计算机应用 2012, 32(03) 705-706 DOI: 10.3724/SP.J.1087.2012.00705 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

无证书代理盲签名方案的安全性分析及改进

葛荣亮,高德智,梁景玲,张云

山东科技大学 信息科学与工程学院,山东 青岛 266590

摘要: 盲签名广泛应用于电子投票系统、电子支付系统等方面,在盲签名方案中签名者不知道所签信息的具体内容。通过对一个新的无证书代理盲签名方案(魏春艳,蔡晓秋.新的无证书代理盲签名方案.计算机应用, 2010,30(12):3341-3342)进行安全性分析,发现了其中的安全漏洞,签名者可以将所签信息与原始消息进行链接,从而无法满足盲签名方案的安全性要求。同时针对这个问题,提出了一个改进方案,改进方案克服了原方案的安全缺陷。

关键词: 无证书公钥密码体制 盲签名 代理盲签名 双线性对 哈希函数

Security analysis and improvement of certificateless proxy blind signature

GE Rong-liang, GAO De-zhi, LIANG Jing-ling, ZHANG Yun

College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao Shandong 266590, China

Abstract: The blind signature is widely applied to the electronic voting system and electronic paying system, etc. While giving a blind signature, the signer does not know the content of the signed message. This paper analyzed the security of a new certificateless proxy blind signature scheme (WEI CHUN-YAN, CAI XIAO-QIU. New certificateless proxy blind signature scheme. Journal of Computer Applications, 2010,30(12):3341-3342) and found out the security loophole. The signer can link the signed message with the original message. Thus the scheme can not satisfy the security requirements of the blind signature scheme. To solve this problem, an improved scheme was proposed. The improved scheme eliminates the defect of the original one.

Keywords: certificateless public key cryptography blind signature proxy blind signature bilinear pairing Hash function

收稿日期 2011-09-14 **修回日期** 2011-11-16 **网络版发布日期** 2012-03-01

DOI: 10.3724/SP.J.1087.2012.00705

基金项目:

青岛市科技发展计划项目(11-2-4-6-(1)-jch)。

通讯作者: 葛荣亮

作者简介: 葛荣亮(1987-),男,江苏盐城人,硕士研究生,主要研究方向:密码学;高德智(1963-),男,新疆昌吉人,教授,博士,主要研究方向:信息安全、密码学;梁景玲(1986-),女,山东滕州人,硕士研究生,主要研究方向:密码学;张云(1985-),女,山东淄博人,硕士研究生,主要研究方向:密码学。

作者Email: gerl123@yahoo.cn

参考文献:

[1]SHAMIR A. Identity-based cryptosystems and signature schemes[C]// Proceedings of CRYPTO 84, LNCS 196.Berlin:Springer-Verlag,1985:7-53.

[2]AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]// Proceedings of Asiacrypt 2003, LNCS 2894. Berlin: Spring-Verlag, 2003:452-473.

[3]MAMBO M, USUDA K, OKAMOTO E. Proxy signature: Delegation of power to sign messages [J]. IEICE Transactions on Fundamentals, 1996, E79-A(9):1338-1353.

[4]CHAUM D. Blind signature for untraceable payments[C]// Adavances in Cryptology: Crypto82.

Berlin: Springer-Verlag, 1982: 199-203.

[5]夏满民, 谷利泽. 一个新型的代理盲签名方案[J]. 北京邮电大学学报, 2006, 29(3): 48-52.

[6]张学军, 王育民. 高效的基于身份的代理盲签名[J]. 计算机应用, 2006, 26(11): 2586-2588.

[7]LI J G, WANG S H. New efficient proxy blind signature scheme using verifiable self-certified public key[J]. International Journal of Network Security, 2007,4(2):193-200.

[8]王天银, 蔡晓秋, 张建中. 一种安全有效的代理盲签名方案[J]. 计算机工程, 2007, 33(2): 148-149.

[9]陈逢林, 胡万宝. 基于超椭圆曲线的代理盲签名方案[J]. 计算机应用, 2010, 30(5):1224-1226.

[10]魏春艳,蔡晓秋.新的无证书代理盲签名方案[J].计算机应用, 2010,30(12):3341-3342.

