计算机工程 2010 36 (06): 173-174 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

安全技术

基于ELGamal数字签名的双向认证方案

胡建军，王 伟，裴东林

(甘肃联合大学数学与信息学院，兰州 730000)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 针对当前认证方案中普遍存在的认证效率较低和认证过程较复杂等问题，提出一种基于ELGamal数字签名的双向认证方案，引入密钥分配中心作为第三方，承担公钥的分发并与认证双方进行通信。分析结果表明，该方案在离散对数问题的基础上提高了难度，在计算量方面优于其他双向认证方案，可广泛用于分布式环境下的身份识别和数字签名。

关键词 数字签名；双向认证；零知识证明；离散对数

分类号 TP309

DOI:

通讯作者:

作者个人主页: 胡建军;王 伟;裴东林