【117】

氏　名（国籍）	王（おう）　立華（りつか）（中　国）
学位の種類	博　士（工　学）
学位記番号	博甲第3949号
学位授与年月日	平成18年3月24日
学位授与の要件	学位規則第4条第1項該当
審査研究科	システム情報工学研究科
学位論文題目	**Protocol Design and Analysis of Authenticated Cryptosystems** （認証暗号系のプロトコル設計と評価）

主　査	筑波大学教授	工学博士	岡本栄司
副　査	筑波大学教授	Ph. D.（組み合わせ論と最適化）	藤原良叔
副　査	筑波大学教授	工学博士	寅市和男
副　査	筑波大学助教授	博士（理学）	繆　瑩

論文の内容の要旨

本研究では，認証暗号系のプロトコル設計と評価を行った。認証は，情報の完全性を守るための暗号技術であり，正当性を示すべき対象により，メッセージ認証，署名（エンティティ認証），鍵認証などに分けられる。これらの中で重要となるのは，基礎的な認証技術としてAuthentication Code（A-Code）であり，応用としてはユビキタスネットワーク向け分散（multiparty）認証暗号系として認証鍵共有，多重署名および委任暗号である。

まず，情報理論的に安全な認証系として2-Splitting Authentication Code（A-Code）を提案した。次に分散認証暗号系への適用としてInsider Impersonation Man-in-the-Middle Attack（InIm-MIM Attack）に強い効率的な三者間鍵共有方式を提案した。続いて，三者よりも多いユーザを対象とする直並列多重署名の研究を行い，実社会に役に立っIdentity-Based直並列多重署名方式を提案した。更に，ユーザにおける役割が階層構造を持つようなタイプの多重署名暗号系として，委任暗号を扱い権限付Transformation-Free委任暗号系を提案した。これは委任者の代わりに，受任者が権限付きの代理権を行使して，送信者の正当性を検証した上で暗号文を復号できる暗号技術である。これらによりユビキタスネットワークに適した，安全で実用的な認証暗号系プロトコルの設計・評価を行うことができた。

審査の結果の要旨

これからのユビキタスネットワーク社会に適した，安全で実用的な認証暗号系プロトコルの設計・評価を行っている。情報理論的に安全な基礎的方式から，実社会への適用を考慮した方式まで提案しており，新規性・有効性の観点から評価できる。

よって，著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。