

多核密码处理器数据缓存机制研究

陈晓钢¹, 李 伟^{1,2}, 徐金甫¹

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

摘 要: 对多核密码处理器的数据缓存特点进行了研究, 提出了一种基于双 RAM 与硬件队列的多核密码处理器数据缓存机制, 并设计了相应的多核数据分配控制器. 最后与现有的数据缓存方式在多核密码处理器中的应用性能进行了对比, 结果证明提出的多核数据缓存机制具有更高的吞吐率与核心利用率, 从而提高了多核密码处理性能.

关键词: 多核密码处理器; 数据缓存; 双 RAM

中图分类号: TP309.7

文献标识码: A

文章编号: 1000—7180(2016)05—0153—04

Research on Data Buffer Mechanism of MCP

CHEN Xiao-gang¹, LI Wei^{1,2}, XU Jin-fu¹

(1 PLA Information Engineering University, Zhengzhou 450000, China;

2 State Key Laboratory of Special Integrated Circuit and System, Fudan University, Shanghai 201203, China)

Abstract: This paper researched the data buffer feature of MCP and proposed a data buffer mechanism based on couple RAM and circuit-queue. Then this paper designed a data buffer controller. At last, different schemes of MCP data buffering are compared. The result shows that the mechanism proposed in this paper has higher throughput rate and higher core use ratio.

Key words: multi-core cipher processor; data cache; couple RAM

1 引言

多核密码处理器以密码处理任务为基本调度单位^[1], 以任务为核心分配数据并组织运算资源, 不同的任务决定不同的多核协同方式与数据分配方式. 任务调度单元的载体可以是多核中最靠近外部接口的单个核^[2]或是专用的调度控制器^[1-3], 由于密码协处理器长于密码运算而控制能力较弱, 一般采用专用控制器调度数据. 调度控制器将外界输入的任务包缓存、解析并进行相应的分配. 因此除单个核的运算能力外, 系统数据分配的高效性与灵活性将成为制约整体性能的关键. 不符合密码处理特征的数据分配方式会使核空闲而降低系统性能.

数据分配效率的关键在于控制器的解析能力与缓存系统的组织. 传统的多核数据缓存方式有基于共享

存储器的方式^[4]和基于先进先出队列(FIFO)的方式^[1]. 然而共享存储器方式具有数据存取复杂的缺陷, FIFO具有调度能力过弱的缺陷, 在应用于基于任务的多核密码处理器时会严重制约处理性能. 基于以上原因, 本文提出了一种基于双 RAM 的多核密码处理器数据缓存机制. 并将缓存机制应用于图 1 所示的多核密码处理器结构中^[1], 对其进行了性能评估.

2 多核数据缓存机制

2.1 双 RAM 数据缓存机制

在基于共享存储器的方式中, 外部输入数据被缓存在公用的存储区中, 控制器依据调度算法将外部输入的数据存入存储器或是从存储器中挑选数据并进行解析分配, 两种操作都需要通过调度算法实现. 由于调度算法是一种查找程序, 过小的存储器容量将会失去

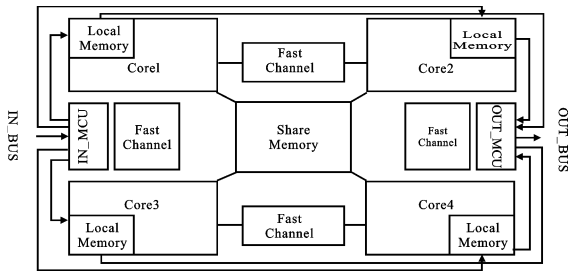


图 1 多核密码处理器架构

共享存储器方式灵活调度数据包的优势,过大的存储器和过多的数据将使查找时间恶化,最终使调度的时间大于数据处理的时间而制约多核的性能。

基于 FIFO 的方式中,控制器以先到先服务的原则调度数据,由于输入的数据不需要安排存储位置,可以快速放入队尾中. 控制器分配数据时调度目标只有处于队列头部的数据包,可以快速解析,但是当队列头部所对应的核忙时控制器无法调度后续的数据包而使本可以被利用的核空闲从而降低性能。

