情報理論的、および計算量的アプローチによる暗号理論の研究

岩本・渡邉 研究室

岩本 貢
Mitugu IWAMOTO

渡邉 洋平
Yohei WATANABE

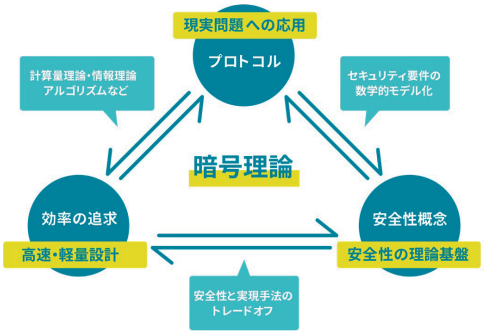
クラウドコンピューティングやビッグデータ、ＩｏＴ（モノのインターネット）、機械学習といった先端情報技術は、２０００年代から目覚ましい発展を遂げてきました。これによって多様なサービスが登場し、利用者の利便性が向上する一方で、データの漏えいやプライバシーの侵害といったセキュリティ上の問題が多発するようになったのも事実です。

こうした先端テクノロジーの安全性を支えるのが暗号技術です。

岩本貢教授と渡邉洋平助教の研究室では、理論的な側面から暗号について研究し、利便性を損なわずに安全性を高める情報セキュリティシステム向けの新しい暗号方式の考案や、その安全性評価、暗号の実装方法の提案などを行っています。数学を道具として、特に「情報理論的」、および「計算量的」という二つの理論的アプローチを駆使して研究しているのが研究室の大きな特徴です。

安全性と効率の追求

岩本教授は暗号理論の中でもとりわけ情報理論的暗号を軸に、計算量的暗号の観点も考慮しながら、トレードオフの関係にある暗号の「安全性」と「効率の追求」について基礎理論の研究を進めています。この二つを土台にして、現実問題に適用可能な暗号プロトコルの提案を目指しています。



岩本教授の研究コンセプト

暗号の安全性には、膨大な計算時間がかかることでこれを保証する計算量的安全性と、原理的に破られない情報理論的安全性があります。このうち、岩本教授は電子カルテなどの重要データの保存などに応用できる情報理論的安全性について研究しています。情報理論的暗号の代表例に秘密情報を分散して管理し、集めると復元できる「秘密分散法」がありますが、岩本教授はこの秘密分散法の効率化に向けて、高い安全性を保ちながらデータサイズを圧縮して暗号を軽量化するといったテーマに取り組んでいます。

これまでに新しい秘密分散法のほか、秘密分散法を画像で実現す

主な研究テーマ

■ プロトコルの安全性評価
・計算量的/情報理論的安全性証明
・安全性の定式化に関する基礎理論

■ 新しい暗号プロトコルの提案
・基礎技術：
公開鍵暗号，電子署名，秘密分散法 etc.
・応用技術：
マルチパーティ計算，カードベース暗号 etc.

■ 機能・効率の追求
・高機能，高安全性をもつ暗号プロトコル
・高速，軽量なアルゴリズム設計

■ そのほか
・数理パズル
・暗号技術を使ったおもちゃ

キーワード
情報セキュリティ、プライバシー、暗号理論、情報理論、計算量理論、計算量的暗号、情報理論的暗号、暗号プロトコル、高機能暗号、物理暗号

所　属	大学院情報理工学研究科 情報学専攻
メンバー	岩本 貢 教授 渡邉 洋平 助教
所属学会	電子情報通信学会、情報処理学会、国際暗号学会（IACR）、電気電子学会（IEEE）
E-mail	mitsugu@uec.ac.jp watanabe@uec.ac.jp

