楕円曲線暗号の攻撃評価*

安田雅哉、伊豆哲也、下山武司、小暮淳
株式会社富士通研究所

1. はじめに

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・インターネット銀行や公的手続きのオンライン申請などのネットワークを活用した便利なサービスが身近になる一方、秘密情報の漏洩対策、電子署名や個人認証など、情報セキュリティを確保するためには暗号技術が必須である。楕円曲線暗号は、1985年に発明された暗号で、現在デファクトの公開鍵暗号技術であるRSA暗号に比べ、より短い鍵長で同等の安全性を提供できると期待される次世代暗号技術であるが、今後電子情報を用いたサービスの基盤技術として利用されていくには、厳密な安全性評価が不可欠である。

2. 楕円曲線暗号の安全性評価研究の現状

これまでの楕円曲線暗号の安全性評価に関する研究は理論検討を中心に行われており、実験に基づく安全性評価研究では1997年から始まったECC Challenge[1]といった解読を目標としたデータ以外あまりない。以下で、現在までのECC Challengeの結果をまとめておく[2]：

表 1:現在までのECC Challengeの結果

年	ECC2	ECC2K	ECCp
1997	79		79
1998	97	95	97
1999			
2000		108	
2001			
2002			109
2003			
2004	109		

注
各値はパラメータサイズのビット数
ECC2 :2 冪楕円曲線 ,ECC2K:Koblitz曲線, ECCp:素体楕円曲線

楕円曲線暗号解読に関する最新情報をまとめておく：

- 表1のECC2-109については、Texas Tech大学のChris Monico助教授の研究チームが約2600台の計算機を用い約17ヶ月かけて解読したと報告している。
- 最近の話題では、2009年7月にECC Challenge問題ではないが、112ビットの素体上の楕円曲線暗号が解読された。解読に要した期間は、2009年1月13日から2009年7月8日までの約半年間で、スイス連邦工科大学にある約200台のPlay Station 3を利用したと報告されている。

3. 従来の問題点および研究目的

楕円曲線暗号に対する過去の実験では、解読を目標としていたため、強度評価・検証が統一的に行われていなかった。本研究では、実用的なすべての種類の楕円曲線暗号に対して、統一環境下で解読実験を網羅的に行い、その実験データを元に鍵長と強度との関係の分析をより精密に行い、鍵長の寿命を予測することにより、鍵更新時期などの運用方針に役立てる。また、RSA暗号との強度比較も行い、複数要素技術を使用する際の強度バランスを明確にすることを目的とする。

4. 研究開発

今回、実用的なすべての楕円曲線暗号に対して、最も効率のよい攻撃プログラムを開発し、統一環境下で攻撃実験を行い、比較的短い鍵長における計算量を測定することで計算量理論式の係数を決定した。以下で、詳細を述べる：

(ア) 攻撃プログラムの設計・開発

楕円曲線暗号の解読の困難さは、楕円曲線離散対数問題と呼ばれる数学的な問題を解くのと同程度と言われ、一部の曲線を除き効率の良い攻撃法はまだ発見されていない。現在最も効率的と考えられているρ法[3]およびその周辺技術を中心に調査し、すべての種類の楕円曲線暗号に対する攻撃プログラムを設計・開発した(図1)。設計・開発の際には、

- 楕円曲線の座標系・演算手法
- 並列化処理による高速化手法
- ρ法における乱数系列生成・分割数

* 本研究は、独立行政法人・情報通信研究機構の平成19年度から平成21年度の「高度通信・放送研究開発」に係る委託研究テーマ「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」として行われました。

