公開鍵暗号を巡る新しい動き：RSAから楕円曲線暗号へ

清藤武暢（せいとうたけのぶ）／四方順司（しかたじゅんじ）

要　旨

金融分野では、各取引においてやり取りされる情報の安全性を確保するために共通鍵暗号や公開鍵暗号等が広く利用されている。RSA は現在主流の公開鍵暗号として幅広く普及しているが、計算機性能向上等に付随する解読リスクの高まりに伴い、鍵長を長くする等の対策が求められており、従来のハードウエア環境での実装が難しくなる等の可能性が無視できなくなりつつある。また、管理者のミス等により脆弱な鍵が発行されやすいという運用上の問題も指摘されている。

こうした状況下、RSA に代わる公開鍵暗号として「楕円曲線暗号」が注目されている。楕円曲線暗号は、RSA と比較したとき、短い鍵長で同程度の安全性を保証できることや、鍵生成に関する運用上の問題が発生しにくいという利点を有しており、近い将来 RSAに代わって公開鍵暗号の中心的な役割を担うことが期待されている。しかし、楕円曲線暗号は RSAとは異なる技術的特徴を有しており、安全に利用するためにはその仕組みや安全性評価の動向に関する専門的な知識を有しておくことが必要である。

そこで、本稿では、楕円曲線暗号の概要や安全性評価に関する最近の研究動向を紹介するとともに、同暗号を安全に利用する際の留意点について考察した。その結果、米国立標準技術研究所（NIST）の公表情報等を適切に活用することにより、楕円曲線暗号を安全に利用することができることがわかった。ただし、攻撃手法の研究は進展途上にあり、今後もその研究動向について注視する必要がある。

キーワード：公開鍵暗号、RSA、楕円曲線暗号、楕円曲線離散対数問題、指数計算法、計算量

本稿の作成に当たっては、株式会社富士通研究所主任研究員の伊豆哲也氏から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

清藤武暢　日本銀行金融研究所（E-mail: takenobu.seitou@boj.or.jp）
四方順司　国立大学法人横浜国立大学大学院環境情報研究院（E-mail: shikata@ynu.ac.jp）

1. はじめに

金融分野では、各種金融取引においてやり取りされる情報の安全性を確保するため、共通鍵暗号や公開鍵暗号等の暗号アルゴリズムが広く利用されている。例えば、銀行 ATM とホストコンピュータ間でやり取りされる情報（暗証番号や口座番号等）の機密性確保や一貫性の保証、インターネット・バンキングにおけるホストやクライアントの認証、ATM における IC カードの真正性確認等で活用されている。情報の機密性を確保する手段としては主に共通鍵暗号が用いられ、トリプル DES や AES（Advanced Encryption Standard）等の暗号アルゴリズムが主に使われている。一方、情報（データ）の一貫性や通信相手を認証する手段としては主に公開鍵暗号が用いられており、RSA 等が主流の暗号アルゴリズムとして幅広く普及している（武藤［2011］）。

一般的に、暗号アルゴリズムにおいては、計算機性能の向上や攻撃手法の進歩等により安全性が経年劣化するという問題がある。この問題を解決するためには、安全性の基準となる「鍵長」と呼ばれるパラメータを適宜長くしていくという運用が必要となる。現在主流の RSA は、この運用により特に鍵長が長くなる傾向があり、いずれ暗号処理等において支障が生じる可能性が指摘されている。特に、IC カードや組込み機器[1]等のように計算機性能（計算能力やメモリ）が制限されている環境では、今後 RSA の利用が厳しくなっていくことが予想される。そのため、このような環境においては、RSA よりも短い鍵長で同程度の安全性を達成できる公開鍵暗号が求められている。また、RSA は、管理者のミスや実装上の不具合等により脆弱な鍵を発行されやすいという運用上の問題も指摘されている。

こうした状況において、RSA に代わる公開鍵暗号として「楕円曲線暗号」が注目されている。楕円曲線暗号は、「楕円曲線離散対数問題」と呼ばれる数学的問題を利用する公開鍵暗号の総称であり、1985 年頃にミラーとコブリッツによりそれぞれ独立に提案された（Miller [1985]、Koblitz [1987]）。この暗号は、RSA と比較して短い鍵長で同程度の安全性を実現できることや、鍵生成に関する運用上の問題が生じにくいという利点を有しているため、RSA に代わる公開鍵暗号として注目されている。実際、同暗号は、デジタルテレビやハードディスク・レコーダにおける映像コンテンツの保護技術や携帯電話のセキュリティ保護技術等、さまざまな場面で実際に利用され始めている。また、情報セキュリティ技術に関するいくつかの国際標準や関連するガイドライン、業界標準等においても楕円曲線暗号が規定されており、今後公開鍵暗号の中心的な役割を担うことが期待されている。

しかし、楕円曲線暗号を実際に利用するためには、暗号処理が前提とする楕円曲線の方程式等を選択するといった特有の準備作業が必要であり、安全に利用するた

1 組込み機器とは、特定の機能を実現するためのコンピュータ・システムが内蔵されている家電や産業用機械を意味する。デジタルテレビ等の身近な家電のほとんどは組込み機器である。組込み機器は、一般的に生産コスト等の制約から計算能力やメモリ等の計算機性能に強い制約がある。

めにはある程度の専門的な知識を有しておくことが必要である。そこで、本稿では、楕円曲線暗号の概要や利用状況、同暗号の安全性評価に関する最近の研究動向について紹介するとともに、楕円曲線暗号を安全に利用する際のいくつかの留意点について考察する。

以下、本稿では、2節においてRSAを取り巻く現状について説明した後、3節では、楕円曲線暗号の概要や利用状況について解説する。そして、4節で、楕円曲線暗号の安全性評価に関する最近の研究動向を整理して紹介し、金融機関が同暗号を安全に利用するための留意点について述べる。さらに、5節において、楕円曲線暗号に対する最新の攻撃手法に関する研究を紹介し、それが同暗号の安全性評価に与える影響について考察する。

2. 現在主流の公開鍵暗号であるRSAの現状

(1) 公開鍵暗号とRSA

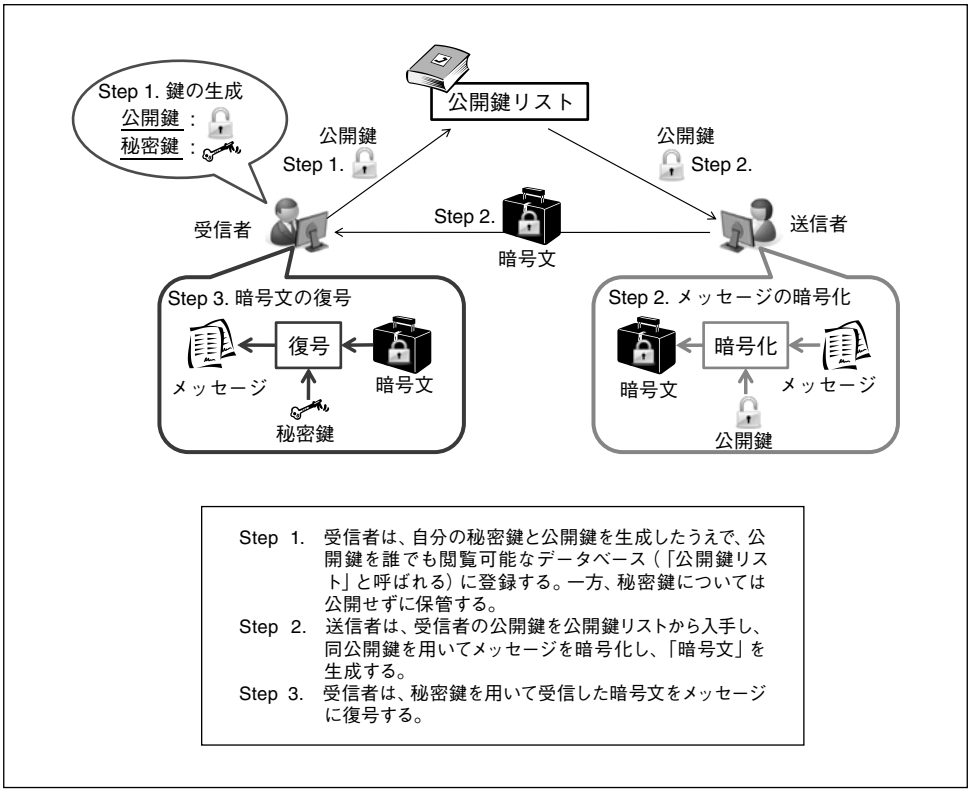
金融分野では、各種金融取引における安全性を確保することを目的として暗号アルゴリズムが広く利用されているが、「情報（データ）の一貫性確保」や「通信相手の認証」、「秘密鍵の共有」という暗号機能を実現する手段として公開鍵暗号が用いられることが多い。

公開鍵暗号は、暗号化に利用する鍵（以下、「公開鍵」と呼ぶ）と復号に利用する鍵（以下、「秘密鍵」と呼ぶ）が異なり、秘密鍵は各利用者が秘密に保管する必要がある一方、公開鍵は全ての利用者に公開できるという特長を有する暗号アルゴリズムである。この方式は、事前に通信相手に鍵を秘密に渡しておく必要がないため、不特定多数の利用者間で行う暗号通信等に適している。公開鍵暗号を用いて「送信者」がメッセージを暗号化し、それを受信した「受信者」が復号するという一連の流れを以下に示す（図表1参照）。

RSAは、公開鍵暗号のアイデアを具体化する方法としてリベスト（Rivest）、シャミア（Shamir）、エーデルマン（Adleman）らによって1978年に考案された（Rivest, Shamir, and Adleman [1978]）。RSAに関しては安全性に関する研究成果が数多く発表され、これまでに効率的な解読法がみつかっていないことや、2000年9月に特許が切れたこともあり、急速に普及が進んでいった[2]。現在では、金融分野における情報セキュリティ技術の国際標準や業界標準仕様に規定されているほか、各種ガイドラインで推奨される等RSAは主流の公開鍵暗号として位置づけられている。しかしながら、最近になって、RSAに関する懸念材料が顕現化しつつあり、RSAに代わる公開鍵暗号が求められるようになってきた。

2 RSAに関する特許はRSA Data Security社が保有していた。

図表１　公開鍵暗号（暗号通信）の流れ



(2) 鍵長増加に伴う暗号処理上の制約

まず１つ目の懸念材料は、RSA の鍵長が長くなり過ぎると暗号処理を行ううえで制約となり実装に支障が出てくるということである。

RSA の安全性は、ある程度桁数が大きくなると２つの素数の積（合成数）から元の素数を求めることが困難であるという数学的問題（「素因数分解問題[3]」）に依拠している[4]。仮に素因数分解問題を今よりも効率的に解くアルゴリズムが考案された

3 素因数分解問題は、自然数 N が与えられたとき、$N = P \times Q$ を満たす異なる 2 つの素数を求めるという数学的問題である。例えば、$N = 33$ のとき、$P = 3$、$Q = 11$（または $P = 11$、$Q = 3$）と容易に解くことができるが、N を非常に大きな数（例えば、10 進数で 600 桁程度）とすることにより、P と Q を求めるのは難しくなる。

