计算机工程　2006 32 (20): 168-169　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

DSS签字标准在密钥交换协议中的应用研究

程 辉1，欧阳旦2

(1. 解放军信息工程大学电子技术学院，郑州 450004；2. 空军电子技术研究所，北京 100089)

收稿日期　修回日期　网络版发布日期 2006-10-16　接受日期

摘要　密钥的安全分配是采用密码技术保证通信安全的重要环节，文章介绍了一种将DSS签字标准与Diffie-Hellman协议相结合的密钥交换协议，指出其在前向安全性上的不足。在此基础上，提出了一种密钥交换协议设计方案，并对其安全和计算量作了简要分析。

关键词　密钥交换　数字签名　数字签字标准　离散对数

分类号

DOI:

对应的英文版文章：2006-20-061

通讯作者:

作者个人主页: 程 辉1;欧阳旦2