[1] カナダCerticom社が楕円曲線暗号の安全性を実証するためにウェブ上に公開しているチャレンジ問題

[2] 楕円曲線暗号では、使用する技術により、いくつかの種類(素体、2冪、Koblitz)の楕円曲線が用いられることに注意しておく。

[3] 過去に解読されたECC Challengeはすべてρ法を用いて解読されている。

• 自己同型写像を用いたρ法高速化手法

などの必要なパラメータの最適なチューニングを図った。

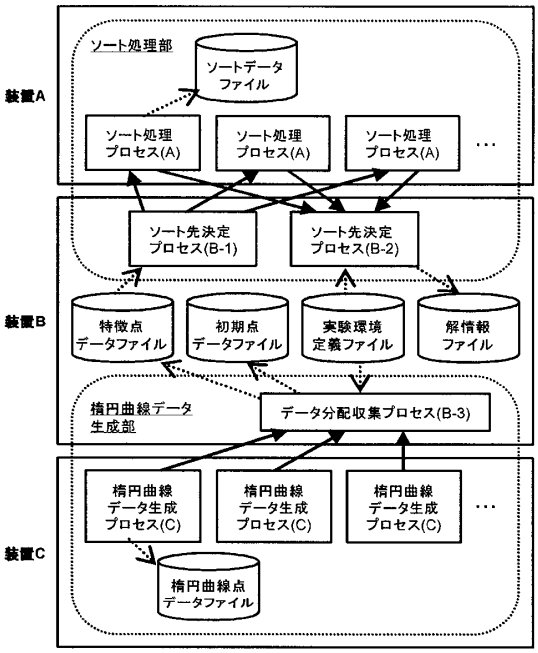

図 1：攻撃プログラム全体システム構成

（イ） 攻撃実験・暗号強度評価

開発した攻撃プログラムによる統一環境下(表 2)での解読実験を網羅的に行い、楕円曲線暗号を 1 年間で解読するために必要な計算量を精密に見積もった[1]。

表 2：実験環境

PC	Intel Core2 Quad CPU 2.6 GHz, 4GB RAM × 10 台
OS	CentOS 5.1-i386
開発環境	GCC v4.1.2, JAVA 1.6.0/07

5. 研究成果：RSA 暗号との強度比較

楕円曲線暗号と RSA 暗号との強度比較については、一部にデータがあるものの、考察が十分に行われているとは言い難く、その強度・安全性をできる限り正確に評価することが重要な課題であった。今回の研究と以前の研究[2]で得ていた RSA 暗号の解読実験データとの比較により、楕円曲線暗号と RSA 暗号との精密な強度比較を行った(表 3)。

表 3：暗号鍵長比較

RSA 暗号（ビット）	楕円曲線暗号（ビット）		
	素体	2 冪	Koblitz
696	105	104	110
768	113	111	117
850	121	119	125
1024	137	136	142
1219	151	150	156
1536	176	174	181
2048	205	203	210
2206	213	212	219
2832	244	243	250
6281	370	369	376
11393	496	495	503

今回の研究成果により、楕円曲線暗号が従来考えられていたよりも数千倍程度強度があることが分かった。

従来	今回
RSA1024≒楕円 160	RSA1024≒楕円 137
RSA2048≒楕円 224	RSA2048≒楕円 205

6. まとめ

今回、実用的なすべての種類の楕円曲線暗号に対して、最も効率的な攻撃プログラムを開発し、統一環境下での解読実験を網羅的に行うことで、楕円曲線暗号を解読するために必要な計算量を精密に見積もった。また、今回の研究と以前の研究で得ていた RSA 暗号の解読実験データとの比較により、楕円曲線暗号と RSA 暗号との精密な強度比較を行い、楕円曲線暗号が従来考えられていたよりも数千倍程度強度があることが分かった。

本成果により、楕円曲線暗号の鍵長ごとの寿命を予測することが可能になり、楕円曲線暗号システムの更新時期を明確にすることができるようになった。また、個々のシステムにおいて、RSA 暗号と楕円曲線暗号のどちらがより適しているかを正確に判断できるようになるため、暗号システムの安全性および利便性の向上に貢献できると期待される。

[1] ここでは、詳しく述べないことにする。

[2] 独立行政法人・情報通信研究機構の平成 16 年度から平成 18 年度の「高度通信・放送研究開発」に係る委託研究テーマ「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」において RSA 暗号の強度評価を行いました。