4 一般的に、公開鍵暗号では「公開鍵から秘密鍵を現実的な時間で求めることが難しい」ことを最低限満たすべき安全性要件としている。これは、少なくとも受信者以外の秘密鍵を持たない第三者は、たとえ暗号文を入手したとしても正しいメッセージを復号できないことを保証するためである。公開鍵暗号では、この安全性を実現するためにある種の「数学的問題」を利用する。対象とする数学的問題とは、その問題の解を計算により求めることは理論上可能であるが、実際に解を求めるには膨大な時間を要する計算が必要となり、事実上その問題を解くのが難しい問題のことである。このような問題を利用して、「ある計算を行うことは簡単」だが「その逆演算を行うのは難しい」という計算の一方向性を実現できれば、上記要件を満たす公開鍵暗号を構成できる。

り、計算機性能の向上に伴いより高速に素因数分解を行うことが可能となると、解読のリスクが高まり、安全性が低下することとなる。さまざまな研究者が、素因数分解問題の難しさに関する評価実験を行っており、この結果を参考に RSA の安全な鍵長の推奨値が考えられている。米国立標準技術研究所（NIST：National Institute of Standards and Technology）等によれば最近までは 1,024 ビット（10 進数で 300 桁程度）あれば安全とされていたが、現在では 2030 年頃までの利用を想定する場合には 2,048 ビット（10 進数で 600 桁程度）の鍵長が推奨されるようになってきている（NIST [2012]）。国内においても、CRYPTREC[5]が電子政府推奨暗号リスト（情報通信研究機構・情報処理推進機構［2012］）に記載されている暗号の安全性に関する監視活動を行っており、例えば 1,024 ビット RSA が解読可能になる時期を 2010〜20 年の間と推定[6]している。こうした研究結果を受けて内閣官房情報セキュリティセンター（NISC：National Information Security Center）では、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA1 及び RSA1024 に係る移行指針」（平成 24 年 10 月 26 日改定）において、各府省庁が保有する情報システムについて 2013 年度末までに 2,048 ビットの RSA に移行するよう求めている。

このように、RSA では計算機性能の向上等に伴う解読リスクの高まりに対応して、鍵長を徐々に長くすることで安全性を確保する運用が採られているが、いずれ従来のハードウエア環境での実装が難しくなる等の支障が出てくるとの指摘がある。特に、IC カードや各種組込み機器等のように、CPU の処理性能やメモリ容量等に制約のある環境において暗号処理を行う際に問題が顕著となる。

(3) 鍵の運用上の留意点

2 つ目の懸念材料は、RSA では、鍵生成を適切に行わなかった場合、公開鍵から秘密鍵を容易に求めることができるということである。具体的には、2 つの素数を秘密鍵、それらの積である合成数を公開鍵としたときに、異なる 2 人の利用者が秘密鍵として同じ素数（少なくとも 1 つ）を使用している場合[7]、両者の秘密鍵を導出できることがわかっている（具体的な導出の仕組みは Box 1 参照。なお、本稿では若干専門的な内容を Box に記述しており、こうした情報が必要ない場合には Box を読み飛ばしても問題ない構成としてある）。

5 CRYPTREC（Cryptography Research and Evaluation Committees）とは、2003 年度までに基盤整備が予定されていたわが国の電子政府で利用可能な暗号アルゴリズムのリスト（電子政府推奨暗号リスト）の公表を主たる目的とし、その候補となる各種暗号アルゴリズムの安全性の評価・監視を行う総務省と経済産業省が主幹のプロジェクトである。

6 CRYPTREC Report 2011（情報通信研究機構・情報処理推進機構）。

7 厳密には、RSA の公開鍵と秘密鍵にはそれぞれ e と d という自然数（ここで、e は $(P-1)\times(Q-1)$ と互いに素な自然数であり、かつ d は $e\times d \equiv 1 \bmod (P-1)\times(Q-1)$ を満たす。ここで、P と Q は素数である）が含まれるが、ここでは説明を簡単にするため省略する。

Box 1　RSA における秘密鍵導出の仕組み

同じ素数 Q を利用して生成された 2 つの公開鍵 $N_1 = P_1 \times Q$ と $N_2 = P_2 \times Q$（P_1, P_2 は素数かつ $P_1 \neq P_2$）が存在する場合、次の手順で P_1, P_2, Q を求めることができる。

Step 1. N_1 と N_2 の最大公約数 Q をユークリッドの互除法[8]を用いて計算する。

Step 2. N_1 と N_2 をそれぞれ Q で割ることにより、残りの素数 P_1, P_2 を求める。

素因数分解問題を解くためには、本来は準指数関数時間の計算量を要するが、上記の方法を利用することにより多項式時間の計算量で解くことができるため、RSA の安全性へ与える影響は大きい（計算量の詳細については、3 節(3)参照）。

通常、異なる利用者が同じ素数を使用する確率は無視できるほど小さいと考えられる[9]。しかし、(a) 鍵生成時に使用する擬似乱数生成器の不具合により生成される素数に偏りが生じる、(b) 管理者のミスや手抜き等により異なる利用者で同じ素数を使い回す等の可能性が指摘されており、この場合脆弱な鍵が発行されやすいという問題が起こる。しかも、一方の素数が同じであったとしても対応する公開鍵は見掛け上異なるため、管理者が公開鍵等を比較しただけでは上記の問題が生じていることを特定できない。近年、レンストラらやヘニンガーらにより、インターネット上で実際に利用されている RSA の公開鍵を多数収集したうえで分析を行った結果、同じ素数を使用している脆弱な鍵が少数ではあるが存在していることが報告されており（Lenstra *et al*. [2012]、Heninger *et al*. [2012]）、鍵生成の適切な運用の重要性が課題となっている。

3. RSA に代わる暗号として注目される楕円曲線暗号

前述のとおり、RSA を今後も利用し続けるにあたっては 2 つの懸念材料が存在するわけであるが、楕円曲線暗号は RSA との比較においてこれらの観点から優位であり、また最近になって学界における安全性の評価も進んできたため、急速に普及が進みつつある。

8 ユークリッドの互除法とは、2 つの自然数の最大公約数を求める手法の 1 つである。例えば、2,240 と 98 の最大公約数を求める場合、次のような手順で求める。① 2,240 を 98 で割って商 22 と余り 84 を得る、② 98 を 84 で割って商 1 と余り 14 を得る、③ 84 を 14 で割って商 6 と余り 0 を得る、④割り切れたときの除数 14 が最大公約数となる。このように、最初に 2 つの数のうち大きい方の数を小さい方の数で割り、もし余りが 0 でなければ除数を余りの数で割る。この計算を余りが 0 になるまで繰り返し、余りが 0 となったときの除数が求める最大公約数となる。この方法を用いることにより、効率よく（多項式時間で）2 つの数の最大公約数を計算できる。

9 例えば、鍵長 2,048 ビットの RSA で用いられる素数の候補は、素数定理（自然数の中に存在する素数の個数を漸近的に示した定理）から 2^{1015} 個程度存在すると考えられている。そのため、2 つの素数を無作為に選択した場合、それらが重複する可能性は無視できるほど小さい。

（楕円曲線暗号がRSAとの比較において優位な点）

① RSAと比較して、約10分の1程度の鍵長で同程度の安全性を保証できるため、ICカードや組込み機器等の計算機性能（計算能力やメモリ等）が制限されている環境での利用に適している（効率面に関する利点）。

② 鍵生成の仕組みがRSAとは本質的に異なるため、脆弱な鍵を発行しやすい等の安全性にかかわる運用上の問題が生じにくい（運用面に関する利点）。

本節では、RSAに代わる公開鍵暗号として今後中心的な役割を担っていく可能性が高いため注目されている楕円曲線暗号について、その実用化動向や概要等を説明した後、RSAと比較したときの同暗号の2つの利点を詳説する。なお、楕円曲線暗号は、「楕円曲線離散対数問題」（後述）と呼ばれる数学的問題を安全性の根拠とする公開鍵暗号の総称であり、複数の具体的な方式が存在する。楕円曲線暗号の機能（用途）別の代表的な暗号アルゴリズムは図表2のとおりである。

（1）楕円曲線暗号の実用化動向

イ．楕円曲線暗号の利用事例等

インターネット・バンキングでは、安全性を確保するために、ブラウザに標準装備されている暗号通信仕様であるSSL/TLS[10]を利用し、利用者の認証や取引情報の機密性保護を行うのが一般的である。そして、楕円曲線暗号は、このSSL/TLSの最新版（TLS 1.2）において利用可能な公開鍵暗号の1つとなっている。その結果、Internet ExploreやGoogle Chrome等の主要なブラウザにおいては、順次楕円曲線暗

図表２　楕円曲線暗号の具体的な方式

暗号機能	方式
守秘（暗号化）	楕円エルガマル暗号（ECElGamal）
鍵共有[11]	楕円ディフィ–ヘルマン鍵共有（ECDH） 楕円メネゼス–チュイ–バンストン鍵共有（ECMQV）
電子署名[12]	楕円DSA[13]署名（ECDSA）

備考：括弧内の名称は各アルゴリズムの略称を表す

10 1994年にSSL（Secure Socket Layer）の仕様が公表されている。その後、機能の追加が行われた仕様がTLS（Transport Layer Security）として、インターネットの技術標準RFC（Request For Comments）において規定されている（Dierks and Rescorla [2008]）。なお、RFCは、インターネットにおける技術上の諸問題を解決することを目的として設置された委員会（IAB：Internet Architecture Board）の下部組織のIETF（International Engineering Task Force）が策定している。

11 鍵共有とは、主に共通鍵暗号において利用する鍵を事前に共有する暗号機能である。

12 電子署名とは、メッセージの一貫性確保や通信相手の認証を実現する暗号機能である。

13 「Digital Signature Algorithm」の略。

号への対応が進められており、利用環境が整備されつつある[14]。

金融分野以外の楕円曲線暗号の身近な利用例としては、デジタル放送における映像コンテンツの著作権保護技術での利用がある。ブルーレイディスクや地上波／BS ／ CS 放送等で配信されるデジタル映像コンテンツの著作権保護技術である AACS（Advanced Access Control System）や、そのコンテンツの正当性確認や機器認証を行う DTCP（Digital Transmission Content Protection）等の技術における利用である。また、オペレーションシステムや IC カード、ハードウエア・セキュリティモジュール等の暗号機能を有する市販製品における実装も進んでおり、3 割弱が楕円曲線暗号をサポートしているとの調査結果が示されている（図表 3 参照）。

ロ．国際標準や業界標準の動向

楕円曲線暗号は、金融業務における公開鍵暗号の鍵管理方法に関する国際標準規格である ISO 11568-4[15]において利用可能な公開鍵暗号として規定されている。また、金融分野における国際標準は、米国内の標準機関である ANSI（American National Standards Institute）配下で米国金融業界内での標準化を行っている ANSI X9 が定める各種標準の影響を受けることが多いが、楕円曲線暗号は ANSI X.9.62 として標準化されている（楕円曲線暗号を規定している主な国際標準および規定されている具体的な暗号アルゴリズムは図表 4 参照）。

国内では、CRYPTREC の電子政府推奨暗号リストに、楕円曲線暗号（ECDH と ECDSA）が取り上げられている。金融機関は、金融情報システムにおけるセキュリティ対策を行う際、「金融機関等コンピュータ・システムの安全対策基準・解説書[16]」（FISC [2009]）を指針としているが、同対策基準においては、利用する暗号アルゴリズム選定の際に、同リストの参照が推奨されている。

