电子与信息学报 2006 28 (8): 1501-1503 ISSN: 1009-5896 CN: 11-4494/TN

论文

带有基于RSA签名的接入控制的不经意传输协议

赵春明, 葛建华,李新国

西安电子科技大学 通信工程学院 西安 710071

收稿日期 2004-12-6 修回日期 2005-4-28 网络版发布日期 2007-11-27 接受日期

摘要
该文在RSA签名及关于数据串的不经意传输的基础上提出了一种增强的不经意传输协议，解决了一种不经意传输的接入控制问题。除了具备一般不经意传输协议的特征外，该方案具有如下特点：只有持有权威机构发放的签字的接收者才能打开密文而且发送者不能确定接收者是否持有签字，即不能确定接受者的身份。在DDH假设和随机预言模型下该方案具有可证明的安全性。该方案使用标准RSA签名及Elgamal加密。

关键词 Elgamal加密 接入控制 不经意传输 RSA签名 决策性Diffie-Hellman假设

分类号 TP309

Oblivious Transfer Protocol with RSA-Based Access Control

Zhao Chun-ming, Ge Jian-hua, Li Xin-guo

School of Telecommunications Engineering, Xidian University, Xi’an 710071, China

Abstract
Based on RSA signature and (string) oblivious transfer, an oblivious transfer protocol is proposed which solved the access control problem for an oblivious transfer protocol. The protocol proposed has the property: the only receiver who has the signature issued by the central authority can open the message which he chose; the sender can not decide whether the receiver has the signature or not. That is the identity of the receiver can not be confirmed after the protocol. Under the Decisional Diffie-Hellman (DDH) assumption the proposed scheme has provable security. The proposed scheme employs the standard RSA signature and Elgamal encryption.

Key words Elgamal encryption Access control Oblivious transfer RSA(Rivest Shamir Adleman) signature Decisional Diffie-Hellman (DDH) assumption

DOI:

扩展功能

本文信息

- Supporting info
- PDF(223KB)
- [HTML全文](0KB)
- 参考文献[PDF]
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 复制索引
- Email Alert
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“Elgamal加密”的相关文章
- 本文作者相关文章

· 赵春明
· 葛建华
· 李新国

通讯作者	
作者个人主页	赵春明; 葛建华;李新国