计算机应用 2007 27 (05): 1033-1034 ISSN: 1001-9081 CN: 51-1307/TP

信息与网络安全

基于ECC的高效可认证组密钥协商协议

余昭平[1];康斌[1]

解放军信息工程大学电子技术学院203教研室[1]

收稿日期 2006-11-14 修回日期 网络版发布日期 2007-4-27 接受日期

摘要 基于椭圆曲线密码体制(ECC)，建立了一个高效可认证的组密钥协商协议。该方案具有如下特点：(1)协议仅需要两轮交互，就可以实现组密钥协商; (2)利用类ElGamal密码系统，无需使用密钥分享技术，因此减轻了各参与方的计算量与通信负担; (3) 协议能够抵抗自适应选择消息攻击。

Abstract An efficient authenticated group key agreement protocol was proposed based on elliptic curve. This scheme is characterized by the following properties: (1) Participants only need two round communications to get the group key; (2) Based on ElGamal encryption system, the computational overheads and the communication costs are lessened without key sharing technique; (3) The scheme is effective against adaptive chosen message attack.

关键词 密钥协商 组密钥协商 椭圆曲线 自适应选择消息攻击

Key words key agreement;group key agreement;elliptic curve;adaptive chosen-message attack

分类号

DOI:

通讯作者:
康斌 kb5702@tom.com

作者个人主页: 余昭平 康斌