计算机应用 2009, 29(09) 2363-2365 DOI: ISSN: 1001-9081 CN: 51-1307/TP

信息安全

可公开验证的短份额秘密共享算法

刘镇[1],杨晓元[2],魏萍[3],肖海燕[4]

1. 西安武警工程学院网络与信息安全实验室
2. 陕西省西安市武警工程学院电子技术系系办
3. 武警工程学院 网络与信息安全武警部队重点实验室
4. 武警工程学院电子技术系

摘要： 为弥补传统秘密共享方案秘密长度不能太长的缺点，同时又能防止参与者作弊，利用Jordan矩阵理论，结合拉格朗日插值公式，提出了一种可验证的短份额门限秘密共享算法。算法能有效抵抗统计攻击和任意少于r个腐败的分享者的合谋攻击；各分享者保存的份额很短。当秘密是一个大的隐私文件、在一个不可信链路上传输的大消息、几个分享者共享的一个秘密数据库或者分布式存储的海量数据时，都具有重要的应用。

关键词： 秘密共享 可验证 门限方案 Jordan矩阵 secret sharing verifiable threshold scheme Jordan matrix

Public verifiable algorithm of threshold secret sharing with short share

Abstract: To make up the limitation that the length of secret can not be too long and prevent the action of cheating, using the theory of Jordan matrix，and combining with the formulary of Lagrange，the authors put forward an algorithm of threshold secret sharing with short share. It could effectively resist the statistical attack and the united attack of corrupt participants less than r. The length of secret share that each participator needed to conserve was very short. It had a very important application when the secret was a big privacy file, a big message transmitted in an insecure channel, a secret database shared by several participants or enormous data in distributed storage.

Keywords:

收稿日期 2009-03-05 修回日期 2009-05-02 网络版发布日期 2009-09-01

DOI:

基金项目:

国家级基金

通讯作者: 刘镇

作者简介:

作者Email:

参考文献：

本刊中的类似文章

1．杨帆 沙瀛 程学旗.一个P2P分布式数字签名系统[J]. 计算机应用, 2007,27(2): 308-310

2．侯整风 段笑言 昂东宇.基于(t,n)门限的代理签名方案[J]. 计算机应用, 2007,27(3): 614-615

3．叶永飞 余梅生.基于簇结构的Ad Hoc网络安全密钥管理方案[J]. 计算机应用, 2007,27(3): 611-613

4．李彬;郝克刚.一种基于双线性配对的可验证秘密分享方案[J]. 计算机应用, 2006,26(4): 809-811

5．张学军 王育民 .一种新的无第三方参与的买方卖方水印协议[J]. 计算机应用, 2006,26(7): 1626-1627

6．殷凤梅 侯整风.可选子密钥的门限多秘密共享方案[J]. 计算机应用, 2007,27(9): 2187-2188

7．石润华 黄刘生 .一种简单的可验证秘密共享方案[J]. 计算机应用, 2006,26(8): 1821-1823

8．杨曦 侯整风.一种可定期更新的多秘密共享方案[J]. 计算机应用, 2007,27(7): 1609-1610

9．赵洋 秦志光 蓝天 王佳昊.一种适用于P2P环境的乐观公平交换协议[J]. 计算机应用, 2007,27(8): 1881-1883

10．张艳硕 刘卓军.基于特殊差分方程的安全的多重秘密门限共享方案[J]. 计算机应用, 2007,27(8): 1913-1914

11．张艳硕 刘卓军.动态的可验证彩色可视多重秘密共享门限方案[J]. 计算机应用, 2007,(12): 2937-2939

12．毛颖颖 毛明 张艳硕.可验证的多等级门限多秘密共享方案[J]. 计算机应用, 2009,29(1): 172-174

13．侯整风 高汉军.一个新的基于多重秘密共享的图像隐藏方案[J]. 计算机应用, 2008,28(4): 902-905

14．柴争义 白浩 张浩军.一种CA私钥的容侵保护机制[J]. 计算机应用, 2008,28(4): 910-911

15．黄宏升 仲红 燕飞飞 孙彦飞.一种抗强制的电子投票方案 [J]. 计算机应用, 2009,29(06): 1725-1727

16．邹惠 王建东.动态安全的多级门限多秘密共享方案 [J]. 计算机应用, 2009,29(08): 2218-2219

文章评论

反馈人		邮箱地址	
反馈标题		验证码	0357