

楕円曲線暗号が支える安全・安心なデジタル社会



夢はバラ色

宮 地 充 子*

Elliptic Curve Cryptography Supporting a Safe and Secure Digital Society

Key Words: Elliptic Curve Cryptography, safe, secure, digital society

1. はじめに

デジタル社会が急速に進展している。デジタル社会とは、アナログの「情報」や「モノ」、「サービス」をデータ化し、デジタルとして活用する社会を指す。例えば、郵送などのアナログ的な送付方法が、電子メールによるデータ送付に置き換わるといった身近な事例から、紙媒体の業務プロセスの自動化、大学の各種事務手続きの全面的な電子化、さらにクラウドやソーシャルメディアを活用した新しいサービスの提供に至るまで、デジタル化の波は社会のあらゆる側面に広がっている。デジタル社会の最大の利点は、コストや時間の大幅な削減にある。さらに、デジタル化によって得られる「データ」は、AIなどの先端技術を用いた社会課題の解決に不可欠な資源である。必要な情報やサービスを、必要な人が、必要なときに受けられること、すなわち社会活動の持続可能性を実現する上でも、デジタル社会は重要な基盤となっている。このように、デジタル化は社会の効率化のみならず、持続可能な社会づくりにも寄与する不可欠な変革である。

一方で、デジタル化された「データ」や「サービス」は、サイバー攻撃やプライバシー漏洩といった新たなリスクを生み出している。こうしたデジタル特有の課題を克服し、安全・安心な社会を実現するために不可欠なのが情報セキュリティ技術である。セキュリティ技術は、情報の秘匿性、完全性、可用性を

確保することで、デジタル社会を支える基盤技術である。特に今日では、経済・教育・医療・生活など、あらゆる分野の活動がデジタル化されており、セキュリティ技術は社会活動を継続するための不可欠な要素となっている。さらに、情報セキュリティ技術は社会を守るだけではなく、新しい価値や仕組みを創造する技術でもある。その代表例がブロックチェーン技術である。ブロックチェーンは、取引や記録を特定の管理者ではなく、ネットワーク上の多数の参加者が共同で管理する仕組みであり、「データの信頼性を保証する技術」として、医療・物流・行政など多様な分野への応用が進んでいる。このブロックチェーンこそ、情報セキュリティ技術が生み出した新たな社会の仕組みの好例といえる。

本稿では、2024年秋の紫綬褒章受章の契機となった、私の情報セキュリティ分野における研究成果について紹介したい。

2. 楕円曲線暗号との出会い

情報セキュリティ技術の中で、「秘匿性」を実現する中心的な技術が暗号技術である。暗号技術には大きく分けて2種類ある。ひとつは、暗号化と復号に同じ鍵を使う秘密鍵暗号、もうひとつは異なる鍵を使う公開鍵暗号である。秘密鍵暗号の身近な例として、ATMでの認証がある。利用者が入力するパスワードと、銀行が保持しているパスワードが一致するかを確認するしくみである。ATMと同様に、秘密鍵暗号では通信の相手ごとに通じる鍵を共有し、両方で秘密に管理する必要がある。一方、公開鍵暗号では暗号化に使う鍵を公開しても安全に通信ができる。受信者は自分の公開鍵を公開しておけば、誰でもその鍵を使って暗号化したメッセージを送ることができる。受信者は自分だけが知る秘密鍵で復号する。つまり、秘密鍵さえ厳重に管理すれば、誰と



* Atsuko MIYAJI

大阪大学 博士(理学) 1997
現在、大阪大学大学院 工学研究科
名誉教授
TEL/FAX: 06-6879-7714
E-mail: miyaji@comm.eng.osaka-u.ac.jp

でも安全に通信できるという画期的な方式である。この概念は1976年に初めて提案されたが、当時は数学的に実現する方法が存在しなかった。公開鍵から秘密鍵を導くことは極めて困難でありながら、暗号化や復号は容易でなければならない。この「非対称性」を満たす構造を見つけることは容易ではなかったからである。

そして1977年、初めて実現された公開鍵暗号がRSA暗号である。RSA暗号は整数の数学的性質を利用しており、映画『サマーウォーズ』にも登場するので、ご存じの人も多いかもしれない。公開鍵暗号の実現は情報セキュリティ技術を飛躍的に発展させ、デジタル社会を支える基盤となった。例えば、インターネットで商品を購入する際には、公開鍵暗号などの暗号技術を利用することで、クレジットカード情報などの個人データを安全に送信することができる。さらに、公開鍵暗号はブロックチェーンの基盤技術や、秘密を明かさずに「正しさ」を証明するゼロ知識証明など、多様な技術の基礎にもなっている。しかしRSA暗号は、解読手法の進展に伴い、1980年代には安全性を確保するために鍵のサイズを大きくせざるを得なくなった。鍵サイズの拡大は、暗号化・復号にかかる時間の増大や、サーバに保存するデータ量の増加といった性能低下を引き起こす。

