教授
四方 順司
シカタ ジュンジ

大学院環境情報研究院　社会環境と情報部門
理工学部　数物・電子情報系学科　情報工学教育プログラム
shikata@ynu.ac.jp
http://www.slab.ynu.ac.jp/

情報学
情報学基礎

情報学基礎理論

暗号理論
情報理論
数理アルゴリズム
理論計算機科学
計算数論

[研究概要]

本研究室では、暗号理論、情報理論、理論計算機科学、計算数論の分野の基礎から応用にわたる幅広いテーマを研究対象としています。中でも、暗号理論とその応用に関する研究には特に力を入れています。今日、暗号・情報セキュリティ技術はインターネットなどを利用したサービスの安全性を支え、多くの人々が安心して通信・契約等を行うために非常に重要な技術であり、他の様々な学問分野と深く関連をもちながら研究が行われています。本研究室では、数理アルゴリズムを巧みに利用した公開鍵暗号技術、情報理論により長期的安全性を保証する暗号技術など、様々な暗号・情報セキュリティ基礎技術に関しての研究開発を行っています。

[アドバンテージ]

暗号・情報セキュリティ関連システムのコアとなる暗号基礎技術に対して、その安全性は客観的に保証されなければなりません。現在、暗号基礎技術を研究開発する場合、その安全性を何らかの理論に基づいて数理的に証明できることが必要であり、世界的にもこれが現代暗号分野の標準的なアプローチです。また、どのような環境下（インターネット、PC、モバイル端末、ICカードなど）で、どのような目的（秘密通信、データ改ざん検知、個人認証、データ保護、コンテンツ保護、著作権保護など）で用いるかによっても、技術に要求する条件（安全性、効率性）が変わってきます。本研究室では幅広い暗号・情報セキュリティの基礎理論を研究しているため、対象とするアプリケーションの環境と目的に応じて、計算理論、情報理論、組合せ論、計算数論などの広い分野から適切な理論をもとに研究開発することが可能です。

[事例紹介]

現在、私達の身の回りには、暗号・セキュリティ基礎技術が使われているモノで溢れています。PCをはじめ、携帯電話等のモバイル端末、各種クレジットカード等のICカード、そしてDVD、オーディオ、ゲーム機器類などが挙げられます。研究成果は、今日（または将来）の情報化社会での利用環境とその目的に応じて様々なアプリケーションが考えられます。例えば、計算量が少なくてすむ暗号化・電子署名システムの研究開発は、計算力の乏しい端末やデバイスでの暗号化・認証機能を実現可能にします。また、現在の公開鍵暗号技術を用いた暗号化や電子署名システムは、安全性の面から長期間の利用（長くても約20年まで）には適していませんが、著作権や重要文書保存など、暗号基礎技術を長期間利用したい場合、本研究室で研究開発した「情報理論的安全性を有する暗号・電子署名システム」は適しています。

■ 相談に応じられるテーマ

長期の安全性を保証する暗号・情報セキュリティに関する基礎技術
実用性を重視した暗号・情報セキュリティに関する基礎技術

■ 主な所属学会

ACM，IEEE，IACR（国際暗号学会），IEICE（電子情報通信学会）

■ 主な論文

『Unconditionally Secure Steganography Against Active Attacks』「IEEE Transactions on Information Theory 54(6)」2008.6

『Construction of Threshold (Hybrid) Encryption in the Random Oracle: How to Construct Secure Threshold Tag-KEM from Weakly Secure Threshold KEM』「Information Security and Privacy: 12th Australasian Conference on Information Security and Privacy (ACISP 2007), LNCS 4586, Springer-Verlag」2007.7

『Unconditionally Secure Anonymous Encryption and Group Authentication』「The Computer Journal, Vol. 49」2006.5

『Identity-Based Hierarchical Strongly Key-Insulated Encryption and Its Application』「Advances in Cryptology - ASIACRYPT 2005, LNCS 3788, Springer-Verlag」2005.12

『Security Notions for Unconditionally Secure Signature Schemes』「Advances in Cryptology - EUROCRYPT 2002, LNCS 2332, Springer-Verlag」2002.4

■ 主な特許

特許第3895244号「鍵の更新が可能な利用者の識別情報に基づく電子署名方法及び電子署名システム」

特許第3895245号「鍵の更新が可能な利用者の識別情報に基づく暗号化方法及び暗号システム」

特許第3989364号「データ復号端末，秘密鍵提供端末，データ暗号化端末，暗号データ復号システム，及び復号鍵更新方法」

■ 主な著書

「暗号と格子」数学セミナー，日本評論社 2001.12

「情報量的安全性に基づく暗号系について」数理科学，サイエンス社 2000.9

「楕円曲線暗号について」臨時別冊・数理科学，サイエンス社 2000.9