计算机工程与应用 2009 45 (16): 80-82 ISSN: 1002-8331 CN: 11-2127/TP

研发、设计、测试

LFSR加密新算法的研究与FPGA实现

梁 伟[1], 徐建波[1], 唐明董[1,2], 刘辉亚[1]
1.湖南科技大学 计算机科学与工程学院，湖南 湘潭 411201
2.中国科学院 计算技术研究所，北京 100080

收稿日期 2008-1-7 修回日期 2008-6-10 网络版发布日期 2009-5-27 接受日期

摘要 提出了一种改进的线性反馈移位寄存器结构的安全加密模型，利用移位寄存器的灵活性高和成本低的特点结合FPGA器件的高速度和可重构的性能，从而使系统达到低成本、可实时配置算法文件和重组安全策略的目的，并详细论述了该模型的改进后的线性反馈移位寄存器加密算法的加密原理，然后介绍了该算法的FPGA实现及可重构技术，最后，通过对改进算法的加密时序图的分析和总体性能的评估，证明了该算法在保证安全性能的基础上具有很好的成本优势和可重构性。

关键词 加密模型 线性反馈移位寄存器 现场可编程门阵列 可重构
分类号

Improved LFSR cryptographic algorithm and FPGA implementation

LIANG Wei[1],XU Jian-bo[1],TANG Ming-dong[1,2],LIU Hui-ya[1]

1.School of Computer Science and Engineering，Hunan University of Science and Technology，Xiangtan，Hunan 411201，China
2.Institute of Computing Technology，Chinese Academy of Sciences，Beijing 100080，China

Abstract
This paper presents a new security encryption model based on improved LFSR（Linear Feedback Shift Register），which combines the high flexibility and low cost of the shift register and the characteristics of the high-speed and reconfigurable performance of FPGA，thereby allowing the system to achieve the purpose of low-cost，real-time allocation algorithm and reorganization of security policy document.This paper elaborates on the model of improved linear feedback shift register encryption algorithm encryption theory，and then introduces the FPGA algorithms and Reconstructable technologies.Finally，with the diagram analysis about the encryption and the valuation of total function，it is proved the arithmetic has good cost advantage and reconfiguration ability as safe is assured.

Key words encryption model Linear Feedback Shift Register（LFSR） Field Programmable Gate Array（FPGA） reconstructable

DOI: 10.3778/j.issn.1002-8331.2009.16.022

通讯作者 梁 伟 idlink@163.com