論文 / 著書情報
Article / Book Information

題目(和文)	グループ署名に関する種々の研究
Title(English)	Studies on Group Signature
著者(和文)	石田愛
Author(English)	Ai Ishida
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10755号, 授与年月日:2018年3月26日, 学位の種別:課程博士, 審査員:田中 圭介,渡辺 治,鹿島 亮,伊東 利哉,尾形 わかは
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第10755号, Conferred date:2018/3/26, 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		石田　愛	
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	渡辺　治	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「Studies on Group Signature（グループ署名に関する種々の研究)」と題し，英文9章よりなる．

利用者の個人情報を守る観点から，さまざまな暗号システムにおいて匿名性が求められている．匿名性が考慮された暗号システムの1つとしてChaumとvan Heystによって提案されたグループ署名がある．グループ署名において，グループに登録されたユーザは署名を匿名で作成することが可能である．より詳細には，検証者は署名がグループに登録されているユーザによって生成された署名であるかどうかを確認できるが，グループ内のどのユーザよって生成された署名であるかは知ることができない．しかしながら管理者のみは，署名から署名者を特定することが可能である．本論文では，グループ署名に対して様々なアプローチによる研究を行っている．

第1章「Introduction」では，本研究の背景，目的および成果の概要を述べている．

第2章「Preliminaries」では，本研究の内容を述べるために必要な定義や仮定を説明している．

第3章「Static Group Signature」では，グループ署名のモデルの一つについて述べている．ここで紹介するモデルは，鍵のセットアップが行われた以降はグループにユーザを追加できないモデルである．また，本章では，このモデルにおいて安全なグループ署名方式を構成するための一般的な構成手法であるBerllare-Micciancio-Warinschi構成も紹介している．

第4章「Dynamic Group Signature」では，ユーザを動的に追加可能なモデルを紹介している．また，このモデルにおいて安全な方式としてGroth方式を紹介している．

第5章「The Minimal Assumptions of Group Signature」では，グループ署名が存在するための最低限の仮定について議論している．より詳細には，完全匿名性を満たすグループ署名が存在するための仮定とセルフレス匿名性を満たすグループ署名が存在するための仮定を議論し，それら2つのグループ署名の理論的な違いについて述べている．

第6章「Group Signature with Verifier Local Revocation」では，失効機能付きグループ署名の一種である，検証者ローカル失効機能付きグループ署名について述べ

ている．具体的には，まず初めに検証者ローカル失効機能付きグループ署名のモデルについて定義し，その後，完全匿名性を満たす検証者ローカル失効機能付きグループ署名方式を提案している．特に，本論文では，達成する機能性と用いる要素技術によって，3 種類の方式を提案している．

第 7 章「Group Signature with Deniability」では，否認機能を持ったグループ署名（否認可能グループ署名）について述べている．否認機能は，管理者が，あるユーザが署名を作成していないこと，の証明を実際の署名者は明かすことなく生成することのできる機能である．本章では，まず，否認可能グループ署名のモデルについて述べ，その後，一般的構成の方法と具体的な方式の提案を行っている．最後に，関連する暗号学的要素技術を紹介している．

第 8 章「The Standardized Group Signature Scheme」では，国際標準 ISO/IEC 20008-2 に記載されているグループ署名方式である Mechanism 6 について安全性解析を行っている．より詳細には，まず，Mechanism 6 で主張されている安全性（強匿名性）を満たさないことを，具体的な攻撃を提示することにより証明している．次に，Mechanism 6 の満たす安全性を見い出すための考察を行い，本論文で提案する弱匿名性を満たすことを示す．最後に，強匿名性を満たすパッチ方式も提案している．

第 9 章「Conclusion」では，本研究の成果についてまとめ，今後の研究課題について述べている．

以上をまとめると，本論文は，グループ署名に対して，様々な理論的アプローチから研究を行っている．特に，検証者ローカル失効機能付きグループ署名における強い安全性を満たす方式の初めての達成やグループ署名に対する新しい機能の提案は，今後のグループ署名分野の研究への発展性は高い．また，国際標準グループ署名方式に対する安全性解析は，社会的にも大きな意味を持つ成果である．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．