

暗号アルゴリズムの安全性評価

2008年9月更新

概要

ユビキタス時代の到来を迎え、プライバシー情報の交換や認証などのサービスがさまざまな場面で必要となつていまふ。これらサービスを安全に実現する上で、暗号技術は欠かすことのできない基盤技術です。富士通研究所では、暗号技術の研究開発の一環として暗号アルゴリズム(RSA暗号^(用語解説1))の精密な安全性評価を行っています。

技術のポイント

RSA暗号は、プライバシー情報をインターネット上で安全に交換する際に、標準的に使用されている技術です。近年、解読(素因数分解^(用語解説2))専用ハードウェアを用いることで、広く使用されている1024ビット鍵のRSA暗号が約15億円の製造費と約1年の計算時間によって解読可能という主張がなされたため、その妥当性の検討が急務となっていました。

富士通研究所は、これまでに蓄積させた理論的評価技術と、独自に開発した素因数分解法の実装技術により、RSA暗号の解読専用ハードウェアの試作・実験に世界で初めて成功しました。このハードウェアによる評価をもとに、上記のような解読専用ハードウェアの実現可能性に関し、否定的な結論を得ました。実験結果の解析をもとに、電子政府向け推奨暗号の安全性を評価・監視するプロジェクト(CRYPTREC)の報告書や、富士通のエンタープライズセキュリティアーキテクチャー(ESA)などを通じて、適切な暗号アルゴリズム・鍵長の利用を推奨していきます。

関連リンク

- ・【プレスリリース 2006年9月1日】 世界初、専用ハードウェアによる素因数分解実験に成功
<http://pr.fujitsu.com/jp/news/2006/09/1-3.html>
- ・富士通のエンタープライズセキュリティアーキテクチャー
<http://segroup.fujitsu.com/secure/solution/esa/>
- ・CRYPTREC Report 2006 暗号技術監視委員会報告(2007年3月)
http://www2.nict.go.jp/y/y213/cryptrec_publicity/c06_wat_final.pdf
 独立行政法人 情報通信研究機構(<http://www.nict.go.jp/>)、独立行政法人 情報処理推進機構(<http://www.ipa.go.jp/>)
- ・近年の素因数分解について(電子情報通信学会 基礎・境界ソサイエティ Fundamental Review Vol.3)
http://w2.gakkai-web.net/gakkai/ieice/vol3pdf/vol3_58.pdf
- ・情報処理学会 平成19年度喜安記念業績賞
http://www.ipsj.or.jp/01kyotsu/award/kiyasu_gyoseki_sho/h19.html



RSA暗号解読専用ハードウェアの試作機

諸元	
FPGA部 ^(用語解説3)	Xilinx社 Virtex4 XC4VLX200
DAPDNA部 ^(用語解説4)	IPFlex社 DAPDNA-2
動作周波数	133MHz (FPGA)
分解可能合成数	768ビット以下
分解性能 (768ビット)	約270年 (3.920秒/関係式1個)

用語解説

1 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名がついている。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、鍵と同程度の大きさの合成数の素因数分解が解ければ、RSA暗号は解読される。

2 素因数分解:

合成数を素数の積に書き下すこと。小さな合成数の素因数分解は短時間で実行可能であるが、大きな合成数については現実的な時間で実行することは不可能と考えられている。

3 FPGA (Field Programmable Gate Array):

論理回路をユーザがプログラム可能なLSI。一般に少量生産の場合、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に適している。

4 DAPDNA-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という特長を持つ。