さらに、国際クレジットカード・デビットカードの業界標準である「EMV 仕様[17]」

図表 3　市販製品における楕円曲線暗号の採用実績（2012 年 6 月現在）

暗号機能	方式	採用実績（%）
守秘・鍵共有（213 製品）	楕円曲線暗号（ECDH）	23.9
	RSA（RSAES-PKCS#1-v1.5）	47.9
電子署名（206 製品）	楕円曲線暗号（ECDSA）	28.2
	RSA（RSASSA-PKCS#1-v1.5）	80.6

資料：情報通信研究機構・情報処理推進機構 [2012]

14 電子認証サービスを提供しているベリサイン社は、楕円曲線暗号を利用する SSL サーバ証明書の提供を 2013 年上半期に開始することを発表している（日本ベリサイン［2013］）。

15 Banking-Key management (retail) -Part 4（Key management techniques using public key cryptography）。

16 財団法人金融情報システムセンター（FISC：The Center for Financial Industry Information Systems）が公表している金融機関の金融情報システムにおけるセキュリティ対策のガイドラインである。

17 EMV 仕様（EMV Specifications）は、IC カード（端子付き）の利用を前提にクレジットカード・デビットカードのビジネスリスク管理を高度化するため、IC カード内での暗号処理をも含めた仕様として 1996 年に公表された。EMVCo が改訂を含めた同仕様の管理を行っている。ここで、EMVCo とは、国際的なクレ

図表４　国際標準における楕円曲線暗号の規定状況

国際標準の名称	規定されている楕円曲線暗号
ISO 11568	【鍵共有】：ECDH、ECMQV 【電子署名】：ECDSA
ISO/IEC 11770	【鍵共有】：ECDH
ISO/IEC 14888	【電子署名】：ECDSA
ANSI X.9.62	
FIPS 186-3	

資料：ANSI [2005]、NIST [2009]、ISO/IEC [2006, 2007, 2008]。

においても、接触／非接触 IC カードの利用を想定した取引環境の安全性向上を目指し、現在採用されている RSA から楕円曲線暗号への将来的な移行等が指針として示されている（EMVCo [2009]）。

このように、楕円曲線暗号は、既にさまざまな分野で利用されているほか、多くの国際標準や業界標準に規定され、その利用環境の整備も進められている。

(2) 楕円曲線暗号とは

公開鍵暗号の安全性は「公開鍵から秘密鍵を現実的な時間で求めることが難しいこと」に基づいており（詳細は脚注 3 参照）、この仕組みを実現するために数学的問題を利用している。楕円曲線暗号で利用する数学的問題は、「2 つの数 g と t が与えられたとき、g を s 乗した値が t と等しくなるような自然数 s（すなわち、$t = g^s$ を満たす s）を求める問題」（「離散対数問題」と呼ばれる）を、「楕円曲線」上のある条件を満たす点のみで扱う数学的問題（「楕円曲線離散対数問題」と呼ばれる）である。離散対数問題の特殊なケースが楕円曲線離散対数問題といえる。

楕円曲線とは、ある 3 次方程式の形で定義される曲線であり、いわゆる「楕円」とは異なるものである[18]。楕円曲線暗号においては、一般的に、方程式の係数を「素体」[19]または「バイナリ体」[20]（これらは、楕円曲線の概形を定める「定義体」と呼ばれるパラメータである）から選んだ楕円曲線を利用する。そして、それぞれの楕円

ジットカード・ブランドである Europay International、Visa International、MasterCard International により設立された組織であり、前述のとおり EMV 仕様の管理を行っている。2002 年に MasterCard International が Europay International を吸収合併した後、2004 年には JCB が新たに EMVCo の出資者に加わった。

18 もっとも、楕円曲線は楕円の性質を調べる際に導入された方程式であり、楕円曲線と楕円の間には密接な関係がある。

19 素体 F_q は、自然数（0 を含む）の全ての値を素数 q で割った余りにより構成される集合である。例えば $q = 2$ の場合は $F_2 = \{0, 1\}$ となり、$q = 7$ の場合は $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$ となる。この素体においては、集合に含まれる要素同士で四則演算（加算、減算、乗算、除算）が定義できる。

20 バイナリ体 F_{2^n} は、素体 $F_2 = \{0, 1\}$ の要素を係数とする全ての多項式を、n 次の「既約多項式」と呼ばれる多項式（係数は素体 F_2 の要素、n は自然数）で割った余りにより構成される集合である。バイナリ体においても、素体と同様、集合に含まれる要素同士で四則演算（加算、減算、乗算、除算）が定義できる。

曲線における楕円曲線離散対数問題を安全性の根拠として利用する（楕円曲線と楕円曲線離散対数問題の概要[21]については Box 2 参照）。

Box 2　楕円曲線と楕円曲線離散対数問題の概要

【楕円曲線】

前述のとおり、楕円曲線暗号においては、方程式の係数を 2 種類の定義体「素体（Prime Field）F_q（q は素数）」または「バイナリ体（Binary Field）F_{2^n}（n は自然数）」から選んだ楕円曲線を利用する。上記の定義体に基づく楕円曲線はそれぞれ「素体 F_q 上の楕円曲線」、「バイナリ体 F_{2^n} 上の楕円曲線」と呼ばれる。

（a）素体 F_q 上の楕円曲線

3 次方程式 $y^2=x^3+ax+b$（$4a^3+27b^2\neq 0$ かつ $a, b\in F_q$）

で定義される曲線上の点の集合に「無限遠点 $\boldsymbol{O}$」と呼ばれる仮想的な点を加えたもの。

（b）バイナリ体 F_{2^n} 上の楕円曲線

3 次方程式 $y^2+xy=x^3+ax^2+b$（$b\neq 0$ かつ $a, b\in F_{2^n}$）

で定義される曲線上の点の集合に「無限遠点 $\boldsymbol{O}$」と呼ばれる仮想的な点を加えたもの。

【楕円曲線離散対数問題】

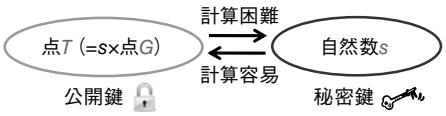
楕円曲線は、「曲線上の点同士で演算（加算）を定義することができる」という特徴を有している。楕円曲線においては、曲線上の点 G を s 回加算する演算（以下、「スカラー倍算」）と自然数 s から点 $T=s\times G$ を求める演算は、演算規則（詳細は補論 1 参照）を利用することにより容易に行うことができる。一方、このスカラー倍算の逆演算（2 点 G と T から、$T=s\times G$ を満たす自然数 s を求める問題）は「楕円曲線離散対数問題」と呼ばれ、自然数 s の桁数（すなわち楕円曲線暗号の鍵長）が大きくなるほど解くのが難しくなる。

【楕円曲線暗号の安全性と楕円曲線離散対数問題】

楕円曲線暗号は、この数学的問題の難しさを安全性の根拠として利用している。つまり、楕円曲線暗号では、自然数 s を秘密鍵、基準点（Base Point）G を秘密鍵 s でスカラー倍算した点 $T=s\times G$ を公開鍵として利用しており（詳細は 4 節(1)参照）、公開鍵から秘密鍵を求めることの難しさは、楕円曲線離散対数問題の難しさと等価になっている（図表 B-1 参照）。

21 ここでは、本稿の議論において最低限必要な定義の紹介に留める。楕円曲線暗号の厳密な定義やその数学的背景の詳細等については、Blake, Seroussi, and Smart [1999] や Hankerson, Menezes, and Vanstone [2004]、伊豆［2012］参照。

図表 B-1　楕円曲線暗号の安全性と楕円曲線離散対数問題の関係



(3) 楕円曲線暗号の効率面に関する利点

楕円曲線暗号は RSA と比較すると、より短い鍵長で同程度の安全性を確保できるため、計算処理等が効率的に行えるという利点がある。これは楕円曲線暗号と RSA では、安全性の根拠とする数学的問題の難しさが異なることに由来する。公開鍵暗号の安全性は、通常、安全性の根拠としている数学的問題を解く手法（以下、「攻撃手法」）の中で最も効率のよい手法を用いた場合に要する計算時間（「計算量」と呼ばれる）により評価される。鍵長を長くしていったときの計算量の増加度合いが激しいと、その数学的問題は現実的な時間で解くことはできない（すなわち、「解くのが困難な問題」）と評価される。鍵長を長くしていったときの計算量増加の程度により、「指数関数時間」、「準指数関数時間」、「多項式時間」という 3 つのカテゴリに分類される。各カテゴリの概要を図表 5 にまとめる。

そして、数学的問題を解くために要する計算量が「指数関数時間」または「準指数関数時間」と評価されるとき、その問題を利用した公開鍵暗号は「計算量的に安全」であると表現される。一般に、「多項式時間」で解ける数学的問題は公開鍵暗号に利用できないが、指数関数時間や準指数関数時間を要する数学的問題は、安全な公開鍵暗号の構成に利用される。

RSA は前述の素因数分解問題と呼ばれる数学的問題を安全性の根拠としているが、

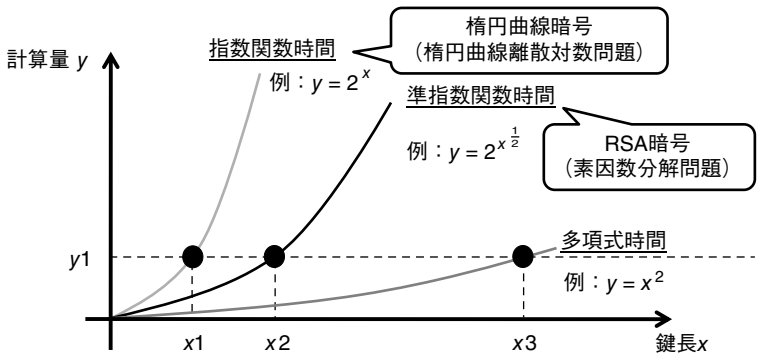
図表 5　計算量の各カテゴリの概要

カテゴリ名	特徴	評価式の例 （鍵長 x に対する計算量 y）
指数関数時間	計算量は、鍵長に比例して指数関数と同じ位急激に増加する。	$y = 2^x$ （鍵長に対して指数関数）
準指数関数時間	指数関数時間と多項式時間の中間に位置する計算量である。	$y = 2^{x^{\frac{1}{2}}}$
多項式時間	計算量は、鍵長に比例して多項式関数と同じ位緩やかに増加する。この増加量は、指数関数時間に比べるとはるかに小さい。	$y = x^n$（$n > 0$ は定数） （鍵長に対して多項式関数）

素因数分解問題には、準指数関数時間で解を導出できる攻撃手法[22]が知られている。一方、楕円曲線暗号は楕円曲線離散対数問題を安全性の根拠としており、楕円曲線離散対数問題は、一部の楕円曲線を除いて指数関数時間で解を導出できる攻撃手法（「ρ（ロー）法」、Pollard [1978]）しか知られていない。つまり、解くのに必要な計算量を同程度（計算量 $y1$、図表 6 参照）に設定した場合、そのときの鍵長は、楕円曲線離散対数問題に依拠した暗号アルゴリズム（鍵長 $x1$）の方が、素因数分解問題に依拠した暗号アルゴリズム（鍵長 $x2$）よりも相対的に短くて済む（$x1 < x2$）。したがって、楕円曲線暗号は RSA と比較して短い鍵長で同程度の安全性を保証することが可能である。

