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、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

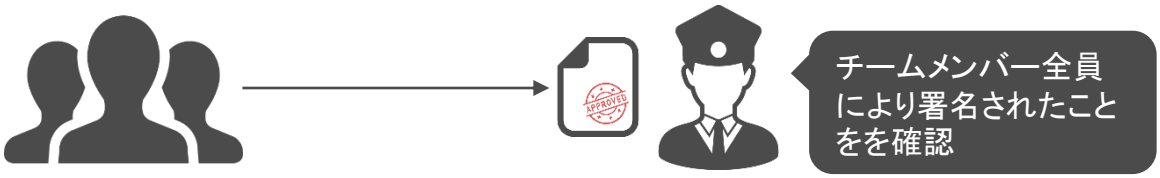
教員情報URL　https://sun.ac.jp/researchinfo/fuku-masa/

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）

①本研究にて開発したディジタル署名技術を用いることで、従来のディジタル署名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開発したディジタル署名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

①日本学術振興会，科学研究費助成事業 若手研究，ブロックチェーンとIoT機器に最適化した署名技術の開発（2019年度～）

②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