P.O.Box 8718, Beijing 100080, China	Journal of Software, Jan. 2005,16(1):151-157
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2005 by The Editorial Department of Journal of Software

ACJT群签名方案中成员撤消的高效实现

陈泽文, 王继林, 黄继武, 王育民, 黄达人

陈泽文1, 王继林2,3, 黄继武1, 王育民3, 黄达人1
1(中山大学 信息科学与技术学院,广东 广州 510275)
2(浙江财经学院 信息学院,浙江 杭州 310012)
3(西安电子科技大学 ISN重点国家实验室,陕西 西安 710071)
作者简介: 陈泽文(1975－),男,福建惠安人,博士,主要研究领域为信息安全;王继林(1965－),男,博士,副教授,主要研究领域为电子商务安全;黄继武(1962－),男,博士,教授,博士生导师,主要研究领域为多媒体信息安全;王育民(1936－),男,教授,博士生导师,主要研究领域为信息论,编码,密码学;黄达人(1945－),男,教授,博士生导师,主要研究领域为小波理论及应用.
联系人: 黄继武 E-mail: isshjw@zsu.edu.cn, http://sist.zsu.edu.cn/graduate/bodao/huangjiwu.htm

Received 2003-09-05; Accepted 2004-02-11

Abstract
The problem of secure and efficient revocation of membership without incurring big costs has been considered, but no satisfactory solution was reported. This paper proposes a new revocation method of membership based on the ACJT group scheme. The solution is efficient in that it only needs one multiplication to update the public key for the group manager to exclude one group member, and the signing and verifying procedure is independent of the number of the current and excluded group members. To the best of our knowledge, the signing and verifying procedure in the existing revocation schemes is dependent on the number of either the current or the excluded group members, and thus the group manager needs a heavy computation load to update the public key.

Chen ZW, Wang JL, Huang JW, Wang YM, Huang DR. An efficient revocation algorithm in ACJT group signature. *Journal of Software*, 2005,16(1):151-157.
http://www.jos.org.cn/1000-9825/16/151.htm

摘要
员撤消问题是设计群签名方案中的一个难题,到目前为止尚无满意的解决办法.在ACJT群签名方案的基础上,提出了新的成员撤消方法.在新方案中,管理员在撤消一个成员时仅需要一次乘法运算来更新群公钥,签名和验证算法的计算量均独立于目前群成员个数和被撤消的成员个数,因而算法是高效的.以前的具有撤消成员功能的群签名方案,签名和验证算法的计算量要么依赖当前的群成员个数,要么依赖被撤消的群成员个数,而且

群公钥的更新或者成员密钥的更新往往需要多次指数运算.

基金项目：Supported by the National Natural Science Foundation of China under Grant Nos.60133020, 69975011, 60172067 (国家自然科学基金); the Natural Science Foundation of Guangdong Province of China under Grant No.04205407 (广东省自然科学基金)

References:

[1] Lysyanskaya A, Ramzan Z. Group blind digital signatures: A scalable solution to electronic cash. In: Financial Cryptography (FC'98). LNCS 1465, Heidelberg: Springer-Verlag, 1998.184-197.

[2] Nakanishi T, Fujiwara T, Watanabe H. A linkable group signature and its application to a fair secret voting. Trans. IPS. Japan, 1999, 40(7):3085-3096.

[3] Bresson E, Stern J. Efficient revocation in group signature. In: Proc. of the PKC'01. LNCS 1992, Heidelberg: Springer-Verlag, 2001. 190-206.

[4] Camenish J, Stadler M. Efficient group signatures for large groups. In: Proc. of the CRYPTO'97. LNCS 1296, Heidelberg: Springer-Verlag, 1997. 410-424.

[5] Song D. Practical forward secure group signature schemes. In: Proc. of the 8th ACM Conf. on Computer and Communication Security (CCS 2001). ACM, 2001. 225-34.

[6] Ateniese G, Camenisch J, Joye M, Tsudik G. A practical and provably secure coalition-resistant group signature scheme. In: Advances in Cryptology- CRYPTO 2000. LNCS 1880, Heidelberg: Springer-Verlag, 2000. 255-270.

[7] Ateniese G, Tsudik G. Quasi-Efficient revocation of group signature. 2001. http://eprint.iacr.org/2001/101/

[8] Kim HJ, Lim JI, Lee DH. Efficient and secure member deletion in group signature schemes. In: Won D, ed. Proc. of the ICISC 2000. LNCS 2015, Heidelberg: Springer-Verlag, 2001. 150-161.

[9] Camenisch J, Lysyanskaya A. Dynamic accumulators and application to efficient revocation of anonymous credentials. In: Advances in Cryptology—CRYPTO 02. LNCS 2442, Heidelberg: Springer-Verlag, 2002. 61-77.

[10] Camenisch J, Lysyanskaya A. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In: Advances in Cryptology—EUROCRYPT 01. LNCS 2045, Heidelberg: Springer-Verlag, 2001. 93-118.

[11] Schnorr CP. Efficient identification and signature for smart cards. In: Proc. of the Crypto'89. LNCS 435, Heidelberg: Springer-Verlag, 1990. 239-252.

[12] Camenisch J, Michels M. A group signature scheme based on an RSA-variant. Technical Report, RS-98-27, BRICS, University of Aarhus, 1999.