楕円曲線暗号と RSA が同程度の安全性を達成するために必要な鍵長について評価が行われている（図表 7 参照）。NIST [2012] では、例えば、鍵長 2,048 ビットの RSA（10 進数で 600 桁程度）と鍵長 224～255 ビット（10 進数で 67～76 桁程度）の楕円曲線暗号が同等の安全性を有すると評価している。また、Yasuda *et al.* [2012] では、攻撃手法の進歩の状況等を考慮し、精緻化された再評価が行われており、鍵長 2,048 ビットの RSA と鍵長 195～196 ビット（10 進数で 58 桁程度）の楕円曲線暗号が同等の安全性を有していると報告している（図表 7 参照）。

図表 6　計算量の各クラスにおける鍵長と計算量の関係



22 1990 年にレンストラらにより「数体ふるい法」が提案されている（Lenstra *et al.* [1990]）。同手法は、素因数分解の対象となる合成数を 2 種類の異なる集合上の要素を用いて表現し、その表現の差分を利用することにより 2 つの素数 P と Q を求める手法である。数体ふるい法が素因数分解問題を解くのに要する計算量は、合成数のビット長に対して準指数関数時間となる。

図表７　RSA 暗号の鍵長と楕円曲線暗号の鍵長の比較

RSA（ビット）	楕円曲線暗号（ビット）		
	NIST	Yasuda *et al.*	
		素体上の楕円曲線[23]	バイナリ体上の楕円曲線
512		87	87
755		112	112
768		113	113
894		124	124
1,024	160～223	133	134
1,308		153	154
1,413		160	160
1,536		168	168
2,048	224～255	195	196
3,072	256～383		
7,680	384～511		
15,360	512～		

資料：NIST [2012]、Yasuda *et al.* [2012]。

(4) 楕円曲線暗号の運用面における利点

2 節(3)でも述べたように、RSA では、脆弱な鍵が発行されやすいという運用上のリスクが存在するが、楕円曲線暗号ではこうした問題が顕現するリスクが低いという利点がある。RSA では、秘密鍵を生成する際、利用者ごとに異なる 2 つの素数を無作為に選択している。仮に一方の素数が重複しても、2 つの素数の積から作られる公開鍵は異なるものとなるため、重複していることに気づきにくいほか、これをシステム管理者が検証によってみつけようとしても現実的には運用が困難という側面があった。

これに対し、楕円曲線暗号では、秘密鍵を生成する際、利用者ごとに異なる 1 つの自然数を無作為に選択するだけであり、鍵生成の仕組みが本質的に異なることから同種の問題は生じにくい。なお、万が一、異なる利用者間で同じ自然数を選択した場合は対応する公開鍵も同じとなるため、同じ公開鍵を使用する利用者間では互いに秘密鍵がわかることになるが、システム管理者等が鍵発行時に既存の公開鍵との重複を検証することは容易であり、この問題が生じることを事前に回避することが可能といえる。よって、楕円曲線暗号では上記問題の安全性への影響は RSA と比較して相対的に低いと考えられており（Lenstra *et al.* [2012]）、運用時における管理者の管理負担を軽減できる公開鍵暗号と考えられる。

23 詳細は 3 節(2)や Box 2 参照。バイナリ体上の楕円曲線も同様。

4. 楕円曲線暗号の安全性と共通パラメータの選択方法

楕円曲線暗号は、離散対数問題を「楕円曲線」上のある条件を満たす点のみで扱う数学的問題（楕円曲線離散対数問題）に基づいて設計されているわけであるが、この楕円曲線がある条件を満たす場合には、効率のよい攻撃手法が存在することが知られている。したがって、楕円曲線暗号で利用する楕円曲線をどのように選択するかは同暗号の安全性に大きくかかわる事項であり、これは以下で説明する「パラメータ」の指定によって行われる。そこで、本節では、同暗号に対する攻撃手法の研究動向について紹介したうえで、安全なパラメータの選び方について説明する。

(1) 楕円曲線暗号と共通パラメータ

実際に楕円曲線暗号を実装しようとした場合には、利用者個別の設定である「秘密鍵と公開鍵の生成」より前に、具体的にどのパラメータで規定される楕円曲線を利用するのか等を決める全ての利用者共通の「パラメータ設定」(「共通パラメータ」と呼ぶ）を行う必要がある。この設定においては、はじめに暗号で利用する楕円曲線の概形（定義体）を素体またはバイナリ体から1つ選んだ後（詳細は3節(2)参照)、選択されたタイプに対応する楕円曲線の係数を指定することによって具体的な楕円曲線を決定する。次に、この曲線上の1点を基準点として定める等を行い、これらの選択した結果を共通パラメータとして設定した後、全ての利用者に公開する。その後、各利用者は共通パラメータを利用して、自身の秘密鍵と公開鍵を生成し、守秘（暗号化）や電子署名、鍵共有といった暗号機能を実現している（図表8、具体的な生成手順はBox 3参照)。図表8のとおり、楕円曲線暗号においては、自然数 s を秘密鍵とし、基準点 G を s 倍した点 T を公開鍵として利用する。そして、同暗号の安全性の根拠である楕円曲線離散対数問題は、公開鍵 T から秘密鍵 s を求めるという問題であり、秘密鍵 s の長さ（桁数）が長いほど解くのが難しくなる（詳細はBox 2参照)。よって、楕円曲線暗号の安全性の基準である鍵長は、この秘密鍵 s の長さにより定義される。

図表8　共通パラメータと秘密鍵、公開鍵

共通パラメータ	秘密鍵	公開鍵
・楕円曲線の定義体（素体またはバイナリ体） ・楕円曲線の係数 ・曲線上の基準点 G および G を自然数倍すると無限遠点となる最小の自然数[24]	自然数 s （s の桁数が鍵長）	曲線上の点 T （T は G を s 倍した点）

24 この自然数は基準点 G の「位数」と呼ばれる。楕円曲線の演算規則より、楕円曲線上の任意の点 G に対

Box 3　共通パラメータ等の生成手順および具体的なアルゴリズムの例

〈共通パラメータや公開鍵、秘密鍵の生成手順〉

【共通パラメータの設定手順】

Step 1. はじめに自然数 n を選択し、素体 F_q（q は n ビットの素数）またはバイナリ体 F_{2^n} から楕円曲線の定義体を決定する。次に係数 a, b を定義体から選択し、利用する楕円曲線の具体的な方程式を決定する[25]（各定義体における楕円曲線の方程式は 3 節(2) Box 2 参照）。

Step 2. 決定した曲線上から基準点 G を選ぶ（ここで、点 G の位数を u とする）。

Step 3. 定義体の種類、曲線の係数 a, b、基準点 G とその位数 u の組を「共通パラメータ」として全ての利用者に公開する。

【公開鍵と秘密鍵の生成手順】

Step 1. 利用者は、自然数から $s(2/u \leq s \leq u)$ を無作為に選び、s を秘密鍵とする。

Step 2. 共通パラメータを利用して公開鍵 $T = s \times G$ を計算する。公開鍵 T は公開鍵リストを介して全ての利用者に公開し、秘密鍵 s は自身で秘密に管理する。

〈楕円曲線暗号の具体的なアルゴリズムの例〉

以下、守秘機能を実現する代表的な暗号化方式「楕円エルガマル暗号」の暗号化と復号の手順を示す。ここで、ある利用者の秘密鍵を s、公開鍵を T（$T = s \times G$）とし、G は共通パラメータに含まれる基準点とする。

【メッセージの暗号化の手順】

Step 1. 乱数 r を生成し、点 $C_1 = r \times G$ を計算する。

Step 2. 楕円曲線上の点として表されたメッセージ msg に対し、公開鍵 T と乱数 r を用いて点 $C_2 = msg + (r \times T)$ を計算する。

Step 3. 得られた（C_1, C_2）が暗号文となる。

【メッセージの復号の手順】

Step 1. 暗号文（C_1, C_2）と秘密鍵 s を用いて、メッセージ $msg = C_2 - (s \times C_1)$ を計算する。

して、ある自然数 u が存在し、$u \times G = O$ を満たす（「ラグランジュの定理」参照）。なお、楕円曲線暗号の鍵長は、この位数の大きさにも依存する。

25 厳密には、楕円曲線上の「有理点」の個数が素数（バイナリ体の場合には $2 \times$ 素数）となるように係数を選択する。詳細については Blake, Seroussi, and Smart [1999] や Hankerson, Menezes, and Vanstone [2004]、伊豆［2012］参照。

(2) 楕円曲線暗号に対する攻撃手法

楕円曲線暗号の安全性の根拠となっている楕円曲線離散対数問題を解く攻撃手法は、2つのアプローチに分類される。

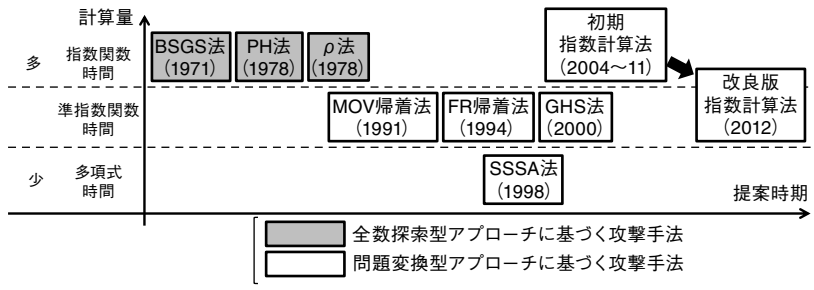
1つは「解候補を1つずつしらみ潰しに探索していく」というアプローチ（「全数探索型アプローチ」と呼ぶ）であり、任意（全て）の共通パラメータを利用する楕円曲線暗号に適用できる。同アプローチでは、最も基本的な全数探索をする手法（「基本的な全数探索法」と呼ぶ）を効率化する方向で研究が進められている。同アプローチにおける主な攻撃手法として、「Pohlig-Hellman（PH）法（Pohlig and Hellman [1978]）」、「BSGS 法（Shanks [1971]）」、ρ 法等が挙げられる。基本的な全数探索法は、攻撃に要する計算量が鍵長に対して指数関数時間であるが、全数探索型アプローチにおいて現在最も効率のよい ρ 法も[26]、攻撃に要する計算量が鍵長に対して指数関数時間に留まっている。したがって、これらの攻撃手法については、鍵長を大きくとるという簡単な対策を行うだけで安全性への影響を回避できる。

もう1つは、共通パラメータが特定の条件を満たすことを前提に、「楕円曲線離散対数問題をより簡単な問題に変換し、変換後の問題を解いた結果から楕円曲線離散対数問題の解を導出する」というアプローチ（「問題変換型アプローチ」と呼ぶ）である。同アプローチに基づく攻撃手法は、適用できる共通パラメータに制約条件があるものの、全数探索型アプローチに基づく攻撃手法よりも効率がよくなる傾向があり、攻撃に要する計算量が多項式時間の攻撃手法（「SSSA 法」、Semaev [1998]、Smart [1999]、Satoh and Araki [1998]）も提案されている。同アプローチにおける主な攻撃手法として、「MOV 帰着法」、「FR 帰着法（Menezes, Vanstone, and Okamoto [1991]、Frey and Rück [1994]）」、「SSSA 法」、「GHS 法（Gaudry, Hess, and Smart [2002]）」、「指数計算法」等が挙げられる。上記の攻撃手法については、それぞれ適用条件が明らかにされているため（詳細は補論2参照）、利用する共通パラメータがこれらの条件を満たさないことを確認することで、安全性への影響を回避できる。

