# 一种面向分组密码的粗粒度可重构阵列及AES算法映射

郭岩松，刘雷波

（清华大学 微电子学研究所，北京 100084）

**摘　要：**为了开发具有一定灵活性的高性能低功耗分组密码处理器，提出了一种粗粒度可重构阵列架构BCORE. 在对分组密码算法进行分析的基础上，在阵列中集成了必要的功能单元和互连，并可以由称为动态部分可重构的配置控制机制在运行时进行配置. 分别用非流水线和流水线方式在可重构阵列上映射了AES算法. 在流水线方式时利用了动态部分可重构能力以提高性能. 仿真和综合结果表明最高吞吐率接近2.5 Gb/s，与其他平台的对比表明粗粒度可重构阵列在实现AES算法时平衡了性能、灵活性和实现效率.

**关键词：**粗粒度可重构阵列；动态部分可重构；算法映射；AES

**中图分类号：**TP302.1　　**文献标识码：**A　　**文章编号：**1000－7180(2015)09－0001－05

# A Block Cipher Oriented Coarse-Grained Reconfigurable Array and AES Algorithm Mapping

GUO Yan-song，LIU Lei-bo

(Institute of Microelectronics，Tsinghua University，Beijing 100084，China)

**Abstract:** For developing a block cipher processor with certain flexibility，high performance and power efficiency，a coarse-grained reconfigurable array architecture named BCORE is proposed. Based on the analysis of a set of block cipher algorithms，the necessary processing elements and interconnections are integrated into the array，which can be programmed at runtime by a control mechanism called dynamically partial reconfigurable. AES algorithm is mapped on the reconfigurable array by non pipeline and pipeline style separately. The dynamically partial reconfigurable ability is exploited for pipeline implementation in order to improve performance. Simulation and synthesis result shows that the maximum throughput achieved is nearly 2.5 Gb/s. Comparing with other platforms reveals that coarse-grained reconfigurable array makes a good balance between performance，flexibility and implementation efficiency.

**Key words:** coarse-grained reconfigurable array；dynamically partial reconfigurable；algorithm mapping；AES

**作者简介：**

**郭岩松**　男，(1976-)，博士后，助理研究员. 研究方向为可重构处理器. E-mail：guoys2005@126.com.

**刘雷波**　男，(1975-)，博士，教授. 研究方向为集成电路设计.

**收稿日期：**2014－12－03；**修回日期：**2015－01－22

**基金项目：**科技部“八六三”重点项目子课题(2012AA011801)