論文 / 著書情報
Article / Book Information

題目(和文)	分散型秘匿 RAM および秘匿データ構造に関する研究
Title(English)	A Study on Distributed Oblivious RAM and Oblivious Data Structure
著者(和文)	市川敦謙
Author(English)	Atsunori Ichikawa
出典(和文)	学位:博士(工学), 学位授与機関:東京工業大学, 報告番号:甲第12705号, 授与年月日:2024年3月26日, 学位の種別:課程博士, 審査員:尾形 わかは,植松 友彦,山田 功,松本 隆太郎,田中 圭介,安永 憲司
Citation(English)	Degree:Doctor (Engineering), Conferring organization: Tokyo Institute of Technology, Report number:甲第12705号, Conferred date:2024/3/26, Degree Type:Course doctor, Examiner:,,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	審査の要旨
Type(English)	Exam Summary

（博士課程）

論文審査の要旨及び審査員

報告番号	甲第　　号		学位申請者氏名		市川 敦謙	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	尾形わかは	教授	審査員	田中圭介	教授
	審査員	植松友彦	教授		安永憲司	准教授
		山田功	教授			
		松本隆太郎	教授			

論文審査の要旨（2000 字程度）

本論文は，「A Study on Distributed Oblivious RAM and Oblivious Data Structure (分散型秘匿 RAM および秘匿データ構造に関する研究)」と題し，英文 7 章より構成されている．

第 1 章「Introduction (はじめに)」では，データを暗号化したまま統計分析など様々なデータ処理を可能とするマルチパーティ計算(multiparty computation, MPC)が近年注目を浴びているが効率の面で課題があることを紹介し，MPC の効率化のためには，計算モデルの一つであるランダムアクセスマシン(random access machine, RAM)の動作を秘匿できる秘匿 RAM(Oblivious RAM, ORAM)が活用可能であり，特に分散型のシステムモデルを持つ Distributed ORAM (DORAM)が MPC と親和性が高いこと，しかしながら既存の DORAM は効率面の欠点を有することを述べたうえで，効率的かつ安全性の高い DORAM を設計することを本研究の主目的とすることを説明している．また，ORAM の派生技術である秘匿データ構造(oblivious data structure, ODS)を紹介し，特に秘匿優先度付きキュー(oblivious priority queue, OPQ)について，既存手法の持つ課題を述べている．その後，本研究では DORAM と OPQ に対し新たな手法を提案していることを説明し，既存手法と比較を行うことで効率や機能の面で優位性を持つことを述べている．

第 2 章「Preliminaries (準備)」では，本論文を通して用いる記法や定義，また本論文の提案手法を構成するための暗号学的プリミティブを説明している．

第 3 章「Efficient Passively Secure Distributed Oblivious Hashing (効率的な受動的安全の分散型秘匿ハッシュ法)」では，DORAM を構成するための重要な要素である分散型秘匿ハッシュ法の効率化を行っている．まず秘匿ハッシュ法に求められる要件を定義し，新規に効率的な秘匿置換プロトコルを提案することにより，求められる要件を満たす秘匿ハッシュ法の構築を行っている．提案する秘匿ハッシュ法は，入力データ数が少ない場合と多い場合のそれぞれで構築方法が異なるが，特にデータが多い場合には効率を最適化することができる．

第 4 章「Optimal DORAM against Passive Adversaries (受動的攻撃者に対する最適 DORAM)」では，前章にて提案した秘匿ハッシュ法を利用して，受動的な攻撃者に対して安全，かつ理論的に最適な効率を持つ新規の DORAM を提案している．本提案手法はアルゴリズムのステップ数を削減することで，理論的最適性と同時に実用的な効率も向上させており，理論・実用の両面で既存手法より高速である．

第 5 章「Security Extension against Active Adversaries(能動的な攻撃者に対する安全性拡張)」では，前章で構築した DORAM の安全性を向上させ，能動的な攻撃者に対しても安全である拡張方式を提案している．本章では，初めに能動的安全性を達成するための基本的なフレームワークを説明した上で，前章で構築した DORAM に単純に既知のフレームワークを適用するのみでは必要な安全性を達成できないことを示している．次に，その安全上の課題となった秘匿置換プロトコルおよび秘匿ハッシュ法について，能動的な攻撃を防ぐためのアイデアを示した上で具体的な攻撃検知方法を提案し，これを踏まえて能動的安全性を持つ秘匿ハッシュ法を構築すると共に，ハッシュ法における攻撃検知が置換プロトコルの安全性も間接的に担保することを示している．最後に，当秘匿ハッシュ法を用いた能動的安全 DORAM の構成を概説している．この安全性の拡張において，DORAM 上で扱う個々のデータに対して攻撃検知のための補助情報を付加する必要があるためデータサイズが大きくなるが，1 回のデータの読み書きをシミュレートするために必要なデータ操作回数は受動的安全な DORAM から増加することなく，安全性の向上を達成している．

第 6 章「Perfectly Secure Oblivious Priority Queue (完全秘匿性を持つ秘匿優先度付きキュー)」では ORAM の派生概念の 1 つである OPQ について，既知の最新手法と比較し，提供する機能と安全性の面で優れた新しい方式を提案している．これまでもいくつかの OPQ が知られているが，通常の優先度付きキューと同等の機能を持つ方式は完全秘匿性を持たず，安全完全秘匿性を持つ方式は機能面で制限があった．本論文で提案する新たな方式は，完全秘匿性と，通常の優先度付きキューと同等の機能を両立する初めての方式である．

第 7 章「Conclusion (まとめ)」では，本論文の成果を要約している．

以上を要約すると，本論文は，効率や安全性において優れる DORAM および OPQ の構築方法について論じたものである．本論文で提案された手法は実用的なマルチパーティ計算，ひいては安全なデータ利活用に資するものであり，工学上貢献するところが大きい．よって我々は，本論文が博士（工学）の学位論文として十分価値があるものと認める．