情報セキュリティの数理

高木　剛

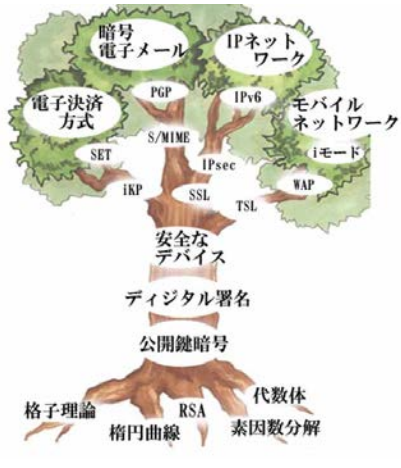
学位: PhD(Technische Universität Darmstadt)
専門分野: 暗号理論

情報セキュリティは、情報社会を支える情報技術(IT)の中で最も重要な要素技術の一つです。特に暗号技術を応用することにより、安全な通信インフラとして使われる暗号プロトコルを構築できます。例えば実際に使われている暗号プロトコルとして、SSL, IPsec, SSHなどが有名です。これらを狭義的に見れば単なる安全な通信路ですが、広義的な暗号プロトコルは実に多くの応用技術を持っています。例えば、電子決済方式、時刻認証システム、位置情報認証方式、電子公証人、電子投票/入札システムなどがあります。これらの技術により、我々の社会活動がインターネット上などで電子的に実現され、より便利で豊かな電子社会が達成できます。

これらのセキュリティパラダイムを実現するために必要不可欠な技術として、公開鍵暗号とデジタル署名が上げられます。この2個の技術をなくして、上で述べた実りある応用技術を実現することはできません。面白いことに、これらのセキュリティコンセプトの安全性は、ある種の数学問題が困難であることに支えられています。例えば、素因数分解問題、楕円曲線上の離散対数、格子理論での最小ベクトル決定問題などが使われています。もし仮にこの基本問題が何らか理由で破られた場合、この問題を基にして構成されているセキュリティシステム全体は全く安全でなくなることを意味します。情報セキュリティにおいて最も重要な研究テーマは、これらの数学問題の安全性を検証し、それらの問題がどのように暗号プロトコルひいては情報セキュリティに影響を及ぼすかを考察することです。本研究室では、特に以下のトピックスについて研究を進めています。

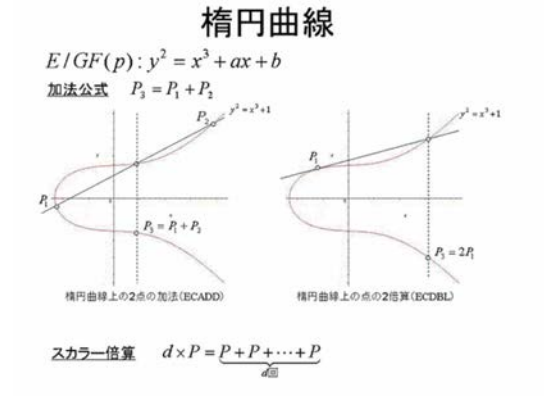
(1)ペアリング暗号

ペアリング暗号は従来の公開鍵暗号では実現が困難であった新たなセキュリティパラダイムが構成できるため、世界中で活発に研究が進展している分野です。代表的な例として、暗号文に含まれるキーワードを検索する技術(暗号文キーワード検索技術)、暗号文の大きさが受信者の数によらず一定となるブロードキャスト暗号(効率的なブロードキャスト暗号)、参加者のIDを利用して柔軟に暗号通信を行う技術(IDベース暗号)などがあります。



(2)安全性証明技術

暗号プロトコルの安全性を正確に判断するには、セキュリティモデルが必要となります。標準的なモデルとして、セマンティックセキュリティ(Semantic Security)が上げられます。安全性証明可能暗号とは、このようなモデルの上で数学的にその安全性が証明できるシステムのことを指します。安全性証明技術は、考察されるセキュリティモデル内では攻撃が不可能という保障があるため、理論的な意味を持つばかりでなく実用的にも重要な研究です。



(3)セキュリティ応用技術

暗号プロトコルは、暗号技術をなくしては実現できなかった新しい応用パラダイムを創造できます。例えば、暗号プロトコルを利用して、電子決済システム、電子選挙システム、電子時刻認証方式などが実現できます。これらの幾つかは既に実際に社会で利用されており、電子社会を支える基本インフラストラクチャとなっています。本研究では、暗号プロトコルを利用して、よりフレキシブルで魅力的な暗号アプリケーションの構築を目指します。