CATEGORY

スマート社会

個人研究

研究者紹介

コンピュータサイエンス学部

教授　布田裕一

主な学会発表
論文・著書・社会活動

【1】Ryo Tokuyama, Yuichi Futa, Hikofumi Suzuki, Hiroyuki Okazaki, "Virtual Environment for Analysis and Evaluation of DDoS Attacks", INTRICATE-SEC-2021, Proceedings of the 35th International Conference on Advanced Information Networking and Applications (AINA-2021), Springer, 459-468, 2021

【2】Mieno Takehiko, Yoshimura Togo, Hiroyuki Okazaki, Yuichi Futa, Kenichi Arai, "Formal Verification of Merkle-Damgård Construction in ProVerif", The International Symposium on Information Theory and Its Applications (ISITA) 2020, 2020.

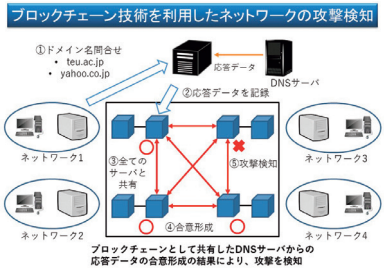
https://www.teu.ac.jp/info/lab/project/com/dep.html?id=178

安全なネットワークやシステムの構築

KEYWORDS　情報セキュリティ、ネットワークセキュリティ、暗号技術

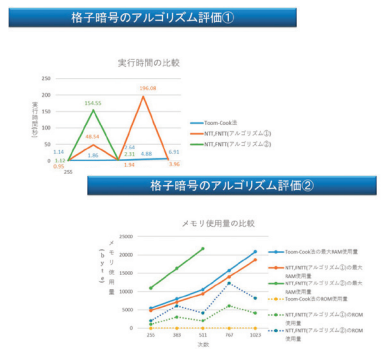
ネットショッピングをはじめとしたWebサービスや、自動車、工場などの様々なシステムにおいて、情報セキュリティの脅威が高まっています。
これらに対抗するために、ネットワーク、クラウドやブロックチェーンのセキュリティ技術や、暗号理論・方式など幅広く研究しています。

01 ネットワークとブロックチェーンの融合



インターネットの通信では、ネットワークの関連情報を取得しながら、データを送信しています。ネットワークに不正な情報が流れてしまうと、クレジットカードのデータや個人データが攻撃者に送られてしまい不正に使用される可能性があります。そこで、ブロックチェーンの基盤とする分散ネットワークや、情報の信頼性を向上させる合意形成を使用し、ネットワークの攻撃を検知します。具体的には、DNSサーバからの応答データをブロックチェーンとして各サーバ間で共有し、合意形成を用いて、DNSキャッシュポイズニング攻撃を検知します。この他に、DDoS攻撃の対策や、工場などの制御システムの攻撃検知も研究しています。

02 暗号方式やアルゴリズムの設計



インターネットで使用される暗号通信SSL/TLSでは、公開鍵暗号やディジタル署名を用いていますが、多くのメモリや処理時間が必要となります。
そこで、メモリ量や処理時間を軽減するアルゴリズムを研究しています。
特に、最近、注目されている格子暗号のアルゴリズムに取り組んでいます。
この他に、ブロックチェーンなどで使用する暗号方式やプロトコルの安全性評価を実施しています。

想定される活用例、相談可能な分野

■ 研究成果は、機器やシステムの暗号通信に適用できます。
■ 機器やシステムのセキュリティ評価のサポートができます。

東京工科大学　実践研究推進課　https://www.teu.ac.jp/karl/〒192-0982　東京都八王子市片倉町1404-1