そのような中、1985～86年にKoblitzとMillerによって新しい公開鍵暗号である楕円曲線暗号(ECC)が提案された。楕円曲線は非特異な3次曲線であり、曲線上の点に加算が定義されることで加法群と呼ばれる数学的構造を形成する。ECCはこの加法群を利用した暗号である。RSA暗号に対して知られている強力な解読手法が存在しないことから、同じ安全性をより小さな鍵サイズで実現できる。提案当初、ECCはRSAの約1/6の鍵長で同等の安全性を実現できるとして大きな注目を集めた。しかし、RSAに比べて構造が複雑で実装が難しいこと、RSAがすでに普及し始めていたこと、そして「提案からの解読されていない期間」が安全性評価の指標として重視されていたことなどから、実用化はすまなかった。

1990年、私は大阪大学大学院理学研究科数学専攻を修了し、現在のパナソニックホールディングス株式会社に入社した。配属先はセキュリティ研究室で、そこで初めて「セキュリティ」という分野を知っ

た。配属直後に与えられたミッションはエキサイトするものであった。「今なら世界で楕円曲線暗号を理解しているのはKoblitz、Miller、Vanstoneの3人だけ。世界初の楕円曲線暗号を実用化したい。」この言葉が私の研究者としての出発点であり、楕円曲線暗号との出会いとなった。その後、北陸先端科学技術大学院大学を経て大阪大学大学院に着任してからも、楕円曲線暗号は私の研究の原点であり続けている。

3. 楕円曲線暗号の分野を切り開く

3.1 世界初の楕円曲線暗号の混合座標系の提案

ECCの主要演算は、楕円曲線上の点Pに対して、Pをk回繰り返して加算するスカラー倍算 kP である。楕円曲線の加算公式は $P=Q$ の場合と $P \neq Q$ の場合で異なり、 $P=Q$ の場合は、 $P+P=2P$ で2倍算公式、 $P \neq Q$ の場合は、 $P+Q$ で加算公式と呼ばれる。2倍算公式と加算公式は異なる式が用いられ、計算量も異なる。ECCはRSAに比べて鍵サイズが小さいという利点を持つ一方、加算公式が複雑で計算量が多いという課題があった。つまり、加算公式の改良はECCの高速化に直結する極めて重要な研究テーマである。

実は楕円曲線は一意ではなく、複数の座標系が存在し、それぞれ異なる加算公式を持つ。提案当初、利用されていた座標系がアファイン座標系とプロジェクティブ座標系である。アファイン座標系は加算公式に逆元を含むが乗算の回数が少ない。一方、プロジェクティブ座標系は逆元を含まないが乗算が多い特長がある。一般に逆元は乗算に比べて計算量が大きいので、楕円曲線暗号ではプロジェクティブ座標系のみ(これを一座標系と呼ぶ)を用いることが一般的であった。しかし、座標系の改良こそが高速化に直結し、常識を覆す研究が必要であった。一方、楕円曲線暗号は小さいとはいえ、160ビット長のデータの演算処理が必要なことから多倍長演算の開発も必要である。そこで、高速な多倍長演算ライブラリPARI/GPの開発に携わる Henri Cohen(ボルドー大学)先生との共同研究を開始することになる。Cohen先生との共同研究では、私が深夜まで研究し、進捗をメールで送ると、ちょうどフランスでは朝を迎える。そして、私が翌朝目覚めて研究に戻る頃には返事が届き、次のフェーズへ進むことができた。時差のお陰で、まさに24時間研究が進んでいく。こ

