P.O.Box 8718, Beijing 100080, China	Journal of Software Jan. 2003,14(1):146-150
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

基于RSA和单向函数防欺诈的秘密共享体制

费如纯, 王丽娜

费如纯1,3, 王丽娜2,4 1(东北大学 信息科学与工程学院,辽宁 沈阳 110004)2(武汉大学 软件工程国家重点实验室,湖北 武汉 430071)3(本溪冶金高等专科学校 信息工程系,辽宁 本溪 117022)4(中国科学院 软件研究所 计算机科学重点实验室,北京 100080)
第一作者: 费如纯(1969－),男,河北昌黎人,讲师,主要研究领域为计算机安全,密码学.
联系人: 王丽娜 Telephone: 86-27-87653733, E-mail: lnawang@163.com
Received 2002-04-08; Accepted 2002-07-02

Abstract
The cheat-proof method in threshold secret sharing scheme is researched. The threshold secret sharing scheme is integrated with RSA and one-way function. And the RSA and one-way function are fully utilized to verify the validity of data. A threshold secret sharing scheme based on RSA is proposed, at which the cheating is equal to attacking RSA scheme. A threshold secret sharing scheme based on RSA and one-way function is also presented, at which the cheating is equal to attacking RSA scheme or one-way function. These two schemes have so strong power to identify cheaters that they can restrict the probability of successful cheating to a very small value no matter how skilled cheaters are, so they are unconditionally secure. In addition, the schemes proposed in this paper have very high information rate.

Fei RC, Wang LN. Cheat-Proof secret share schemes based on RSA and one-way function. *Journal of Software*, 2003,14(1):146~150.
http://www.jos.org.cn/1000-9825/14/146.htm

摘要
对门限秘密共享体制中的防欺诈措施进行了研究,将门限秘密共享体制与RSA与单向函数相结合,充分利用RSA和单向函数进行数据合法性的验证.提出了基于RSA防欺诈的门限秘密共享体制,对该体制的欺诈等价于攻击RSA体制;又提出了基于RSA和单向函数防欺诈的门限秘密共享体制,对该体制的欺诈等价于攻击RSA体制或单向函数.这两个体制具有很强的防止欺诈能力,使欺诈成功的概率限定于一个很小的值,而不论欺诈者具有多么高的技术,因而是无条件安全的.另外,所提出的防欺诈的门限秘密共享体制具有很高的信息率.

基金项目：Supported by the National Natural Science Foundation of China under Grant Nos.90104005, 66973034, 60173051 (国家自然科学基金)

References:

[1] Blakley GR. Safeguarding cryptographic keys. In: Merwin RE, Zanca JT, Smith M, eds. Proceedings of the National Computer Conference. Montvale, NJ: AFIPS Press, 1979. 313~317.

[2] Shamir A. How to share a secret. Communications of the ACM, 1979,24(11):612~613.

[3] Asmuth C, Bloom J. A modular approach to key safeguarding. IEEE Transactions on Information Theory, 1983,29(2):208~210.

[4] He J, Dawson E. Multistage secret sharing based on one-way function. electronics letters, 1994,30(19):1591~1592.

[5] Liu HP, Yang YX, Yang, FC. Multistage secret sharing based on one-way function. Journal of Electronics, 1999,21(4):561~564 (in Chinese with English abstract).

[6] Karnin ED, Greene JW, Hellman ME. On secret sharing systems. IEEE Transactions on Information Theory, 1983,29(1):231~241.

[7] McEliece RJ, Sarwate DV. On sharing secrets and Reed-Solomon codes. Communications of the ACM, 1981,24(8):583~584.

[8] Okada K, Kurosawa K. MDS secret sharing scheme secure against cheaters. IEEE Transactions on Information Theory, 2000,46(3): 1078~1081.

[9] Rabin T, Ben-Or M. Verifiable secrets sharing and multiparty protocols with honest majority. In: Johnson DS, ed. Proceedings of the 21st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1989. 73~85.

[10] Zhang JZ, Xiao GZ. A secret sharing scheme to identify cheaters. Journal of Electronics, 1999,21(4):516~521 (in Chinese with English abstract).

[11] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 1978,21(2):120~126.

[12] Blundo C, Santis AD, Simone RD, Vaccaro U. Tight bounds on the information rate of secret sharing schemes. Designs, Codes and Cryptography, 1997,11(2):102~122.

附中文参考文献:
[5] 刘焕平,杨义先,杨放春.基于单向函数的多级秘密共享方案.电子科学学刊,1999,21(4):561~564.

[10] 张建中,肖国镇.一个可防止欺诈的秘密分享方案.电子科学学刊,1999,21(4):516~521.