要 旨

フォワードセキュア RFID プライバシ保護方式

寺尾 良

近年，RFID(Radio Frequency IDentification) システムは，バーコードに代わる商品管理システムだけでなく，書籍等の万引き防止など，様々な分野への利用が可能な基盤技術として注目されている．RFID システムは，無線通信を用いているため，第三者による電波傍受の可能性がある．また，RFID タグに保存されている情報はリーダを用いることで簡単に読み取ることができる．そのため，特定の RFID タグの情報を追跡することにより，RFID タグ所有者の追跡が可能になるというプライバシ問題が懸念されている．既存技術として，RFID タグに複数のセキュリティ機構を搭載することで，プライバシ問題を解決する方式が提案されているが，RFID タグのコストが高くなるという問題がある．本論文では，ハッシュ関数を用いて，RFID タグの ID 情報を毎回変化させることで，RFID タグが持つ秘密情報を盗む等の攻撃手法に対処するだけでなく，少ないセキュリティ機構でプライバシ問題を解決する方式を提案する．

キーワード　RFID，プライバシ，認証，識別不能性，フォワードセキュリティ

Abstract

Forward Secure RFID Privacy Protection Scheme

Ryo TERAO

In these years, radio frequency identification (RFID) systems are expected to be a basic technology which can be used for various fields, for example supply-chain management applications. RFID systems are using a radio communications, so the radio messages may be intercepted. In addition, information preserved in RFID tags can easily read with a RFID reader. Therefore, the RFID tag owner can be traced by pursuing specific information on the RFID tag. The problems are called privacy problems on RFID. This paper proposes a forward secure RFID privacy protection scheme. The scheme protects the privacy problems by encrypting a tag to a different value every time using a hash function. Additionally, the scheme can satisfy the forward secure requirement at low cost. It means that an adversary cannot trace the RFID tag data back through previous events in which the RFID tag was involved even if the adversary acquires the secret data stored in the RFID tag.

key words RFID, privacy, authentication, untraceability, forward security