计算机应用研究
Application Research Of Computers

基于Merkle身份树的动态对等群组密钥协商*

Key agreement scheme for dynamic peer groups based on Merkle identity tree

中文关键词：动态对等群组 密钥协商 身份树 双线性对

英文关键词：dynamic peer groups key agreement identity tree bilinear pairing

基金项目：国家自然科学基金资助项目（60673070）；江苏省自然科学基金资助项目（BK2006217）；淮阴工学院青年教师科研基金项目（HGC0916）

作者	单位
陈礼青	（淮阴工学院 计算机工程学院， 江苏 淮安 223003）

中文摘要：

针对设计高效的分布式密钥协商方案是动态对等群组组播通信的难点，提出了一个新的基于Merkle身份树的密钥协商方案，并具体地分析了子组之间的通信过程，以及组成员动态变化时密钥的更新过程。结果表明该方案在降低计算和通信代价方面取得了较好的效果。

英文摘要：

Abstract:Designing efficient distributive key agreement scheme was a difficult problem in multicast communication of dynamic peer groups. This paper proposed a new key agreement scheme for multicast groups based on Merkle identity tree . Then analyzed the procedures of secret communications between subgroups and updating of group keys with the dynamic change of group members in detail. The analysis shows that the new scheme is efficient in computation and communication.