本刊中的类似文章

1．高海英.高效的基于身份的认证密钥协商协议[J]. 计算机应用, 2012,32(01): 35-37

2．舒剑.高效的强安全的基于身份认证密钥协商协议[J]. 计算机应用, 2012,32(01): 95-98

3．薛冰 景伟娜.无对运算的无证书部分盲签名[J]. 计算机应用, 2011,31(11): 2990-2993

4．李志敏 徐馨 李存华.一个在线/离线签密方案的分析和改进[J]. 计算机应用, 2011,31(11): 2983-2985

5．袁猷南 游林.增强的基于网格的无线传感器网络密钥分配方案[J]. 计算机应用, 2011,31(07): 1872-1875

6．王晚 杜伟章.基于离散对数问题的多级代理盲签名方案[J]. 计算机应用, 2011,31(07): 1904-1905

7．范函 张少武.对两个基于离散对数的数字签名方案的攻击分析与改进[J]. 计算机应用, 2011,31(07): 1859-1861

8．牛淑芬 王彩芬 刘雪艳.抵御污染攻击的双源网络编码签名算法[J]. 计算机应用, 2011,31(06): 1512-1514

9．黄明军 杜伟章.一种无证书签名方案的安全性分析及其改进[J]. 计算机应用, 2011,31(06): 1536-1538

10．万丽 李方伟 闫少军.一个代理盲签名方案的分析与改进[J]. 计算机应用, 2011,31(04): 989-991

11．张小萍 钟诚.高效无可信私钥生成中心部分盲签名方案[J]. 计算机应用, 2011,31(04): 992-995

12．谢川.结合Hash函数和密钥阵列的RFID安全认证协议[J]. 计算机应用, 2011,31(03): 805-807

13．柏骏 张串绒 崔晓臣.基于多接收者签密算法的门限密钥更新协议[J]. 计算机应用, 2011,31(02): 507-510

14．向新银.标准模型下的无证书签密方案[J]. 计算机应用, 2010,30(8): 2151-2153

15．柳菊霞 苏靖枫.基于离散对数的代理盲签名方案[J]. 计算机应用, 2010,30(8): 2167-2169

16．陈宁宇 顾永跟 苏晓萍.数字签名方案的同底构造攻击[J]. 计算机应用, 2010,30(4): 1042-1044

17．罗黎霞 张峻.基于双线性映射的动态门限签名方案[J]. 计算机应用, 2010,30(3): 677-679

18．梁红梅 黄振杰.高效无证书签名方案的安全性分析和改进[J]. 计算机应用, 2010,30(3): 685-687

19．魏春艳 蔡晓秋.新的无证书代理盲签名方案[J]. 计算机应用, 2010,30(12): 3341-3342

20．屈娟 张建中.基于双线性对的动态广义秘密共享方案[J]. 计算机应用, 2010,30(11): 3036-3037

21．李明祥 赵秀明 王洪涛.对一种部分盲签名方案的安全性分析与改进[J]. 计算机应用, 2010,30(10): 2687-2690

22．洪东招 谢琪.有效的无证书签名方案[J]. 计算机应用, 2010,30(07): 1809-1811

23．陈逢林 胡万宝.基于超椭圆曲线的代理盲签名方案[J]. 计算机应用, 2010,30(05): 1224-1226

24．张永洁 王彩芬 张玉磊.两个指定验证者签名方案的分析与改进[J]. 计算机应用, 2010,30(05): 1227-1229

25．吴晨煌 陈智雄 王海明 沈毅军.一个无证书代理签名方案的安全性分析及改进[J]. 计算机应用, 2009,29(4): 944-946,

26．彭长艳 张权 唐朝京.基于IBC的TLS握手协议设计与分析[J]. 计算机应用, 2009,29(3): 633-637

27．樊玫玫 彭长根.一种基于身份的多方公平交换协议[J]. 计算机应用, 2009,29(2): 367-369

28．张学军.高效的使用双线性对的自认证公钥签名[J]. 计算机应用, 2009,29(2): 355-356

29．陈礼青.基于公钥广播加密的安全组播方案[J]. 计算机应用, 2009,29(11): 2948-2951

