第５号様式

論文審査の要旨

博士の専攻分野の名称	博　士　（　工学　）	氏　名	Shahidatul Sadiah Binti Abdul Manan
学位授与の要件	学位規則第４条第[1]・２項該当		

論　文　題　目

A Study on Privacy-Enhancing User Authentication Systems with Efficiency Improvements

(プライバシーを保護したユーザ認証システムの効率改善についての研究)

論文審査担当者

主　　査	教　授	中西　透	印
審査委員	教　授	藤田　聡	印
審査委員	教　授	岩本　宙造	印

〔論文審査の要旨〕

ユーザ認証におけるプライバシーを保護するために，匿名属性認証やグループ署名などの匿名認証技術が盛んに研究されている．しかし，従来提案されている方式では，計算時間や通信データサイズの面で効率的とはいえず，実用化に問題があった．本論文(本研究)では，効率的な匿名認証方式を提案し，その実装により実用性を示すことを目的とする．

第１，２章では，上述の問題の背景の説明と，提案方式で利用する暗号技術について導入を行なっている．

第３章では，匿名属性認証について，モノトーン論理式を検証可能なアキュームレータ方式を構築することにより，論理式のサイズが増大したときに，従来方式よりも効率的に認証可能な匿名属性認証システムを提案している．また，ベースとなるペアリング計算の高速ライブラリを使用して，提案システムの認証処理の実装を行ない，通常の PC 環境で，年齢認証の実用的な例において，従来方式よりも十分に高速な時間で認証できることを確認している．

第４章では，ユーザを失効可能なグループ署名について，従来方式よりも失効リストサイズが削減された方式を提案している．失効リストは署名時に常に取得する必要があるため，通信時間が大きく軽減される．第５章では，提案グループ署名方式を PC 上で実装して失効リストサイズの軽減を確認するとともに，処理時間のオーバヘッドが実用的な範囲に収まっていることを確認している．

最後に，第６章で提案手法の意義と今後の課題についてまとめている．

口頭試問において，審査委員から，性能評価の妥当性や，提案方式の意義，方式構築の直感的アイデアなどについて詳しい説明を求められ，申請者はそれぞれに対し，的確かつ丁寧に回答することができていた．

以上，審査の結果，本論文の著者は博士（工学）の学位を授与されるに十分な資格があるものと認められる．

備考：審査の要旨は，1,500 字以内とする。