# 可重构 S 盒替换单元研究与设计

常忠祥，陈卓
(国防科技大学 信息通信学院， 湖北 武汉 430010)

摘要： 针对微型终端资源受限导致加密算法单一的问题，对分组密码中的关键部件 S 盒进行可重构设计，提出以 8-1 S 盒为基本可重构单元，将 S 盒转换位布尔函数表达式，采用变量分组、递进计算的方式，大幅减少表达式中的与项个数，提升中间结果的利用率.在此基础上，设计了一种可重构 S 盒单元，并在 TSMC 45nm CMOS 工艺下进行综合，工作频率可达 1.67Ghz，与现有研究成果相比，本设计不仅能够很好的满足当前微处理器的速度需求，且资源占用仅为同类设计的 2/3.

关键词： 分组密码；S 盒；可重构；变量分组；递进计算；

# A Reconfigurable S-box Unit Design for Micro Terminal

CHANG Zhong-ixang, CHEN Zuo
(College of Information and Communication， National University of Defense Technology，
Wuhan 430010， China)

Abstract： Based on the limited resources of tiny terminals lead to the problem of single encryption algorithm， the S-box as the key components of the block cipher is reconfigurable designed. This paper put forward an 8-1 S box as the basic reconfigurable unit， converts S box of Boolean function expressions， with the method of grouping variable， and recursive calculation， dramatically reduced expression of and-item number， increase the utilization of intermediate results. On this basis， we design a reconfigurable unit S box， and under the TSMC 45 nm CMOS technology synthetically. The working frequency can reach 1.67 Ghz， compared with the existing research results， this design can well satisfy the current demand of the speed of the microprocessor. At the same time， the resource usage is only two-thirds of similar design.

Key words： Block cipher; S box; Reconfigurable; Variables Grouping; Progressive calculation;

作者简介：
常忠祥男，(1985-)，讲师，博士.研究方向专用处理器设计. E-mail：changzhongxiang0@126.com.