安全性と機能を両立する暗号技術の開発

研究分野：情報学基礎論、情報セキュリティ

キーワード：高機能暗号、軽量暗号、耐量子計算機暗号

貢献できるSDGsの区分：

情報システム学部　情報セキュリティ学科　教授　星野　文学

教員情報URL　https://sun.ac.jp/researchinfo/hosh-fumi/

研究概要

情報セキュリティは大雑把に言うと、権限のない人が情報を勝手に読めない性質「機密性」、権限のない人が情報を勝手に操作できない性質「完全性」、権限のある人が情報をいつでも自由に読んだり操作できる性質「可用性」の三つの要素から構成されると考えられています。

一般に暗号技術においては機密性と完全性は非常に重視されますが可用性は軽視される傾向があります。機密性や完全性を守るために、特定の人以外一切情報を読んだり書いたり出来なくしてしまう、即ち可用性を犠牲にして機密性や完全性を確保するのが暗号の機能です。この意味で可用性は機密性や完全性とは一種のトレードオフの関係にあります。

実は機密性や完全性を損なわずに、如何に可用性を拡張するか？というのが近年の暗号研究の一つの大きな流れとなっています。高機能暗号はそのような背景の元で形成された概念で、高機能暗号を用いると きめ細かな権限の設定が出来たり、暗号文同士で何らかの演算が可能であったりします。本研究ではそのような暗号について研究します。

$$Enc(m_0) \times Enc(m_1) = Enc(m_0 + m_1)$$

図：高機能暗号のイメージ

産学連携の可能性（アピールポイント）

①本研究にて開発した暗号技術を用いることで、従来の暗号技術では解決が困難であった実社会の問題解決を図るシステムやアプリケーションの開発ができるようになることが期待できる。

②開発した暗号技術を活用した新たなアプリケーションを実現できることも期待できる。

外部との連携実績等

九州大学マス・フォア・インダストリ研究所，2022年度 共同利用 採択研究，高度化する暗号技術と数学的技法の進展。