暗号理論とその応用

藤崎　英一郎 研究室

- 専門分野：暗号理論
- Home Page：http://www.seclab.ecl.ntt.co.jp/member/fujisaki.html

研究目的

本研究室は暗号の理論について研究しています。暗号理論とは、「敵」が存在するなかで目的のコミュニケーションを果たす、または必要な情報を守るにはどうしたら良いかを探求する学問です．暗号というと秘匿通信の研究と思われがちですが、それは狭義の意味での暗号であり、現代の暗号研究が扱うテーマはそれより遥か多岐に渡っています。本研究室では暗号に係わるどのようなテーマにも興味がありますが、対象を出来る限り「理論的に安全性を証明できる」やり方で取り扱います。安全で魅力的な暗号プロトコルを数多く生み出し、最終的に便利で安全な社会の実現に役立つことが当研究室のミッションです。

研究テーマ

特徴

公開鍵暗号、ディジタル署名、ゼロ知識証明、マルチパーティプロトコル、頑強性や汎用結合安全性理論、その他にもより高機能な暗号プロトコルを研究対象にします。暗号理論を研究テーマとする場合、大体「魅力的なコミュニケーションの概念「対象」の創造」、「安全性モデルの定式化」、「実現方式の提案」という道筋をたどります。魅力的なコミュニケーションの中には、一見相矛盾する要求を実現するものも数あります（例えば、匿名性と追跡性を同時に満たす等）。もちろん全てを一から行うのではなく、既に存在する対象（例えば公開鍵暗号）の安全性モデル（と複数のモデルがあればそのお互いの関係）を学んだ上で、より効率的な実現法を研究する、または異なる安全性モデルを考案しそれを実現する方式を提案するなどが一般的です。新しい安全性モデルを考案すれば、既存の安全性モデルとの関係の整理が必要になり、既存の安全性モデルに対して、より強かったり、より現実世界を良く捉えていたり、具体的な実現方式の設計が容易になったりなどの特徴があれば良い定式化であると言えます。また方式を実現するためにテクニックを開発した結果、そのテクニックが汎用的で有用であればそれがまた一つの研究分野として発展する可能性があります。提案した実現方式が安全性モデルを満足していることを示すには証明が必要となります。安全性証明をつける際には計算複雑さの理論が関係してきます。また、多くの効率的な実現方式やその技法は、線形代数や数論の知識を背景としています。以下に本研究室が現在取り組んでいるテーマを幾つか紹介します。

公開鍵暗号の研究

公開鍵暗号とは、暗号化鍵と復号鍵が異なる秘匿通信のシステムであり、暗号化鍵（公開鍵）を公開し、復号鍵（秘密鍵）を秘密にしておくことでそれまで何の面識も無い（秘密情報を共有していない）不特定の相手と秘匿通信を行うことが可能となります。 公開鍵暗号は、現代暗号理論誕生のきっかけとなった画期的概念であり、暗号研究の魅力がほぼ全て詰まっているといっても過言ではありません。そして依然として暗号研究の中心にあります。本研究室では、新しい構成技法の発見、より高速な実現法などの研究に取り組みます。

高機能ディジタル署名の研究

ディジタル署名とは、電子化された文章に承認印をつける技術です。ここで必要とされる要求条件は、誰が署名をつけたか誰でも確認でき、かつ署名者以外は他の文書に勝手に署名を偽造してつけることが出来ないことです。電子情報は容易にコピー可能なためディジタル署名は現実世界とは違う技術が必要になりますが、この技術のおかげでネットワークを介して契約を結ぶことができるようになります。本研究室では、ディジタル署名の概念を拡張した高機能署名として、グループに属する誰かが署名したかは分かるが、グループの誰であるかは分からない（匿名性）という条件を満たしながら、規則に反した署名をした場合は、誰が署名をしたか自動的に判明する（追跡性）という追跡可能匿名署名の研究をしています。この署名を使うと、匿名の掲示板などで管理者に秘密情報を預けなくても容易に匿名投票などを行うことができるようになります。

情報漏洩やタンパリング可能な環境における安全性の研究

従来の暗号研究では、正直なプレーヤーの秘密情報や使用される乱数は敵に一切漏れないという状況を想定した安全性モデルで考えられていました。しかし、そのようなモデルは、昨今のストレージをネットワークに置く環境や、秘密情報を保有したICカードに敵が直接攻撃できる環境にはそぐわないため、それに適した情報漏洩モデル、又はタンパリング可能なモデルが考えられるようになりました。例えば、公開鍵暗号で言うと、受信者の秘密鍵の一部が漏洩したり、送信者が暗号化する時の乱数が漏洩することに対応します。本研究室では、このような状況での安全性モデルの研究や具体的な構成法の研究に取り組みます。

汎用結合安全性の研究

公開鍵暗号やディジタル署名のような暗号プリミティブは、単体ではなく組み合わせによって、より高度な暗号プロトコルを構成できます。ただし、各プリミティブがそれぞれ安全であったからと言って、組み合わせによって出来た暗号プロトコルが安全であることは一概に保証されないため、新しいプロトコルが出来るたびに新しい安全性証明をつけなければいけません。汎用結合安全性とは、汎用結合安全と承認された暗号プリミティブであれば、組み合わせにより出来た暗号プロトコルの安全性を自動的に保証する安全性のモデルです。当然厳しい安全性の要求条件がありますが、この条件を満たす効率のよい暗号プリミティブの研究に取り組んでいます。

教員からのメッセージ

この分野の研究を進めていく中で、学生の皆さんは暗号理論を学んでいかなければならないのですが、それを学習する上で役に立つと思われる知識には、線形代数や代数の知識、計算複雑さの理論、情報理論などが挙げられます．ただし最も必要とされるのはやる気と継続的努力であり、これらの知識はスタート時点で知っていれば多少有利であるという程度です。やる気のある学生の皆さんの参加を待っています。

参考文献

1. 翻訳「現代暗号・確率的証明・擬似乱数」（ゴールドライヒ著）シュプリンガー・フェアラーク東京, 2001
2. 解説記事「選択暗号文攻撃安全な公開鍵暗号の構成について」電子情報通信学会誌 vol.90, No.6, 2007
3. 解説記事「知識ベース　知識の森」1群3編 暗号理論 6章 ディジタル署名, 電子情報通信学会, 2010
4. E. Fujisaki and T. Okamoto, “Secure integration of asymmetric and symmetric encryption schemes”, Journal of Cryptology, Volume 26, Issue1, pp 80-101, January 2013
5. E. Fujisaki, “Sub-Linear Size Traceable Ring Signatures without Random Oracles”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E95-A (1) :151-166, 2012
6. E. Fujisaki, “New Constructions of Efficient Simulation-Sound Commitments Using Encryption and Their Applications”, In Topics in Cryptography-CT-RSA, pages 136-155, 2012.