西安电子科技大学学报 2006 33 (6): 953-955+984 ISSN: 1001-2400 CN: 61-1076/TN

对几种部分盲签名方案的安全性分析与改进

辛向军(1，2), 李发根(3), 肖国镇(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) 郑州轻工业学院 信息与计算科学系，河南 郑州 450002
(3) 西安电子科技大学 教育部网络与信息安全重点实验室，陕西 西安 710071

收稿日期 修回日期 网络版发布日期 2006-12-12 接受日期

摘要 对张彤等人最近提出的几种基于离散对数的部分盲签名方案进行了安全性分析，发现敌手可在不被察觉的情况下将盲化的消息乘以部分盲因子的逆而成功地去掉该方案中签名的部分盲特性，并且可以伪造签名中的嵌入常数．利用大数分解困难性隐匿张等方案中有限域中生成元的阶，对方案进行了一些改进．新的方案不仅满足部分盲特性要求，并可以防止敌手伪造嵌入参数，同时具备张等方案的其他安全性要求．

关键词 盲签名 部分盲签名 安全性分析 离散对数

分类号 TN918.1

Security analysis and improvement of several partial blind signature schemes

XIN Xiang-jun(1,2),LI Fa-gen(3),XIAO Guo-zhen(1)

(1) State Key Lab. of Integrated Service Networks, Xidian Univ., Xi’an 710071，China
(2) Dept. of Information and Cmputing Science, Zhengzhou Univ. of Light Industry, Zhengzhou 450002，China
(3) Ministry of Edu. Key of Computer Network and Infor. Security, Xidian Univ., Xi’an 710071，China

Abstract

The security of several partial blind signature schemes based on the discrete logarithm proposed recently by Zhang et al. is analyzed, and it is found that the adversary can get rid of the partial blind property of the signature without being detected by multiplying the reverse of the partial blind factor to the blind message, and the adversary can forge the embedding parameter in the signature. Then, by using the factoring difficulty and covering the order of the generator of the finite field, the improved partial blind signature schemes not only have the partial blind property but also can withstand the forgery of the embedding parameter, and at the same time they have the same other security requirements as those of the schemes by Zhang et al.

Key words blind signature partial blind signature security analysis discrete logarithm

DOI:

通讯作者