楕円曲線暗号と RSA 暗号の安全性比較*†

富士通株式会社, 株式会社富士通研究所

2010 年 8 月 20 日

概要

本稿では、楕円曲線離散対数問題に関して実施した計算機実験に基づく計算量評価ならびに従来知られている素因数分解問題の困難性に関する評価を比較し、楕円曲線暗号と RSA 暗号の強度比較を検証した結果を述べる。1024 ビット鍵を用いた RSA 暗号は、実用的な条件を仮定した下で、138 ビット鍵を用いた素体上の楕円曲線暗号、および、137 ビット鍵を用いた 2 の拡大体上の楕円曲線暗号とほぼ同じ安全性であるとの見積もりを得た。また、今回の研究成果は、既存成果として利用される NIST SP800-57 と比較した場合、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を示すものである。

1 はじめに

楕円曲線暗号は、Neal Koblitz と Victor Miller により独立に提案された、楕円離散対数問題 ECDLP (Elliptic Curve Discrete Logarithm Problem) の困難性を根拠とした公開鍵暗号である。楕円曲線暗号は、RSA 暗号と比較して短い鍵長で同等の安全性を満たすことができるという特長があることから、Blu-ray におけるコンテンツ保護技術 AACS (Advanced Access Control System) や DTCP (Digital Transmission Content Protection) などの標準規格で利用され始めており、今後より広く使われていく可能性があるとみられる暗号技術である。

従来、RSA 暗号への安全性評価実験は、ソフトハード共に多くの方法が多数試みられているのに対し、楕円曲線暗号の安全性評価実験は、ECC Challenge といった解読を目標としたデータ以外あまり知られていない。さらに楕円曲線暗号の、RSA 暗号や共通鍵暗号との強度評価比較については、一部にデータがあるものの、考察が十分に行なわれているとは言いがたく、今後情報システムに楕円曲線暗号を組み入れるにあたり、セキュリティバランスを保つ為にも、その強度・安全性を出来る限りより正確に評価することが重要な課題である。

楕円曲線暗号の安全性の根拠である楕円曲線離散対数問題 (ECDLP) とは、楕円曲線 E (素体 $GF(p)$ の場合 $y^2 = x^3 + ax + b$、標数 2 の体 $GF(2^n)$ の場合 $y^2 + xy = x^3 + ax^2 + b$) と楕円曲線上の点であるベースポイント S が与えられたとき、S が生成する巡回群 $\langle S \rangle$ から選ばれた任意の点 T に対し、$T = [d]S$ を満たす整数 d を見つける問題である。一部の Anomalous, Supersingular 等の曲線を除き、一般的な楕円曲線の ECDLP を解くための、総当り法よりも優れた現時点で最も効率のよいアルゴリズムは Pollard の ρ 法である。

本稿では、ECDLP に関して実施した計算機実験に基づく ρ 法の攻撃計算量評価を元に、既知の素因数分解問題の困難性に関する評価と比較することにより、楕円曲線暗号と RSA 暗号の強度比較を行った検証結果について述べる。

* 本研究は、独立行政法人情報通信研究機構 (NICT) による委託研究「適切な暗号技術を選択可能とするための新しい暗号等技術の評価手法」として行われました。

† 本稿は、2010 年暗号と情報セキュリティシンポジウム (SCIS 2010) における “楕円曲線暗号と RSA 暗号の安全性比較” というタイトルの発表資料 [20] に加筆したものです。

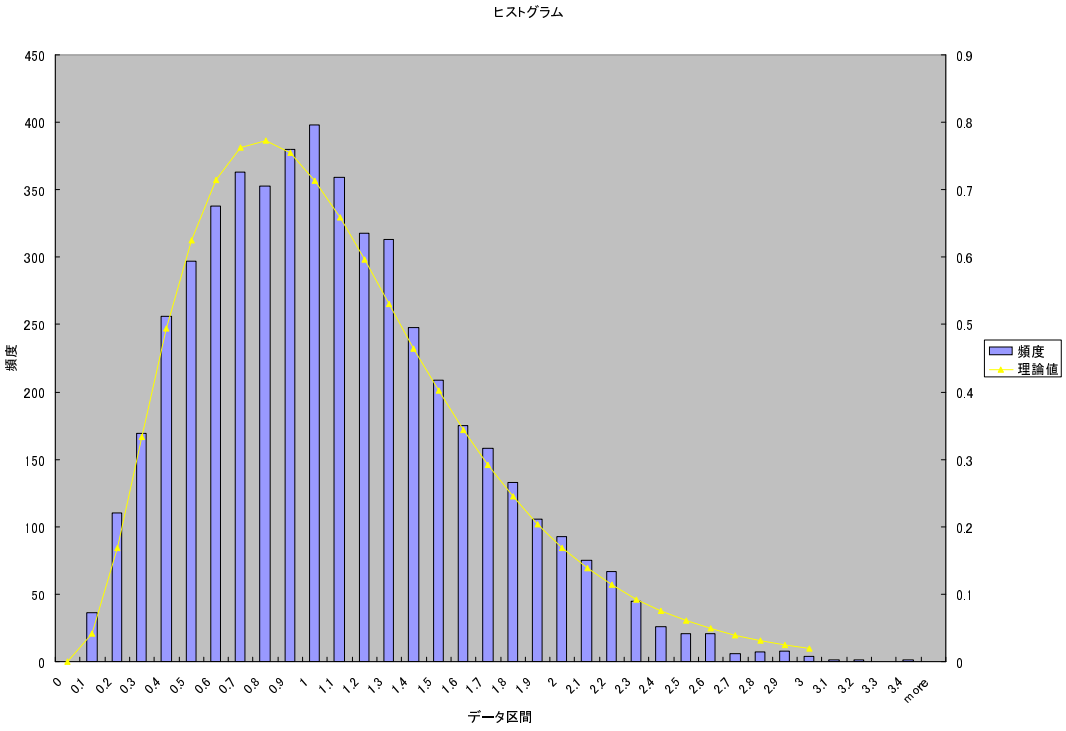

図 1　楕円演算処理回数の分布 (40-bit 素体)

