審査の結果の要旨

論文提出者氏名　　繁富　利恵

本論文は,「Anonymous Authentication Techniques for Finite State Multi-Transactions（多重トランザクション向け匿名認証技術に関する研究）」と題し,ユーザ自身が自分のプライバシ情報を管理できる匿名技術の一つとして匿名認証に着目し,「リフレッシャブル匿名トークン方式」という新しい匿名認証方式の提案を行ったものである．これは，匿名で認証を行う際，トークンとよばれる認証のための権利証を介して認証を行う方式である．このような権利証を介する技術は種々提案されているが，本論文の方式は，トークンが更新(リフレッシュ)できるという点に高い新規性を持っている．ここでは，更新の概念を明確にし，その安全性要件を定義し，本提案方式がそれを満たしていることを証明している．また，本匿名認証方式は，投票や決済など既存のサービスを電子化した際のプライバシ保護に有効であるばかりでなく，電子社会における新たなプライバシ問題である履歴情報のプライバシ侵害についても有用であることが示されている．さらに，このような観点も含め，この技術の利用方法や適用例を複数示し，実装可能性についても実証的に示している．論文の構成は「Introduction」を含めて５章からなる．

第１章は「Introduction(序論)」で，本研究の背景を明らかにした上で，研究の動機と目的について言及し，研究の位置付けについて整理している．

第２章は「Refreshable Anonymous Tokens(リフレッシャブル匿名トークン)」と題し，本論文で提案する新技術である リフレッシャブル匿名トークン方式について基本原理を概括し，安全性証明を行っている．これは，部分的ブラインド署名の応用であるため，それらの基本技術の説明および安全性定義を行い，次いで提案技術の三つの安全性要件である①匿名性，②偽造不可能性および③追跡可能性を定義し，本方式がそれらを満たすことを証明している．これにより，安全性を保証したまま権利の更新を行える方式が，初めて提示された．

第３章は「Applications(応用例)」と題し，前章において提案した技術の適用例を複数示している．ここでは，まず，複数の具体例を挙げ，権利確認手段であるトークンの授受に対し更新技術をいかに利用するかを説明し，様々な場合に提案技術が利用可能であることを示している．たとえば，この技術により，同時処理数を制限した複数のトランザクション管理が可能となる． このようなトランザクションが絡む例として，特に外貨交換，掲示板システム，匿名貸し出しプロトコルに関しての安全性定義および安全性証明を行い，これらに対し

更新を利用したプロトコルの提案を行うことによって，リフレッシャブル匿名トークン方式の応用範囲の広さを示している．

第４章は「Implementation(実装)」と題し，前章で提案した技術の実装方法について述べている．特に，匿名性を保ったまま実装することの困難性と実現可能性について詳細な検討を行い，実装に活かしている．また，この実装を利用するためのトークン伝達手段の一つとして二次元バーコードを利用する方法を説明し，この場合でも匿名性などの安全性要件が満たされることを証明している．

最後に第５章は「Conclusion（結言）」で，本研究の総括を行い，併せて将来展望について述べている．

以上これを要するに，本論文は，新たな匿名認証を実現した暗号プロトコル「リフレッシャブル匿名トークン方式」の提案を行い，安全性を証明するとともに，その応用範囲を具体的に示し，さらに実装可能であることを実証的に示したものであり，電子情報学，特に情報セキュリティ工学上貢献するところが少なくない．

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる．