计算机工程与应用 2009 45 (32): 98-100 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

新的基于Legendre扰动的混沌序列

王 冰[1，2]，赵 耿[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 2008-6-27 修回日期 2008-10-8 网络版发布日期 2009-11-26 接受日期

摘要 由于混沌系统对初始条件和混沌参数非常敏感以及生成的混沌序列具有非周期和伪随机性的特征，近年来混沌系统在密码学研究领域得到了较多的研究。提出一种基于混沌的序列密码生成方法，该方法通过引入扰动序列使得输出的混沌序列具有良好的均匀分布和随机统计特性，同时为了克服扰动序列数量的有限性，设计了一个素数表用来不定时更新扰动序列的输入。理论研究和模拟结果表明，该混沌序列具有较好的保密性而且便于软件实现。

关键词 混沌映射 Legendre序列 素数

分类号 TN918

New chaotic sequence based on Legendre sequence

WANG Bing[1，2]，ZHAO Geng[2]

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

Abstract

Chaotic systems are sensitive to initial conditions and chaotic paramenters，and chaotic sequences are non-periodic and pseudo-random.These properties of chaotic systems are suitable for sequence encryption.A sequence encryption method based on chaos is proposed.Meanwhile，a Legendre sequences is uesd as the parameter sequence and the perturbation sequence.In order to avoid a limitation of the number of Legendre sequences，a prime number table is applied.The computer simulation results show that the chaotic sequence has good cryptography properties.Therefor，this method is fairly good in security and can be implemented easily in software.

Key words chaos-map Legendre-sequence a prime number

DOI: 10.3778/j.issn.1002-8331.2009.32.031

通讯作者 王 冰 buddy0112@163.com