暗号解読

受賞業績　素因数分解専用ハードウェアの開発と RSA 暗号の安全性評価

小暮　淳 [*1]　下山武司 [*1]　伊豆哲也 [*1]　鳥居直哉 [*1]　笛木俊介 [*2]

[*1]（株）富士通研究所ソフトウェア＆ソリューション研究所セキュアコンピューティング研究部
[*2] 富士通マイクロエレクトロニクス（株）ASSP 事業部マーケティング部

このたび，栄えある喜安記念業績賞を受賞し，大変光栄に思います．本研究開発に直接・間接にかかわった方々は 50 名近くにおよび，この方々の支えなしには本研究開発の成功はありませんでしたので，この場を借りまして改めて感謝と敬意を表したいと思います．横浜国立大学，立教大学，電気通信大学，日本電信電話（株），富士通九州ネットワークテクノロジーズ(株)，富士通マイクロソリューションズ(株)，(株)ロジック・リサーチの皆様には多大なるご協力をいただきました．また，本研究開発は（独）情報通信研究機構（NICT）の支援（研究委託）を受けて実施したものです．その他数多くの方々に感謝いたします．

今やあらゆる IT システムにおいて情報セキュリティの重要性が叫ばれていますが，受賞テーマの対象となった暗号技術は，情報セキュリティの基盤を支えるものであり，身近なところでは Web ブラウザの暗号通信（SSL : Secure Sockets Layer）などで使われています．

暗号技術の中でも，RSA 暗号☆1 と呼ばれる暗号が最も広く使われていますが，もし RSA 暗号が使用している合成数が素因数分解されれば，RSA 暗号は解読されてしまうことが分かっています．そこで，実際に RSA 暗号を使うときには，簡単に素因数分解できない大きな合成数を使えばよいのですが，一体どの程度大きな合成数なら素因数分解できない(安全)といえるのでしょうか？　たとえば，15 の素因数分解は 15=3×5 と暗算でもできてしまいますが，128 桁の数

1100292287249685340593831918273088033131374251433916869047585356090653266276431398241062784801654937155714269698644175648895865 7

は素因数分解できるでしょうか？

我々の研究は，大きな合成数の素因数分解実験を実際に行うことによって，将来にわたって安全な合成数の大きさを見積もり，暗号システムの安全性を保証することを目的としています．上記 128 桁の数は，このたび開発しました素因数分解専用ハードウェアにより素因数分解されてしまいましたので，RSA 暗号ではもっと大きな合成数を使わなければなりません．

素因数分解専用ハードウェア

実用化されている RSA などの暗号の安全性評価に関する研究は，我が国の電子政府システムの安全性向上等に貢献しています．このたびの受賞を励みに，これからも地道な研究を続け，本分野の発展に寄与すべく精進する所存です．

（平成 20 年 4 月 30 日受付）

小暮　淳（正会員） kogure@jp.fujitsu.com
1987 年東京大学大学院理学系研究科数学専攻修士課程修了．同年富士通（株）入社．1993 ～ 95 年米国駐在．1998 年より（株）富士通研究所にて暗号理論研究に従事．2007 年東京大学客員教授．電気科学技術奨励賞受賞．

下山　武司 shimo@labs.fujitsu.com
1991 年（株）富士通研究所入社，1996 ～ 98 年通信放送機構出向，以来共通鍵暗号設計や素因数分解に関する研究に従事，現在主任研究員，博士（工学）．2007 年電気科学技術奨励賞受賞．著書「情報セキュリティ事典」等．

伊豆　哲也（正会員） izu@labs.fujitsu.com
1997 年より（株）富士通研究所に勤務．情報セキュリティ・暗号理論の研究に従事．2001 年 Waterloo 大学客員研究員．2007 年文部科学大臣表彰若手科学者賞受賞．IACR, IEICE, SIAM 各会員．博士(工学)．

鳥居　直哉 torii.naoya@jp.fujitsu.com
1983 年大阪大学大学院工学研究科通信工学専攻修士課程修了．同年(株）富士通研究所入社．セキュリティの研究に従事．現在，セキュアコンピューティング研究部部長．電気科学技術奨励賞受賞．IEEE，電子情報通信学会会員．

笛木　俊介 fueki@jp.fujitsu.com
1984 年富士通（株）入社．2008 年より富士通マイクロエレクトロニクス（株）．2000 年よりスマートカード暗号機能開発等を担当．2005 年よりダイナミックリコンフィグデバイス開発に従事．電子情報通信学会会員．

☆1 RSA 暗号：公開鍵暗号（暗号化に用いる鍵データを公開できる暗号）の 1 つ．発明者（Rivest，Shamir，Adleman）の頭文字をとって命名された．