计算机工程 2011, 37(24) 100-102 DOI: 10.3969/j.issn.1000-3428.2011.24.033 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于向量空间的防欺诈秘密共享方案

雷 娟，李志慧，张倩倩

(陕西师范大学数学与信息科学学院，西安 710062)

摘要： 传统秘密共享方案在防止成员间的欺诈方面存在缺陷。为此，基于线性方程组理论，提出一种新的防欺诈秘密共享方案。新方案在秘密恢复前，需要分2步对授权子集中的参与者份额进行验证，并证明了凡是通过以上2步验证的参与者一定是诚实的。分析结果表明，与其他基于向量空间的秘密共享方案相比，该方案具有更高的安全性。

关键词： 秘密共享 访问结构 授权子集 向量空间 黑盒子

Secret Sharing Scheme for Fraud Prevention Based on Vector Space

LEI Juan, LI Zhi-hui, ZHANG Qian-qian

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

Abstract: The traditional secret sharing scheme has defects in preventing cheating between participants. Based on systems of linear equations, this paper proposes a new scheme. Before the recovery phase, the new scheme needs two steps in which authorized participants shares must be verified, and it is shown that any participant who has passed the verification in these two steps must be honest. The new scheme is more safer than the other vector space secret sharing schemes.

Keywords: secret sharing access structure authorized subset vector space black box

收稿日期 2011-06-17 **修回日期** **网络版发布日期** 2011-12-20

DOI: 10.3969/j.issn.1000-3428.2011.24.033

基金项目:

国家自然科学基金资助项目(60873119)；陕西师范大学优秀科技预研基金资助项目(GK200902051)

通讯作者:

作者简介: 雷 娟(1986－)，女，硕士研究生，主研方向：有限域，密码学；李志慧(通讯作者)，教授、博士；张倩倩，硕士研究生

通讯作者E-mail: snnulzh@yahoo.com.cn

参考文献：

[1] Shamir A. How to Share a Secret[J].Communications of ACM.1979, 22(11):612-613

[2] Blakley G R. Safeguarding Cryptographic Keys[D]. Rudder Tower.[J].Texas, USA: Texas A&M University.1979,:-

[3] Rima C. How to Avoid Cheaters Succeeding in the Key Sharing Scheme[J].Designs, Codes and Cryptography.1993, 3(3):221-

[6] Jorge L V. Detection of Cheaters in Vector Space Secret Sharing Schemes[J].Designs, Codes and Cryptography.1999, 16(1):75-

本刊中的类似文章

1. 邹惠, 王建东, 宋超.加权门限多秘密共享方案[J]. 计算机工程, 2012,38(3): 148-149,165
2. 蒋效宇.基于关键词抽取的自动文摘算法?[J]. 计算机工程, 2012,38(3): 183-186
3. 向河林, 张明西, 李珀瀚, 何震瀛, 汪卫.一种基于聚类的语义检索算法[J]. 计算机工程, 2012,38(2): 36-38
4. 乔晓林, 张建中.参与者有权重的多等级秘密共享方案[J]. 计算机工程, 2011,37(9): 176-177,180
5. 钟将, 孙启干, 李静.基于归一化向量的文本分类算法[J]. 计算机工程, 2011,37(8): 47-49
6. 张建中, 李瑞.访问结构上可公开验证的秘密共享方案[J]. 计算机工程, 2011,37(7): 173-174,180
7. 李庆诚, 左珊珊, 董振华, 张金.中文RSS信息自动检索与分类研究[J]. 计算机工程, 2011,37(6): 79-81
8. 贾秀芹, 赖红.抗欺诈的动态(t, n)门限秘密共享方案[J]. 计算机工程, 2011,37(4): 152-154
9. 徐忠波, 卢建朱, 任洪庆.一种改进的匿名奖励方案[J]. 计算机工程, 2011,37(4): 155-157
10. 蒋凯, 关佶红.基于重启型随机游走模型的图上关键字搜索[J]. 计算机工程, 2011,37(3): 42-43,46

文章评论

反馈人		邮箱地址	
反馈标题		验证码	6274