2　ρ 法

有限体上の楕円曲線 E とベースポイント S とターゲットポイント T の組 (E, S, T) に対して、$T = [d]S$ を満たす整数 $d \in [0, n-1]$ (ただし、n はベースポイントの点位数) を見つけるために、何らかの方法で $[u]S + [v]T = [u']S + [v']T$ となる整数 u, v, u', v' を見つける。このとき、$[v - v']T = [u - u']S$ となるので、この関係式から $d = (v - v')(u - u')^{-1} \mod n$ となり、ECDLP の解を得ることができる。

上記性質を満たす $u, v, u', v' (u \neq u', v \neq v')$ を見つける手段として、Paul らによる ρ 法の改良を以下に示す。

まず、$L \geq 1$ を選び、適当な写像 $H : \langle S \rangle \to \{1, 2, \ldots, L\}$ をとる。ここでは L を分割数、写像 H を分割関数と呼ぶ。また写像 $f : \langle S \rangle \to \langle S \rangle$ を次のように定める。$f(X) = X + [a_i]S + [b_i]T, (H(X) = i)$ ただし、$a_1, b_1, ..., a_L, b_L \in [0, n-1]$ は、ランダムに選ばれた整数とする。ここでは、写像 f をランダムウォーク関数と呼ぶことにする。次に群 $\langle S \rangle$ からランダムに元 X_0 を選び、写像 f を用いて群 $\langle S \rangle$ 上の点列 $\{X_0, X_1, \ldots\}$ を $X_i = f(X_{i-1}) (i \geq 1)$ と定める。この時、点 X_0 を初期点と呼ぶ。初期点 X_0 が $[u_0]S + [v_0]T$ という点 S, T の線形和の形であらわされていれば、写像 f の取り方から $X_1 = f(X_0)$ も $[u_1]S + [v_1]T$ という点 S, T の線形和でかける。同様に、$X_i = [u_i]S + [v_i]T, (i \geq 1)$ とかける。群 $\langle S \rangle$ は有限集合なので、点 X_i を順に計算していくと、やがて既に点列に現れた点と等しくなる (衝突が起こると呼ぶ)。点 X_{s+t} がはじめて既に点列に現れた点 X_t と等しくなったとすると、整数 $i \geq s + t$ に対して、$X_i = X_{i-s}$ となる。この 2 点 X_i, X_{i-s} を同値なデータと呼ぶことにする。

整数 i に対して $X_i = X_{i-s}$ となることから、関係式 $[u_i]S + [v_i]T = X_i = X_{i-s} = [u_{i-s}]S + [v_{i-s}]T$ が成り立つ。以上によって、$[u]S + [v]T = [u']S + [v']T$ の形の関係式を構成することができる。ちなみに ρ 法という名前は、点列 X_i がギリシャ文字の ρ のように点在することが由来している。与えられた組 (E, S, T) に対して、ランダムウォーク関数 f を定め、衝突が起こるまで点列を計算し続けて衝突が起こる

表 1　NIST SP800-57 による Security Parameter

bit	Block	FFC (DSA,DH)		IFC (RSA)	ECC (ECDSA)
80	2TDES	$L = 1024$	$N = 160$	$k = 1024$	$f = 160 \cdots 233$
112	3TDES	$L = 2048$	$N = 224$	$k = 2048$	$f = 224 \cdots 255$
128	AES-128	$L = 3072$	$N = 256$	$k = 3072$	$f = 256 \cdots 383$
192	AES-192	$L = 7680$	$N = 384$	$k = 7680$	$f = 384 \cdots 511$
256	AES-256	$L = 15360$	$N = 512$	$k = 15360$	$f = 512+$

L:公開鍵長, N:プライベート鍵長, k:対応する鍵長, f:対応する鍵長

表 2　ANSI X9.62 における ECDLP 評価

n のサイズ	$\sqrt{\pi n/4}$	175G MIPS 年
160	2^{80}	8.5×1011
186	2^{93}	7.0×1015
234	2^{117}	1.2×1023
354	2^{177}	1.3×1041
426	2^{213}	9.2×1051

までに必要な点列 $\{X_0, X_1, \ldots\}$ の個数の期待値は、$\sqrt{\frac{\pi n}{2}} + \theta$ で見積もられている。ただし、実際に解読する際には、Iteration 関数や、数多くの実装パラメータ値に依存して、演算量が変化する可能性がある。本件に関するアルゴリズムならびに理論検討、実験評価値については、文献 [18, 19] において素体・2 冪・Koblitz それぞれ詳細に述べられている。

