パネル2「公開鍵暗号技術の最新動向について」

解読の最新動向と鍵長の選択

2010年3月3日（水）

株式会社富士通研究所
セキュアコンピューティング研究部
伊豆 哲也

電子政府推奨暗号（公開鍵暗号）

FUJITSU

署名	DSA
	ECDSA
	RSASSA-PKCS1-v1_5
	RSA-PSS
守秘	RSA-OAEP
	RSAAES-PKCS-v1_5
鍵共有	DH
	ECDH
	PSEC-KEM

安全性の根拠となる数学的問題

素因数分解問題

離散対数問題

楕円曲線
離散対数問題

暗号方式が安全 ＝根拠となる数学的問題を解くことが困難

最新の解読状況

FUJITSU

素因数分解問題

- 768ビットの合成数の分解（2009年12月, NTT等）

離散対数問題

- 676ビットの離散対数問題の求解（2010年2月, はこだて未来大・NICT）

楕円曲線
離散対数問題

- 112ビットの楕円曲線離散対数問題の求解（2009年7月, スイス連邦工科大等）

数学的問題の困難性が時間とともに低下
→ 暗号方式の安全性も時間とともに低下

鍵長選択時の問題点（1）

FUJITSU

- 他の暗号方式と同等な鍵長（等価安全性）が不明

ドキュメント名	共通鍵暗号	楕円曲線暗号	RSA暗号
NIST SP800-57	80	160～223	1024
Lenstra 等	80	160	1300
RSA Labs.	80	160	760
NESSIE	80	160	1536
IETF RFC 3766	80	----	1228
ECRYPT II	80	160	1248

鍵長選択時の問題点（2）

FUJITSU

■ 鍵長がいつまで安全かが不明（ライフタイム）

等価安全性	共通鍵暗号	ハッシュ関数	公開鍵暗号			NIST指針
			DSA・DH	RSA	楕円曲線暗号	
80 ビット	2-key TDES	SHA-1	L=1024 N=160	1024	160	
112 ビット	3-key TDES	SHA-224	L=2048 N=224	2048	224	2010年までに移行
128 ビット	AES-128	SHA-256	L=3072 N=256	3072	256	2030年までに移行
192 ビット	AES-192	SHA-384	L=7680 N=384	7680	384	
256 ビット	AES-256	SHA-512	L=15360 N=512	15360	512	

CRYPTRECへの要望

FUJITSU

1. 等価安全性の明確化
   - 特に共通鍵暗号・RSA暗号・楕円曲線暗号の間の等価安全性を評価して欲しい

2. 暗号アルゴリズム/鍵長のライフタイムの明確化
   - どの暗号アルゴリズム・鍵長をいつまで安全に（安心して）使用できるか、あるいは、いつから安全でなくなるのかを評価して欲しい

3. 攻撃情報・脆弱性情報のリアルタイムでの提供
   - 暗号アルゴリズム・暗号プロトコル・暗号実装の脆弱性情報をリアルタイムに提供して欲しい。特に問題点を指摘して欲しい
   - 例：ハッシュ関数MD5を使用したCA証明書の偽造
     GSM携帯電話の暗号アルゴリズムの危殆化
     EMVプロトコルにおける Chip and PIN 方式の脆弱性

富士通・富士通研究所の取組み

FUJITSU

FUJITSU THE POSSIBILITIES ARE INFINITE

Japan 検索

ホーム　国・地域のサイト | サイトマップ

ホーム > プレスリリース > 楕円曲線暗号とRSA暗号の強度比較基準を策定

PRESS RELEASE

2010年1月18日
富士通株式会社
株式会社富士通研究所
独立行政法人情報通信研究機構

楕円曲線暗号とRSA暗号の強度比較基準を策定

インターネット通信などを安全に利用するための基準作りに成功

富士通株式会社(代表取締役社長: 間塚道義)および株式会社富士通研究所(代表取締役社長: 村野和雄)は、インターネット通信などの新暗号技術である楕円曲線暗号(注1)について、現在標準的に用いられているRSA暗号(注2)との精密な強度比較基準を策定することに成功しました。今回の成果により、楕円曲線暗号が従来よりも数千倍程度相対的に高い強度であると考えられることが分かりました。今後は、得られた強度比較基準に基づき、最適な暗号システムを構築することで、インターネット通信などをより安全かつ便利に使用していただくことが可能になります。

なお、本成果の一部は、独立行政法人 情報通信研究機構(略称:NICT、理事長: 宮原秀夫)の委託研究「適切な暗号技術を選択可能とするための新しい暗号技術の評価手法」によるものです。また、本技術の詳細は、2010年1月19日(火曜日)から22日(金曜日)に、香川県高松市で開催される「暗号と情報セキュリティシンポジウム」で発表いたします。

背景

暗号技術はインターネット通信などを安全に利用するために広く用いられています。暗号技術のひとつであるRSA暗号は、ウェブの暗号通信プロトコルSSL(注3)でも採用されており、現在インターネットで最もよく使われているものです。一方、RSA暗号よりも短い鍵長(注4)で同等の強度を実現できるため、使い勝手の良い新技術としてデジタルコンテンツ保護規格に採用されるなど、楕円曲線暗号が使われる例が増加しています。

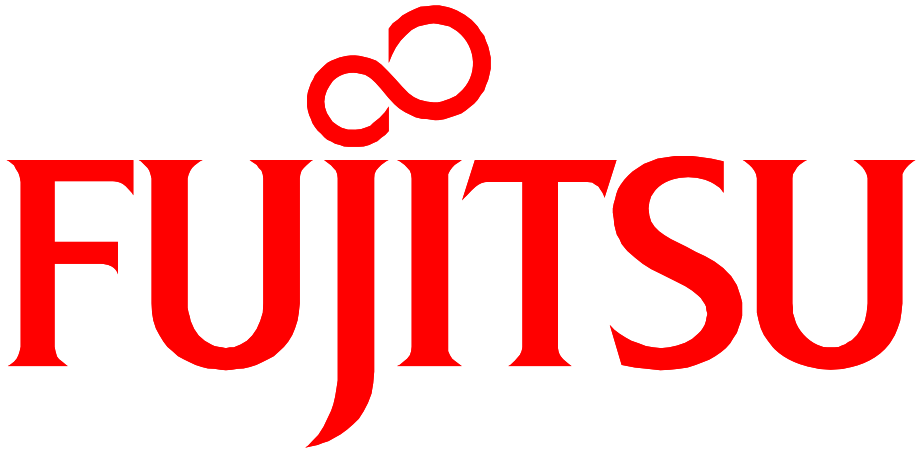
富士通・富士通研究所の取組み

FUJITSU

- 等価安全性の評価結果（抜粋、暫定版）のご紹介

共通鍵暗号	RSA	楕円素体	楕円2巾	楕円Koblitz
56	696	105	104	110
60	768	113	111	117
64	850	121	119	125
72	1024	137	136	142
80	1219	151	150	156
92	1536	176	174	181
108	2048	205	203	210
112	2206	213	212	219
128	2832	244	243	250

最終的な評価結果は2010年3月に報告の予定



THE POSSIBILITIES ARE INFINITE