计算机工程与应用 2010 46 (12): 97-98 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于RSA的防欺诈的动态多重秘密共享方案

郭 振，张建中

陕西师范大学 数学与信息科学学院，西安 710062

收稿日期 修回日期 网络版发布日期 接受日期

摘要 基于RSA加密体制，提出了一个可防欺诈的动态门限多重秘密共享方案。该方案能够实现多重秘密共享，灵活地更新群组密钥，动态地加入新的参与者。在方案的实现过程中，能及时检测和识别分发者对参与者以及参与者之间的欺骗行为，从而提高了重构秘密的成功率和方案的实用性。

关键词 秘密分享 欺诈 RSA加密体制

分类号 TP309

Dynamic multi-secret sharing scheme to identify cheaters based on RSA cryptosystem

GUO Zhen，ZHANG Jian-zhong

College of Mathematics and Information Science，Shaanxi Normal University，Xi’an 710062，China

Abstract

The paper proposes a dynamic threshold multi-secret sharing scheme based on RSA cryptographic system.In this scheme，multi-secret can be shared.The shadows needn’t be changed when the shared secret is renewed or new participants are added.Moreover，the paper proposes the efficient solutions against multiform cheating，therefore the scheme is high security and practicality.

Key words secret sharing cheating RSA cryptographic system

DOI: 10.3778/j.issn.1002-8331.2010.12.027

通讯作者 郭 振 jzzhang@snnu.edu.cn