P.O.Box 8718, Beijing 100080, China | Journal of Software Dec. 2003,14(12):2021-2027
E-mail: jos@iscas.ac.cn | ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn | Copyright © 2003 by The Editorial Department of Journal of Software

A Nonrepudiable Threshold Proxy Signcryption Scheme with Known Proxy Agent

LI Ji-Guo, LI Jian-Zhong, CAO Zhen-Fu, ZHANG Yi-Chen

Full-Text PDF Submission Back

LI Ji-Guo1, LI Jian-Zhong1, CAO Zhen-Fu2, ZHANG Yi-Chen3, 1(School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China)2(Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200030, China)3 (Department of Computer Science and Engineering, Qiqihar University, Qiqihar 161005, China)

Authors information: LI Ji-Guo was born in 1970. He is a Ph.D. candidate at the School of Computer Science and Technology, Harbin Institute of Technology. His current research interests include cryptography and its application. LI Jian-Zhong was born in 1950. He is a professor and doctoral supervisor at the School of Computer Science and Technology, Harbin Institute of Technology. His research interests include are database system technology and parallel computation technology. CAO Zhen-Fu was born in 1962. He is a professor and doctoral supervisor at the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests include number theory, cryptography and its application. ZHANG Yi-Chen was born in 1971. He is a lecturer at the Department of Computer Science and Engineering, Qiqihar University. His research interests include cryptography and its application.

Corresponding author: LI Ji-Guo, Phn: 86-451-86410291, E-mail: ljg1688@163.com

Received 2002-09-18; Accepted 2003-07-02

Abstract

In 1996, Mambo et al. introduced the concept of proxy signature. However, a proxy signature only provides the delegated authenticity and doesn't provide the confidentiality. Chan and Wei proposed a threshold proxy signcryption scheme (denoted as Chan-Wei scheme), which extended the concept of proxy signature. In this paper, the authors demonstrate Chan-Wei scheme does not satisfy strong unforgeablity, strong nonrepudiation and strong identifiability. Based on Chan-Wei scheme, a nonrepudiable threshold proxy signcryption scheme with known proxy agents is proposed. The proposed scheme overcomes the weaknesses of Chan-Wei scheme. Completeness proof and security analysis of the proposed scheme are presented. In addition, compared with Chan-Wei scheme, the proposed scheme exactly finds out which proxy agents present bogus secret shadow or tamper secret shadow.

Li JG, Li JZ, Cao ZF, Zhang YC. A nonrepudiable threshold proxy signcryption scheme with known proxy agent. *Journal of Software*, 2003,14(12):2021~2027.
http://www.jos.org.cn/1000-9825/14/2021.htm

摘要

1996年,Mambo等人提出了代理签名概念.但是,代理签名仅能提供授权的认证而不能提供保密性.Chan和Wei提出一个门限代理签密方案(记为Chan-Wei方案),扩展了代理签名的概念.指出他们的方案不满足强不可伪造性、强不可否认性和强识别性.基于Chan-Wei方案,提出一个能够克服Chan-Wei方案缺点的不可否认门限代理签密方案.给出方案的完备性证明和安全性分析.此外,与Chan-Wei方案相比,所提出的方案能够确切地发现哪些代理人提供假子密钥或篡改子密钥.

基金项目：Supported by the National Natural Science Foundation of China under Grant Nos.60072018, 60273082 (国家自然科学基金); the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No.60225007 (国家杰出青年科学基金); the National Research Foundation for the Doctoral Program of Higher Education of China under Grant No.20020248024 (国家教育部博士点基金); the National High-Tech Research and Development Plan of China under Grant No.2001AA41541 (国家高技术研究发展计划(863)); the National Grand Fundamental Research 973 Program of China under Grant No.G1999032704 (国家重点基础研究发展规划(973))

References:

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures: Delegation of the power to sign messages. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1996,E79-A(9):1338~1353.

[2] Lee B, Kim H, Kim K. Secure mobile agent using strong non-designated proxy signature. In: Varadharajan V, Mu Y, eds. Proceedings of the ACISP2001. LNCS 2119, Berlin: Springer-Verlag, 2001. 474~486.

[3] Lee B, Kim H, Kim K. Strong proxy signature and its application. In: Proceedings of the SCIS2001. 11B-1, 2001. 603~608.

[4] Kim S, Park S, Won D. Proxy signatures, revisited. In: Han Y, et al. eds. Proceedings of the ICICS'97 International Conference on Information and Communications Security. LNCS 1334, Berlin: Springer-Verlag, 1997. 223~232.

[5] Sun HM, Lee NY, Hwang T. Threshold proxy signatures. IEE Proc.-Computers & Digital Techniques, 1999,146(5):259~263.

[6] Sun HM. An efficient nonrepudiable threshold proxy signature scheme with known signers. Computer Communications, 1999, 22 (8):717~722.

[7] Hwang MS, Lin IC, Lu EJL. A secure nonrepudiable threshold proxy signature scheme with known signers. International Journal of Informatica, 2000,11(2):1~8.

[8] Sun HM. Design of time-stamped proxy signatures with traceable receivers. IEE Proc.-Computers & Digital Techniques, 2000, 147 (6):462~466.

[9] Hsu CL, Wu TS, Wu TC. New nonrepudiable threshold proxy signature scheme with known signers. The Journal of Systems and Software, 2001,58(2):119~124.

[10] Yi LJ, Bai GQ, Xiao GZ. Proxy multi-signature scheme: A new type of proxy signature scheme. Electronics Letters, 2000,36(6): 527~528.

[11] Li JG, Cao ZF, Zhang YC. Improvement of M-U-O and K-P-W proxy signature schemes. Journal of Harbin Institute of Technology, 2002,9 (2):145~148.

[12] Li JG, Cao ZF. Improvement of a threshold proxy signature scheme. Journal of Computer Research and Development, 2002, 39 (11):1513~1518 (in Chinese with English abstract).

[13] Li JG, Cao ZF, Zhang YC, Li JZ. Cryptographic analysis and modification of proxy multi-signature scheme. High Technology Letters, 2003,13(4):1~5 (in Chinese with English abstract).

[14] Li JG, Cao ZF, Zhang YC. Nonrepudiable proxy multi-signature scheme. Journal of Computer Science and Technology, 2003,18(3): 399~402.

[15] Gamage C, Leiwo J, Zheng Y. An efficient scheme for secure message transmission using proxy-signcryption. In: Edwards J, ed. Proceedings of the 22th Australasian Computer Science. Auckland: Springer-Verlag, 1999. 420~431.

[16] Chan WK, Wei VK. A threshold proxy signcryption. In: Proceedings of the 2002 International Conference on Security and Management (SAM2002). Monte Carlo Resort, Las Vegas, Nevada, 2002.

[17] Pedersen TP. A threshold cryptosystem without a trusted party. In: Davies DW, ed. Proceedings of the Advances in Cryptology-Eurocrypt'91. LNCS 547, Brighton: Springer-Verlag, 1991. 552~526.

附中文参考文献：

[12] 李继国,曹珍富.一个门限代理签名方案的改进.计算机研究与发展,2002,39(11):1513~1518.

[13] 李继国,曹珍富,张亦辰,李建中.代理多重签名方案的密码分析与修改.高技术通讯,2003,13(4):1~5.