计算机工程与应用 2007 43 (19): 118-122 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

RFID重加密技术中的一种防置换攻击算法

李章林[1]，卢桂章[1]，辛运帏[2]
1.南开大学 信息技术科学学院 机器人所，天津 300071
2.南开大学 信息技术科学学院 计算机系，天津 300071

收稿日期 修回日期 网络版发布日期 2007-6-20 接受日期

摘要 重加密技术是解决RFID（射频识别）安全问题的一种方法，它周期性地改变标签名以防止标签跟踪。重加密要求标签名可修改，这就使得攻击者可以交换两个合法标签的标签名，形成置换攻击。防置换攻击仍然是重加密中未完全解决的问题，其难点在于防置换攻击时需保持标签匿名性。提出了一种重加密中的防置换攻击算法，在“攻击失效”模型下，实现了防ID置换攻击和公钥置换攻击，并给出了证明。该算法要求标签内增加一个硬件乘法器，目前的RFID芯片水平可实现该要求。

关键词 射频识别 安全 重加密 置换 伪造
分类号

Swapping defending algorithm in RFID re-encryption technology

LI Zhang-lin[1]，LU Gui-zhang[1]，XIN Yun-wei[2]

1.Institute of Robot，College of Information Technical Science，Nankai University，Tianjin 300071，China
2.Department of Computer，College of Information Technical Science，Nankai University，Tianjin 300071，China

Abstract
Re-encryption is an approach for RFID security，which periodically renames the tags in order to avoid tag tracking.Re-encryption demands that the name of tag is rewriteable，so the adversary can swap two valid names of tags，forming swapping attack.Defending swapping attack is still an un-solved problem in re-encryption with the difficulty of keeping anonymity and anti-swapping simultaneously.The paper promotes a swapping defending algorithm in re-encryption under the “attack-invalid” model，and realizes the ID anti-swapping and public-key anti-swapping，and gives proof.The tag requires a hardware multiplier，and it’s applicable with the current RFID chip technology.

Key words Radio Frequency Identification（RFID） security re-encryption swapping counterfeit

DOI:

通讯作者 李章林 E-mail：wzzlin@eyou.com