为同时利用共享存储器的随机查找、存取优势与 FIFO 的快速缓存、分配优势,本文拟采用两块随机存取存储器(RAM)分别实现两者的功能. 三种缓存方式的流程图如图 2 所示。

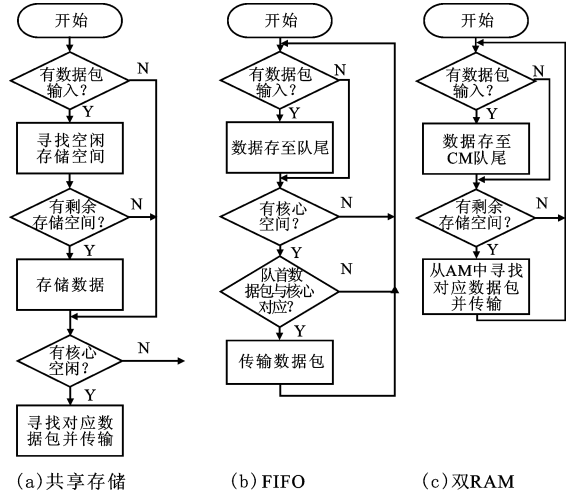


图 2 三种缓存方式流程图

其中缓存 RAM(CM)负责数据缓存,分配 RAM(AM)负责数据分配. CM 包含队尾指针,在初始状态下其指向 RAM 的 0 地址,当有数据输入时将数据写入队尾然后指针自增指向下一地址. 工作时 CM 的表现行为就如同一个 FIFO,不断将输入数据以先入先出原则写入 CM. 由于不存在定位存储位置与解析问题,在状态机控制下可以以每周期 1 组数据的速度缓存数据。

AM 包含上组 CM 所缓存的数据,工作时 AM

只输出数据而不存储数据,因此控制器面对的是一个静态队列,查找算法将简单很多。

当 AM 中的数据包全都分配完成时,将 AM 与 CM 功能互换,既将原先的 CM 作为 AM,AM 作为 CM,此时 CM 完全清空,AM 再次填满. 由于只涉及两个 RAM 的功能互换而不是实际存储内容互换,因此这一操作可以在单个周期内完成。

通过采用双 RAM 的缓存结构并附加很少的额外控制资源本文很好的解决了共享存储查找缓存过慢,FIFO 调度不够灵活的矛盾,利用了两者的优势提高缓存性能。

2.2 基于硬件队列的查询机制

双 RAM 的数据缓存机制降低了一定的复杂性并增加了数据缓存效率,但是数据分配依然依赖软件查找算法,搜寻可用数据时需要对整个 AM 进行查找,软件查找严重制约了数据分配效率,造成数据缓存与数据分配速率的失衡,引起性能损失. 为加速数据分配过程,本文针对多核密码处理器的任务包分配特点设计了基于硬件队列的数据包查询机制。

在以任务包为核心的多核密码处理器中,任务包包含了待处理数据的数据长度、所需的密码算法与工作模式,由于在单次映射方案中,多核面对有限的任务进行调度映射,数据包类型可事先获知,因此可通过快速硬件解析的方式解析出映射方案与对应核,并将解析结果存储在不同硬件队列中. 那么进行数据分配时只需取出相应队列队首便可知其数据包存储位置,从而同样可以在周期级做到数据包的分配而不需要软件查找数据包. 硬件队列的工作流程如图 3 所示。

本文通过双 RAM 的缓存机制加速了数据缓存,将数据的缓存与分配分离执行,并通过硬件队列的方式加速了数据分配,从而在周期级实现了整个数据包的缓存、查找、分配过程,极大加速了多核密码处理器的数据分配效率。