上記の主な攻撃手法について、各手法が楕円曲線離散対数問題を解くために要する計算量と提案された年を軸に整理したものを図表9に示す（各攻撃手法の概要については Box 4 参照）。なお、指数計算法については、最近、これを改良した新たな攻撃手法が発表され、今後の研究の進展の可能性も含め学界で注目されているため、5節でやや詳しく取り上げる。

26 ρ 法は、並列処理により処理を高速化できる。例えば 100 台の計算機を併用すれば 1 台の計算機のみを利用する場合よりも 100 倍程度効率化できる。詳細は Hankerson, Menezes, and Vanstone [2004] 参照。

図表９　楕円曲線暗号に対する主な攻撃手法



Box 4　各攻撃手法の概要

【全数探索型アプローチに基づく主な攻撃手法の具体例】

（a）基本的な全数探索法

基本的な全数探索法は、基準点 G を秘密鍵 s によりスカラー倍すると公開鍵 T（T も楕円曲線上の点）になるという関係を利用する。具体的には、G を 1 倍した値、2 倍した値、…というように計算していき、T と同じ値が得られるまで順番に探索を行う方法である[27]。計算結果が T と等しくなったときの倍数の値が秘密鍵 s である。

（b）ρ 法

ρ 法も、他の全数探索法と同じく、基準点 G を秘密鍵 s によりスカラー倍すると公開鍵 T（も楕円曲線上の点）になるという関係を利用する。具体的には、点 T, G について、こうした関係を踏まえたある条件を満たす関係式を 1 つみつけ出し、この関係式を方程式とみなして解くことで秘密鍵 s を導出する。なお、ρ 法では、一般に、関係式の探索に要する計算量が、攻撃全体に要する計算量の大部分を占める。ρ 法の技術的な概要は以下のとおり。

楕円曲線離散対数問題において与えられる楕円曲線上の 2 点 G, T に対して、以下の関係式

$$c_1 \times G + d_1 \times T = c_2 \times G + d_2 \times T,$$

を満たす G の位数 u 以下の自然数 c_1, d_1, c_2, d_2（ここで、$c_1 \neq c_2, d_1 \neq d_2$）がみつかれば、$G$ と T に関して

$$T = \frac{(c_2 - c_1)}{(d_1 - d_2)} G,$$

27 鍵長が 195 ビットの場合、最大 2^{195} 回の探索が必要となる。なお、現在は 2^{60} 程度の探索は現実的に可能と考えられている。

という関係式を得ることができるため、$(c_2 - c_1)/(d_1 - d_2)$ を計算することにより、問題の解 s を求めることができる。

このような自然数の組 c_1, d_1, c_2, d_2 を探索する最も単純な手法としては、c_1, d_1, c_2, d_2 に対して $R_1 = c_1G + d_1T$ と $R_2 = c_2G + d_2T$ としたとき、$R_1 = R_2$ となるような点の組（衝突ペア）がみつかるまで、しらみ潰しに探索を行うという手法がある。ρ 法とは、この R_1, R_2 という 2 点を選ぶ際に「反復関数」と呼ばれる関数を利用することにより、衝突ペアの探索を上記の単純な手法よりも効率よく行うことを目的とする手法である。同様の考えに基づく方式として、λ 法も知られている（Pollard [1978]）。

【問題変換型アプローチに基づく主な攻撃手法の具体例】

これらの攻撃手法は、楕円曲線上の点を別の集合の要素に変換し、変換した要素が含まれる集合において定義される離散対数問題を解くという手法である。この変換は、楕円曲線が有する数学的特徴を利用して構成される「特殊な関数」を利用して行われる。共通パラメータが満たす条件によってさまざまな種類の関数が存在し、各手法によって利用する関数が異なる。以下、それぞれの攻撃手法が利用する関数および変換後の数学的問題をまとめたものを図表 B-2 に示し、その次に各手法の概要について述べる。各攻撃手法が適用できる共通パラメータの詳細な条件については、補論 2 参照。

（a）MOV 帰着法、FR 帰着法

MOV 帰着法と FR 帰着法は、楕円曲線離散対数問題を「ペアリング」と呼ばれる関数を利用して、定義体の拡大体の乗法群上の離散対数問題に変換し、その後変換された離散対数問題を既存の効率のよい攻撃手法（指数計算法）を用いて解く手法である。特に、ある種の楕円曲線（超特異楕円曲線等）に基づく楕円曲線離散対数問題は、この手法により準指数関数時間の計算量で解くことができる。

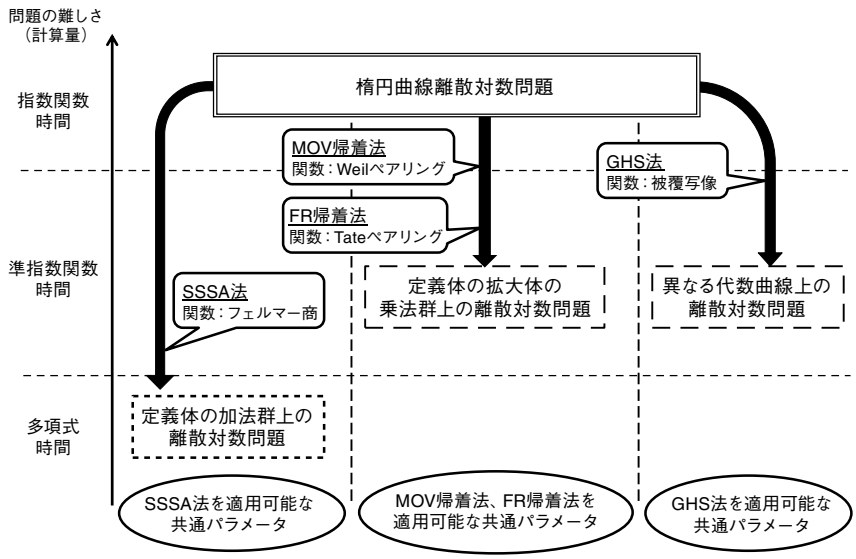
（b）SSSA 法

SSSA 法は、「フェルマー商」と呼ばれる関数を利用し、ある種の楕円曲線（アノマラス（anomalous）楕円曲線）に基づく楕円曲線離散対数問題を、定義体の加法群上の離散対数問題に変換する手法である。加法群上の離散対数問題はユークリッドの互除法を利用して多項式時間で解くことができる。

（c）GHS 法

GHS 法は、バイナリ体を定義体とする楕円曲線に基づく楕円曲線離散対数問題を、「被覆写像（Covering Mapping）」と呼ばれる関数を用いて、異なる代数曲線のヤコビ多様体における離散対数問題に変換し、その変換後の問題を効率のよい攻撃手法（指数計算法）を利用して解く手法である。変換後の代数曲線がある条件（「種数」と呼ばれるパラメータの値が大きい）を満たしているとき、この手法により準指数関数時間の計算量で解くことができる。

図表 B-2　問題変換型アプローチに基づく主な攻撃手法



(3) 安全な共通パラメータの選択方法

楕円曲線暗号を安全に利用するためには、各攻撃手法に耐性を有する共通パラメータ等を選択する必要がある。前述のように各攻撃手法は 2 つのアプローチに大別できるため、各アプローチの観点から安全な共通パラメータを設定するための要件を満たすことが必要となる。

（要件 1）　全数探索型アプローチに基づく任意の攻撃手法でも楕円曲線離散対数問題を容易に解くことができないこと。

全数探索型アプローチにはさまざまな攻撃手法が存在し、それらのうち現在最も効率のよい攻撃手法が ρ 法である（ρ 法の詳細は Box 4 参照）。ρ 法を用いても楕円曲線離散対数問題を現実的な時間で解くことができなければ、他の攻撃手法を用いても現実的な時間で解けないことは自明である。ρ 法を用いて楕円曲線離散対数問題を解く計算機実験の結果、解読可能な鍵長は図表 10 のとおり推移している。最近、移行が進みつつある鍵長 2,048 ビット（10 進数で 600 桁程度）の RSA と同等の安全性（NIST [2012] では 2030 年までの利用を推奨[28]）を確保するためには、Yasuda

28 NIST のガイドラインでは、RSA の鍵長の使用推奨期限について、1,024 ビットは 2010 年まで、2,048 ビットは 2010～30 年まで、3,072 ビット以上は 2030 年以降と示されている（NIST [2012]）。

図表 10　楕円曲線離散対数問題の解読状況（2013 年 3 月時点）

解読時期	1997 年 12 月	1998 年 1 月	1998 年 3 月	2002 年 10 月	2009 年 7 月
解かれた鍵長（単位：ビット）	79	89	97	109	112

資料：Certicom [2009]

et al. [2012] によれば鍵長 195～196 ビット（10 進数で 58 桁程度）が必要となる（前掲図表 7 参照）。

（**要件 2**）　問題変換型アプローチに基づく任意の攻撃手法でも楕円曲線離散対数問題を容易に解くことができないこと。

問題変換型アプローチにも、MOV 帰着法、SSSA 法、指数計算法等のさまざまな攻撃手法が存在する。各攻撃手法を適用可能な共通パラメータの条件は異なるため（詳細は補論 2 参照）、生成した共通パラメータが各攻撃手法の条件を満たさないことを確認する必要がある。

システム管理者が楕円曲線暗号の共通パラメータを生成する際は、まず、暗号の利用用途を勘案して想定する利用期間に則して、要件 1 に基づいて推奨される鍵長を決める。次に、当該鍵長以上を前提とする共通パラメータを無作為に生成したうえで、問題変換型アプローチに基づく各攻撃手法の適用条件に合わないことを確認する（要件 2）。仮に、ある攻撃手法の適用条件に合う場合には、再度共通パラメータを無作為に生成し、同様の確認作業を行うことになる[29]。なお、一度決定した共通パラメータを変更する場合には、システムの全ユーザの秘密鍵と公開鍵を生成し直す必要がある点に注意が必要である。

もっとも、他のシステム等と同じ共通パラメータを利用したとしても安全性の問題はなく、利用できるものがあれば、必ずしもシステム管理者が独自のパラメータ生成を行う必要はない。したがって、NIST や SECG[30]等の信頼できる機関が推奨される共通パラメータを公表しているため、そうした公表情報を参照することが有用である（図表 11、図表 12 参照）。

29 同手法による共通パラメータの生成には非常に時間が掛かるため、より効率的な生成方法が研究されている。例えば、「スクーフ（Schoof）手法」や「虚数乗法の理論に基づく手法」等がある（詳細は Blake, Seroussi, and Smart [1999] や Hankerson, Menezes, and Vanstone [2004] 参照）。

30 SECG（The Standards for Efficient Cryptography Group）とは、楕円曲線暗号の商用的な標準仕様の策定を行っている国際コンソーシアムである。同組織には、情報セキュリティに携わる組織や企業等（NIST、VISA 等）が会員として参加している。

