論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Cryptographic Credential Schemes and Their Applications in Contact Tracing
著者(和文)	WangPengfei
Author(English)	Pengfei Wang
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第12832号, 授与年月日:2024年9月20日, 学位の種別:課程博士, 審査員:田中 圭介,伊東 利哉,尾形 わかは,鹿島 亮,安永 憲司
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第12832号, Conferred date:2024/9/20, 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

別　　紙　1（論文博士）

論文審査の要旨及び審査員　　（2000字程度）

報告番号	乙 第　　号	学位申請者	Pengfei Wang	
論文審査員	氏　　名	職　　名	氏　　名	職　　名
	主査　田中 圭介	教授	安永 憲司	准教授
	伊東 利哉	教授		
	尾形 わかは	教授		
	鹿島 亮	准教授		

本論文は「Cryptographic Credential Schemes and Their Applications in Contact Tracing（クレデンシャル方式と接触者追跡におけるその応用）」と題し、英文全6章からなる。

COVID-19の流行により世界の国々で接触者追跡システムが導入され利用されていた。しかしながらこれらシステムは、空気感染を無視することや、秘匿性と完全性に欠けることなど、多くの問題点も抱えていたことが現在ではわかっている。本研究ではこれら問題点を解決するために暗号学的構成要素であるクレデンシャル方式に注目し、これをベースに新たな接触者追跡システムを提案する。さらにこれとは異なる利点をもつ別の接触者追跡システムも提案する。

第1章「Introduction」では、研究の背景と動機を述べ、研究成果の概要を紹介する。これまでにわかっている接触者追跡システムの主要な問題点に対処するために本研究では、コミットされた記録に属性を埋め込みでき、二つの感染モード（空気感染、飛沫感染）をもち、ユーザが独立して追跡を行うことができるシステムを考察する。さらに本研究では、システムの秘匿性、完全性や、スケーラビリティについても考察する。これら考察に基づき、本論文では監査可能な属性ベースのクレデンシャル方式とその応用として環境適応型接触追跡システムを提案する。これに加え、異なる利点をもつ別の接触者追跡システムも提案する。

第2章「Preliminaries」では、本論文で使用する表記と、疫学研究で議論されている環境要因についての物理学的な簡単な説明を与える。この章では、それぞれの環境要因がウイルスの拡散に影響を与えるかどうか、またその影響をどのように計算できるかについて紹介する。なお、本論文の目的は空気力学や疫学ではないため、各疫学的機能がなぜ、どのように働くのかについては触れない。ただしこれらの要因を測定する方法については簡単に触れている。

第3章「Cryptographic Assumptions and Building Blocks」では、システムの種々の動作条件について述べたのち、提案方式の暗号学的構成要素について述べる。ここでの主要な構成要素はBoneh-Lynn-Shacham署名とStructure-Perserving Signature on Equivalent Classesである。また安全性証明を行う際に必要となるDiffe-Hellman計算仮定とそのバリエーションの説明を行なっている。

第4章「Our New Functionalities to Anonymous Credentials」では、完全性確保と秘匿性保護のジレンマを解決するために監査可能な公開鍵利用方式をまず提案する。この方式をBoneh-Lynn-Shacham署名やStructure-Perserving Signature on Equivalent Classesと組み合わせる方法についても述べ、その組み合わせによるクレデンシャル方式の提案を行なっている。

第5章「The Enhanced Contact Tracing Frameworks」では、環境適応型接触追跡システムを提案する。このシステムは前章のクレデンシャル方式に基づいており、Boneh-Lynn-Shacham署名と更新可能な公開鍵メカニズムを用いて構築されている。このシステムにより環境要因を利用してスキャン結果をフィルタリングし誤検出率を下げることが可能であることを述べている。さらに異なる利点をもつ別の接触者追跡システムも提案する。この後者のシステムは極力、非対話で行うものでありゼロ知識証明などの要素も使わない。安全性としては前者よりやや劣るものの効率性に優れる。

第6章「Conclusion」では、本論文の動機、二つの接触者追跡システムについての長所と短所をまとめ、本暗号方式が今後の疫病対策において、プライバシーの向上と効率化に貢献できることを述べている。

以上のように、本論文はクレデンシャルに対してモデルと具体的方式の提案、さらに接触者追跡に対してモデルと秘匿性を保ちつつ完全性も確保する具体的方式の提案など多くの知見を与えており、理学上貢献するところ大である。よって、本論文は博士(理学)の学位論文として十分価値があるものと認める。