3 多核数据缓存控制器设计

3.1 数据缓存控制器总体结构

基于多核数据缓存机制的研究本文设计了相应的数据缓存控制器,控制器采用 3 级流水的 RISC 结构,采用 16bit 指令压缩代码密度,嵌入了双 RAM,硬件队列,硬解析部件,并设计了相应的专用指令以加速数据缓存分配. 控制器的总体结构如图 4 所示。

控制器采用了取指、译码、执行/回写 3 级流水线,由于控制器结构简单,可以工作在比密码协处理器快数倍的时钟域下,进一步加快了数据分配效率。

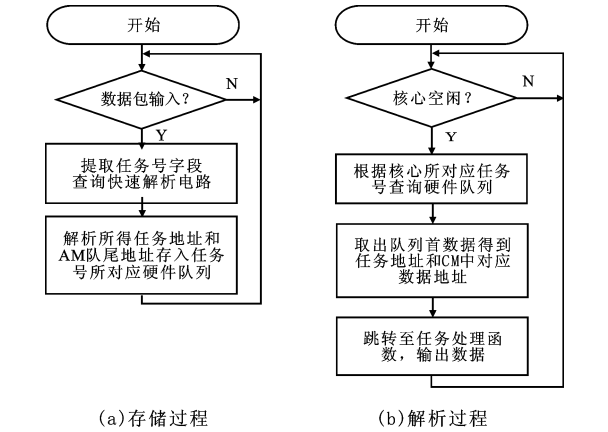


图 3 硬件队列工作流程图

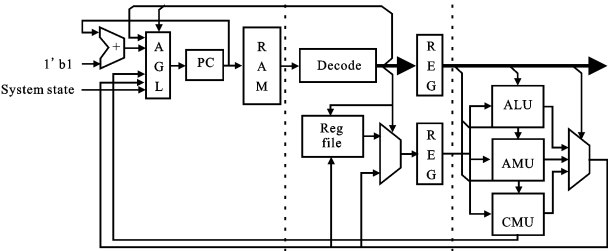


图 4 数据缓存控制器总体结构图

控制器的取指级加入了地址生成逻辑部件(AGL)用于处理函数调用、跳转,以及 AM、CM 的异常处理。控制器将 AM、CM 及其相应的控制逻辑组合成 AMU、CMU 单元并嵌入到控制器的执行/回写级中。位于执行级中的 AMU、CMU 单元能够快速被配置或是将结果输出至寄存器中。

3.2 缓存存储单元设计

缓存存储单元(CMU)主要包含 CM,快速解析电路(HP),硬件队列(HQ)以及相应的控制逻辑。其结构图如图 5 所示。

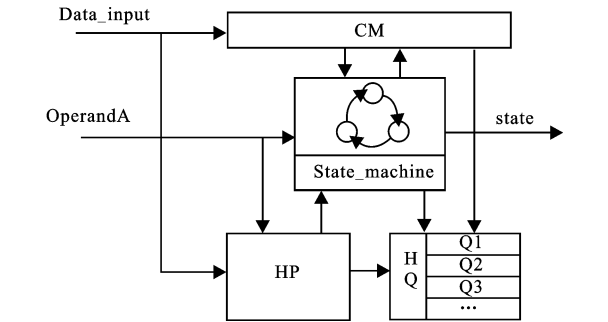


图 5 缓存存储单元结构图

整个缓存存储单元以状态机为核心,在有数据输入时高速将数据存入 CM 中,同时输入数据进入快速解析电路,快速解析电路由一块事先由控制器配置好的小 RAM 组成,RAM 以输入包头中的任务号为地址输出其对应的密码处理任务地址,并将其放入硬件

队列中。硬件队列以分块的 RAM 组成,以包头中的任务号为索引,存入了密码处理任务地址以及相应的 CM 指针地址。当一个任务包被缓冲入 CM 中时,其对应的任务地址和在 CM 中的首地址同时被存入了硬件队列中,在任务解析时只需根据所需任务寻找相应队列,从队列中取出的数据既是任务处理程序的地址以及所需数据在 CM 中的首地址。

