西安电子科技大学学报 2007 34 (4): 634-637 ISSN: 1001-2400 CN: 61-1076/TN

一个新的强RSA假设下的数字签名方案

李用江1, 2, 李蔚3, 朱晓妍1, 葛建华1

(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071;2. 广东海洋大学 信息学院，广东 湛江 524088;3. 郑州轻工业学院 信息与计算机系，河南 郑州 450002)

收稿日期 修回日期 网络版发布日期 2007-7-10 接受日期

摘要 为提高强RSA困难假设条件下随机签名的生成和验证运算速度，提出一个新的签名方案．通过随机选取模n下的幂指数e，并采用RSA算法直接对与e绑定的消息签名，简化并去掉了曹等人方案中的冗余参数，在随机预言机模型下可证明该方案是安全的．通过比较分析发现新方案的运算速度比类似的方案至少提高一倍．

关键词 数字签名 强RSA假设 自适应性选择消息攻击

分类号 TP309

New signature scheme based on the strong RSA assumption

LI Yong-jiang1,2,LI Wei3,ZHU Xiao-yan1,GE Jian-hua1

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi′an 710071， China;2. School of Information, Guangdong Ocean Univ., Zhanjiang 524088， China;3. Dept. of Information & Computing Science, Zhengzhou Univ. of Light Ind., Zhengzhou 450002， China)

Abstract

To promote the speed of the random signature generation and verification algorithms under the strong RSA hardness assumption, a new signature scheme is proposed. In this scheme, by randomly selecting the exponent e under modular n and using the RSA algorithm to sign the message bound with e, the redundant parameters in Cao et al.'s signature scheme are simplified or deleted. The new scheme is proved to be secure in the Random Oracle Model. Detailed comparisons show that the speed of the new scheme is at least two times faster than that of the other schemes of such a kind.

Key words digital signature strong RSA assumption adaptive chosen-message attack

DOI:

通讯作者