数学理論にもとづくトップダウンアプローチ、実装からのボトムアップアプローチにより、暗号システムを総合的に研究する

太田（和）・崎山・岩本 研究室

太田 和夫
Kazuo OHTA

崎山 一男
Kazuo SAKIYAMA

岩本 貢
Mitsugu IWAMOTO

研究概要

データのやり取りの安全性やハッシュ関数の評価を行う

インターネットでデータのやり取りが盛んになってきた今日、データの盗み見をされないように「安全性」を確保すること、またそのデータが本人によって書かれたものかどうかを証明・保証することが必要となっている。

そこで重要になるのが暗号である。世の中にはあまたの暗号が存在し、次々に新しく生まれているが、そのなかには安全性が示されていない暗号や情報漏れの心配な実装法がある。

当研究室では、安全性に確証のない暗号が世間一般で使われると大変な問題となるので、その前に安全性を「理論」と「実装」の2つの観点から評価している。

暗号技術の安全性を示すのに使う基本ツールは、計算量理論である。ある暗号やハッシュ関数を攻撃することが数学の難しい問題（例えば、素因数分解）を解くのと同じくらい難しいことを証明し、素因数分解が解けなければ、その暗号技術も安全であることを保証している（安全性証明技法）。

サイドチャネル攻撃対策研究

ところで、最近、装置から漏れてくる電磁波や消費電力などの情報を集めると、暗号処理で使っている秘密情報を推定できるということが分かってきた（サイドチャネル攻撃）。今まで、安全性の理論を考えるときに想定していたよりも、現実には攻撃者は多くの情報を利用できるのだ。

サイドチャネル攻撃に対しても安全な暗号システムの実装法を確立することが、当研究室が追究する重要課題である。

より強力な攻撃者が現れても、安全性を保証できるように、既に確立された安全性証明技法を、サイドチャネル攻撃にも耐えうるように拡張、充実させる研究にも取り組んでいる。

特にICカードといった組み込み向け用途を主な研究対象とし、従来の組み込みシステム開発時に重視されたコストパフォーマンスの高効率化に加え、サイドチャネル攻撃をはじめとする秘密情報取得を試みる種々の攻撃に対して、耐性強化の研究に着手している。

人材養成

当研究室は、企業の要請に基づく社員の受け入れなど人材養成にも積極的だ。例えば、企業は電子決済のシステムはつくれるが、実際にデータをやり取りしたときに安全かどうかを保証できる人材がいないので、当研究室が育成しているのである。これまで、大手電気メーカーや通信事業者から社員を博士コースの学生として受け入れたり、卒業生を送り込んだりしており、教育プログラムが確立してきた。

セキュリティシステムの研究開発コンサルティング

当研究室では、セキュリティシステムの研究開発をトップダウンアプローチ（太田）、ボトムアップ

キーワード

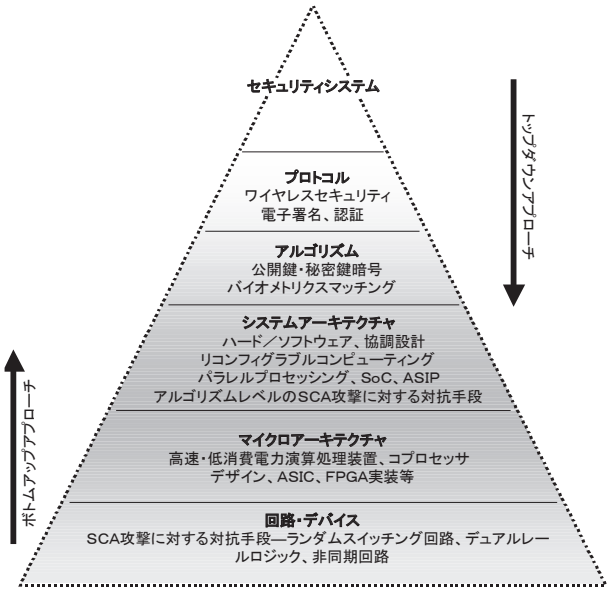
暗号理論、暗号システム、公開鍵暗号、秘密鍵暗号、安全性証明、サイドチャネル攻撃、組み込み向け暗号LSI、ハッシュ関数、セキュリティシステム

