吉首大学学报自然科学版 » 2003, **Vol. 24** » Issue (3): 90-91 DOI:

科研简报

基于Meta-El Gamal方案的多重签名体制的改进

（1.吉首大学数学与计算机科学系，湖南 吉首 416000;2.西南交通大学计算机与通信工程学院，四川 成都610031）

Modification of Multisignature Schemes Based on Meta-El Gamal

(1.Dept.of Mathematic and Computer Science,Jishou University,Jishou 416000,Hunan China;2.College of Computer and Communication Engineering,Southwest Jiaotong University,Chengdu 610031,China)

- 摘要
- 参考文献
- 相关文章

全文: PDF (453 KB) HTML (1 KB) **输出:** BibTeX | EndNote (RIS) **背景资料**

摘要 对Meta-El Gamal方案的多重签名体制进行分析，发现该体制存在一个安全漏洞，即多个签名者如果在生成自己的密钥时相互合作就能达到日后否认消息签名的攻击手段.通过改进Meta-El Gamal多重签名体制的密钥生成部分，避免了上述攻击，体制的安全性得到提高.

关键词： Meta-El Gamal 多重签名体制 密钥生成

Abstract: This paper shows the security flaw which extends from the multisignature scheme based on Meta-El Gamal,i.e.,the attackers can deny having taken part in the process of signing some message with others.A modification is made for these schemes' key generations,which can efficiently avoid this attack.

Key words: Meta-El Gamal multisignature schemes' key generation

作者简介：鲁荣波（1970-），男，湖南省慈利县人，西南交通大学通信与信息系统专业硕士研究生，吉首大学数学与计算机科学系讲师，主要从事码分多址与个人通信、信息安全理论的研究.

服务
- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- E-mail Alert
- RSS

作者相关文章
- 鲁荣波
- 朱西平

引用本文:

鲁荣波,朱西平. 基于Meta-El Gamal方案的多重签名体制的改进[J]. 吉首大学学报自然科学版, 2003, 24(3): 90-91.

LU Rong-Bo,ZHU Xi-Ping. Modification of Multisignature Schemes Based on Meta-El Gamal[J]. Journal of Jishou University(Natural Sciences Edit, 2003, 24(3): 90-91.

[1] 王育民，刘建伟.通信网的安全理论与技术 [M].西安：西安电子科技大学出版社，1999.

[2] 曹珍富.公钥密码学 [M].哈尔滨：黑龙江教育出版社，1993.

[3] JI J,ZHAO R J.Digital Multisignature Schemes Based on the Schnorr Scheme [A].Advance in Cryptography-CHINACRYPT' 96 [C].1996.170-176.

[4] 祈明，HARNL.基于离散对数的若干新型代理签名方案 [J].电子学报，2000,28（11）：114-115.

[5] BYOUNGCHEON L,HEESUN K,KWANGJO K.Strong Proxy Signature and Its Applications [A].Symposium on Cryptography and Information Security [C].2001.104-110.

没有找到本文相关文献

通讯地址：湖南省吉首市人民南路120号《吉首大学学报》编辑部　邮编：416000
电话传真：0743-8563684　E-mail：xb8563684@163.com　办公QQ：1944107525