論文内容の要旨

論文題目　　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）

氏 名　　辛 星漢

（本文） 認証された鍵を確立するための AKE プロトコル（Authenticated Key Establishment protocol）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基本構成要素である。このプロトコルの実現については、本論文中にも整理されるように、これまでにも非常に多くの研究が行われている。しかしながら、以下のような状況を考慮すると、これまで提案されてきた全てのプロトコルはその安全性について問題が存在することが知られている。

(1) デバイス上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) パスワードなど利用者が記憶すべき秘密情報が、記憶できる程度に短い場合。
(3) 利用者が多くの異なるサーバとの交信に対して、一つのパスワードを利用した場合。

本論文では、このような状況に対しても安全性を保証することができる新しい AKE プロトコルを提案する。このプロトコルは、耐漏洩 AKE プロトコルと呼ばれ、（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。

本方式は、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、

(i) 現実環境への導入が極めて容易な点（記憶容量をも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。）
(ii) 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

についても、提案方式は際立った特徴を有している。本論文では、ユーザによる記録媒体の携帯という非常に小さな負担により、効率と安全性の際立った向上が可能である上記新方式を提案し、その解析についてまとめる。