计算机工程 2012, 38(2) 144-145 DOI: 10.3969/j.issn.1000-3428.2012.02.046 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

一种前向安全的代理重签名方案

邓宇乔

(广东商学院数学与计算科学学院，广州 510320)

摘要： 基于二次剩余问题求解的困难性，提出一个具有前向安全性的代理重签名方案，通过半可信代理方，将代理者对消息的签名转化为委托者对同一消息的签名。理论分析结果证明，该方案能抵抗伪造攻击，即使当前周期的签名密钥被泄露，也不会影响此周期前签名的有效性。

关键词： 二次剩余问题 代理重签名 前向安全性 强RSA假定 数字签名

Forward Secure Proxy Re-signature Scheme

DENG Yu-qiao

(College of Mathematics and Computer Science, Guangdong University of Business Studies, Guangzhou 510320, China)

Abstract: Based on the difficulty in solving quadratic residues problem, this paper proposes a forward secure proxy re-signature scheme. Through a semi-trusted proxy, proxy's signature on a message is transformed into consignor's signature on it. Theroy analysis proves that the scheme can resist forgery attack, and it can maintain the security of former signature even if signature key of current cycle leaks.

Keywords: quadratic residues problem proxy re-signature forward security strong RSA assumption digital signature

收稿日期 2011-05-16 **修回日期** **网络版发布日期** 2012-01-20

DOI: 10.3969/j.issn.1000-3428.2012.02.046

基金项目:

广东商学院博士基金资助项目(10BS41302)

通讯作者:

作者简介: 邓宇乔(1980－)，男，博士，主研方向：密码学，安全电子支付系统，数字版权管理系统

通讯作者E-mail: dengyuqiao80@yahoo.cn

参考文献：

[5] 孙超亮, 曹珍富, 梁晓辉. 门限代理重签名方案[J].计算机工程.2009, 35(4):128-130 浏览

本刊中的类似文章

1. 周才学, 周顽, 胡日新, 江永和.基于身份的签密方案分析与改进[J]. 计算机工程, 2012,38(2): 132-134
2. 杨宏宇, 李东博.EFBS数据交换模型与完整性检查机制[J]. 计算机工程, 2012,38(01): 29-32
3. 马昌社.PPK模型下的有序多重数字签名方案[J]. 计算机工程, 2011,37(9): 19-21
4. 王勇兵, 张学亮, 仇宾.一种新的基于身份的代理签名方案[J]. 计算机工程, 2011,37(7): 157-159
5. 朱月珍.基于身份的改进门限代理重签名方案[J]. 计算机工程, 2011,37(7): 125-126,129

扩展功能

本文信息

Supporting info

PDF(337KB)

[HTML] 下载

参考文献[PDF]

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

引用本文

Email Alert

文章反馈

浏览反馈信息

本文关键词相关文章

二次剩余问题

代理重签名

前向安全性

强RSA假定

数字签名

本文作者相关文章

邓宇乔

PubMed

Article by Deng, Y. J.

6. 归奕红.无线传感器网络HEDSA数据聚合研究[J]. 计算机工程, 2011,37(7): 160-162
7. 钟翔.具有失败-中止性质的代理签名[J]. 计算机工程, 2011,37(5): 179-180,183
8. 黄玉颖, 马华, 张应辉, 史来婧.基于身份的链式验证签名方案[J]. 计算机工程, 2011,37(4): 142-144
9. 周萍, 何大可.基于强RSA假定的代理多重签名方案[J]. 计算机工程, 2011,37(4): 165-167
10. 许德武, 陈伟.基于椭圆曲线的数字签名和加密算法[J]. 计算机工程, 2011,37(4): 168-169

文章评论

反馈人		邮箱地址	
反馈标题		验证码	4601
	5		