論文 / 著書情報
Article / Book Information

題目(和文)	集約署名の研究
Title(English)	Studies on Aggregate Signature
著者(和文)	手塚真徹
Author(English)	Masayuki Tezuka
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11711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11711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		手塚 真徹	
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「Studies on Aggregate Signature（集約署名の研究）」と題し，英文で全５章から構成される．

論文は大きく分けて二つの結果を含む。一つめの同期集約署名では，同じ期間に作成された複数の署名を一つの集約署名に圧縮することが可能である．膨大な数の機器がインターネットで繋がる IoT システムでも通信の真正性を保証するために電子署名は重要であり，同期集約署名を用いることで署名の保存容量を削減することができる．これまでに最も効率のよい同期集約署名方式は Le, Lee, Yung により提案され，安全性は対話型計算仮定により証明されており，これは欠点と考えられる．本論文ではこれに対し，非対話型計算仮定を用いた安全性証明に成功している．

二つめの消去署名では署名されたメッセージに対し，一部分を消去したメッセージに対する署名を署名鍵なしに更新することが可能である．この署名を用いることで個人情報などの秘密情報が含まれる署名された文書から，秘密情報を取り除いた文書の署名を生成できる．しかし，従来の消去署名では消去すべきでないメッセージの情報があるにもかかわらず，単独で消去できてしまう欠点がある．そこで本論文では，消去権限を分散できる t-out-of-n 消去署名方式を新たに提案し，集約署名を用いた消去署名を基に構成している．

第１章「Introduction」では論文全体の成果の概要を述べ，論文の構成を示している．

第２章「Preliminaries」では共通する双線形群や電子署名などの基本的な概念を説明している．

第３章「Synchronized Aggregate Signature」ではまず，同期集約署名の背景と最も効率の良い同期集約署名方式，その構成の元となった Camenisch-Lysyanskaya(CL)署名方式について説明している．つぎに，同期集約署名の定義と同期集約署名の特殊なモデルである Certified-Key Model での偽造不可能安全性について導入した後，Pointcheval と Sanders により提案された Modified Camenish-Lysyanskaya (MCL)署名方式とその方式の偽造不可能性が非対話型の計算仮定で証明された結果について説明している．また，Lee, Lee, Yung により提案された最も効率のよい同期集約署名方式の構成について説明している．その後，MCL 署名の偽造不可能性から Lee らの同期集約署名の偽造不可能性の証明を行なっている．その証明手法で重要な役割を果たす MCL 署名から Lee らの同期集約署名の変換手法についても説明している．この変換方法は Lee らの CL 署名から Lee らの同期集約署名への変換法を参考にしているが，この変換方法を直接 MCL 署名から Lee らの同期集約署名に用いることができない．そこで新たに MCL 署名から Lee らの同期集約署名の変換方法を提案している．さらに，MCL 署名の偽造不可能性から Lee らの同期集約署名の安全性証明を示している．この MCL 署名が非対話型の計算仮定を用いていることから，Lee らの同期集約署名が非対話型の計算仮定のもとで安全性証明可能であることを示している．

第４章「T-out-of-N Redactable Signature」ではまず，消去署名の背景と従来の消去署名の問題点について説明し，新たに提案する t-out-of-n 消去署名の概要について説明し，そのモデルと安全性の提案を行っている．つぎに，Boneh, Gentry, Lynn, Shacham により提案された集約署名と Shamir により提案された秘密分散を組み合わせることにより t-out-of-n 消去署名の構成を与えている．この構成では署名者の秘密情報である署名鍵に対し Shamir の秘密分散を用い n 個のシェアを生成する．生成されたシェアを n 人の消去者にそれぞれ一つずつ委託する．消去者は委託されたシェアの情報を用いてメッセージの一部分の消去を可能にする補助情報を生成することができる．署名されたメッセージの一部分を消去するときには，その消去したい部分に該当する補助情報を t 個以上集めることにより，該当のメッセージ部分が消去できることを利用し，メッセージ消去の権限分散を実現している．また，構成した方式に対し安全性証明を与えている．

第５章「Conclusion」では論文全体のまとめと今後の課題について述べている．

以上をまとめると，本論文で同期集約署名方式に関する安全性証明の改良，消去権限が分散できる新たな消去署名の提案や集約署名と秘密分散の技術を組み合わせた方式の構成など，集約署名技術に関する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。