33卷 第1期
2016年1月

微电子学与计算机
MICROELECTRONICS & COMPUTER

Vol. 33 No. 1
January 2016

基于共享存储器的密码多核处理器核间通信机制研究与设计

李 伟[1],李 洋[2],陈 帆[3]

(1 复旦大学 专用集成电路与系统国家重点实验室,上海,201203;2 中国人民解放军66005部队,天津 300300;
3 解放军信息工程大学,河南 郑州 450000)

摘　要:为有效解决多核密码处理器中核间通信对密码处理性能制约的问题,研究了分组、序列、杂凑密码算法多核处理过程中核间通信的特点.依托分簇式的密码多核处理器,提出了基于共享存储器的硬件结构,能够有效支持256 bit以内的任意数据位宽的核间通信传输.提出了基于自选锁邮箱的同步器硬件结构,具备加1、置数、乒乓同步等功能.结合此共享存储器与同步器结构,提出了基于共享存储器的密码多核处理器核间通信机制.基于65 nm CMOS工艺库,对共享存储器与同步器进行了实现,实验结果表明,提出的核间通信机制具有硬件开销小、同步效率高的特点,2个时钟周期能够完成4个处理器核对于4组256 bit数据的核间通信与同步操作,相比其他核间通信方式,具有明显的优势.

关键词:核间通信;密码多核处理器;共享存储;同步器

中图分类号:TN4　　**文献标识码**:A　　**文章编号**:1000—7180(2016)01—0019—05

Research and Implementation of Communication Mechanism Among Cores Based on Shared Memory for Cryptographic Multi-core Processor

LI Wei[1], LI Yang[2],CHEN Fan[3]

(1 State Key Laboratory of Special Integrated Circuit and System,Fudan University, Shanghai 201203, China;
2 Troops 66005 of PLA, Tianjin 300300, China;3 PLA Information Engineering University, Zhengzhou 450000, China)

Abstract: In order to solve the problem that communication mechanism among cores cannot satisfy the high speed cryptographic operations' demand, this paper analyzed the communication characteristic of block, stream and hash cryptographic algorithms in the multi-core processor. Based on the multi-cluster structure, this paper proposed a new structure of shared memory, which could support communication among cores of random data width under 256bit. Besides, this paper proposed a way of email data synchronization which is based on improved spin lock. Each synchronization unit includes the function of add 1,. In the combination of shared memory and synchronization unit, this paper put forward the communication mechanism among cores based on shared memory. Based on the 65nm CMOS technology, the synthesis of shared memory and synchronization unit has been achieved, the result proves that our proposed the hardware area of communication mechanism among cores is small, the efficiency of data synchronization is high. The 256-bit data could be synchronized in two clock cycles among four processors, Comparing with other communication mechanisms, the communication mechanism get a better efficiency.

Key words: communication mechanism; cipher multi-core processor; shared memory; synchronization

作者简介:

李　伟　男,(1983-),博士研究生,讲师.研究方向为专用集成电路设计. E-mail:liwei12@fudan. edu. cn.

李　洋　男,(1983-),硕士研究生.研究方向为安全专用芯片设计.

陈　帆　男,(1991-),硕士研究生.研究方向为安全专用芯片设计.