新たなディジタル署名技術の開発

研究分野：情報学基礎論，情報セキュリティ

キーワード：ディジタル署名，耐量子計算機暗号，高機能署名，ディジタル署名の応用

貢献できるSDGsの区分：

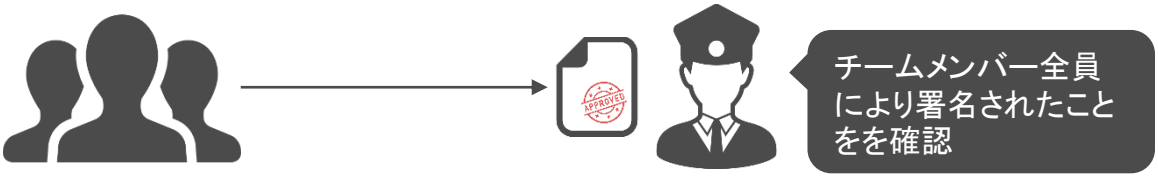
情報システム学部　情報セキュリティ学科　准教授　福光正幸

教員情報URL　https://sun.ac.jp/researchinfo/fuku-masa/

研究概要

ディジタル署名は，なりすましや改ざんがないことを保証する暗号技術の一種であり，SSHやFIDOなどの認証プロトコルやブロックチェーン，電子契約システムなどさまざまなシステムの基盤技術として活用されている．一方，暗号研究の中では，「なりすましと改ざんがないこと」+αの保証を実現する署名技術（以降，高機能署名と呼ぶ）の開発が進んでいる．その一例として，「マルチ署名」を挙げる．これは，複数人で構成されるチームメンバー全員によりデータを保証するための技術である．

本研究では，これまでに実現されている高機能署名を更に発展させることによる，新たな高機能署名技術の開発や，既存のディジタル署名技術を用いた新たなアプリケーションの開発を行う．



図：マルチ署名のイメージ

産学連携の可能性（アピールポイント）

- 本研究にて開発したディジタル署名技術を基盤とすることで、従来のディジタル署名技術では困難であった新たなシステムやアプリケーションが実現されることが期待できる。
- 高機能署名の開発のアプローチには近年報告されているディジタル署名技術を進化させる方向性もあるが、本研究では実社会の問題をベースにこれを解決できる新たな高機能署名を開発するアプローチも視野に入れている。
- 近年著しく研究開発が進む量子コンピュータを用いた攻撃について考える必要があるが、本研究においても、量子コンピュータを用いた攻撃に耐性のある高機能署名技術の開発を進めている。

外部との連携実績等

- 日本学術振興会，科学研究費助成事業　基盤研究(C)，AIデータの保証に特化した暗号技術の開発（2023年度～）．
- 電子情報通信学会などのゲストエディタ・プログラム委員への就任