计算机工程与应用 2009 45 (21): 71-73 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于GH-PKC体制的盲签名方案

端木庆峰[1]，王衍波[1]，张凯泽[1]，王 熹[2]
1.解放军理工大学 通信工程学院，南京 210007
2.广东湛江市 92146部队，524001

收稿日期 2008-5-13 修回日期 2008-8-21 网络版发布日期 接受日期

摘要 GH-PKC是一种新的基于GF（q）上三级线性反馈移位寄存器序列的公钥密码体制。其安全性基于有限域GF（q3）上的离散对数困难问题，但运算却在有限域GF（q）中进行。文中给出了一种新的基于GH-PKC的类ELGamal数字签名算法，并在此基础上构建了基于GH-PKC的盲签名方案，其安全性等价于解GF（q3）上离散对数困难问题，但是传输的数据量只有传统方案的1/3。

关键词

3级线性反馈移位寄存器 特征序列 不可约多项式 盲签名

分类号

Blind signature scheme based on GH-PKC

DUANMU Qing-feng[1]，WANG Yan-bo[1]，ZHANG Kai-ze[1]，WANG Xi[2]

1.Institute of Communications Engineering，PLA University of Science and Technology，Nanjing 210007，China
2.Unit 92146，Zhanjiang，Guangdong 524001，China

Abstract
GH-PKC is a new public-key cryptosystem based on third-order LFSR sequences over GF（q），whose security is based on the difficulty of solving the discrete logarithm in GF（q3），but all computation are performed in GF（q）.This paper proposes a ElGamal-like digital signature algorithm based on GH-PKC and then constructs a new blind signature scheme based on this，the security of which is equivalence to solving the discrete logarithm in GF（q3） while the datum transmitted is only as 1/3 as that of tranditional scheme.

Key words 3rd-order linear feedback shift register characteristic sequence irreducible polynomial blind signature

DOI: 10.3778/j.issn.1002-8331.2009.21.019

通讯作者 端木庆峰 duanmuziyun@126.com