図表 11　NIST と SECG が公表している推奨共通パラメータ

（1）定義体が素体の場合

鍵長（ビット）	NIST	SECG
192	P-192	secp-192k1 secp-192r1
224	P-224	secp-224k1 secp-224r1
256	P-256	secp-256k1 secp-256r1
384	P-384	secp-384r1
521	P-521	secp-521r1

（2）定義体がバイナリ体の場合

鍵長（ビット）	NIST	SECG
163	K-163 B-163	sect-163k1 sect-163r1 sect-163r2
223	K-223 B-223	sect-223k1 sect-223r1
239		sect-239k1
283	K-283 B-283	sect-283k1 sect-283r1
409	K-409 B-409	sect-409k1 sect-409r1
571	K-571 B-571	sect-571k1 sect-571r1

備考：NIST の共通パラメータでは、定義体が素体の場合を「P」、バイナリ体の場合を「K」または「B」と表記している。SECG の共通パラメータでは、定義体が素体の場合を「secp」、バイナリ体の場合を「sect」と表記している。
資料：Certicom [2010]、NIST [2009]。

図表 12　NIST の推奨公開パラメータ（P-192）の具体例

定義体の種類（素体）	q = 6277101735386680763835789423207666416083908700390324961279
曲線の係数	$a = -3$ b = 64210519 e59c80e7 0fa7e9ab 72243049 feb8deec c146b9b1
基準点 G の座標 (G_x, G_y)	G_x = 188da80e b03090f6 7cbf20eb 43a18800 f4ff0afd 82ff1012 G_y = 07192b95 ffc8da78 631011ed 6b24cdd5 73f977a1 1e794811
基準点 G の位数	u = 6277101735386680763835789423176059013767194773182842284081

備考：q, u は 10 進数表記、a, b, G_x, G_y は 16 進数表記となっている。
資料：NIST [2009]

5. 攻撃手法に関する最新の研究動向と安全性への影響

本節では、最近、学界で注目されている指数計算法を楕円曲線暗号の攻撃に適用する新たな研究の動向について紹介したうえで、その安全性評価に与える影響等について考察する。

(1) 指数計算法を巡る研究の進展

イ．指数計算法に関する最新動向

離散対数問題に対する攻撃手法である指数計算法を、楕円曲線離散対数問題に適用する研究が進展している。指数計算法を楕円曲線離散対数問題に適用する基本アイデアは知られていたが、途中の処理を効率的に実施できない（指数関数時間を要する）ため、基本アイデアのままでは全数探索法よりも効率が劣るという状況であった。もっとも近年、これらの課題を解決したうえで指数計算法を楕円曲線離散対数問題に適用する攻撃手法（以下、「改良版指数計算法」と呼ぶ）が示された。同攻撃手法は、問題変換型アプローチの 1 つであるが、その適用条件が既存の攻撃手法（MOV 帰着法、SSSA 法等）よりも緩く、また、攻撃に要する計算量が準指数関数時間になる等、効率も改善されているとの見積り結果が示されている。ただし、攻撃に要する計算量を見積る際に、厳密な検証が困難な仮定を前提としているため、同仮定の正当性について学界で議論が行われている状況である。楕円曲線暗号を利用する金融機関等の立場からは、同仮定の正当性が確認可能という安全サイドに立った状況を想定し、予め同攻撃の影響を分析しておくことが有用といえる。

以下では、指数計算法の概要、改良版指数計算法の概要および同攻撃手法を巡る議論について説明する。

ロ．指数計算法の概要

指数計算法は、現在、ある種の離散対数問題に対する最も効率のよい攻撃手法である。同手法は、「直接解くことが困難な問題」（ここでは「離散対数問題」に相当）を、解法が知られている等「相対的に扱いやすい問題」に変換して解き、その結果から元の問題の解を導くというアイデアに基づいている[31]（Kraitchik [1922]、Adleman [1979]）。

楕円曲線離散対数問題に対しても、離散対数問題同様に指数計算法を適用し、「点の分解問題（詳細は Box 5 参照）」に変換して解くという基本アイデアは以前から知られているものの、点の分解問題を効率よく解くことができず、全数探索法よりも効率が劣るという状況であった（楕円曲線離散対数問題に指数計算法を適用する基本アイデアは Box 5 参照）。

31 なお、同手法では、変換後の問題の解の導出に成功する確率を高めようとすると、解の導出に要する計算量が増加するというトレードオフの関係がある。ある種の離散対数問題（有限体の乗法群上の離散対数問題）については、解の導出の成功確率と解の導出に要する計算量の最適なバランスが知られており、その場合の計算量は準指数関数時間となる（詳細は、岡本・太田［1995］や宇根・岡本［1999］参照）。

Box 5　楕円曲線離散対数問題に指数計算法を適用する基本アイデア

【楕円曲線離散対数問題に指数計算法を適用する基本アイデア】

楕円曲線上の 2 点 G, T に対して、$T = s \times G$ を満たす自然数 s を求めるという楕円曲線離散対数問題を想定する。点 T は、楕円曲線上から適切な方法により選ばれた複数個の点 $G_1, G_2, \cdots, G_m$（これらの点の集合は「因子基底」と呼ばれる）により、以下のように表現できるとする。

$$T = G_1 + G_2 + \cdots + G_m, \tag{1}$$

また、因子基底に含まれる各点 G_i について、

$$G_i = s_i \times G, \tag{2}$$

という関係を満たす s_i $(1 \leq i \leq m)$ が既知であるとする。$s_1, s_2, \ldots, s_m$ は、まとめて「離散対数表」と呼ばれる。このとき、(1) 式、 (2) 式から、次式

$$\begin{aligned} T &= s_1 \times G + s_2 \times G + \cdots + s_m \times G \\ &= (s_1 + s_2 + \cdots + s_m) \times G, \end{aligned} \tag{3}$$

が得られる。したがって、離散対数表を参照し、解 s $(= s_1 + s_2 + \cdots + s_m)$ を導出できる。

上記の基本アイデアでは、(1) 式や離散対数表が既知であると仮定したが、実際にはこれらも求める必要がある。そのため、まず、①適切な因子基底 $\{G_1, G_2, \cdots, G_m\}$ を選択し（(1) 式の導出)、②離散対数表を求めるために必要な関係式を探索する。具体的には、因子基底と楕円曲線上の任意の点に関する以下の関係式（m 個）を探索する問題（点の分解問題）を解く。

関係式：

$$R_i = c_{i.1} \times G_1 + c_{i.2} \times G_2 + \cdots + c_{i.m} \times G_m \text{（}c_{i.j}\text{は定義体の要素}, 1 \leq i, j \leq m\text{）},$$

を求める。その後、③探索により得られた関係式を連立方程式とみなして解くと、多項式時間で離散対数表が得られ、元の問題の解 s を導出することができる。一般に、因子基底の要素数 m（初期パラメータ）が多いほど、関係式の探索に成功する確率が高くなる反面、有効な関係式か否かの検証（変換後の問題の解の導出）に要する計算量が増加するというトレードオフの関係がある。

ハ. 改良版指数計算法の提案と同攻撃手法を巡る議論

近年、いくつかの指数計算法の効率化を図る方法が考案されており、特に昨年、ある仮定のもと、準指数関数時間で解を導出する手法が新たに提案された。以下では、

そうした研究の概要について取り上げる。

指数計算法により「楕円曲線離散対数問題」を変換した「点の分解問題」について、近年、効率的な解法が提案されている。まず、2004年にセマーエフが「点の分解問題」をさらに「複数の多項式による連立方程式を解く問題」というより簡単な問題に変換する方法を提案した（Semaev [2004]）。その後、ゴードリーとディエムが、セマーエフの変換方法をベースに、楕円曲線離散対数問題を指数計算法により解く攻撃の枠組み（以下、「初期指数計算法」）を完成させた（Gaudry [2009]、Diem [2011a, b]）。しかし、同枠組みは、具体的にソフトウエア等で実装することが難しいという課題があった。そこで、2012年にフォジェールらが、「多数の多項式を解く問題」を解法が十分に確立した問題へ再度変換することで、具体的に実装可能な新たな枠組み（改良版指数計算法）を提案した（Faugére *et al*. [2012]）。同攻撃手法は、「バイナリ体[32]を定義体とする楕円曲線離散対数問題」に適用可能であり、既存の攻撃手法（MOV帰着法、SSSA法等）よりも適用範囲が広いという特徴を有する（改良版指数計算法に関する研究の概要はBox 6参照）。

改良版指数計算法に要する計算量については、提案者フォジェールの共同研究者であるペティットらが、準指数関数時間になるとの評価結果を示している（Petit and Quisquater [2012]）。しかしながら、同評価結果は、その正当性を検証することが困難な仮定[33]を前提としているため、学界では、同評価結果の信頼性について意見が割れているのが実情である。同仮定の正当性が確認された場合、改良版指数計算法は、適用範囲が広い準指数関数時間の攻撃となるため、学術的には非常に大きな研究成果といえる。

Box 6　改良版指数計算法に至るまでの研究の概要

【改良版指数計算法に至るまでの研究動向】

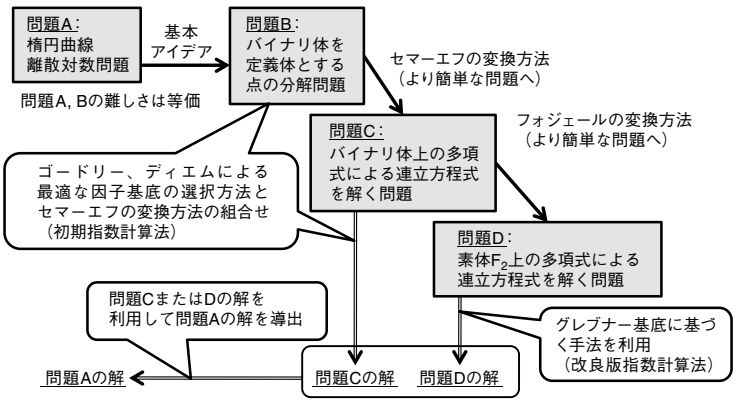
・セマーエフは、「バイナリ体を定義体とする点の分解問題（問題B）」を、「バイナリ体上の多数の多項式による連立方程式を解く問題（問題C）」に変換する方法を示した。問題Bにおける楕円曲線上の点同士（点 A, B）の演算（$A + B$ 等）よりも、問題Cにおける定義体上の要素（$a, b \in \mathrm{F}_{2^n}$）同士の演算（$a+b$ 等）の方が高速に実施可能であるため、問題Cの方が相対的に簡単な問題となる。

32 ゴードリーやディエムの提案は、厳密には、バイナリ体だけでなく、その他の「拡大体」（標数2以外の有限体）を定義体とする楕円曲線にも適用できる。バイナリ体は、拡大体の特殊なケース（標数2のケース）であり、バイナリ体に限定して議論しても、改良版指数計算法の議論には影響を与えないため、本稿では、バイナリ体に限定して議論する。

33 こうした仮定は、「ヒューリスティックな仮定」と呼ばれており、限られた範囲においては数値実験により仮定の正当性が確認されているものの、一般的にはその正当性の検証が困難であるため同仮定の正当性が数学的に示されていない。