所　属	大学院情報理工学研究科 情報学専攻
メンバー	太田 和夫 教授 崎山 一男 教授 岩本 貢 特任准教授（先端領域教育研究センター）
所属学会	電子情報通信学会、情報処理学会、IACR、IEEE
E-mail	[太田] kazuo.ohta@uec.ac.jp [崎山] sakiyama@uec.ac.jp [岩本] mitsugu@uec.ac.jp
研究設備	暗号プログラム開発・実験用「FPGAボード」、各種測定機器「オシロスコープ、ロジックアナライザ」、オープンラボスペース1室（73m^2）、FPGAボード

アプローチ（崎山）で進めてきた経験に基づいて、企業のコンサルティングも引き受けている。さらに、安全性を確保するための細かな技術、例えば、鍵の長さはどの程度か、サイドチャネルに強い暗号製品はどれかなどの情報提供もコンサルティングの内容である。

太田は、NTT研究所、アメリカの暗号研究の中心であるマサチューセッツ工科大学（MIT）で、証明可能安全性の理論研究を進める一方で、電子マネーや電子入札などのプロトタイプ開発の経験をもつ。

崎山は、日立の半導体事業部で3G（第3世代）携帯電話向けのシステムLSIの開発、欧州の暗号研究の中心であるベルギー王立ルーベン大学（KUL）で、サイドチャネル攻撃に耐性をもつ暗号実装法の研究経験をもつ。



セキュリティシステムにおける階層構造と研究のアプローチ

アドバンテージ

暗号の安全性の概念・理論からセキュリティシステムの構想・実装法までわかる人材を育成する

暗号を安全性の「概念・理論」にまで遡って教える研究室はそうは存在しない。当研究室では、数学理論に基づいた解析を通じて、なぜ安全なのかを証明できる人材を育成しようと考えている。

また、ハードウェアとソフトウェアの両方を駆使して、攻撃耐性のあるセキュリティシステムの「構築と実装」ができる人材の育成を図っている。システムの安全性を証明し誰もがわかるように説明できる人材を輩出できるのが、当研究室のアドバンテージである。

今後の展開

安全で効率のよいハッシュ関数の設計を企業と共同で研究する

これまで安全性の理論に重きを置いて研究を展開してきた。幹の部分はしっかりしているので、今後は枝の部分、すなわち理論を応用する分野に研究を広げていきたいと考えている。

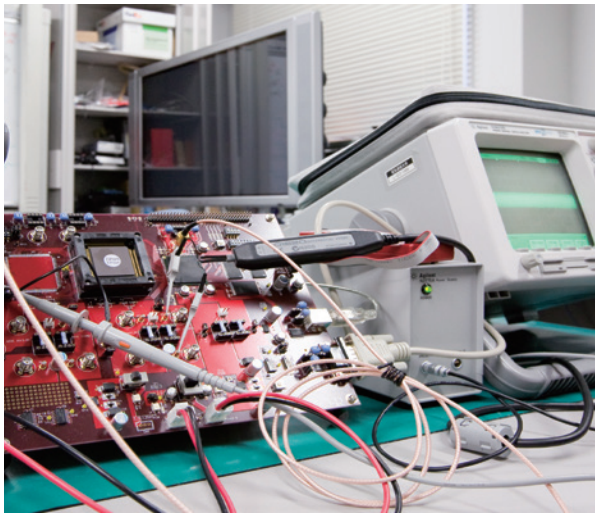
例えば、安全で効率のよいハッシュ関数の設計である。ますます高度化する情報化社会のセキュリティシステムを導入しても、実用に耐えうる新しいハッシュ関数のニーズが大きいからだ。

もう1つ例を挙げると、近い将来バーコードに替わる識別タグとして期待される電子タグ「RFID」の実装法の研究がある。電子タグは低コストでつくらないと広く普及しないため、高価な公開鍵を使うことは難しい。だが安価な技術のみでは、理論的にも実装面からも高い安全性を確保することは不可能である。コストと安全性のバランスを考え、どこで割り切るのかも含めて電子タグに関連したモデルづくりに挑もうと考えている。

いずれの場合でも、安全性の理論だけで解決する問題ではない。コストと安全性に対する企業のスタンスを条件に入れることが必要なので、企業との共同研究の方法を模索している。

今日、インターネットによって膨大な重要データや個人情報がやり取りされるほか、ICカードや携帯電話で金銭の支払いやトレーディングが可能になり、いっそうセキュリティ問題がクローズアップされている。悪意があれば、ワイヤードタップで情報を盗むことも可能な社会である。

そんな社会情勢にあって、当研究室に寄せられる期待と担う役割も大きくなってくるはずだ。


SASEBOボードを用いた安全性評価環境