論文の内容の要旨

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）

氏名　繁富 利恵

現在，急速にサービス提供において情報の電子化が進んでいる．こういった電子情報は，情報の収集・検索や統合などが容易となるため，蓄積情報つまり履歴情報に対する配慮がより重要となっている．特に履歴情報は，個人を特定する情報だけではなく，個人の趣味指向や生活レベルさえも推測できるような情報を含んでいるため，ユーザのプライバシを浸食する大きな問題となっている．それらを解決するために匿名性を保証した暗号プロトコル技術があり，様々な匿名に関する技術が提案されている．これらの技術の中において，利用者の権利確認を行うことができる匿名認証技術に注目が集まっている．

従来の匿名認証技術は，トランザクションのはじめに権利確認を行うものであった．これは，サービスを提供する手前で権利確認を行うことにより，サービス提供可能の有無を確認するためのものである．しかしながら，これでは，あるユーザに対してサービスをあるその時点で終わったかどうかの確認ができず，全てのサービスに対して十分とは言うことができない．例えば，複数回利用可能なサービスの場合，ある同一のユーザが一度に全ての権利を利用することが可能となるため，サービス提供者の管理を行うことが困難となる．この問題を解決するため，我々は "refreshing" をいう手法を提案する．

この技術は，匿名性を保証しているが権利確認をすることができる token という権利証明書を refresh，つまり，更新をすることができるものである．この token の中にはサービス提供者に見ることができないユーザの ID が埋め込まれており，更新後も同じ ID が含まれていることを確認することができるが，サービス提供者には見ることができない．また，この ID は何らかの不正利用があった場合にのみ，特定される．これらの token は unlinkability を保証している．

この refresh を利用することにより，下記のことを実現することができる：

- 数制限が可能
  並列の数制限が可能となる．これは，図書館などにおいて本を返却後に権利を更新することを利用して，冊数制限などを行うことができる．
- 権利交換
  権利変換や変換後の数の変更が可能となる．これにより，外貨交換などにおいて変換後に日本円から米ドルへの変換ができ，変換において数の変更も可能となる．
- 権利剥奪
  条件を満たさないことにユーザに対しては，refresh を行わないことによって匿名性を保ったままユーザから権利を剥奪することも可能である．これは，匿名の掲示板などにおいて一度悪いことをした場合に権利更新を行わないことによって権利の剥奪を行うものである．

また，refresh 手法を利用し，ユーザが認めた場合にのみ、サービス提供者が匿名性を保ったまま token の 関連性をつけることのできる方式にも対応している．

すなわち，この Refreshable Tokens という手法は，ユーザのプライバシを保ちながらサービス提供者の管理をより複雑にすることが可能となり，応用範囲が広がる匿名認証技術である．本博士論文では，Refreshable Tokens を提案し，安全性などを定義しスキームを構成する．また，応用範囲を説明するために，応用例を列挙する．特に，匿名掲示板，外貨交換および匿名貸し出しについて詳しい説明を行う．