计算机工程与应用 2009 45 (21): 68-70 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

# 基于身份具有错误容忍的会议密钥分配协议

林 鹏[1]，王 维[2]，李秀莹[3]
1.河北大学，保定 071002
2.咸阳师范学院 信息工程学院，陕西 咸阳 712000
3.江南信安（北京）科技有限公司，北京 100080

收稿日期 2009-3-17 修回日期 2009-5-22 网络版发布日期 接受日期

摘要 利用Yang等人的一个基于身份的并且错误容忍的会议密钥分配方案，提出了一种改进的会议密钥分配协议算法，并分析了该协议的正确性和安全性。分析结果表明，该方案不但实现了即使存在恶意参与者的情况下，诚实参与者也能协商出一个共同的会议密钥的目的；而且能够有效地抵抗被动攻击和主动攻击，安全高效，具有很强的实用性。

关键词 基于身份 错误容忍 会议密钥
分类号

# Identity-based with fault-tolerant conference key distribution

LIN Peng[1]，WANG Wei[2]，LI Xiu-ying[3]

1.Hebei University，Baoding，Hebei 071002，China
2.College of Information Engineering，Xianyang Normal University，Xianyang，Shaanxi 712000，China
3.Jiangnan Principal （Beijing） Technology Co，Ltd.，Beijing 100080，China

**Abstract**
Abstract： An improved protocol for conference key distribution algorithms is proposed based on the identity-based with fault-tolerant conference key distribution which is put foroard by Yang et al，and the correctness and security of the protocol is analyzed.This method makes the honest participants consult a common conference key even in the presence of malicious participants；and be able to effectively resist passive attacks and active attacks.

**Key words** identity-based fault-tolerant conference key

DOI: 10.3778/j.issn.1002-8331.2009.21.018

通讯作者 林 鹏 linpeng@hbu.edu.cn