論文 / 著書情報
Article / Book Information

題目(和文)	アドホックグループ上の匿名認証
Title(English)	Anonymous Authentication over Ad-Hoc Groups
著者(和文)	原啓祐
Author(English)	Keisuke Hara
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11712号, 授与年月日:2022年3月26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11712号, Conferred date:2022/3/26, 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		原　啓祐	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	田中　圭介	教授	審査員	安永　憲司	准教授
	審査員	伊東　利哉	教授			
		尾形　わかは	教授			
		鹿島　亮	准教授			

論文審査の要旨（2000 字程度）

本論文は「Anonymous Authentication over Ad-Hoc Groups（アドホックグループ上の匿名認証）」と題し、英文で全７章から構成されている。

近年、SNS などを通して個人がインターネット上に情報を発信することが多くなり、インターネット上で個人の匿名性を保証することは、情報化社会における個人の発言の自由を保護するために重要である。その一方で、個人に対して無制限な匿名性を与えてしまうことは、逆に無秩序をもたらし、サイバー犯罪を増長させてしまう恐れもある。よって、ユーザの匿名性と否認不可性の両立を維持することは重要である。 本論文では、このような現代におけるユーザの匿名性と否認不可性の問題を同時に解決するための代表的な暗号技術である ring signature 及び (deniable) ring authentication に対する安全性や効率の様々な改良に成功している。

第 1 章「Introduction」では、本論文の導入として、論文全体の概要について述べるとともに、研究対象とする二つの暗号技術 ring signature と (deniable) ring authentication に関するこれまでの研究を振り返り、その概要を紹介している。そして、本論文で示される三つの各成果について各研究成果に対する背景と動機を明らかにしている。

第 2 章「Preliminaries」では、本論文で用いられる表記の導入に始まり、第 4 章～第 6 章で示される各提案方式を構成する際に必要となる暗号学的な要素技術の導入を行っている。

第 3 章「Formal Definitions of Ring Signature and Deniable Ring Authentication」では、本論文の研究対象である ring signature と deniable ring authentication の導入を行っている。

第 4 章「A Ring Signature Scheme with Unconditional Anonymity in the Plain Model」では、第一の成果として、人工的な仮定や第三者によるセットアップを仮定しない Plain Model において，情報理論的な匿名性を満たす標準的な仮定に基づくリング署名の提案を行っている。具体的に、このリング署名方式は、learning with errors (LWE) 仮定という格子上で定義される最も標準的な仮定に基づき構成可能である。

第 5 章「A Tightly Secure Ring Signature Scheme in the Plain Model」では、第二の成果として、安全性の根拠とする困難性問題に対してタイトな帰着をつけることができるリング署名方式を、Plain Model において提案することに成功している。この提案方式は、双線形写像群上の標準的な困難性仮定の一つである Decision Linear (DLIN) 仮定の下で安全であることが証明されている。

第 6 章「Round-Optimal Deniable Ring Authentication in the RO Model」では、第三の成果として、ランダムオラクルモデルの下で、任意の放送型暗号方式を deniable ring authentication に変換する一般的な手法を提案している。この変換手法を用いることにより、2 ラウンドの通信回数しか必要とせず、各通信量や計算量が最適である、concurrent deniability を満たす deniable ring authentication の提案に成功している。

第 7 章「Conclusion and Future Work」では、本論文の総括と、今後の課題について述べている。

以上のように、本論文は匿名性を持つ署名と認証である，ring signature と (deniable) ring authentication に対して、安全性の強化や効率の向上などを達成した様々な方式の提案、さらにはそれらの提案方式に対する各種のモデルにおける数学的な安全性証明を与える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。

注意：「論文審査の要旨及び審査員」は、東工大リサーチリポジトリ(T2R2)にてインターネット公表されますので、公表可能な範囲の内容で作成してください。