P.O.Box 8718, Beijing 100080, China	Journal of Software Jan. 2007,18(1):168-176
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*

RSA Verifiable Signature Sharing Scheme Based on Secure Distributed Key Generations

Lü Ke-Wei

Lü Ke-Wei,
(State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100049, China)
Authors information: Lü Ke-wei was born in 1970. He is an associate professor at the Graduate School of Chinese Academy of Sciences. His current research areas are complexity theory, secure protocols, signature, and zero knowledge proof.
Corresponding author: Lü Ke-Wei, Phn: +86-10-88256432 ext 62, Fax: +86-10-88258713, E-mail: conwaylu@tom.com
Received 2004-09-30; Accepted 2005-07-28

Abstract
This paper studies the Verifiable Signature Sharing (V(S) introduced by Franklin and Reiter, which enables the recipient of a signature to share it among n proxies so that a subset of them can reconstruct it later. By the use of secure distributed key generation based on discrete-log, threshold cryptosystems and verifiable secret sharing scheme, new protocols for RSA V(S are presented. The protocols are efficient and provable secure and can tolerate the malicious behavior of up to half of the proxies.

Lü KW. RSA verifiable signature sharing scheme based on secure distributed key generations. *Journal of Software*, 2007,18(1):168-176.
DOI: 10.1360/jos180168
http://www.jos.org.cn/1000-9825/18/168.htm

摘要
主要研究由Franklin和Reiter提出的可验证签名分享(V(S).它可以允许一个签名的接受者在n个代理之间分享该签名,使得代理者的一些子集以后可以重构该签名.利用安全的分布式密钥生成方式、门限密码系统以及可验证秘密分享,给出了一个RSA V(S的新协议.该协议是有效的、可证安全的,并且可以容忍至多一半代理的恶意行为.

基金项目：Supported by the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z434 (国家高技术研究发展计划(863)); the President's Foundation of Graduate School, the Chinese Academy of Sciences under Grant No.yzjj2003010 (中国科学院研究生院校长基金)

References:

[1] Franklin m, Reiter M. Verifiable signature sharing. In: Proc. of the Eurocrypt'95. LNCS 921, Springer-Verlag, 1995. 50-63.

[2] Catalano D, Gennaro R. New efficient and secure protocols for verifiable signature sharing and other applications. In: Proc. of the CRYPTO'98. LNCS 1462, Springer-Verlag, 1998. 105-120.

[3] Gennaro R, Jarecki S, Krawczyk H, Rabin T. The secure distributed key generation for discrete-log based cryptosystems. In: Proc. of the EUROCRYPT'99. LNCS 1592, Springer-Verlag, 1999. 295-310.

[4] Diffie W, Hellman ME. New directions in cryptography. IEEE Trans. on Information Theory, 1976,IT-22(6):644-654.

[5] ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985, IT-31(4):469-472.

[6] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust and efficient sharing of RSA functions. In: Proc. of the EUROCRYPT'96. LNCS 1109, Springer-Verlag, 1996. 157-172.

[7] Pederson T. Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum J, ed. Advances in Cryptology CRYPTO'91. LNCS 576, Berlin: Springer-Verlag, 1991. 129-140.