3.3 分配存储单元设计

分配存储单元(AMU)主要包含 AM 和硬件队列(HQ)以及相应的控制逻辑。其结构图如图 6 所示。

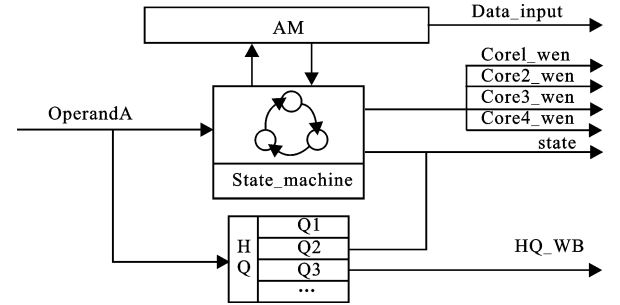


图 6 分配存储单元结构图

当 AM 与 CM 功能互换后两边的硬件队列也互换,则 AMU 中的硬件队列已存储有数据。当控制器检测到有核心空闲后便可通过任务号查询队列,从队首取出的数据既为对应任务程序地址以及相应数据在 AM 中的位置,则控制器只需配置好需要将数据写至哪个核以及数据包的大小便可启动状态机将数据连续输出至对应核中,从而在数个周期内做到数据包的解析。

4 性能评估

为对缓存模型性能进行评估,本文使用 MATLAB 建立了每种缓存的周期级模型,并将多核分别适配为 AES,DES,SMS4,IDEA 四种密码算法,随机生成 1 000 组不同算法,不同大小的用户数据包,以多核最终处理完所有数据的时间衡量每种缓存模型的性能。

由于文献[1-6]中的处理器处理性能各不相同,本文首先评估了核心的密码运算性能对总运算时间的影响。结果如图 7 所示,当核心运算速率和数据传输速率处于同一数量级时采用双 RAM 具有和 FIFO 一样的性能,RAM 缓存方式由于寻找数据包时间限制了总体性能;当数据传输速率为核心运算速率的一百倍时采用双 RAM 的方式体现出了最高的性能;当数据传输速率为核心运算速率的一千倍

时运算时间远大于 RAM 寻找数据包时间,因此 RAM 的性能大于 FIFO,而采用双 RAM 具有和 RAM 近似的性能.就实际密码运算应用场景中,运算时间比为百倍最常出现,因此采用双 RAM 缓存做到了局部最优.

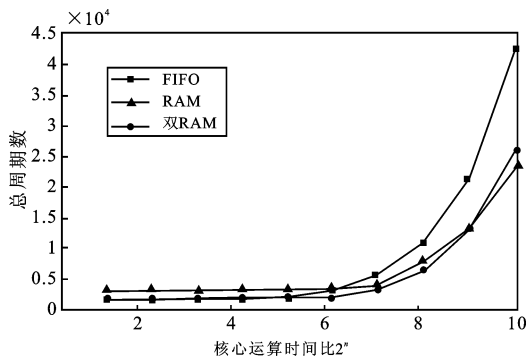


图 7 不同运算时间比的处理时间

本文在 200 MHz 下评估了数据包大小对缓存性能的影响如图 8 所示.当数据包过小时每种缓存方式数据分配都占用了大量时间,当数据包变大时运算时间所占时间比增加,整体性能增加,在数据足够大时 FIFO 缓存方式不再具有数据分配优势而性能稳定,在数据包大小是 3 200 bit 左右采用双 RAM 方式取得最佳的性能,当数据包大小进一步增加 RAM 中可供分配的数据包数量变少,RAM 调度优势变小,双 RAM 和 RAM 的性能趋于稳定.双 RAM 方式同样获得了最优的性能.

