P.O.Box 8718, Beijing 100080, China	Journal of Software March 2007,18(3):746-754
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2006 by *Journal of Software*

Constructing Optimistic ID-Based Fair Exchange Protocols via Proxy Signature

XU Jing, ZHANG Zhen-Feng, FENG Deng-Guo

XU Jing1, ZHANG Zhen-Feng2, FENG Deng-Guo2,
1(Institute of Mathematics, AMSS, the Chinese Academy of Sciences, Beijing 100080, China)
Authors information: XU Jing was born in 1972. She is an associate professor at the State Key Laboratory of Information Security, Graduate School of the Chinese Academy of Sciences. Her research areas are design and analysis of security protocols. ZHANG Zhen-Feng was born in 1972. He is an associate professor at the Institute of Software, the Chinese Academy of Sciences, and a CCF senior member. His research areas are theoretical and applied cryptography, design and analysis of security protocols, theory and technology of information security. FENG Deng-Guo was born in 1965. He is a professor and doctoral supervisor at the Institute of Software, the Chinese Academy of Sciences, and a CCF senior member. His research areas are information security and network security.
Corresponding author: XU Jing, Phn: +86-10-88258713, Fax: +86-10-88258713, E-mail: xujing@is.iscas.ac.cn, http://www.is.ac.cn
Received 2005-01-10; Accepted 2005-10-19

Abstract
This paper introduces a natural paradigm for fair exchange protocols, called ID-based partial proxy signature scheme. A security model with precise and formal definitions is presented, and an efficient and provably secure partial proxy signature scheme is proposed. This is a full ID-based optimistic fair exchange protocol. Unlike the vast majority of previously proposed protocols, this approach does not use any zero knowledge proofs, and thus avoids most of the costly computations.

Xu J, Zhang ZF, Feng DG. Constructing optimistic ID-based fair exchange protocols via proxy signature. *Journal of Software*, 2007,18(3):746-754.
DOI: 10.1360/jos180746
http://www.jos.org.cn/1000-9825/18/746.htm

摘要
为公平交换协议引入了一个自然的范例——基于身份的部分代理签名,给出其形式化的安全模型,同时提出了一个高效可证安全的部分代理签名方案.这是一个完全基于身份的优化公平交换协议.与以前协议不同的是,该方案没有使用任何零知识证明,有效地避免了大量计算.

基金项目：Supported by the National Natural Science Foundation of China under Grant Nos.60373039, 90604010 (国家自然科学基金); the National Science Fund for Distinguished Young Scholars of China under Grant No.60025205 (国家杰出青年科学基金)

References:

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

[2] Asokan N, Shoup V, Waidner M. Optimistic fair exchange of digital signatures. IEEE Journal on Selected Areas in Communication, 2000,18(4):593-610.

[3] Camenisch J, Damgard IB. Verifiable encryption, group encryption, and their applications to group signatures and signature sharing schemes. In: Okamoto T, ed. Proc. of the Advances in Cryptology—ASIACRYPT 2000. LNCS 1976, Berlin, Heidelberg: Springer- Verlag, 2000. 331-345.

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

[5] Ateniese G. Verifiable encryption of digital signatures and applications. ACM Trans. on Information and System Security, 2004, 7(1):1-20.

[6] Bao F. Colluding attacks to a payment protocol and two signature exchange schemes. In: Lee PJ, ed. Proc. of the Advances in Cryptology—ASIACRYPT 2004. LNCS 3329, Berlin, Heidelberg: Springer-Verlag, 2004. 417-429.

[7] Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham E, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2003. LNCS 2656, Berlin, Heidelberg: Springer-Verlag, 2003. 416-432.

[8] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakley GR, ed. Proc. of the Advances in Cryptology—Crypto'84. LNCS 196, Berlin, Heidelberg: Springer-Verlag, 1984. 47-53.

[9] Zhang ZF, Zhou YB, Feng DG. Efficient and optimistic fair exchange based on standard RSA with provable security. IACR Cryptology ePrint Archive, Report 2004/351, 2004.

[10] Dodis Y, Reyzin L. Breaking and repairing optimistic fair exchange from PODC 2003. In: Proc. of the ACM Workshop on Digital Rights Management (DRM). New York: ACM Press, 2003. 47-54.

[11] Lee JY, Cheon JH, Kim S. An analysis of proxy signatures: Is a secure channel necessary- In: Joye M, ed. Topics in Cryptology—CT-RSA, The Cryptographers' Track at the RSA Conference 2003. LNCS2612, Berlin, Heidelberg: Springer-Verlag, 2003. 68-79.

[12] Xu J, Zhang ZF, Feng DG. ID-Based proxy signature using bilinear pairings. In: Chen G, ed. Parallel and Distributed Processing and applications—ISPA 2005 Workshops. LNCS 3759, Berlin, Heidelberg: Springer-Verlag, 2005. 359-367.

[13] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Proc. of the 1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 62-73.