2023 年度年次報告書
社会変革に向けた ICT 基盤強化
2021 年度採択研究代表者

照屋 唯紀

産業技術総合研究所 情報・人間工学領域
主任研究員

プライバシ保護メカニズムデザインのための秘密計算技術

研究成果の概要

複数のユーザがそれぞれの入力値を持ち、秘密計算プロトコルを実行してそれぞれの入力値を秘匿しながら計算し、その結果に基づいて意思決定を行う際、秘密計算で処理するデータを改ざんし、本来のものとは異なる計算結果を出力させることで、不当な意思決定を行わせる攻撃を考えることができる。なお、改ざんなど、プロトコルに従わない振る舞いをする攻撃者を Malicious 攻撃者と呼ぶ。秘密計算を利用して意思決定を行う際、不当な意思決定がなされないように Malicious 攻撃者に対して安全な秘密計算プロトコルを利用することが望ましい。しかし、これまでに多数報告されている効率的な秘密計算プロトコルは、Semi-honest 攻撃者に対して安全なプロトコルであり、その安全性概念では改ざん攻撃を防げない。本研究では、Semi-honest 攻撃者に対して安全かつ効率的な秘密計算プロトコルを元に、その効率性をできるだけ失うこと無く Malicious 攻撃者に対して安全な秘密計算プロトコルに拡張する方法について研究を行い、その構成方法や安全性の証明、高速に計算を行うためのアルゴリズムやその実装方法について検討した。特に、通信コストの観点で効率的な秘密計算プロトコルを構成する部品として利用されている関数秘密分散方式に注目し、この技術を利用した際の拡張方法や応用プロトコル、その高速実装法について検討を行い、これらについて一定の知見を得た。

また、本研究では、効率的な秘密計算システムの実装を支援する技術として、隔離実行環境(TEE)とリモートアテステーション(RA)についても研究を行った。その結果、TEE と RA の実装の一つである SGX について、ECDSA Attestation を利用して、信頼できないノードに対して検証サービスを安全に委譲する方法を提案した [1]。これにより、例えば、RA の実行が大量に必要となった場合、提案法を適用することで、RA の検証サービスの負荷分散を容易に行うことが期待できる。

【代表的な原著論文情報】

1) 矢川 嵩、照屋 唯紀、須崎 有康、阿部 洋丈, TEE を利用した Remote Attestation の検証委任プロセスの提案, SCIS 2024, 3B5-1, pp.1-7, 2024