・ゴードリーとディエムは、変換後の問題 C の解を効率よく導出できるように、最適な因子基底の選択方法を示した。同選択方法は、定義体が拡大体（バイナリ体を一般化した集合）の場合に適用可能である。また、ゴードリーとディエムは、問題 C への変換方法と最適な因子基底の選択方法を組み合わせることで、楕円曲線離散対数問題に指数計算法を適用する攻撃の枠組み（初期指数計算法）も示した。
・フォジェールは、「バイナリ体上の多数の多項式による連立方程式を解く問題（問題 C）」を「素体 F_2 上の多項式による連立方程式を解く問題（問題 D）」に変換する方法を示した[34]。同変換は、「バイナリ体を定義体とする点の分解問題（問題 B）」を問題 C に変換した場合に、問題 C に含まれる多変数多項式が有する特徴（多変数斉次構造[35]）を利用している。問題 D を効率よく解く手法（「グレブナー基底に基づく手法[36]」）を利用することで、フォジェールは点の分解問題を効率よく行う枠組み（改良版指数計算法）を示した。各研究者の成果は図表 B-3 のようにまとめられる。

図表 B-3　改良版指数計算法に関する研究動向



(2) 改良版指数計算法が安全性評価に与える影響と留意点

本項では、改良版指数計算法について、安全サイドに立ち、同手法が利用する仮定の正当性が確認されている前提で、楕円曲線暗号の安全性に与える影響について考察する。

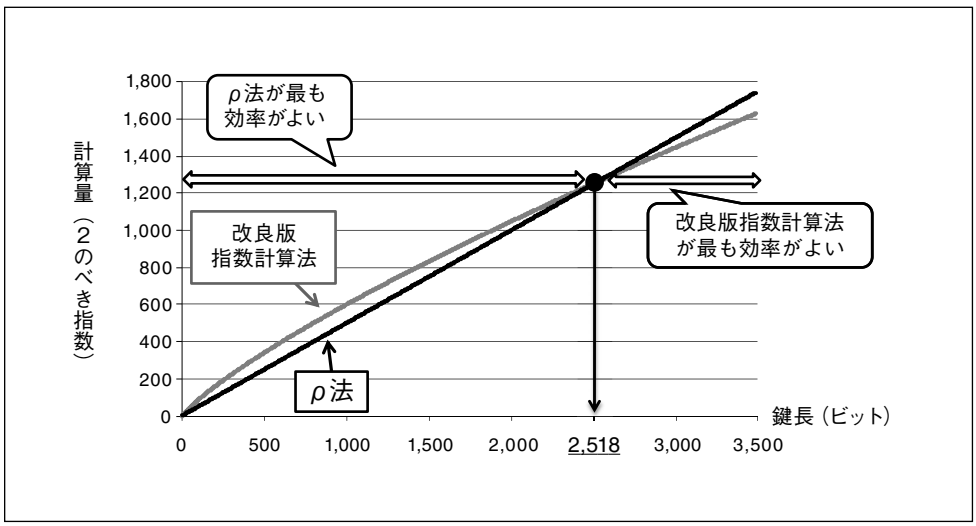
34 この変換には、バイナリ体 F_{2^n} 上の多項式を素体 F_2 上の多項式に展開する「Weil Descent」と呼ばれる処理が使われている。
35 多変数多項式における各項の次数が等しいという特徴。
36 グレブナー基底は、共通解を持つ多項式集合の中で最も解きやすい形をしている多項式集合である。与えられた多項式系を解くとき、事前に対応するグレブナー基底を求めることにより、解を効率よく求めることができる。このグレブナー基底を求める効率的な手法として、F4 や F5 が挙げられる（Faugére [1999, 2002]）。

同攻撃手法は、前述したように適用条件が「バイナリ体を定義体とする共通パラメータを利用していること」のみであり、適用範囲が広いという特徴を有する。したがって、同攻撃への根本的な対策は、バイナリ体を定義体とする共通パラメータを利用せず、素体が定義体のパラメータを設定することであり、楕円曲線暗号のパラメータを適宜更新できる仕組みが存在する場合や、新たに楕円曲線暗号をシステムに実装する場合には有効と考えられる。しかしながら、実際に当該パラメータを利用した楕円曲線暗号を実装・運用しているシステムの場合は、対策の要非を判断する必要があるため、以下で安全性に対する改良版指数計算法の影響について評価する。

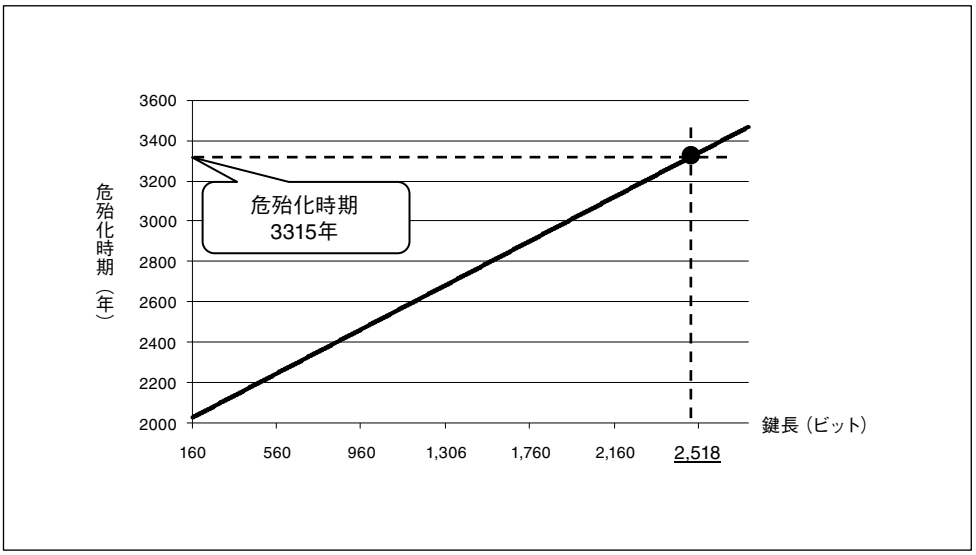
フォジェール（Faugére *et al.* [2012]）らは、鍵長が 2,000 ビット（10 進数で 600 桁程度）以上の楕円曲線暗号に対しては、改良版指数計算法は ρ 法よりも効率がよい（すなわち計算量が少ない）攻撃手法であると主張している。同文献に基づき、2 つの攻撃手法の計算量を比較すると、2,000 ビットまでは ρ 法の計算量の方が明らかに少ない。しかし、鍵長が 2,000 ビットを超えると徐々に計算量の差が小さくなり、そして 2,518 ビット付近で計算量の大小関係が逆転する。それ以上の鍵長では改良版指数計算法の方が計算量は少なくなり、ρ 法よりも効率のよい攻撃法になることがわかる（図表 13 参照）。

したがって、鍵長が 2,000 ビット以下のときは ρ 法への耐性にのみ留意すればよい。NIST や SECG の推奨共通パラメータでは、ρ 法への耐性が考慮されているほか、同パラメータの鍵長は 160～570 ビット（10 進数で 49～172 桁程度）となっているため、同パラメータを利用している間は改良版指数計算法の影響を受けない。また、鍵長 2,000 ビット以上の楕円曲線暗号は、ρ 法を用いると西暦 3000 年頃（予測では、約 3315 年）に解読可能となるレベルであり（図表 14 参照）、改良版指数計算

図表 13　指数計算法と ρ 法の計算量比較

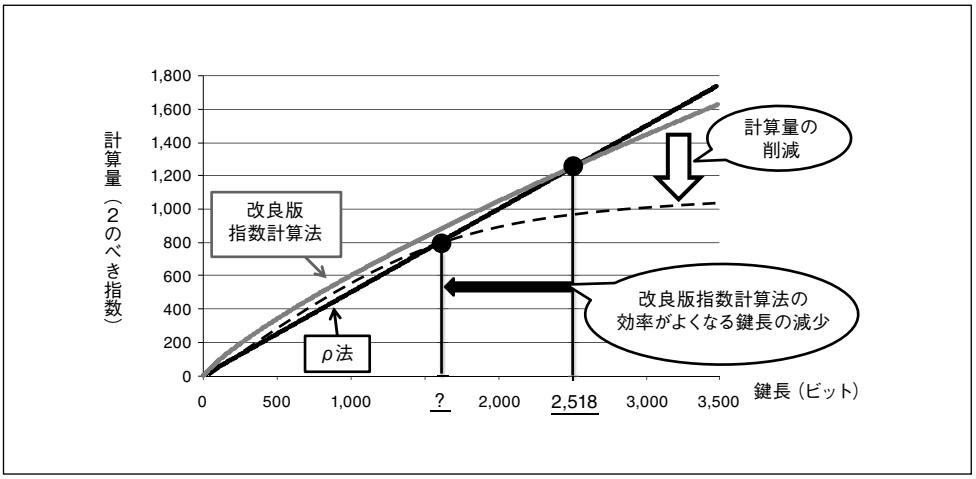


図表 14　楕円曲線暗号における鍵長の解読可能時期の予測



備考：解読時期の予測については、森川らにより提案された予測手法を利用（森川・下山［2011］）。

図表 15　指数計算法の今後の動向



法は現時点では直ちに影響があるわけではない。

以上の分析結果から、NIST や SECG の公表している情報等を参照したうえで共通パラメータを適切に設定することが、安全な楕円曲線暗号の利用において有効であり、RSA より短い鍵長で同程度の安全性を確保できるといえる。ただし、今後の研究の進展により、指数計算法が ρ 法より効率がよくなる鍵長は短くなっていくことが予想されるため（図表 15 参照）、これらの研究動向について、今後も引き続き注視していく必要がある。

6. おわりに

本稿では、RSA に代わる公開鍵暗号として注目されている楕円曲線暗号の概要および研究動向等について紹介した。楕円曲線暗号は RSA と比較して短い鍵長で同程度の安全性を保証できる利点を有しているほか、管理者のミス等により脆弱な鍵が発行されにくいという運用上の利点もあることから、計算能力やメモリ等が制限された計算機環境（IC カードや組込み機器）における利用に適しており、既にデジタルテレビにおける映像コンテンツ保護技術等で利用され始めている。さらに、IC カードを前提としたクレジットカード等の業界標準である EMV 仕様や、インターネットの暗号通信プロトコルである SSL 等、金融分野と関連の深い技術において、楕円曲線暗号の利用に向けた動きが進んでいる。現時点では、楕円曲線以外には RSA に代わる候補となる公開鍵暗号は存在しないため、上記のように楕円曲線暗号への移行が進み、近い将来公開鍵暗号の主流となると考えられる。また、カナダの Certicom 社が保有する楕円曲線暗号に関するいくつかの特許が、2015～20 年代にかけて期限切れを迎えるため、これをきっかけに普及がさらに加速することも予想される。

同暗号に関しては、これまでさまざまな攻撃手法が提案されているが、これらの手法の安全性への影響については厳密に評価が行われており、NIST や SECG が公表している推奨共通パラメータを利用することにより、安全な楕円曲線暗号を実現できることが明らかにされている。よって、今後、金融機関等で楕円曲線暗号を利用する場合には、これらの推奨共通パラメータを利用することが望ましい。

一方、楕円曲線暗号や RSA が安全性の根拠としている計算困難な数学的問題は、「量子コンピュータ」が実現された場合、現実的な時間で効率よく解かれることが知られている（Shor [1994]）。したがって、量子コンピュータの研究動向やその実現に向けたスケジュール等を注視する必要がある[37]。また、量子コンピュータが実現されたとしても、解読できないと考えられている「量子公開鍵暗号」や「格子暗号」等のポスト量子暗号と呼ばれる暗号アルゴリズムについても、その実用化に向けた研究が盛んに進められている。これらの内容に関しても、今後の動向に着目することは有用であろう。