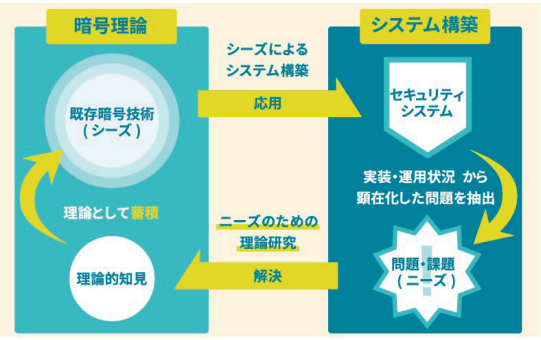
る「視覚復号型秘密分散法」の提案などを行ってきました。そのほか、多人数が参加する秘密計算（マルチパーティ計算）や、トランプのようなカードを使った秘密計算（カードベース暗号）などの暗号プロトコルの研究も手がけています。

二つの理論をつなぐ

安全性と効率の関係を明らかにするためには、「安全」とは何かを数学的に表現（定式化）しなければなりません。ただ、安全性の定式化にあたっては、情報理論的安全性と計算量的安全性の違いをいかに考慮するかが大変難しいのだそうです。これまで両者は互いに関連しつつも、情報理論と計算量理論という異なる理論を背景にして成長してきました。しかし、大きな視点で見れば、二つの理論は同じ土俵で議論できるのではないか。このような問題意識が、岩本教授の研究の動機の根底にあるといいます。「情報理論的暗号と計算量的暗号の関係性が分かれば、両者の本質的な違いが明らかになるだけでなく、両者の良いところをうまく利用できる可能性がある」と岩本教授は期待しているのです。

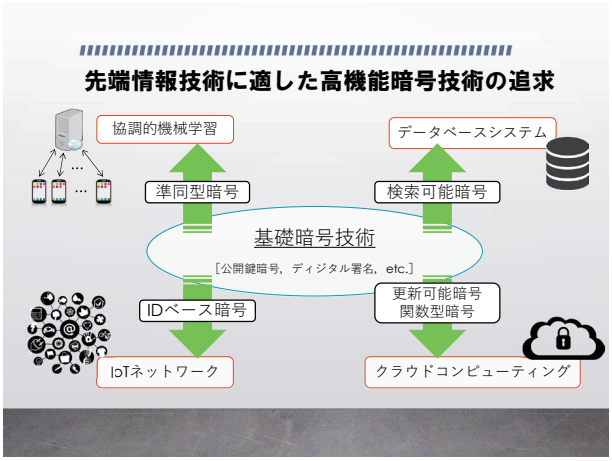
新しい暗号プロトコルを提案

一方、渡邉助教はより社会実装を意識した研究を進めており、特に計算量的暗号の観点から利便性と安全性を両立した高機能暗号などを考案しています。「実際のセキュリティシステムの運用状況から課題を抽出し、これを解決する理論を蓄積していき、暗号技術として実装するという暗号の〝エコシステム〟として循環させていく」と渡邉助教はその研究コンセプトについて語ります。



渡邉助教の研究コンセプト

例えば、通信データの漏えいを防ぐ「公開鍵暗号」やデータの改ざんを防ぐ「デジタル署名技術」、暗号化したまま処理できる「準同型暗号」、暗号化したまま検索できる「検索可能暗号」など多様な暗号理論について研究しています。なかでも最近注力している検索可能暗号では、攻撃の対象になりやすいデータベースに対して、データを秘匿しつつ、検索などの操作をより効率化できる新しい暗号プロトコルを提案しました。情報通信研究機構（ＮＩＣＴ）と共同で、実際の運用に近いデモシステムなども作成しています。



基礎をベースに応用まで

このようにして、岩本教授と渡邉助教はそれぞれの立場から研究し、基礎的な知見を基に、応用までを見通した暗号理論の幅広い研究を協力して進めています。情報技術の進歩とともに高度な暗号技術がより一層求められており、国家プロジェクトへの参画や企業との共同研究を活発に行っているのも研究室の特色でしょう。

【取材・文＝藤木信穂】