2.1　ECDLP と ρ 法の計算量

文献 [18, 19] において、素体、2 巾各々の ECDLP に対する並列 ρ 法に基づく詳細な攻撃実験評価を実施している。図 1 のグラフは、40 ビット素体楕円曲線パラメータを用いた攻撃実験を 5000 回実施した際、解読までに必要な演算回数の頻度分布を示したものである。横軸は演算回数、縦軸は出現頻度をあらわしている。横軸の演算回数は、期待値 $\mu = \sqrt{\pi n/2} = 1314195$ を 1 に正規化して記載している。棒グラフは実験による値、折線はガンマ分布を仮定した理論値である。実験値は、ほぼ理論値に近い値が得られている。ちなみに解読成功確率 80% を超えるためには、平均値の 1.54 倍、同じく 99% を超えるには、3 倍の計算量を用意する必要がある。また、約 7% のデータは、期待値計算量の 1/10 以下で解読に成功する。

3　既存結果

本章では、楕円曲線暗号の安全性評価に関する既存の結果についてまとめる。

3.1　従来の楕円曲線暗号安全性比較

表 1 は、NIST SP800-57 に記載されているセキュリティパラメータ比較である。表 2 は ANSI X9.62 [3] から引用した、楕円曲線のビットサイズと、計算量を示したものである。例えば、160 ビットサイズの ECDLP を 1 年で解くには、8.5×10^{11} MIPS の計算機が必要であることを意味している。Odlyzko は 2014 年には世界中の計算機の 0.1% を集めた計算量がおよそ 10^{10} から 10^{11} MIPS 年となるであろうと予測している [1]。ちなみに 2010 年現在の世界最速スーパーコンピュータ Jaguar は、1.75×10^{15} FLOPS (＝およそ 1.75×10^9 MIPS) であり [21]、上記見積もり用いると、160 ビット ECDLP を解くには Jaguar

表 3　80bit セキュリティ鍵長比較 (単位：ビット)

Report	ECC	RSA
NIST [13]	160	1024
Lenstra [6]	160	1300
RSA Labs [7]	160	760
NESSIE [8]	160	1536
IETF [9]	—	1228
ECRYPT II [15]	160	1248

表 4　ECDLP 及び GNFS 解読年表

year	ECC2	ECC2K	ECCp	GNFS
1997	79		79	
1998		95	97	
1999				463
				512
2000		108		
2001				
2002			109	524
2003				530
				576
2004	109			
2005				582
				663
2006				
2007				
2008				
2009			112	
2010				768

1 台を用いたと仮定しておよそ 485 年かかる計算になる。

表 3 は、これまでに各組織によって示された楕円曲線暗号 (ECC) と素因数分解ベースの暗号 (RSA) の安全性等価鍵長比較結果の一部であり、80 ビット全数探索計算量を基準として並べたものである。

3.2　解読世界記録による評価と考察

表 4 は、Pollard-ρ 法に基づく ECDLP 解読ならびに数体篩法に基づく素因数分解の世界記録の推移をしめしたものである。2009 年現在の素体 ECDLP 解読世界記録は 112 ビットである。

ρ 法は、群の加算の繰り返しが本質的演算であり、加算演算操作自体にはあまり多くのメモリーを必要としないことに加え、コリジョン探索部は、ディスティングイッシングポイントという技術を利用することで、省メモリ化が可能である。このことから、ρ 法は大規模分散計算に向けた実装が可能な攻撃アルゴリズムであり、インターネット上の有志による計算機といった、不統一な環境でも、うまく機能させることができる。

その一方で、一般的な合成数を素因数分解する最も効率的な方法である数体篩法は、以下の点に課題があり簡単には取り掛かりづらい。まず、数体篩法アルゴリズム自体が複雑で、高度な数学をベースとし、数多くの代数的整数論に基づくパラメータを適切に抽出しなければ、動作させることが難しく、そもそも敷居が

表 5　1 秒間の楕円演算処理回数

2 冪		素体	
bit	処理回数/秒	bit	処理回数/秒
60	27669.530	60	28192.019
70	23964.119	70	24662.572
79	23422.941	79	23852.054
89	22217.386	89	22899.097
97	20905.142	97	20491.775
109	19528.305	109	18504.164
131	16225.767	131	17260.161
163	13956.855	163	14550.941
191	12945.539	191	13329.266
238	10270.626	239	10122.312
353	6140.169	359	5536.9711

(Intel Core2 Quad CPU 2.6 GHz)

高いこと。また、計算量の点で本質的な、関係式探索部では、因子基底 (factor base) と呼ばれる大量の素数情報をメモリ上に展開し保持する必要があるのと共に、篩処理を行うために、各関係式 (relation) 候補に対応する領域に、篩結果を保持するため、結果として大量のメモリが必須であり、CPU パワーとメモリパワーをフルに利用しなければならないことである。現時点で、この問題を解決し少量のメモリで、安易に実施できる関係式探索アルゴリズムは知られておらず、特に、分散計算を行ううえでは通例となっている、計算機の空いた時間に行う、という戦略が使いづらいことが、プログラムを実施する上で、ネックとなっている。また、同じく多量の計算量が必要となる線形代数部では、アルゴリズムとして主流である Lanczos 法、Wiedemann 法共に、計算機ノード間の大容量かつ高速な通信が必要であり各計算機が同期して駆動しなければならないことから、数体篩アルゴリズムを実装実験する際には、緊密にネットワーク接続された均一な計算機環境が必要となる。以上の理由から、数体篩法に基づく素因数分解については、プロジェクトの規模を拡大しづらく、分散計算ではよく見られる数万台規模の解読実験を行うことが困難で、せいぜい数百台レベルの実験環境に留まってしまう。このような事情によって、世界記録に基づく評価では、楕円曲線暗号解読と比較して、素因数分解世界記録更新が遅れる傾向がある。いずれにせよ、解読世界記録の推移は、ひとつの具体的な資料ではあるものの、この数値に基づいて精密な暗号強度の比較を実施することは、あまり適切な方法ではないと思われる。

