一种面向分组密码的指令扩展方法

刘 恺[1],敖天勇[1,2],饶金理[1],戴 葵[1],邹雪城[1]
(1 华中科技大学 光学与电子信息学院,湖北 武汉 430074;
2 河南大学 物理与电子学院,河南 开封 475004)

摘 要:针对信息安全领域广泛存在的分组密码运算需求,提出一种面向分组密码的指令扩展方法.通过统计分析47种分组密码算法的运算特点,发现了四种需要加速的基本运算,并设计了四个密码运算单元对这四种基本运算进行加速.将这四个密码运算单元设计成为一个数据触发单元植入微处理器中,从而实现了分组密码运算的加速.该方法具有实现简单、灵活性高等优点.评估结果显示扩展后的微处理器对于常见分组密码算法的加速比为2.4~9.3,且硬件开销仅为原微处理器的1.3倍.

关键词:分组密码;指令扩展;微处理器;数据触发
中图分类号:TP309 **文献标识码**:A **文章编号**:1000-7180(2015)11-0087-05

An Instruction Set Extension Method for Block Cipher

LIU Kai[1], AO Tian-yong[1,2], RAO Jin-li[1],
DAI Kui[1], ZOU Xue-cheng[1]
(1 School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China; 2 School of Physics and Electronics, Henan University, Kaifeng 475004, China)

Abstract: In order to meet the high-performance block cipher processing need existed in the information security field, an instruction set extension method for block cipher calculation is proposed. Based on the analysis of 47 kinds of block cipher algorithms, four basic operations that should be accelerated were found. Therefore, four crypto-operation units to accelerate these operations are designed. Moreover, a data trigger unit which includes the four crypto-operation units is designed and added to the microprocessor to accelerate the block cipher operations. This method has the advantages of briefness, flexibility and so on. The evaluation result shows that the modified microprocessor's speed-up ratios of common block cipher algorithms are about 2.4-9.3 and the hardware cost is only 1.3 times as large as the original microprocessor.

Key words: block cipher; instruction set extension; microprocessor; data trigger

作者简介:
刘 恺 男,(1990-),硕士研究生.研究方向为数字集成电路设计.E-mail:u200818077@gmail.com.

收稿日期:2014-12-11;**修回日期**:2015-01-16
基金项目:国家自然科学基金(61376031);湖北省自然科学基金(ZRZ0051);河南省重点科技攻关(152102210055)