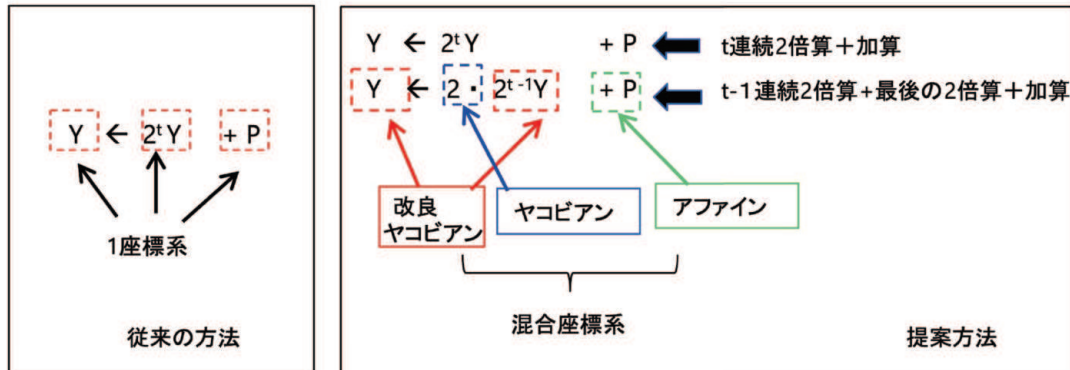


図1 従来の方法と混合座標系

んなに効率的な共同研究はないと実感する日々だった。

私達のターゲットは座標系であった。まず、新たに、ヤコビアン座標系を発見した。ヤコビアン座標系はプロジェクト座標系と同様、逆元が不要な座標系であるが、プロジェクト座標系と比べて、2倍算の計算量が小さい特徴がある。つまり、スカラー倍算をヤコビアン座標系に変更するだけで、既存のプロジェクト座標系より高速になる。しかし、それはどれか一つの座標系を選択して利用する一座標系による演算のパラダイムと同じである。加算が効率的な座標系、2倍算が効率的な座標系など、うまく複数の座標系を組み合わせるパラダイム変化が必要であった。そのとき、アファイン座標系は加算、2倍算とも逆元が必要だが、アファイン座標系の加算結果をヤコビアン座標系で出力すると、アファイン座標系間の加算より計算量を削減できることを発見し、ある座標系の加算や2倍算の結果を別の座標系の出力にすることで、計算量の削減のみならず、複数の座標系の混合が可能になることがわかった。そこで改良ヤコビアン座標系を新たに構築し、スカラー倍算 kP がアファイン座標系の P に対して、連続2倍算と加算、つまり、 $Y \leftarrow 2^t Y + P$ の計算の繰り返しであることに注目し、 kP の計算を t 連続2倍算と加算を $t-1$ 回の連続2倍算と最後の2倍算とその結果と P との加算の3つに分割し、それぞれ最小の計算量をもつ座標系を利用する混合座標系の概念を提案した。この結果、従来の一座標系による演算から、複数の座標系の長所を組み合わせ、より効率的な演算が可能となった。(図1)。

3.2 世界初の安全性を数学的に陽に決定できる一般の楕円曲線MNT曲線

1991年にECCに、最初の解読法、MOV帰着攻撃、が提案された。この攻撃は、ECCの安全性をより単純な「整数演算による暗号」に変換して解読を試みるものである。具体的には、鍵長が k ビットのECCを鍵長 $n \times k$ ビットの整数暗号に「帰着(変換)」する。このときの n を拡大次数と呼び、ECCの安全性はこの n の大きさに強く依存する。つまり、「拡大次数 n 」が大きいほど安全性は高くなる。ところが当時、この n を数学的に正確に求められるのは超特異楕円曲線と呼ばれる特殊な曲線だけであり、一般の楕円曲線の安全性を理論的に明示することは不可能だった。これは、MOV帰着の基盤となる「Weil対」と呼ばれる複雑な写像が解析困難だったためである。

この限界を超えるために、発想を根本から転換した。Weil対の複雑な構造を直接解析するのではなく、代数学における群の性質を利用して、数論の問題として捉え直したのである。このアプローチの転換が、一般の楕円曲線の安全性を数学的に陽に表す成果に繋がった。具体的には、素数 p と楕円曲線上の点の総数 N に注目し、「 k ビット鍵の安全性のECCが $n \times k$ ビットの鍵の安全性の整数暗号に帰着する必要十分条件は N が $p^n - 1$ を割り切ること」というシンプルで表せることを用いて、MOV帰着の条件を初等整数論の問題に変換することに成功する。

さらに、楕円曲線論におけるHasseの定理を用いて、 N の取りうる範囲を素数 p で明示的に示すことで、拡大次数 n を数学的性質として陽に決定できる、一般的な楕円曲線の構成法を提示した。この新しい

楕円曲線は、発見者の頭文字をとってMiyaji-Nakabayashi-Takano曲線(MNT曲線)と名付けられた。MNT曲線は当初、楕円曲線暗号の安全性解析のために提案されたものであった。しかしその後、MNT曲線がIDベース暗号(利用者の名前やメールアドレスなどを直接公開鍵として使う新しい暗号方式)を実現できることが分かり、一般の楕円曲線を用いたIDベース暗号を実現するための基盤となった。

この発見により、楕円曲線暗号研究の新たな分野が開かれた。MNT曲線をもとに、より高い拡大次数を持つ曲線や新しい安全性理論が次々に提案され、多様な応用技術が生まれることになる。

