCプロセッサと、DNA （Distributed Network Architecture）と呼ばれるマトリクス状に論理演算装置が配置された独自プロセッサのデュアルコアプロセッサ。DNA内には376個の演算器が配置され、アプリケーションに応じて論理回路を動的に再配置可能であるという特長を持つ。

＊7Cunningham Project
$b^c \pm 1$（b=2,3,5,6,7,10,11,12,c：大）という形で表される数を素因数分解するプロジェクト。