暗号の数理と物理で情報基盤のレジリエンスを高める

崎山・宮原 研究室

崎山 一男
Kazuo SAKIYAMA

宮原 大輝
Daiki MIYAHARA

人々の豊かな暮らしを支える情報化社会において、安心・安全な情報インフラを維持するためには、環境の変化があってもしなやかに対応できる情報基盤のレジリエンス(復元力)が欠かせません。しかし、情報システムに対する攻撃は日々高度化し、その脅威は一段と増しています。組織にとって、サイバー攻撃への対策は喫緊の課題になっています。

この情報基盤のレジリエンス向上に向けて必須となるのが暗号技術です。崎山一男教授と宮原大輝助教の研究室では、暗号技術を用いたセキュリティ対策を研究しています。特に、崎山教授はＩｏＴ(モノのインターネット)システムへの実装など、基礎から応用までのハードウェアセキュリティを研究しており、宮原助教は物理的なカードを使って秘密計算を行う「カードベース暗号」などの物理暗号を中心に扱っています。

ＩｏＴデバイスのセキュリティ対策

崎山教授は現在、暗号技術でＩｏＴシステムのレジリエンスを高める研究プロジェクトを推進しています。ＩｏＴデバイスはすでに世界で３００億個近くが稼働しており、その安全性は国家基盤にも影響します。崎山教授は「暗号の数理(コト)と物理(モノ)を一体化し、ＩｏＴに適したセキュリティ対策を施すことが大切だ」と考えています。

従来のセキュリティ対策では、数理については安全性の証明は可能でも実装ができず(オーバースペック)、一方の物理は実装可能でも証明ができない(攻撃と対策のいたちごっこ)といった課題がありました。暗号の数理と物理のいいとこ取りができれば、安全性を証明しつつ実装ができるようになります。また、数理と物理の境界領域の学術的な進歩にもつながるでしょう。

攻撃を検知する暗号チップを開発

崎山教授が進めるプロジェクトでは、これまでに約３００個の光センサーを敷き詰めた共通鍵暗号方式(ＡＥＳ)の暗号チップを開発し、〝半導体のオリンピック〟と呼ばれる半導体分野で最高峰の国際会議「国際固体素子回路会議(ＩＳＳＣＣ)」で発表するなど大きな成果を収めています。これは悪意のあるレーザー攻撃を瞬時に検知するデバイスで、敵に攻撃する隙を与えません。暗号の数理と物理を融合したＩＳＳＣＣ初の成果であり、その発表とデモンストレーションは会場で高い関心を集めました。チップの理論的安全性も実験で確認しています。

現在はＩｏＴシステムを安全性の状態が推移する「エコシステム」とみなし、暗号鍵の情報が外に漏れる「リーク」は不可避であるとの前提で、リークの度合いに応じて柔軟なセキュリティ対策を施す研究を進めています。リーク検知技術(ハードウェアセキュリティ)の開発から、攻撃に耐えるリーク耐性暗号(暗号理論)の考案、安全な鍵だけを抽出するリーク鍵の蒸留(情報理論)手法の提案

キーワード

情報セキュリティ、応用暗号学、暗号工学、ハードウェアセキュリティ、サイドチャネル攻撃、カードベース暗号、ゼロ知識証明、理論計算機科学、ゲーム情報学

所　属	大学院情報理工学研究科 情報学専攻
メンバー	崎山 一男 教授 宮原 大輝 助教
所属学会	国際暗号学会(IACR)、電子情報通信学会、米電気電子学会(IEEE)
E-mail	sakiyama@uec.ac.jp miyahara@uec.ac.jp

といったサイクルを回していくことで、IoTシステムのレジリエンスを向上させる試みです。

安全性を実感しやすい物理暗号

一方、宮原助教が取り組むのは、物理的な道具を用いた暗号プロトコルの研究です。現在、情報通信の安全性を担保するために現代暗号が用いられていますが、例えばインターネット上で通信を暗号化し、盗聴や改ざんを防ぐTLS通信はコンピュータ上で自動的に実行されるため、その仕組みを実感するのは難しいでしょう。これに対して、物理暗号は実際に手を動かして実行するため、計算機が不要になるだけでなく、正当性や安全性を実感しやすいという利点があります。カードベース暗号プロトコルで言えば、6枚のカードを使って、入力カードの絵柄を秘匿したまま出力カードを得る秘密計算なら1分未満で実行できます。このようなカード組で計算可能な理論限界を明らかにするなどの暗号プロトコルの研究は、「入力情報を漏らさずに出力だけを得たいといった問題に応用できるだけでなく、暗号の注目分野である秘密計算の適用例として暗号の教育にも活用できる」と宮原助教は言います。

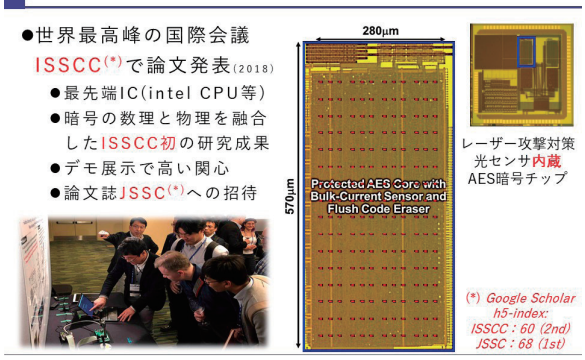
入力を漏らさず出力だけを求める

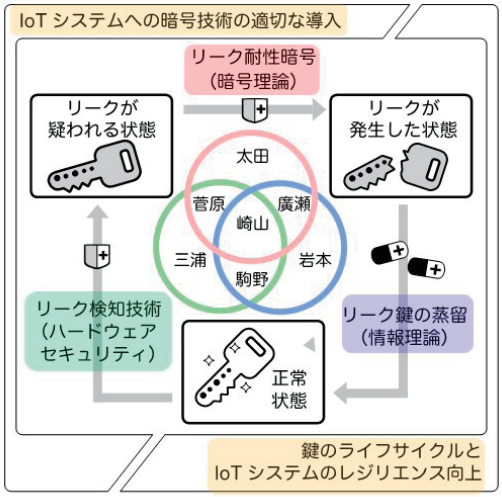
具体的なテーマとして、入力値を漏らさずに結果の大小だけを求める「大小比較秘密計算」問題では、カード組と、いわゆるカードを切るシャッフル操作を併せることで比較計算ができることを示しました。市販のトランプや論理回路でも計算が可能なほか、複数人の計算にも応用できるそうです。

また、答えを明かさずに、自分が答えを知っていることを証明する「パズルに対するゼロ知識証明」問題では、数独など多くのパズルに対する物理的ゼロ知識証明プロトコルを構成しました。既存研究では避けられなかったエラーの確率はゼロに改善しています。このほか、「ボールと袋を用いる秘密計算」などの問題でも最適なプロトコルを提案しています。

このように、崎山教授と宮原助教はそれぞれ暗号の物理、数理に強みを持ち、互いに連携しながら研究室を運営しています。崎山教授は企業の出身であり、かつベルギーで暗号研究に従事した経験があることから、企業との共同研究も積極的に行っているほか、国際ネットワークを生かした幅広い研究を進めているのも大きな特徴です。

【取材・文＝藤木信穂】





IoTシステムのレジリエンス向上に向けた暗号技術の開発