暗号とサイバーセキュリティ - 宮地研究室-

安全・安心な社会を実現する情報セキュリティの骨格となる暗号理論，プライバシ，セキュア応用，サイバーセキュリティまで情報セキュリティ全領域を研究．

基盤研究

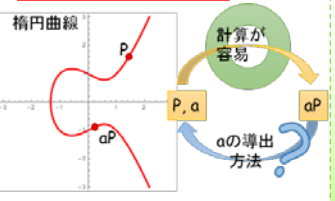
情報セキュリティの基礎理論

情報
セキュリティ

$$F_q|x\rangle = \frac{1}{\sqrt{q}}\sum_y \omega_q^{xy}|y\rangle$$

数理・情報科学の基礎理論

楕円曲線暗号の安全性



■ 情報セキュリティの基礎理論

情報セキュリティは数理・情報科学の強固な理論的基盤によって支えられている．研究室では，数学，計算量理論，符号理論，情報理論などを駆使し，ポスト量子暗号などの情報セキュリティ技術の限界に挑む．

■ 楕円曲線暗号の安全性

楕円曲線暗号の安全性はECDLP に依存する．研究室では，指数計算法(index calculus)の解析と連立多変数多項式を解く研究を行っている..

■ 共通鍵暗号の解読

共通鍵暗号はデータ及び通信の暗号化に利用され，情報秘匿と改ざん防止を実現する．研究室では，共通鍵暗号に対して様々な攻撃を加え，共通鍵暗号の解読を行うことで安全な暗号の実現を目指す．

■ 準同型暗号

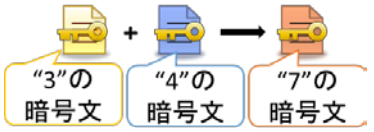
準同型暗号とは情報を暗号化したまま様々な演算が可能となる新しい技術であり，ビッグデータ処理でのプライバシ保護を達成する基盤として大きな期待を集めている．研究室ではこの新しい暗号技術の効率化や多機能化，それらに基づくビッグデータ処理への応用技術に関する研究を行っている．

■ Private Set Intersection（PSI）

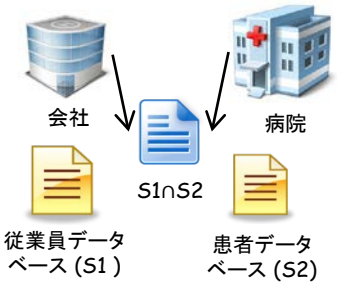
データを利活用する方法として，Private Set Intersection（PSI）に関する研究を行っている．PSI とはデータのプライバシを秘匿し，各機関のデータを解析する技術である．研究室では，PSI を拡張した新たなデータ解析手法やPSI にかかる計算量・通信量の削減等の最適化に関する研究を行っている．また，PSI を利用する研究機関と連携し，実用的な PSI に関する研究を行っている．

ビックデータ

準同型暗号

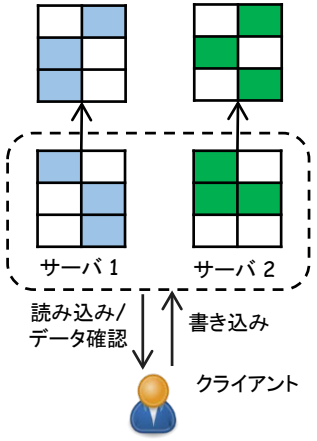


Private Set Intersection



クラウド

Oblivious RAM（ORAM）



■ ネットワークコーディング

ネットワークコーディングは複数の異なるノードから受け取ったデータを一括で符号化し，伝送する手法である．スループットを向上させ，ネットワーク資源を効率的に運用できる．研究室では通信データへの汚染攻撃を検知する手法，汚染されたパケットが発生した場合でも正常な通信データを回復可能なコーディング方式について研究に取り組んでいる．

■ Obvious RAM (ORAM)

データからのメモリのアクセスパターンを保護できる方式である．データの読み書き中に，サーバからのアクセスを隠すためにデータの領域先をシャッフルし、メモリのデータ配置を変えることで，信頼できないサーバがアクセスパターンを把握することができなくなる．

■ 楕円曲線暗号

楕円曲線暗号は短い鍵長で実現可能であるため，計算資源やメモリ容量が制限された組込み機器に利用される．研究室では安全性を高める研究や，処理の高速化等の楕円曲線暗号の最適化全般に関する研究を行っている．

■ 安全かつ高速的疑似乱数生成器

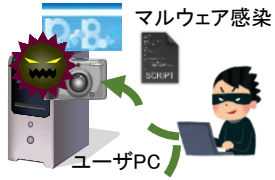
擬似乱数生成器は暗号技術のセキュリティ強度に直接影響する．研究室ではエントロピー操作などの強力な攻撃へ対応できる高ランダム性，低コスト，高速性をもつ実用的疑似乱数生成器の構築を取り組んでいる．

■ 耐タンパー技術

ソフトウェア・ハードウェアの構造を解析から守る技術を耐タンパー技術と呼ぶ．研究室では，ソフトウェア難読化技術を適用した暗号の性能評価を実施している．

IoT

ハッキング



不正な遠隔操作

カード偽造・不正使用