# 審査の結果の要旨

論文提出者氏名　　辛 星漢

本論文は「Leakage－Resilient Authenticated Key Establishment Protocols for Secure Channels （情報漏洩に強い認証付き鍵交換プロトコル）」と題し，認証された鍵を共有するためのAKE（Authenticated Key Establishment）プロトコルについて研究を行っている．AKEプロトコルとは,必ずしも安全ではない通信路を用いて相互認証やセッション鍵の生成を提供するための暗号要素技術であり,このプロトコルの実現についてはこれまで非常に多くの研究が行われてきた．しかし，これまで提案されてきた全てのプロトコルは，秘密情報の漏洩が起こり得るような現実的な状況において，安全性を維持することは難しい．本論文では，そのような状況においても安全性を保証できる新しいAKE（Leakage－Resilient AKE, LR-AKE）プロトコルを提案し，その安全性を理論的に証明するとともに，従来のプロトコルと比較して，実運用における有効性を示したものである．論文の構成は「Introduction」を含めて４章からなる．

第１章は「Introduction（序論）」で，AKEプロトコルとは何かを説明した上で，既存研究を認証に使われる情報に応じて分類している．特に，パスワードを用いて認証を行うプロトコルについて詳細にまとめ，以下のような状況では従来のAKEプロトコルの安全性に問題が生じることを示している．

① デバイスに安全に確保されるべき秘密情報が，設計あるいは実装上のミスなどにより漏洩した場合．（なお，耐タンパーモジュールを使用したとしてもこのような危険性をゼロにすることは非常に難しい．）
② パスワードなどユーザが記憶すべき秘密情報が，人が容易に記憶できる程度に短い場合．
③ ユーザが多くの異なるサーバと通信するにもかかわらず，一つのパスワードのみしか利用しない場合．

本章最後に本研究の目的について言及し,提案するLR-AKEプロトコルの位置付けとそれがどのような効果をもたらすかについてまとめている．

第２章は「Diffie-Hellman based Leakage-Resilient AKE Protocol（Diffie-Hellman法に基づくLR-AKEプロトコル）」と題し，鍵交換プロトコルとして初めて提案されたDiffie-Hellmanプロトコルを要素として使うLR-AKEプロトコルの基本原理を示し，その構成法を記述している．その上で，前章で述べた状況で要求される安全性を定義し，提案したプロトコルの理論的な安全性をスタンダードモデルで証明している．さらに情報漏洩に強いLR-AKEプロトコルの拡張方法を示し，その有効性を明確にしている．

第３章は「RSA-based Leakage-Resilient AKE Protocol（RSA法に基づくLR-AKEプロトコル）」と題し，公開鍵暗号のひとつであるRSAアルゴリズムを要素として使うLR-AKEプロトコルの基本原理を示し，その構成法を記述している．その上で，第２章と同じように，提案プロトコルの安全性を理論的に証明している．なお，この証明はランダムオラクルモデルを想定したものである．提案したLR-AKEプロトコルは，既存のプロトコルに比べて，安全性が高いばかりでなく，ユーザ側の計算量が少ないという特長を持っている．

最後に第４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．

本論文で提案されているLR-AKEプロトコルは，ユーザによって記憶されるパスワードと必ずしも安全ではないデバイス上に記録された秘密情報を用いて，サーバとの間に認証されたセッション鍵を構築するものであるが，ユーザの保有する秘密情報のための記録媒体を利用しながらも，その媒体の耐タンパ性，あるいは，公開鍵基盤(PKI)に全く依存しないという優れた特性を有している．ユーザによるデバイスの保持は，保持しない場合より若干強い仮定ではあるものの，①現実環境への導入が極めて容易な点（記憶装置を持つ携帯通信装置を保持しているユーザの設定は，むしろ非常に現実性がある．）②効率のみならず，安全性の意味においても，これまでに提案されてきた方式を凌駕している点，を考慮すると十分受け入れられる仮定であると言える．

以上これを要するに，本論文は，既存のAKEプロトコルにおいて実際的な使用状況で生じ得る秘密情報漏洩に対処し得る新しいAKEプロトコルを提案して，その安全性を証明するとともに，このプロトコルが従来の方式にくらべ効率的でもあることを示したものであり，電子情報学，特に情報セキュリティ工学に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．