面向可重构并行化处理的线性反馈移位寄存器统一架构研究

郑诚玮，戴紫彬，李 伟
（解放军信息工程大学，河南 郑州 450001）

摘 要：为了解决目前线性反馈移位寄存器实现方式在运算速度、灵活性和安全性三个方面存在的不足，研究了Fibonacci LFSR和Galois LFSR的结构特点，提取出了两者可重构和并行化实现方式的共同点，研究并实现了两者的统一架构.统一架构的可重构实现方式提高了电路的灵活性，并行化处理方式提高了电路的运算速度，灵活可变的结构增加了电路的安全性.和文献[6]中的设计相比，面积减小了47.4%，电路延迟缩减了11.5%.

关键词：Fibonacci LFSR；Galois LFSR；并行化；可重构；统一架构
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1000－7180(2015)11－0111－05

Research on Linear Feedback Shift Register United Architecture for Parallel and Reconfigurable Processing

ZHENG Cheng-wei，DAI Zi-bin，LI Wei
（PLA Information Engineering University，Zhengzhou 450004，China）

Abstract：The parallel and reconfigurable united architecture of LFSR is represented to improve the speed，flexibility and security of communication system and cipher algorithms. It can be reconfigured to Fibonacci LFSRs and Galois LFSRs according to different applications. The random lengths and feedback taps can be achieved to meet the demands of different applications. The parallel updating method has an obvious advantage on speed and efficiency. Furthermore，the flexibility and complexity increases the security of the communication system and cipher algorithms. Compared with design in Ref [6]，the area decreases 47.4% and the delay time shortens 11.5%.

Key words：Fibonacci LFSR，Galois LFSR，Parallel，Reconfigurable，United architecture

作者简介：

郑诚玮 男，(1990-)，硕士研究生.研究方向为专用集成电路设计.E-mail：cwzheng660@163.com.

戴紫彬 男，(1966-)，教授，博士生导师.研究方向为专用集成电路设计、芯片可重构设计.

李 伟 男，(1983-)，博士，讲师.研究方向为专用集成电路设计.

收稿日期：2015－01－20；**修回日期**：2015－03－11
基金项目：国家自然科学基金(61404175)