通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

肖锋,周亚建,周景贤,钮心忻.标准模型下可证明安全的RFID双向认证协议[J].通信学报,2013,(4):82~87

标准模型下可证明安全的**RFID**双向认证协议

Provable secure mutual authenticationprotocol for RFID in the standard model

投稿时间： 2012-08-31

DOI：10.3969/j.issn.1 000-436x.2013.04.009

中文关键词：射频识别 电子标签 认证协议 隐私保护

英文关键词:RFID digital tag authentication protocol privacy protection

基金项目:国家自然科学基金资助项目(60972077, 61121061)；国家重大专项基金资助项目(2010ZX03003-003-01)；北京市自然科学基金项目(9092009)

作者	单位
肖锋，周亚建，周景贤，钮心忻	北京邮电大学 信息安全中心，北京 100876

中文摘要:

目前RFID(radio frequency identification)系统安全问题日益突出，为了实现RFID系统信息安全与隐私保护，在标准模型提出了一个基于HB协议的RFID双向安全认证协议。利用规约技术证明协议的安全性，将攻击者的困难规约到伪随机函数与真正随机函数的不可区分性上。协议仅使用轻量级的伪随机发生器以及向量点乘运算，具有较高的安全性和效率。通过从安全性及性能两方面与其他认证协议进行比较，表明协议适用于低成本及存储资源受限的RFID标签。

英文摘要:

The security issue of RFID is becoming more and more serious, in order to protect the RFID’s information security and privacy, a mutual authentication protocol for RFID based on HB protocol was proposed in the standard model. The security proofs for this novel protocol was given by using the reduction method, and the attacker’s hardness was reduced to the indistinguishability between pseudo-random function and real random function. The implementation of proposed protocol only required lightweight pseudo-random generator and vector dot product operation and provided higher security and efficiency. The comparisons of security and performance were also given with other authentication protocols, the results show that the proposed protocol is feasible for RFID tags which are low cost and resource-constrained.

查看全文 查看/发表评论 下载PDF阅读器

关闭