『安全を安心に導く情報セキュリティ技術』

電気電子情報通信専攻
栄誉教授　宮地充子

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，世界初の情報セキュリティ技術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共通の鍵を共有し，両者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.たとえば,インターネットで商品を購入する際,商品情報やクレジットカード情報などの個人データは,店舗が公開している公開鍵を用いて暗号化され,安全に送信されている.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≠Q の場合で異なり,P=Q の場合は,P+P=2P で 2 倍算公式,P≠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ため,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 を構築している 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 24 時まで研究して,

Cohen 先生に進捗箇所をメールして送ると，ちょうど，フランスでは朝が始まり，私が目覚めて研究活動に戻ると，返事が来て，次のフェーズに進める．時差のお陰で，まさに 24 時間の研究が実現できる．こんなに効率的な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ティブ座標系と同様，逆元が不要な座標系であるが，プロジェクティブ座標系と比べて，加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，既存のプロジェクティブ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が削減することを発見し，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世界で初めて提案した．この結果，従来の一座標系から，複数のベストの座標系を混合させる最適な計算量の実現が可能となった．（図 1）．

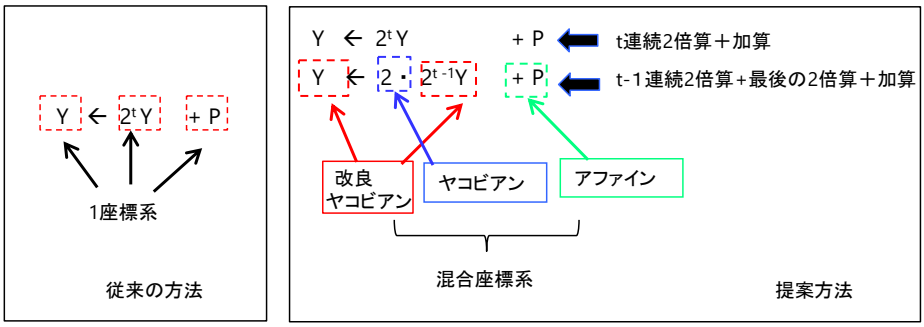

図1 従来の方法と混合座標系

3.2 世界初の安全性を数学的に陽に決定可能な一般の楕円曲線 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×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，世界初の一般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，「ECC が n×k ビットの整数暗号に帰着する必要十分条件は，N が p^k-1 を割り切ること」というシンプルな式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世界で初めて提示した．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，

この曲線が 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，世界初の一般の楕円曲線を用いた ID ベース暗号基盤となった．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，過去の通信内容を安全（フォワードセキュア）に保つ暗号である．一方，未来の通信内容は守れない．侵入耐性暗号は現在の秘密鍵が漏洩しても，過去も未来の通信内容もある一定の条件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，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，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，それを応用した ID ベース暗号を考案した Matt との国際的な協働研究が開始する．こうして，世界で初めて「秘密鍵が漏洩しても，過去・未来すべての通信の安全性を保つ」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，成果を生む三つの要素を考えてみた．**第一は多様性である**．三つの研究のうち，どの二つの論文にも共通している著者は私だけである．情報セキュリティ分野は総合科学と呼ばれ，多様な学問を吸収して発展してきた．そのため，研究者のバックグラウンドが異なることが特徴である．実際，第一の分野の研究者が第二や第三の研究を行う例は少ない．これを可能にしたのが共同研究者の多様性である．私は学生との二人共著が多く，異なる専門をもつ学生との研究が多くの成果を生んだ．私の研究道具は紙と鉛筆とパソコンだけであり，関わる人の多様性こそがターニングポイントを創出し，新しい発想を生む力になってきたと思う．**第二はプラス思考である**．第二の研究は現在では ID ベース暗号などの基盤技術として知られるが，当初は「安全でない暗号の解明」が目的だった．そのため，研究の意義を問われて不採録となったこともあった．しかし，この研究を重要なテーマと捉え直し，前向きに続けたことが転機となった．もし査読者の指摘をそのまま受け入れて諦めていたら，暗号学の一分野は生まれなかったかもしれない．プラス思考は研究を前に進める原動力である．**第三は継続である**．学生と一対一で行う研究では，学生の修了とともに研究が途切れる課題がある．だからこそ，個々の研究を途切れさせず，次の世代へと繋げて発展させることが重要である．第二の研究も，最初の学生が修了した後，次の学生へと引継ぎ，完成させたものだ．もし途中で終えていたら，MNT 曲線は生まれなかっただろう．

最後に，紫綬褒章受章は皆様のご指導，ご支援のたまものと深く感謝を申し挙げます．今後は，この栄誉を励みとして，よりいっそう精進し，情報セキュリティの技術の発展と後身の育成に貢献したいと思います．