30．张玉磊 王彩芬 张永洁 程文华 韩亚宁.一类无证书签名方案的密码学分析与启示[J]. 计算机应用, 2009,29(11): 2957-2959

31．王文强 陈少真.一种基于身份的高效环签名方案[J]. 计算机应用, 2009,29(11): 2990-2992

32. 耿永军 张延红 崔国华.基于身份的结构化重签名方案[J]. 计算机应用, 2009,29(09): 2339-2341
33. 章志明 邓建刚 邹成武 余敏.安全有效的无线传感器网络匿名通信方案[J]. 计算机应用, 2009,29(09): 2351-2354
34. 蔡晓秋 李金周 王天银.代理多重盲签名方案的改进[J]. 计算机应用, 2009,29(06): 1646-1658
35. 张玉磊 王彩芬 张永洁 程文华 韩亚宁.基于双线性对的高效无证书签名方案[J]. 计算机应用, 2009,29(05): 1330-1333
36. 农强 吴顺祥.一种基于身份的代理盲签名方案的分析与改进[J]. 计算机应用, 2008,28(8): 1940-1942
37. quietloner.高效的动态安全组播密钥协商方案[J]. 计算机应用, 2008,28(8): 1943-1945
38. 雷治军 刘文化 禹勇.对一种代理盲签名方案的密码学分析[J]. 计算机应用, 2008,28(5): 1144-1145
39. 樊睿 王彩芬 蓝才会 左为平.新的无证书的代理签名方案[J]. 计算机应用, 2008,28(4): 915-917
40. 向新银.可认证的无证书密钥协商协议[J]. 计算机应用, 2008,28(12): 3165-3167
41. 高伟 李飞 徐邦海.依托BLS签名的基于身份盲签名方案[J]. 计算机应用, 2008,28(11): 2827-2828
42. 王泽成 斯桃枝 李志斌.改进的带签名者意向的结构化多重签名方案[J]. 计算机应用, 2008,28(1): 71-73
43. 王玲玲 张国印 马春光.一种基于双线性对的可验证无证书环签密方案[J]. 计算机应用, 2007,27(9): 2167-2169
44. 强永妍 杨庚.中文垃圾邮件的索引分词法的研究与设计[J]. 计算机应用, 2007,27(9): 2334-2336
45. 黄辉 秦静 李丽.一个改进的代理盲签名方案[J]. 计算机应用, 2007,27(6): 1539-1541
46. 徐吉斌 叶震.一种可公开验证的基于身份的签密方案[J]. 计算机应用, 2007,27(6): 1553-1555
47. 徐丽娟 徐秋亮 郑志华.基于身份的指定验证人的门限代理签名方案[J]. 计算机应用, 2007,27(5): 1058-1061
48. 邱成刚 李方伟.一种不使用Hash和Redundancy函数的代理盲签名[J]. 计算机应用, 2007,(12): 2960-2961
49. 杜焕强 吴铤 叶春涛.基于身份的代理盲签名[J]. 计算机应用, 2007,27(11): 2715-2717
50. 胡振鹏 钱海峰 李志斌.一种新的代理多重盲签名方案[J]. 计算机应用, 2007,27(11): 2718-2721
51. 刘军龙 王彩芬 .基于身份的可截取门限签名方案[J]. 计算机应用, 2006,26(8): 1817-1820
52. 王天银 蔡晓秋 张建中 .对一种门限代理签名方案的密码分析及改进[J]. 计算机应用, 2006,26(7): 1631-1633
53. 张学军 王育民 .高效的基于身份的代理盲签名[J]. 计算机应用, 2006,26(11): 2586-2588
54. 张学军 王育民 .基于身份无可信中心的盲签名和代理签名[J]. 计算机应用, 2006,26(10): 2307-2309
55. 陆洪文，郑卓.基于双线性对的门限部分盲签名方案[J]. 计算机应用, 2005,25(09): 2057-2059
56. 陈黎明，俞研，黄皓.一个日志完整性检测方法[J]. 计算机应用, 2005,25(04): 867-869
57. 张亚玲，禹勇，王晓峰，王铁英.基于RSA签名的安全数字时间戳方案[J]. 计算机应用, 2005,25(02): 381-382
