计算机工程 2012, 38(3) 148-149,165 DOI： 10.3969/j.issn.1000-3428.2012.03.050 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

加权门限多秘密共享方案

邹 惠[1]，王建东[1]，宋 超[2]

(1. 石家庄经济学院信息工程学院，石家庄 050031；2. 中共中央办公厅机要局，北京 100034)

摘要： 现有加权秘密共享方案一次只能共享一个秘密。为此，提出一种参与者有权重的门限多秘密共享方案。利用中国剩余定理，将每次要共享的多个秘密映射到一个参数中，当参与者权重之和大于等于门限值时，恢复多个秘密。分析结果表明，该方案具有较高的安全性，且通信量较低。

关键词： 加权门限 多秘密共享 离散对数 Hash函数

Weighted Threshold Multi-secret Sharing Scheme

ZOU Hui [1], WANG Jian-dong [1], SONG Chao [2]

(1. Department of Information Engineering, Shijiazhuang University of Economics, Shijiazhuang 050031, China; 2. Confidential Bureau General Office, Central Committee of the Communist Party of China, Beijing 100034, China)

Abstract: In the available weighted secret sharing scheme, only one secret can be shared in one sharing session. A weighted threshold multi-secret sharing scheme is proposed. By using the Chinese remainder theorem, many secrets mapping to one parameter is presented, when the sum of weights of the participants is as big as or bigger than the threshold value, they can recover the secret. Analysis shows that the proposed scheme is secure and has advantages of less communication.

Keywords: weighted threshold multi-secret sharing discrete logarithm Hash function

收稿日期 2011-07-07 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.050

基金项目:

通讯作者:

作者简介: 邹 惠(1978－)，女，讲师、硕士，主研方向：信息安全；王建东，讲师、硕士；宋 超，学士

通讯作者E-mail: zhfirst11@163.com

参考文献：

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

[2] Blakley G R. Safeguarding Cryptographic Keys[C]//Proc. of SFIPS'79 National Computer Conference. [S. l.]: IEEE Press.[J]..1979,:-

[3] 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

[4] 庞辽军, 柳 毅, 王育民. 一个有效的(t, n)门限多重秘密共享体制[J].电子学报.2006, 34(4):587-589
[5] 黄东平, 刘 铎, 戴一奇. 加权门限秘密共享[J].计算机研究与发展.2007, 44(8):1378-1382
[6] 张艳硕, 刘卓军. 参与者有权重的动态多重秘密广义门限方 案[J].北京邮电大学学报.2008, 31(1):130-134

本刊中的类似文章

1. 轩秀巍, 滕建辅, 白煜.基于二次剩余的增强型RFID认证协议[J]. 计算机工程, 2012,38(3): 124-125,129
2. 曹素珍, 王彩芬, 陈小云, 吕浩音.一种不含双线性对的可截取签名方案[J]. 计算机工程, 2012,38(3): 110-112
3. 牛淑芬, 王彩芬.多源线性网络编码的同态签名算法[J]. 计算机工程, 2012,38(2): 126-128
4. 杨路.无对运算的无证书隐式认证及密钥协商协议[J]. 计算机工程, 2012,38(2): 138-140
5. 张亚玲, 张超奇, 马巧梅.读写器可移动的RFID高效认证协议[J]. 计算机工程, 2012,38(01): 264-267
6. 方俊, 赵英良.基于RBF神经网络的一次性口令认证方案[J]. 计算机工程, 2011,37(9): 157-159
7. 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
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. 王永, 朱艳琴.一种新的共享验证签名方案[J]. 计算机工程, 2011,37(3): 116-118
10. 张艳丽, 张建中.椭圆曲线上的可验证多秘密共享方案[J]. 计算机工程, 2011,37(3): 124-125,128

文章评论

反馈人		邮箱地址	
反馈标题		验证码	1476