计算机工程与应用 2009 45 (24): 84-86 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于双线性对的前向安全短门限代理签名方案

肖 鹏[1，2]，毛 明[2]，张艳硕[2]

1.西安电子科技大学 通信工程学院，西安 710071
2.北京电子科技学院，北京 100070

收稿日期 2008-5-7 修回日期 2008-8-31 网络版发布日期 接受日期

摘要 将前向安全的概念结合到基于双线性对的门限签名方案中，提出了一个基于双线性对的前向安全短门限代理签名方案。该方案将密钥更新算法应用在原始签名者计算过程中，更有效增强了代理签名密钥的安全性。对该方案的性能进行了分析，表明该方案是安全有效的。

关键词 双线性对 前向安全 短签名 门限签名 代理签名

分类号 TP309

Forward secure short threshold proxy signature scheme from bilinear pairing

XIAO Peng[1，2]，MAO Ming[2]，ZHANG Yan-shuo[2]

1.Department of Communication Engineering，Xidian University，Xi’an 710071，China
2.Beijing Electronic Science and Technology Institute，Beijing 100070，China

Abstract

A forward secure short threshold proxy signature scheme from bilinear pairing is proposed by combining the concept of forward security with threshold signature from bilinear pairing.In this scheme，the key updating algorithm is used by the original signer，so the security of the proxy signature key is promoted to a higher level.The performance of the scheme is also analyzed，and it is shown that this proposed scheme is secure and effective.

Key words bilinear pairing forward secure short signature threshold signature proxy signature

DOI: 10.3778/j.issn.1002-8331.2009.24.026

通讯作者 肖 鹏 luolanjuban@163.com