安全性とプライバシー機能を強化したRFID認証方式の提案

Mohammad Shahriar Rahman(710079)

北陸先端科学技術大学院大学 情報科学研究科

2009年2月5日

キーワード： RFID, セキュリティ, プライバシー, Batch-mode Authentication, Aggregate Hash.

近年, 注目されている情報セキュリティ技術の1つとしてRFID (Radio Frequency IDentification) がある. RFIDとは無線通信を利用した自動識別技術で, タグ, リーダ, データベースの3つの要素から構成される. 認証ではリーダーと呼ばれる受信機が各タグと通信を行い, タグが正当なものであるのかを判別する. 運送業における物品の管理や, 図書館の本管理, 回転寿司のお皿のカウント, 乗車カードなど, 幅広い領域に応用が可能であることから, RFIDに関する研究が盛んとなっている.

RFIDに要求される安全性として, タグの識別不可能性, DoS攻撃耐性, Forward Securityなどがある. タグの識別不可能性とは, リーダとタグの間の認証を2回行なった際に, リーダが1回目の認証相手と2回目の認証相手が同じタグであるかどうかを識別できないことを言う. 仮に識別不可能性が満たされない場合, 例えば洋服に付いているタグと帽子に付いているタグをリンク付けすることで, 持ち主の服装の趣味嗜好という個人情報が漏洩することになる. このタグとリーダー間の認証をリンク付けする攻撃をTrackingと呼ぶ. また, 攻撃者がタグを偽造できる場合, リーダが大量の偽造タグからの通信を扱うこととなり, リーダーの計算資源を圧迫することとなる. この攻撃に対応するのがDoS攻撃耐性である. 通常各タグには個別の秘密情報が埋め込まれており, 認証はこの値を利用して行なわれる. Forward Securityとは, もしタグの秘密情報が漏洩したとしても, 過去に行なった認証に対する安全性が保存されるという性質である. 永久に秘密情報が漏洩しないという仮定は非現実的であり, Forward SecurityはRFIDが満たすべき重要な安全性である.

RFIDを構成する技術として, 様々な暗号化方式が用いられる. 暗号化方式は大きく分けて公開鍵方式と秘密鍵方式がある. 公開鍵暗号方式では, 各ユーザの公開鍵を用いてデータを暗号化し, 公開鍵に対応した秘密鍵を所持しているユーザのみが復号処理を行うことができる方式である. 公開鍵から対応する秘密鍵が計算できないという性質をみたす必要があるため, その構成法は楕円曲線など代数学に依存しており, 一般的に計算量は秘密鍵方式に比べて大きい. 秘密鍵方式では, あらかじめユーザ同士が秘密鍵を共有しており, この共有鍵を用いて暗号化及び復号を行なう方式である. 鍵共有という問題点はあるが, 一

般にその計算量は公開鍵方式と比較して小さいという特徴がある. RFID において, 一般的にタグの計算能力やメモリ量は制限されるため, その構成には秘密鍵方式が主に用いられる. また, ハードウェア実装がよく用いられ, 計算量を評価する指標としてゲート数が用いられる. RFID に対する重要な要請として, タグが安価 (約 10 円程度) であることが挙げられ, そのため実装可能なゲート数としては 2000 ゲート程度に制限される. また, リーダーは大量のタグに対し通信を行なうため, 通信量の削減は大きな課題となっている. また一括認証を行なうバッチ処理 (Batch-mode Authentication) が可能であることが望ましい.

本論文では, 近年提案された RFID 方式についての調査を行なうと共に, 既存方式と比較してリーダーとタグ間の通信量を削減し, バッチ処理によるタグの一括認証が可能な方式を提案する. バッチ処理による一括認証を実現するためにアグリゲートハッシュ (Aggregate Hash) 関数を利用した. また, 本方式はタグの識別不可能性, Dos 耐性, Forward Security を満たす.

今後の課題として, タグに対する鍵配布問題や Backward Security があげられる. Backward Security とは秘密鍵が漏洩したとしてもそれ以降の通信に対する安全性が保たれることをいう. Forward Security と Backward Security を同時に実現することにより, 秘密鍵漏洩に対する強固な安全性を実現することができる.