4　楕円曲線暗号の解読計算量見積もり

本節では、楕円曲線暗号の解読計算量予測に関して検討を行う。楕円曲線暗号の解読計算量は、各楕円曲線パラメータに対する楕円曲線演算処理速度、ならびに解読までの処理回数を用いることにより求めることができる。

4.1　解読に必要となる演算処理回数

まず、解読までの楕円曲線演算の処理回数について、開発した楕円曲線暗号攻撃プログラムを用いて実験を行った結果について述べる。図 25、図 26 は、それぞれ 40-bit の素体楕円曲線暗号ならびに 40-bit の 2 冪楕円曲線暗号の解読に必要な ρ 法の iteration 関数の処理回数について、5000 回の実験に基づく頻度分布を求めたものである。併せて γ 分布による近似曲線を記載する。横軸は、演算回数を表しており、期待値

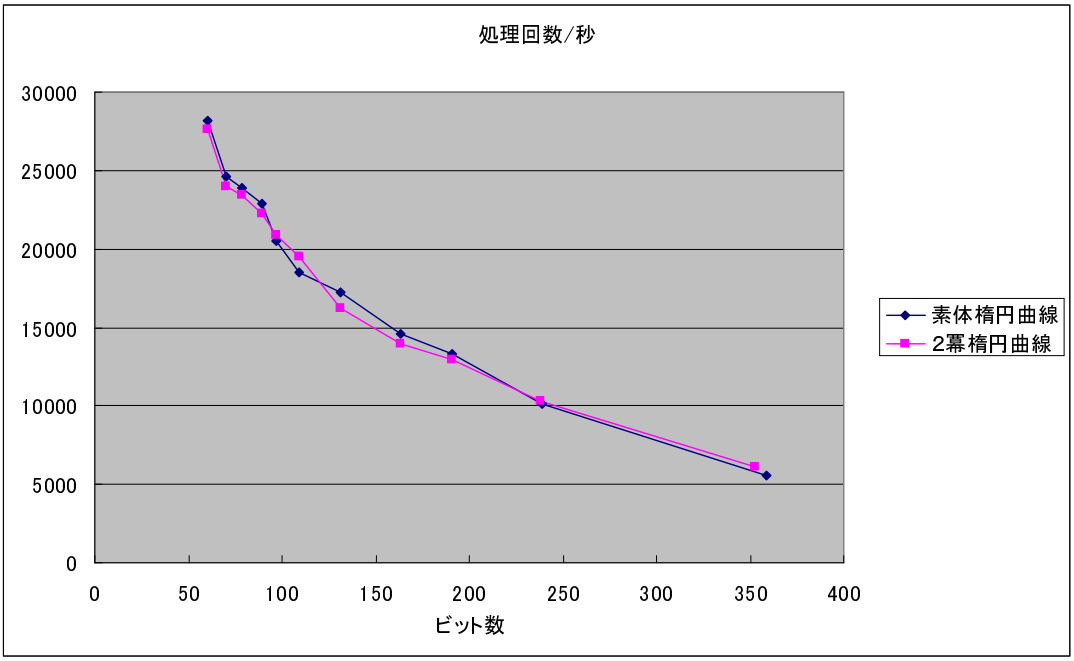

図 2　1 秒間の楕円演算処理回数

の理論値を 1 に正規化した値で示している。縦軸は演算回数の区間毎の頻度を表している。

上記は 40 ビット楕円曲線パラメータによる実験結果から導かれたものであるが、他の鍵サイズでも、同じ傾向が得られると考えられる。これらの実験結果から楕円曲線演算回数に応じた解読成功確率を導くことができる。特に期待値の 3 倍まで楕円曲線計算処理を進めれば、99.1% の確率で解読に成功するとみなすことが出来る。今後、楕円曲線暗号の解読計算量を見積もるに当たり、成功確率 99%、すなわち楕円曲線演算回数として期待値の 3 倍を指標として用いる。

4.2　楕円曲線演算処理速度

本章の目標である楕円解読計算量を見積もる場合、楕円曲線演算の処理性能が重要な因子として現れる。本節では、この楕円曲線処理性能について見積もりを行う。

4.2.1　実験による処理速度

楕円演算の処理速度は、法となる素数の大きさに依存して変化し、ビット数が大きくなるに従い単位時間に行える演算回数が減少する。一般的にはビット数に対し 2 乗のオーダーの処理時間が必要であることが知られている。表 5 は、60 ビットから 353 ビットまでの各 2 冪楕円曲線パラメータに対して、一秒間に処理された楕円曲線上の演算回数を実験に基づいて算出したものである。なお、任意多倍長整数演算は、CPU に依存した高速化テクニックが考えられるが、今回の実装では、シングルタスクで Jacobian 座標に基づく C 言語による楕円演算処理実装を用い、アセンブラ等によるカスタマイズやマルチコアを用いた処理は用いなかった。今後の改良により、単位時間当たりの処理を高速化できる可能性が残されている。

