P.O.Box 8718, Beijing 100080, China	Journal of Software, July. 2004,15(7):1049-1055
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2004 by The Editorial Department of Journal of Software

基于RSA签名的优化公平交换协议

周永彬, 张振峰, 卿斯汉, 季庆光

周永彬1,2, 张振峰1,2, 卿斯汉1,3, 季庆光1,3 1(中国科学院 软件研究所,北京 100080)2(中国科学院 软件研究所 信息安全国家重点实验室,北京 100080)
3(中国科学院 信息安全技术工程研究中心,北京 100080)
作者简介: 周永彬(1973－),男,山东阳信人,博士,主要研究领域为应用密码学,网络与信息安全理论与技术;张振峰(1972－),男,博士,副研究员,主要研究领域为密码学,信息安全理论与技术;卿斯汉(1939－),男,研究员,博士生导师,主要研究领域为信息安全理论与技术;季庆光(1968－),男,博士,主要研究领域为安全系统形式化分析.
联系人: 周永彬 Phn: +86-10-82612797, E-mail: zhouyongbin@sina.com, http://www.is.iscas.ac.cn
Received 2003-08-01; Accepted 2003-10-31

Abstract
Fairness is the basic requirement of E-Commerce protocols. RSA is one of the most widely used cryptosystems. A fair-exchange protocol allows two parties to exchange items in a fair way so that either each party gets the other's item, or neither party does. In this paper construction and architecture of the existing fair exchange protocols are analyzed. Both practicality and efficiency problems of these protocols are also presented. Based on this analysis, an optimistic fair exchange protocol totally based on RSA signature scheme is proposed. The novel scheme employs verifiably encrypted RSA signatures in the extended integer ring that is elaborately constructed. The security and efficiency of the newly devised scheme are also proved and examined. It is showed that the proposed scheme is secure and efficient.

Zhou YB, Zhang ZF, Qing SH, Ji QG. A fair exchange protocol based on RSA signature scheme. *Journal of Software*, 2004,15(7):1049~1055.
http://www.jos.org.cn/1000-9825/15/1049.htm

摘要
公平性是电子商务协议的基本安全要求.RSA是应用最为广泛的公钥密码体制之一.公平交换协议可以使得参与交换的双方以公平的方式交换信息,这样,要么任何一方都可以得到对方的信息,要么双方都得不到对方的信息.分析了现有的公平交换协议构造方法、体系结构及其在实用性和效率方面存在的问题.在此基础上,利用精心构造的扩环中可公开验证的、加密的RSA签名,提出了一种完全基于RSA签名方案的优化公平交换协议,并对其安全性和效率进行了证明和分析.分析表明,提出的方案是简洁、高效、安全的.

基金项目：Supported by the National Natural Science Foundation of China under Grant Nos.60373039, 60083007 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973))

References:

[1] Diffie W, Hellman M. New directions in cryptography. IEEE Trans. on Information Theory, 1976,22(6):644~654.

[2] Menezes AJ, Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. New York: CRC Press, 1996. 385~420.

[3] Verheul ER, Tilborg ER. Binding ElGamal: A fraud-detectable alternative to key escrow proposals. In: Fumy W, ed. Proc. of the Eurocrypt'97. Berlin: Springer-Verlag, 1997. 119~133.

[4] Guillou LC, Quisquater JJ. A paradoxical identity-based signature scheme resulting zero-knowledge. In: Goldwasser S, ed. Advances in Cryptolgy-Crypto'88. Taiwan: Springer-Verlag, 1988. 216~231.

[5] Park JM, Chong E, Siegel H, Ray I. Constructing fair exchange protocols for E-commerce via distributed computation of RSA signatures. In: Proc. of the 22th Annual ACM Symp. on Principles of Distributed Computing. Boston: Massachusetts Press, 2003. 172~181.

[6] Dodis Y, Reyzin L. Breaking and reparing optimistic fair exchange from PODC 2003. In: Yung M, ed. Proc. of the 2003 ACM Workshop on Digital Rights Management. New York: ACM Press, 2003. 47~54.

[7] 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.

[8] Ray I, Ray I. Fair exchange in E-commerce. ACM SIGecom Exchanges, 2002,3(2):9~17.

[9] Bao F, Deng RH, Mao W. Efficient and practical fair exchange protocols with off-line TTP. In: Proc. of the 1998 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Press, 1998. 77~85.

[10] Zhou J, Gollmann D. A fair non-repudiation protocol. In: Proc. of the 1996 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Press, 1996. 55~61.

[11] Franklin MK, Reiter MK. Fair exchange with a semi-trusted third party. In: Proc. of the 4th ACM Conf. on Computer and Communications Security. Switzerland: ACM Press, 1997. 1~5.

[12] Boyd C, Foo E. Off-Line fair payment protocols using convertible signatures. In: Ohta K, Pei DY, eds. Advances in Cryptology (ASIACRYPT'98). Beijing: Springer-Verlag, 1998. 271~285.

[13] Asokan N, Shoup V, Waidner M. Optimistic fair exchange of digital signatures. In: Nyberg K, ed. Advances in Cryptology-EUROCRYPT'98. Helsinki: Springer-Verlag, 1998. 591~606.

[14] Zhou YB, Feng DG, Xu Z, Li DQ. IPsec: Securing VPNs. Beijing: Tsinghua University Press, 2002. 80~100 (in Chinese).

[15] Feng DG, Zhou YB, Zhang ZF, Li DQ. RSA Security's Official Guide to Cryptography. Beijing: Tsinghua University Press, 2001. 85~121 (in Chinese).

附中文参考文献:

[14] 周永彬,冯登国,徐震,李德全.IPSec:VPN的安全实施.北京:清华大学出版社,2002.80~100.

[15] 冯登国,周永彬,张振峰,李德全.密码工程实践指南.北京:清华大学出版社,2001.85~121.