计算机应用 2007 27 (10): 2475-2477 ISSN: 1001-9081 CN: 51-1307/TP

网络与信息安全

基于BB84与椭圆曲线的数字签名方案

杨春[1];简丽[2];何军[3];[3]

四川师范大学设备处[1]

四川师范大学计算机科学与技术学院[2]

收稿日期 2007-5-22 修回日期 网络版发布日期 2007-10-8 接受日期

摘要 利用BB84协议在量子密钥分配过程中的安全性与椭圆曲线加密体制在经典加密算法中的优越性相结合，提出了一种基于BB84协议和椭圆曲线的数字签名方案，该方案利用量子密钥作为会话密钥从而使得签名过程高效、简易，此会话密钥在密钥分配过程中具备的可证明安全性与椭圆曲线加密体制的安全性相结合对该数字签名方案提供了双重安全保护，同时可以达到互相认证的效果。

Abstract Based on the quantum key distribution protocol of BB84 and elliptic curve cryptography, a new digital signature scheme was proposed. This project used the quantum key as conversation key to make the signature process be highly effective and simple. The certifiable security of this conversation key in the key distribution process combined with the elliptic curve encryption system has provided the dual safekeeping of security to the new scheme and simultaneously achieved mutually authenticated effect.

关键词 量子密码 BB84协议 数字签名 Hash函数

Key words quantum cryptography;BB84 protocol;digital signature;Hash function

分类号

DOI:

通讯作者:
杨春 chunyang_2000@263.net

作者个人主页: 杨春 简丽 何军