Certicom 社は、Certicom Challenge における ECCp-109 の、1 秒間に行える楕円演算処理回数は 27000 回、ECC2-108 では、9000 回 (CPU は 100MHz と仮定 [2]) と見積もっている。文献 [11] では、[10] に記載されている、32 ビット CPU における演算に適した、特殊な 256bit 素体楕円曲線上でのスカラー倍算処理速度 832475 cycle (Pentium III) から、素体楕円曲線加算を 1626 cycle と見積もっている。また、文献 [16] では、ECC2-131 の Cell 実装における単一 SPU 上の単位楕円演算処理が 1157cycle(通

表 6　楕円曲線暗号の解読計算量 (計算能力は 10 の冪指数で表記)

素体楕円曲線		2 冪楕円曲線		Koblitz 楕円曲線	
位数 (bit)	計算能力	位数 (bit)	計算能力	位数 (bit)	計算能力
106	11.47	105	11.55	110	11.59
114	12.74	112	12.66	117	12.68
122	14.00	120	13.92	125	13.93
138	16.52	137	16.60	142	16.57
152	18.71	151	18.79	156	18.74
177	22.61	175	22.53	181	22.60
206	27.10	204	27.03	210	27.06
214	28.34	213	28.42	219	28.44
245	33.12	244	33.21	250	33.20
371	52.45	370	52.54	376	52.43
497	71.67	496	71.76	503	71.73

常実装),1047 cyle (bitslice 実装) と記載されている。これらの既存実装は、各々実装環境やパラメータが異なるが、上記から、我々の実験で用いた楕円実装は、およそ 100 倍程度は改良の余地があるものと推測される。

4.3　既存文献による演算処理速度

前節において、単位時間当たりの楕円曲線処理性能に関して、実装実験に基づくビット毎の性能データを抽出したが、その性能データは、既知文献の中で示されているトップデータと比較しておよそ 100 倍程度の差が見込まれている。本書で目指す楕円曲線暗号の解読計算量は、現実的に解読可能となり得る量を基準として設定することにより、異なる暗号プリミティブ間でも、安全性に関する相対的な比較が可能となるものである。その際、最高速レベルの実装による処理速度を用いることで、より精密な評価が求められるものと考える。今回の実装では楕円曲線演算処理自体の高速化は実施していないが、ρ 法アルゴリズムの解読実験、すなわち楕円曲線演算回数に関する詳細なデータを取得することに注力し、演算処理速度については信頼性の高い既存文献のデータを利用することとする。以降では、楕円曲線処理速度のトップデータに関する考察を行う。

■素体楕円処理速度　文献 [17] より、224 ビット素体楕円曲線暗号 (NIST P-224) の処理時間として、スカラー乗算 1 回の処理性能として 595537 cycle (Athlon) の値が記載されている。この記録は素体楕円処理速度に関し、現時点で調査した範囲では、最良の結果である。(特殊な素体を利用した楕円曲線演算については、さらに高速化を図ることが可能であることが知られている。文献 [10]) 本数値データを下に、スカラー乗算 1 回につき、平均して 224 回の 2 倍算と 224/2 回の加算が実施されていると仮定し、さらに加算と 2 倍算が同じ処理速度と仮定し、また、iteration function は、加算 1 回と等価とすることにより、素体楕円曲線における iteration function の処理性能を次のように見積もることが出来る。

$$595537/(224+112) = 1772 \text{ cycle/iteration}$$

更に、鍵ビット数 N の素体楕円曲線の処理性能は、ビット長の 2 乗に比例すると考えられることから、以下のように見積もることができる。

$$1772 \times (N/224)^2 \text{ cycle/iteration.}$$

■2 冪楕円処理速度　文献 [16] より、131 ビット 2 冪楕円曲線 (ECC2-131, NIST2-131) の処理性能は以下の値であると記載されている。

表 7　素因数分解処理 (篩処理) の推測（単位は Athlon64 2.2GHz 年）

サイズ	768	1024	1536	2048
計算量	1108	8.4×10^6	4.6×10^{12}	25×10^{16}

(条件：実メモリ制約有り)

表 8　素因数分解処理 (篩処理) の推測（単位は FLOPS、10 の冪指数）

サイズ	768	1024	1536	2048
計算量	12.6879	16.3395	22.2319	27.0413

(条件：実メモリ制約有り)

1047cycle/iteration (Cell SPE 3GHz, Bitslice 実装)

鍵ビット数 N の 2 冪楕円曲線の処理性能は、通常ビット長の 2 乗に比例することから、以下のように見積もることができる。

$$1047 \times (N/131)^2 \text{ cycle/iteration}$$

■Koblitz 楕円処理速度　Koblitz 楕円曲線については、2 冪楕円処理に対して、1.82 倍 (1+ 0.62 (基底変換) + 0.2 (L 計算 [Gallant 改良 [4]])) の演算時間がかかることが示される。よって、以下のように見積もることが出来る。

$$1.82 \times 1047 \times (N/131)^2 \text{ cycle/iteration}$$

4.4　解読計算量見積もり

本章では、楕円曲線暗号の解読計算量を見積もる。本評価を行うに当たり、下記の基準を考慮することとする。

- 暗号を 1 年間で解読するために必要な計算機能力を FLOPS を単位として求め、比較の基準とする
- 解読成功確率：99%（ρ 法は確率的アルゴリズムであるため）
- 最適な iteration 関数を用いた場合の実験データを利用。
  - 素体・2 冪楕円曲線： ADD 関数
  - Koblitz 曲線：Gallant らの関数 [4]
- 素体・2 冪の場合における、Negation Map による $\sqrt{2}$ 倍の高速化を仮定。
- 演算処理速度：最新かつ最高性能の数値を利用
  - 素体：1772cycle/iteration（224bit）
  - 2 冪：1047cycle/iteration（131bit）
  - Koblitz：2 冪楕円処理の 1.82 倍の処理時間