37 ただし、量子コンピュータ実現のためには、多くの技術的課題を解決する必要があり、20～30 年後という近い将来に実現される可能性は極めて低いと考えられている。

参考文献

伊豆哲也、「楕円曲線暗号入門」、2012 年
宇根正志・岡本達明、「公開鍵暗号の理論研究における最近の動向」、『金融研究』第 18 巻第 2 号、日本銀行金融研究所、1999 年、195～251 頁
岡本龍明・太田和夫、『暗号・ゼロ知識証明・数論』、共立出版、1995 年
財団法人金融情報システムセンター（FISC）、『金融機関等コンピュータ・システムの安全対策基準・解説書（第 7 版追補改訂）』、FISC、2009 年
情報通信研究機構・情報処理推進機構、「CRYPTREC 暗号リスト（案）に係る意見募集について」、2012 年
日本ベリサイン、「日本ベリサインのウェブサイトセキュリティソリューションがインターネットでの信頼性とセキュリティをさらに強化」、日本ベリサイン、2013 年（https://www.verisign.co.jp/press/2013/pr_20130214.html）
武藤健一郎、「SSL における暗号危殆化サンプル調査の報告」、PKI Day 2011、2011 年
森川郁也・下山武司、「暗号等価安全性」、『電子情報通信学会論文誌』、94 (11)、2011 年
Adleman, Leonald, “A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography,” Proceedings of Foundations of Computer Science (FOCS), 1979, pp. 55–60.
American National Standards Institute (ANSI), “X9.62: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),” ANSI, 2005.
Blake, Ian, Gadiel Seroussi, and Nigel Smart, “Elliptic Curves in Cryptography,” London Mathematical Society Letcure Note Series, No. 256, Cambridge University Press, 1999.
Certicom, “The Certicom ECC Challenge,” Certicom, 2009. (http://www.certicom.com/index.php/the-certicom-ecc-challenge)
———, “SEC 2: Recommended Elliptic Curve Domain Parameters version 2.0,” Standards for Efficient Cryptography Group (SECG), 2010.
Diem, Claus, “On the Discrete Logarithm Problem in Elliptic Curves,” *Compositio Mathematica*, 147, 2011a, pp. 75–104.
———, “On the Discrete Logarithm Problem in Elliptic Curves II,” Presented at ECC 2011, 2011b.
Dierks, Tim, and Eric Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” Request for Comments (RFC), no. 5246, 2008.
EMVCo, “EMVCo Common Contactless Terminal Roadmap,” General Bulletin, no. 43, EMVCo, 2009.
Faugére, Jean-Charles, “A New Efficient Algorithm for Computing Gröbner Bases (f_4),” *Journal of Pure and Applied Algebra*, 139 (1-3), 1999, pp. 61–88.

———, "A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (f_5)," Proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC), Association for Computing Machinery (ACM), 2002, pp. 75–83.

———, Ludovic Perret, Christophe Oetit, and Guénaël Renault, "Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields," Proceedings of Eurocrypt, LNCS 7237, Springer-Verlag, 2012, pp. 27–44.

Frey, Gerhard, and Hans-Georg Rück, "A Remark Concerning m-divisiblity and the Discrete Logarithm in the Divisor Class Group of Curves," *Mathematics of Computation*, 62 (206), 1994, pp. 865–874.

Gaudry, Pierrick, "Index Calculus for Abelian Varieties of Small Dimension and the Elliptic Curve Discrete Logarithm Problem," *Journal of Symbolic Computation*, 44 (12), 2009, pp. 1690–1702.

———, Florian Hess, and Nigel Smart, "Constructive and Destructive Facets of Weil Descent on Elliptic Curves," *Journal of Cryptology*, no. 15, 2002, pp. 19–46.

Hankerson, Darrel, Alfred Menezes, and Scott Vanstone, "Guide to Elliptic Curve Cryptography," Springer-Verlag, 2004.

Heninger, Nadia, Zakir Durumeric, Eric Wustrow, and Alex Halderman, "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices," Proceedings of USENIX Security Symposium, 2012.

International Organization for Standarization (ISO), and International Electrotechnical Commission (IEC), "ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms," ISO and IEC, 2006.

———, and ———, "ISO/IEC 11568-4: Banking-Key management (retail) – Part 4: Key management techniques using public key cryptography," ISO and IEC, 2007.

———, and ———, "ISO/IEC 11770-3: Information technology –Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques," ISO and IEC, 2008.

Koblitz, Neal, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, 48, 1987, pp. 203–209.

Kraitchik, Maurice, "Théorie des nombres," Gauthier-Villars, 1922.

Lenstra, Arjen K., James Hughes, Maxime Augier, Joppe Bos, Thorsten Kleinjung, and Christophe Wachter, "Ron was Wrong, Whit is Right," International Association for Cryptologic Research (IACR) Cryptology ePrint Archive, no. 64, 2012.

———, Hendrik W. Lenstra, Jr., Mark S. Manasse, and John M. Pollard, "The Number Field Sieve," Proceedings of ACM Annual Symposium on Theory of Computing, 1990, pp. 564–572.

Menezes, Alfred, Scott Vanstone, and Tatsuaki Okamoto, "Reducing Elliptic Curve

Logarithms to Logarithms in a Finite Field," Proceedings of Symposium on Theory of Computing (STOC), 1991, pp. 80–89.

Miller, Victor, "Use of Elliptic Curves in Cryptography," Proceedings of Crypto, LNCS 218, Springer-Varlag, 1985, pp. 417–426.

National Institute of Standards and Technology (NIST), "The Digital Signature Standard (DSS)," Federal Information Processing Standardization (FIPS) 186-3, NIST, 2009.

————, "Recommendation on Key Management," Special Publication (SP) 800-57, 2012.

Petit, Christophe, and Juean-Jacques Quisquater, "On Polynomial Systems Arising from a Weil Descent," Proceedings of Asiacrypt, LNCS 7658, Springer-Verlag, 2012, pp. 451–466.I

Pohlig, Stephen, and Margin Hellman, "An Improved Algorithm for Computing Logarithms over GF (p) and Its Cryptographic Significance (Correspondance)," IEEE Transactions of Information Theory, 24 (1), 1978, pp .106–110.

Pollard, John. M., "Monte Carlo Method for Index Computation (mod p)," *Mathematics of Computation*, 32 (143), 1978, pp. 918–924.

Rivest, Ronald, Adi Shamir, and Leonard Adleman, "A Method of Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, 21, 1978, pp. 120–126.

Satoh, Takakazu, and Kiyomichi Araki, "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves," *Commentarii Mathematici, Universitatis Sancti Pauli*, 47, 1998, pp. 81–92.

Semaev, Igor, "Evaluation of Discrete Logarithms in a Group of p-torsion Points of an Elliptic Curve in Characteristic p," *Mathematics of Computation*, 67 (221), 1998, pp. 353–356.

————, "Summation Polynomials and the Discrete Logarithm Problem on Elliptic Curves," IACR Cryptology ePrint Archive, no. 31, 2004.

Shanks, Daniel, "Class Number, a Theory of Factorization, and Genera," Proceeding of Symposia in Pure Mathematics, 20, 1971, pp. 415–440.

Shor, Peter, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proceedings of Foundations of Computer Science (FOCS), 1994, pp. 124–134.

Silverman, Joseph, *The Arithmetic of Elliptic Curves (2nd Edition)*, Graduate Text in Mathematics (GTM) 106, Springer-Verlag, 2009.

Smart, Nigel, "The Discrete Logarithm on Elliptic Curves of Trace One," *Journal of Cryptology*, 12 (3), 1999, pp. 193–196.

Yasuda, Masaya, Takeshi Shimoyama, Tetsuya Izu, and Jun Kogure, "On the Strength Comparison of ECC and RSA," Proceedings of Security and Cryptography for Networks (SCN), 2012.

※各 URL は 2013 年 4 月 30 日に確認

補論 1. 楕円曲線上の有理点同士の演算規則

ここでは、素体 F_q を定義体とする楕円曲線上で点同士の加算を行う際に利用する演算規則を示す。同様の演算規則は、バイナリ体 F_{2^n} を定義体とする楕円曲線においても定義されているが、本稿では説明は省略する。詳細については Silverman [2009] や Hankerson, Menezes, and Vanstone [2004] 参照。

(a) 楕円曲線上の 2 点 $A = (x_1, y_1)$、$B = (x_2, y_2)$（A、$B \neq \boldsymbol{O}$）に対して、

・$x_1 = x_2$ かつ $y_1 = y_2 = 0$ のとき、$A + B = \boldsymbol{O}$

・それ以外のとき

$$A + B = (x_3, y_3)$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda x_3 - \mu$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & (x_1 \neq x_2 \text{のとき}) \\ \frac{3x_1^2 + a}{2y_1} & (x_1 = x_2 \text{のとき}) \end{cases}$$

$$\mu = \begin{cases} \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} & (x_1 \neq x_2 \text{のとき}) \\ \frac{-x_1^3 + a x_1 + 2b}{2y_1} & (x_1 = x_2 \text{のとき}) \end{cases}.$$

(b) 楕円曲線上の任意の点 A と無限遠点 $\boldsymbol{O}$ に対して、

$$A + \boldsymbol{O} = \boldsymbol{O} + A = A.$$

補論２．楕円曲線暗号に対する攻撃手法の適用条件および計算量

楕円曲線暗号に対する各攻撃手法について、攻撃手法を適用可能な共通パラメータの条件と攻撃に要する計算量を図表 A-1 にまとめる。

図表 A-1　楕円曲線暗号に対する攻撃手法の適用条件および計算量

攻撃手法の名称	適用可能な共通パラメータの条件	攻撃に要する計算量
全数探索法 Pohlig-Hellman 法 衝突探索法 　Baby-Step Giant-Step 法 　ρ 法	条件なし （任意の共通パラメータに適用可能）	指数関数時間
MOV 帰着法 FR 帰着法	・定義体が素体 F_q の場合： $q^B = 1 \bmod u$ を満たす最小の自然数 B が小さい（$1 \leq B \leq 100$）。 ・定義体がバイナリ体 F_{2^n} の場合： $2^B = 1 \bmod u$ を満たす最小の自然数 B が小さい（$1 \leq B \leq 100n$）。	準指数関数時間
SSSA 法	・定義体が素体 F_q の場合： 点 G の位数 u について、$u = q$ を満たす。 ・定義体がバイナリ体 F_{2^n} の場合： 点 G の位数 u について、$u = 2^n$ を満たす。	多項式時間
GHS 法	定義体がバイナリ体 F_{2^n}（ここで、n は合成数）かつ変換後の代数曲線の「種数」と呼ばれるパラメータが大きい。	準指数関数時間
初期指数計算法	定義体が拡大体（バイナリ体 F_{2^n} 含む）。	指数関数時間
改良版指数計算法	定義体がバイナリ体 F_{2^n} である。	ヒューリスティックな仮定のもとで準指数関数時間

備考：図表中の各記号の定義は、3 節(2)の Box 2 および脚注 21、22 参照。