3.3 世界初の侵入耐性暗号の提案

暗号の安全性は、秘密鍵が漏洩しないことを前提に成り立っている。しかし現実には、サイバー攻撃を完全に防ぐことも、秘密鍵漏洩の可能性をゼロにすることも困難である。この課題に対して登場したのが、フォワードセキュア暗号と侵入耐性暗号という新しい概念である。フォワードセキュア暗号とは現在の秘密鍵が漏洩しても過去および未来の通信内容を、一定の条件のもとで安全に保つ暗号である。つまり、侵入耐性暗号はフォワードセキュア暗号をさらに発展させた、より強固な安全性を実現する方式である。このような概念を実現するには、「秘密鍵を時間ごとに更新する」必要があるが、これらの暗号の構築は容易ではなかった。その理由は、公開鍵暗号が「公開鍵」と「秘密鍵」の2つの要素を持つ点にある。秘密鍵を時間ごとに更新するたびに、対応する公開鍵まで更新しなければならないとすれば、運用が極めて複雑になる。したがって、秘密鍵だけを時間ごとに更新しつつ、秘密鍵に対応する公開鍵はそのまま維持する。この相反する要求を同時に満たす仕組みを構築する必要があった。

この難題を解決する鍵となったのが、私が3.2節で述べた楕円曲線などが実現するIDベース暗号である。IDベース暗号は、ユーザーの名前やメールアドレスなどを秘密鍵に対応する公開鍵として利用できる仕組みを持つ。最初に、フォワードセキュア暗号がIDベース暗号の考えを適用して実現された。残る侵入耐性暗号の実現を目指して、ペアリングベースのIDベース暗号の提案者であるMatt Franklin

教授(UC Davis)と共同研究を開始した。IDベース暗号を実現する楕円曲線(MNT曲線)を提案した私と、IDベース暗号を考案したMattとの国際共同研究が始まった。こうして、「秘密鍵が漏洩しても、過去・未来の通信の安全性を一定の条件のもとで保つ」侵入耐性暗号が誕生した。

4. まとめ

紫綬褒章受章にあたり、これまでの研究を振り返り、成果を生み出す上で大切であった三つの要素を考えてみた。

第一は多様性である。本稿で紹介した三つの研究では、どの二つの論文にも共通している著者は私だけである。情報セキュリティは総合科学ともいわれ、数学、計算機科学、通信など、多様な分野を取り込みながら発展してきた。私自身も、異なる専門や発想をもつ研究者や学生との共同研究から、多くの新しい研究テーマを生み出すことができた。私の研究道具は、紙と鉛筆とパソコンだけである。だからこそ、人との出会いと多様性こそが研究のターニングポイントを生み、新しい発想につながってきたのだと思う。

第二はプラス思考である。MNT曲線の研究は、現在ではIDベース暗号などにつながる基盤技術として知られているが、当初の目的は「安全でない楕円曲線を明らかにすること」であった。そのため、研究の意義を問われ、論文が不採録となったこともある。しかし、そこで諦めず、別の角度から研究の価値を考え、前向きに研究を続けたことが大きな転機となった。もし査読者の指摘をそのまま受け入れて研究をやめていたならば、その後の新しい暗号研究へはつながらなかったかもしれない。一見すると失敗に見える出来事も、次の発見への入口になる。プラス思考は、研究を前へ進める大きな原動力である。

第三は継続である。学生と一対一で進める研究では、学生の修了とともに研究が途切れてしまうことがある。だからこそ、一つの研究をそこで終わらせず、次の学生、次の研究者へとつなぎながら発展させていくことが重要である。MNT曲線の研究も、最初の学生が修了した後に次の学生へと引き継ぎ、研究を続けたことで完成した。途中で研究を終えていたならば、MNT曲線は生まれなかっただろう。

振り返ってみると、私の研究人生は、最初から計画したとおりに進んできたわけではない。偶然の出会いがあり、思いどおりにならないことがあり、失敗と思ったことが後になって大きな研究へとつながることもあった。だからこそ、これから何が生まれるのかは誰にも分からない。分からないからこそ、研究は面白い。

紫綬褒章の受章は、これまでご指導、ご支援くだ

さった多くの皆様、そして一緒に研究を続けてきた共同研究者や学生の皆様のおかげであり、心より感謝申し上げたい。この受章は一つの到達点ではなく、次の研究への出発点だと考えている。これからも新しい人、新しい分野、新しい発想との出会いを楽しみながら、研究を続けていきたい。

研究の未来に何が待っているかは分からない。だからこそ、夢はいつでもバラ色である。