以上より、楕円曲線暗号を 1 年で解読するために必要な計算機能力 (FLOPS) について以下の式が導かれる。(ただし $Y = 365 \times 24 \times 60 \times 60$ 秒)

解読計算量 = 3 × 平均計算量 × 単位演算サイクル数/年

素体楕円曲線暗号解読= $3 \times \sqrt{\pi 2^N}/2 \times 1772 \times (N/224)^2/Y$

2 冪楕円曲線暗号解読= $3 \times \sqrt{\pi 2^N}/2 \times 1047 \times (N/131)^2/Y$

Koblitz 楕円曲線暗号解読= $3 \times \sqrt{\pi 2^N/N}/2 \times 1.82 \times 1047 \times (N/131)^2/Y$

この式より、表 6 の値を得ることができる。

5　暗号強度比較

本節では、楕円曲線暗号を一年間で解読するために必要な計算量と、CRYPTREC Report 2006 図 2.2 にて得られている素因数分解篩処理の評価値を利用することで、楕円曲線暗号と RSA 暗号との暗号強度比

表 9　理論値による値 (単位は FLOPS、10 の冪指数)

サイズ	768	1024	1536	2048
計算量	12.6879	16.3393	22.2308	27.0434

表 10　素因数分解を 1 年間で行うために必要な計算機能力 (10 の冪指数 FLOPS)

サイズ (ビット数)	計算能力
696	11.52
768	12.69
850	13.93
1024	16.34
1219	18.76
1536	22.23
2048	27.04
2206	28.38
2832	33.21
6281	52.46
11393	71.73

較を行う。

5.1　素因数分解計算量について

CRYPTREC Report 2006、表 2.4 において、Athlon 2.2GHz を 1 年間使用する計算量を 1 単位とし、素因数分解において本質的な処理である「篩処理」にかかる処理の計算量の上限値（実メモリに制約（2GB）がある場合）として、表 7 のように見積もっている。さらに CRYPTREC Report 2006 では、Athlon64 2.2GHz のピーク性能として、(クロック周波数) × (浮動小数点演算ユニット数) を用いて、4.4GFLOPS (=4.4×10^9 FLOPS) とみなし、上記表を FLOPS 単位とした処理性能に換算した値を利用して素因数分解をベースとした暗号の安全性評価へ結び付けている。その値を表 8 に示す。

ここで、上記ビットサイズと計算量の関係から、上記以外のビット数への評価が可能なものに一般化するため、一般数体篩法における計算量評価式として知られている評価式

$$L_N(1/3, (64/9)^{1/3} + C)$$

への代入を試みる。ちなみに、

$$L_N(s, c) = \exp(c(\log(N)^s \log(\log(N))^{1-s}), (64/9)^{1/3} = 1.9230$$

である。上記式のパラメータとして、$C = 1.4949$, log の底 $= 2^{260}$ とすると、ビットサイズに対し、それぞれ表 9 に示す値となる。これらの値は、表 8 の値と十分近いことから、素因数分解計算量として、以下この式の値を利用する。表 10 ならびに 図 3 に、上記式を用いた素因数分解計算量の評価一覧を記載する。

5.2　RSA 暗号と楕円曲線暗号の強度比較

各種暗号の強度比較に関し、NIST は SP800-57 において表 1 で示される評価を公表している。一方で、上記表における楕円曲線暗号の扱いは、例えば 1024 ビット RSA と等価な楕円曲線暗号が、160 ビットか