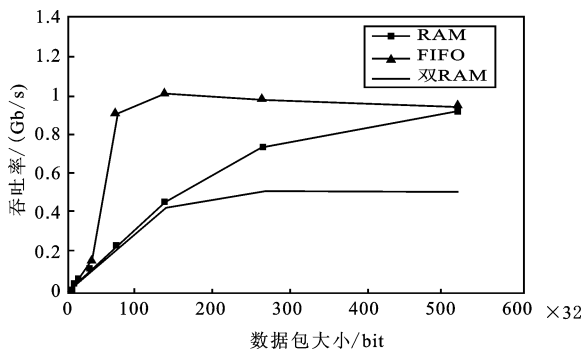


图 8 数据包大小对吞吐率的影响

本文用 verilog 实现了整个多核数据缓存控制器,并在 CMOS 65ns 工艺库下进行了综合,综合结果如表 1 所示.

表 1 综合结果		
时钟频率/MHz	整体面积/mm ²	最大功耗/W
1250	0.782	0.510

在固定密码处理核心为文献[7]的密码协处理

器,数据包大小为 32 kB,频率为 200 MHz 时本文对不同的文献方案的性能进行了比较,如表 2 所示.

表 2 不同文献性能对比				Gb/s
算法/协议	本文	文献[1]	文献[3]	文献[4]
四算法并行	1.069	0.650	0.554	0.670
4 路 AES	2.507	2.633	2.012	1.222
AH 协议	2.013	1.889	1.176	—
握手协议	1.593	1.839	1.452	—

结果表明在映射越复杂的情况下本文所取得的性能优势越明显,在映射 4 路完全不同算法时取得优势最大,而在映射 4 路相通算法时本文和最快的文献[1]相差不大,在映射串行的协议时由于调度非常简单本文较 FIFO 结构有一定性能差距.

5 结束语

本提出了双 RAM 结构的数据缓存机制,并与不同的缓存方式进行了对比.结果表明,采用双 RAM 结构数据缓存存在一些极限情况中不输于传统缓存机制的性能,而在一般应用场景中具有最高的数据吞吐率.解决了多核密码处理器接口数据吞吐率的瓶颈问题和数据分配灵活性问题,进一步提高了多核密码处理器的数据缓存和分配效率,提升了多核处理性能.

参考文献:

[1] 戴乐育,李伟,徐金甫,等.面向任务级的多核密码处理器数据分配机制[J].计算机工程与设计,2015,36(1):65-71.

[2] Intel. Intel IXP1200 Network Processor Family HardwareReferenceManual[EB/OL]. [2015-04-20] (2001-01-01). <http://www.intel.com>.

[3] Zhiyi Yu, Kaidi You, Ruijin Xiao, et al. An 800MHz 320mW 16-Core Processor with Message-Passing and Shared-Memory Inter-Core Communication Mechanisms[C]// IEEE Internation Solid-state Grcuits Conference. [s. l.]:IEEE, 2012 : 64-65.

[4] WANGHaixin, BAI Guoqiang, CHEN hongyi. Design of a high performance network security processor[J]. J Tsinghua University (Science & Technology), 2010, 50(1) : 13-17.

[5] 肖瑞瑾,多核处理器层次化存储体系结构[D].上海:复旦大学,2012.

[6] 权衡,多核处理器运算及核间通讯模块设计研究[D].上海:复旦大学,2012.

储系统温湿度监测,准确性较高,通过监测优化,提高了温湿度监测跟踪能力,改善仓储存储条件.

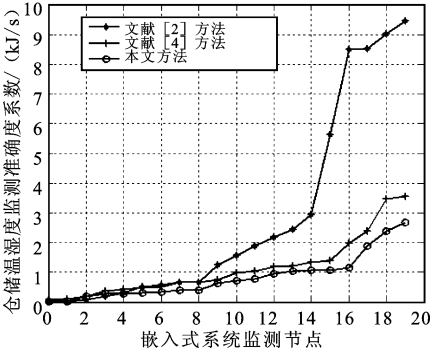


图 4 性能分析

5 结束语

基于嵌入式设计的仓储系统温湿度监测设计是保证仓库系统稳定运行,提高仓储存储条件的关键.传统的仓储系统温湿度监测方法采用 RFID 射频读写监测方法,无法有效监测电路静态功耗的变化特征,对仓储温湿度监测结果不准确.对此,本文提出一种基于活性因子激励的嵌入式仓储系统温湿度监测方法.研究得出,采用本文监测方法,能实时有效地实现对基于嵌入式设计的仓储系统温湿度监测,准确性较高,稳定性好.

