審査の結果の要旨

論文提出者氏名　ラーマン・モハマッド・グーラム

本論文は「A Study on Security Aspects of Mobile Communications – Authentication and End-User Security（モバイルコミュニケーションにおける認証と利用者情報保護に関する安全性研究）」と題し，携帯電話などモバイルコミュニケーションにおける認証と利用者のプライバシー保護を中心とする情報セキュリティの問題に関して論じたものである．モバイル環境においては，携帯端末のプロセッサーの能力やメモリに関する制約，帯域の制約，また傍受に対する物理的対策が困難であることなどから，情報セキュリティ対策やプライバシー保護が特に重要となってくる．モバイルコミュニケーションにおいて情報セキュリティを達成するための基本は相手認証（エンティティ認証）である．しかし，一方，この認証によりプライバシーが漏洩する可能性があり，安全なエンティティ認証と利用者のプライバシー保護を両立させ，安心できるモバイルコミュニケーションを実現することは，重要な課題となっている．本論文は，このような課題に対し，有効な解決策を示したものであり，「Introduction」を含め6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「Cryptographic Preliminaries（暗号に関する準備）」と題し，本論文で提案する認証プロトコルで用いられる暗号技術について述べている．

第3章は「Mobile Communications Scenario（モバイルコミュニケーションのシナリオ）」と題し，モバイル環境における情報セキュリティの問題について論じている．

第4章は「Authentication and Key Establishment Protocol（認証と鍵設定プロトコル）」と題し，モバイル環境下でのエンティティの匿名性を実現する相互認証プロトコルを提案している． これは，エンティティの他のドメインへの移動も考慮し，一つのドメイン内の場合とドメイン間に渡る場合の両者について示される．このプロトコルによって，エンティティ同士の間で守秘や文書認証に利用できる暗号鍵を共有することができる．しかも，このプロトコルは他の標準的な方式やこれまでに提案されている方式に比べ安全性が高く，効率のよいプロトコルとなっている． 特に，通信する両エンティティが暗号鍵の決定に同等に関与できるなど，当事者がその役割において対称性を持つこと，また，匿名性や所在地に関するプライバシーが保護されることなどセキュリティ上際立った特長を備えている．

第5章は「End-User Authentication and End-to-End Security（利用者認証と端末間セキュリティ）」と題し，モバイル環境下での利用者認証とそれを組み込んだ利用者間のセキュリティプロトコルを提案している．モバイルコミュニケーション

において利用者認証は基本的に重要である．ここでは，モバイル環境下で匿名性を確保できる利用者認証プロトコルを提案し，ついで前章で述べた相互認証プロトコルとこの利用者認証プロトコルに基づいて，利用者間で安全に暗号鍵を設定するためのプロトコルを提案している．また，このプロトコルの安全性の検証を行い，モバイル環境において，既知のすべての受動および能動攻撃に対し安全であることを示している．

最後に第6章は「Conclusion and Recommendation（結言と提言）」で，本研究の総括を行い，併せて将来の研究課題について提言する．

以上これを要するに，本論文は，モバイルコミュニケーションにおいて，利用者の匿名化などによりプライバシー情報を保護し，しかも利用者間の守秘通信や文書認証のための暗号鍵を安全に設定するための各種のプロトコルを提案し，その安全性を検証したものであり，電子情報工学，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（工学）の学位請求論文として合格と認められる．