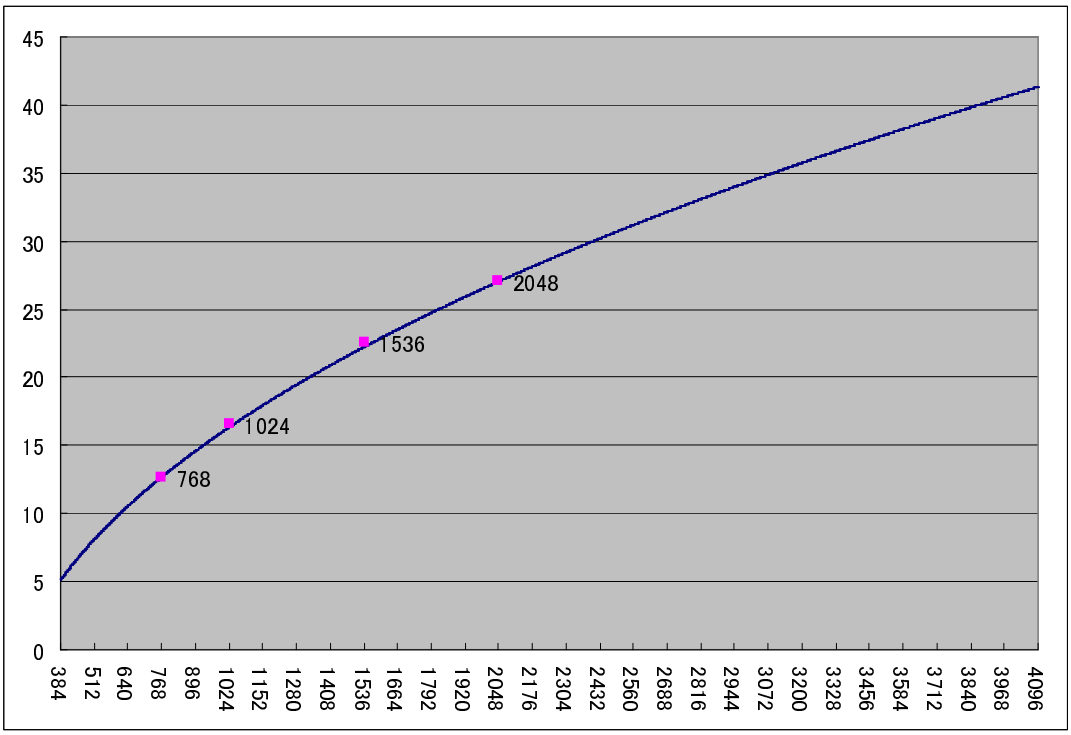

図 3　RSA 暗号解読計算量

ら 223 ビットの間と、ビット値の範囲で示されているのみであり、RSA 暗号と楕円曲線暗号の等価安全性に関する何らかの知見を得たい場合、本表は必ずしも適切なものではないことが推測される。本節では、前節までに得られた結果を基に、楕円曲線暗号と RSA 暗号との安全性に関して詳細な比較を行う。暗号強度の比較を行うに当たり、その条件を再掲する。

> 各々の暗号を 1 年間で解読するために必要な計算機能力を FLOPS を単位で求めたものを比較の基準とする

上記条件のもと、楕円曲線暗号の解読計算量また、RSA 暗号の安全性の根拠である素因数分解の演算量については前節にて実験・理論両面から考察を行った。以上の結果を基に、各暗号の等価安全性を表 11 に示す。なお、本表には共通鍵暗号の安全性比較についても記載した。共通鍵暗号に対する攻撃手法は鍵全数探索、演算処理速度については AES (147 cycle/block [14]) を利用している。本表において、横方向に並べられた暗号パラメータの安全性は、ほぼ等価であることを表している。

なお、2010 年 7 月現在の素因数分解ならびに素体楕円曲線暗号の解読世界記録は、それぞれ RSA768 ビット (2010 年)、素体楕円 112 ビット (2009 年) であり、時期も近いことから、本結果の信憑性を示す証拠の一つであると思われる。

6　まとめ

本稿では、各ビット長の楕円曲線暗号について、得られた解読必要演算量と楕円演算処理速度から、1 年間で解読を行うために必要な計算量を見積もり、その結果を元に RSA 暗号との比較を行った。その結果、1024 ビット鍵を用いた RSA 暗号は、実用的な条件を仮定した下で、138 ビット鍵を用いた素体楕円曲線暗号、137 ビット鍵を用いた 2 冪楕円曲線暗号とほぼ同じ安全性であるとの見積もりを得た。また、今回の研究成果は、既存成果として利用される NIST SP800-57 と比較した場合、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を示すものである。

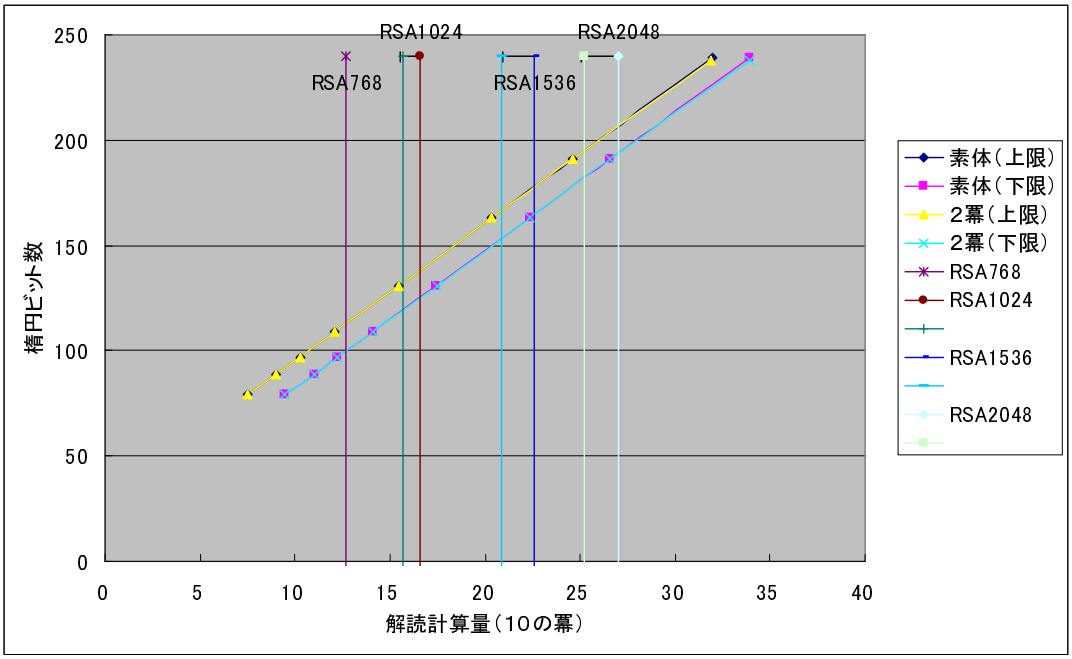

図 4　楕円曲線暗号と RSA 暗号解読計算量比較

表 11　RSA 暗号と楕円曲線暗号の強度比較 (鍵ビット長)

