P.O.Box 8718, Beijing 100080, China
Journal of Software Mar. 2005,16(3):453-461
E-mail: jos@iscas.ac.cn
ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn

An Adaptively Secure Distributed Key Generation Scheme Against General Adversary without Erasure

HE Yun-Xiao, LI Bao, Lü Ke-Wei

Full-Text PDF Submission Back

HE Yun-Xiao, LI Bao, Lü Ke-Wei,
(State Key Laboratory of Information Security, Graduate School, The Chinese Academy of Sciences, Beijing 100039, China)
Authors information: HE Yun-Xiao was born in 1979. He is a graduate student at Graduate School, the Chinese Academy of Sciences. His current research areas are secure multi-party computation and zero-knowledge proof. LI Bao was born in 1962. He is a professor at Graduate School, the Chinese Academy of Sciences. His current research area is information security. Lü Ke-Wei was born in 1970. He is an associate professor at Graduate School, the Chinese Academy of Sciences. His current research areas are secure protocols and proof of security.
Corresponding author: E-mail: HE Yun-Xiao, heyx@ustc.edu, heyx97@yahoo.com
Received 2003-12-25; Accepted 2004-05-04

Abstract

Transformation of the widely used Pedersen's Verifiable Secret Sharing (Pedersen-VSS) to Pedersen-VSS-General secure against general adversary is first presented. Then a misunderstanding about the use of zero-knowledge (ZK) proof in the DL-Key-Gen scheme proposed by R. Canetti etc. is pointed out, and an improvement to it is made. An adaptively secure distributed key generation scheme against general adversary without the assumption of erasure is developed. A detailed black-box simulator for the security proof of the proposed scheme is also given.

He YX, Li B, Lü KW. An adaptively secure distributed key generation scheme against general adversary without erasure. *Journal of Software*, 2005,16(3):453-461.
http://www.jos.org.cn/1000-9825/16/453.htm

摘要

首先将基于门限结构的彼得森可验证秘密共享方案(Pedersen-VSS)转换成可以抵抗一般结构敌手攻击的方案(Pedersen-VSS-General).指出R. Canetti等人在设计分布式密钥生成方案(DL-Key-Gen)时,关于零知识证明使用的一个错误,并给出一种改进方案.基于以上设计,提出一个可以抵御一般结构敌手攻击的自适应安全的分布式密钥生成方案,该方案的安全性不依赖于"擦除"假设.对于这个方案给出详细的基于黑盒模拟的安全性证明.

基金项目：Supported by the National Natural Science Foundation of China under Grant No.90304013 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2003AA144151 (国家高技术研究发展计划(863)); the Foundation of President of Graduate School of the Chinese Academy of Sciences under Grant No.yzjj2003010 (中国科学院研究生院院长基金)

References:

[1] Pedersen T. A threshold cryptosystem without a trusted party. In: Proc. of the Eurocrypt'91. LNCS 547, Springer-Verlag, 1991. 522-526.

[2] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust threshold DSS signatures. In: Proc. of the Eurocrypt'96. LNCS 1070, Springer-Verlag, 1996. 354-371.

[3] Feldman P. A practical scheme for non-interactive verifiable secret sharing. In: Proc. of the 28th FOCS. 1987. 427-437.

[4] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Secure distributed key generation for discrete-log based cryptosystems. In: Proc. of the Eurocrypt'99. LNCS 1592, Springer, 1990. 295-310.

[5] Pedersen T. Non-Interactive and information-theoretic secure verifiable secret sharing. In: Proc. of the Crypt'91. LNCS 576, Springer-Verlag, 1991. 129-140.

[6] Canetti R, Gennaro R, Jarecki S, Krawczyk H, Rabin T. Adaptive security for threshold cryptosystems. In: Proc. of the Crypto'99. LNCS 1666, Springer-Verlag, 1999. 98-115.

[7] Schnorr CP. Efficient signature generation by smart cards. Journal of Cryptology, 1991,4(3):161-174.

[8] Karchmer M, Wigderson A. On span programs. In: Proc. of the 8th Annual Structure in Complexity Theory Conf. IEEE Computer Society Press, 1993. 102-111.

[9] Fehr S. Efficient construction of dual Span Program. Manuscript, 1999.

[10] Beimel A. Secure schemes for secret sharing and key distribution [Ph.D. Thesis]. Israel Institute of Technology, 1996.

[11] Cramer R, Damagard I, Maurer U. General secure multi-party computation from any linear secret sharing scheme. In: Proc. of the Eurocrypt2000. LNCS 1807, Springer-Verlag, 2000. 316-334.

[12] Goldreich O. Foundations of Cryptography Basic Tools. Publishing House of Electronics Industry, 2003.

[13] Canetti R. Studies in secure multi-party computation and application. [Ph.D. Thesis]. Weizmann Institute of Science, 1995.