计算机工程与应用 2009 45 (17): 9-10 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

基于RSA的防欺诈多秘密共享方案

郭现峰

西南民族大学 计算机科学与技术学院，成都 610041

收稿日期 2009-2-11 修回日期 2009-3-16 网络版发布日期 2009-6-9 接受日期

摘要 针对秘密共享方案进行了分析和研究，指出基于二元单向函数和Shamir（*t*，*n*）门限方案的YCH多秘密共享方案无法有效防止欺诈，进而提出了一个基于RSA的防欺诈的多秘密共享方案。该方案在保留了YCH方案的优良特性同时，利用秘密片段和认证片段信息的模余关系来检测欺诈者，具有较强的实用性。

关键词 多秘密共享 RSA 防欺诈 Shamir

分类号

cheat-proof multi-secret sharing scheme based on RSA

GUO Xian-feng

College of Computer Science and Technology，Southwest University for Nationalities，Chengdu 610041，China

Abstract

Through investigating the secret sharing schemes，points out that YCH scheme is an efficient multi-secret sharing scheme，but it does not has the property of cheat-proof.To overcome this flaw，this paper presents a cheat-proof multi-secret sharing scheme based on RSA.Security analyses indicate that the proposed scheme can resist cheat efficiently.It is capabilities for many applications.

Key words multi-secret sharing scheme Rivest-Shamir-Adleman（RSA） cheat-proof Shamir

DOI: 10.3778/j.issn.1002-8331.2009.17.003

通讯作者 郭现峰 guoxianf@126.com