共通鍵暗号	RSA 暗号	楕円素体	楕円 2 冪	楕円 Koblitz
56	696	106	105	110
60	768	114	112	117
64	850	122	120	125
72	1024	138	137	142
80	1219	152	151	156
92	1536	177	175	181
108	2048	206	204	210
112	2206	214	213	219
128	2832	245	244	250
192	6281	371	370	376
256	11393	497	496	503

参考文献

[1] A. Odlyzko, “The Future of Integer Factorization”, CryptoBytes, vol.1, no.2, pp.5-12, 1995. ftp://ftp.rsasecurity.com/pub/cryptobytes/crypto1n2.pdf

[2] Certicom, “Certicom ECC Challenge”, 1997 (revised November 2009). http://www.certicom.com/pdfs/cert_ecc_challenge.pdf

[3] ANSI, “The Elliptic Curve Digital Signature Algorithm (ECDSA)”, ANSI X9.62-1998, 1998.
[4] R. Gallant, R. Lambert, and S. Vanstone, “Improving the Parallelized Pollard Lambda Search on Anomalous Binary Curves”, Mathematics of Computation, vol.69, no.232, pp.1699-1705, 2000. http://www.ams.org/journals/mcom/2000-69-232/S0025-5718-99-01119-9/S0025-5718-99-01119-9.pdf
[5] M. Brown, D. Hankerson, J. Lopez, and A. Menezes, “Software Implementation of the NIST Elliptic Curves over Prime Fields”, technical report, CORR 2000-56, University of Waterloo, 2000. http://www.cacr.math.uwaterloo.ca/techreports/2000/corr2000-56.ps.
[6] A. Lenstra and E. Verheul, “Selecting Cryptographic Key Sizes”, Journal of Cryptology, vol.14, no.4, pp.255-293, 2001.
[7] RSA Labs., “A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths”, RSA Labs Bulletin, no.13, April 2000 (Revised November 2001). http://www.rsa.com/rsalabs/node.asp?id=2088
[8] NESSIE, “NESSIE Security Report”, February 19, 2003. http://www.cosic.esat.kuleuven.be/nessie/deliverables/D20-v2.pdf
[9] H. Orman and P. Hoffman, “Determining Strengths for Public Keys Used for Exchanging Symmetric Keys”, IETF RFC 3766/BCP 86, April 2004. http://www.apps.ietf.org/rfc/rfc3766.html
[10] D. Bernstein, “Cuvre25519: New Diffie-Hellman Speed Records”, Proceedings of PKC 2006, LNCS 3958, pp.207-228, Springer-Verlag, 2006.
[11] CRYPTREC, CRYPTREC Report 2006, 情報処理推進機構・情報通信研究機構, March 2007.
[12] T. Gueneysu, C. Paar, and J. Pelzl, “Attacking Elliptic Curve Cryptosystems with Special Purpose Hardware”, Proceesings of ACM SIGDA 2007, 2007.
[13] NIST, “Recommendation for Key Management-part1: General (Revised)”, SP800-57, August 2007.
[14] M. Matsui and J. Nakajima, “On the Power of Bitslice Implementation on Intel Core2 Processor”, Proceedings of CHES 2007, LNCS 4727, pp.121-134, Springer-Verlag, 2007.
[15] ECRYPT II, “ECRYPT2 Yearly Report on Algorithms and Keysizes (2008-2009)”, July 2009. http://www.ecrypt.eu.org/documents/D.SPA.7.pdf
[16] D. Bailey, B. Baldwin, L. Batina, D. Bernstein, P. Birkner, J. Bos, G. van Damme, G. de Meulenaer, J. Fan, T. Güneysu, F. Gurkaynak, T. Kleinjung, T. Lange, N. Mentens, C. Paar, F. Regazzoni, P. Schwabe, and L. Uhsadel, “The Certicom Challenges ECC2-X”, IACR ePrint Archive, 2009/466, 2009. http://eprint.iacr.org/2009/466
[17] D. Bernstein, “Speed Reports for Elliptic-Curve Cryptography”, 2010. http://cr.yp.to/ecdh/reports.html
[18] 下山武司, 安田雅哉, 伊豆哲也, 小暮淳, “素体楕円曲線暗号攻撃評価システム”, 2009 年暗号と情報セキュリティシンポジウム (SCIS 2009), 2009.
[19] 小暮淳, 安田雅哉, 下山武司, 伊豆哲也, “2 冪楕円曲線暗号の攻撃評価”, 2010 年暗号と情報セキュリティシンポジウム (SCIS 2010), 2010.
[20] 下山武司, 伊豆哲也, 小暮淳, 安田雅哉, “楕円曲線暗号と RSA 暗号の安全性比較”, 2010 年暗号と情報セキュリティシンポジウム (SCIS 2010), 2010.
[21] TOP500 Supercomputing Sites, 2010. http://www.top500.org/

担当著者

- 下山 武司 (富士通株式会社/株式会社富士通研究所)
- 伊豆 哲也 (富士通株式会社/株式会社富士通研究所)
- 小暮 淳 (富士通株式会社/株式会社富士通研究所)
- 安田 雅哉 (富士通株式会社/株式会社富士通研究所)

本稿に関する連絡先

- security_white_paper@ml.fujitsu.com