参考文献:

[1] 杨石,王艳玲,王永利. 云计算环境下基于蜜蜂觅食行为的任务负载均衡算法[J]. 计算机应用, 2015, 35(4): 938-943.

[2] Zhang Huanguo, Li Jing, Pan Danling, et al. Trusted Platform Module in Embedded System[J]. Journal of Computer Research and Development, 2011, 48(7): 1269-1278.

[3] 王爱珍,侯成郭,任国风. 直接序列扩频的分层级联联机共振接收算法[J]. 计算机应用, 2015, 35(4): 934-937, 959.

[4] 何炎祥,喻涛,陈勇,等. 面向嵌入式系统绿色需求的数据分配方法[J]. 计算机研究与发展, 2015, 52(1):

94-104.

[5] 赵威. 基于鱼雷自导的舰船尾流回波模型建立方法[J]. 舰船电子工程, 2013, 33(4): 81-83.

[6] 张金宏,王兴伟,黄敏. 面向绿色互联网的低功耗多播路由算法[J]. 通信学报, 2014, 35(增刊 1): 134-140.

[7] 许海洋,庄毅,顾晶晶. 一种面向嵌入式软件体系结构的形式化建模方法[J]. 电子学报, 2014, 42(8): 1515-1521.

[8] 林颖,张智雄. 构建基于 DSpace 的中文机构仓储系统[J]. 图书情报工作, 2007, 51(2): 87-91.

[9] 黄志雨,嵇启春,陈登峰. 物联网中的智能物流仓储系统研究[J]. 自动化仪表, 2011, 32(3): 12-15.

[10] 陈俊,魏光磊,高建,等. 大运汽车仓储系统分析与优化对策研究[J]. 中国储运, 2015, 24(2): 112-115.

[11] 邢志光,杨艳玲. 新型港口散料清洁环保船舱式地下仓储系统的探讨[J]. 港口装卸, 2015, 37(2): 29-31.

[12] 王秀星. 电子商务环境下智能仓储系统的应用[J]. 信息技术与信息化, 2015, 32(4): 73-74.

[13] 王丹竹,郎茂祥. 物流仓储系统可靠性请假 Petri 网仿真研究[J]. 生产力研究, 2015, 29(6): 60-63.

[14] 戴善溪,张效民. 基于 ZigBee 技术的数字式温湿度监测网络设计[J]. 国外电子测量技术, 2010, 29(2): 47-49.

[15] 王志强,陈平. 基于 GPRS 技术的粮库温湿度监测系统设计[J]. 安徽农业科技, 2010, 38(14): 7552-7553.

[16] 刘庆赞,焦斌亮,刘永富. 仓库温湿度监测与 nRF905 无线传输系统的设计[J]. 传感器与微系统, 2011, 30(5): 101-103.

[17] 李正民,张兴伟,柳宏川. 基于 CC2530 的温湿度监测系统的设计与实现[J]. 测控技术, 2013, 31(5): 25-28.

[18] 张璘,陶琳,袁江南,等. 基于 GSM 网络的远程温湿度监测系统研究及实现[J]. 电子技术应用, 2012, 38(6): 93-96.

[19] 郭东平,陈军,熊刚,等. 基于手机短信的设施农业温湿度远程监测系统的设计[J]. 电子设计工程, 2015, 23(21): 58-60.

作者简介:

李宏升 男, (1973-), 工学硕士, 讲师. 研究方向为互联网与嵌入式系统. E-mail: li-hs@sohu. com.

(上接第 156 页)

[7] Zibin Dai, Wei Li, Xiaohui Yang, et al. The Research and Implementation of Reconfigurable Processor Architecture for Block Cipher Processing[C]// ICES. San Francisco, CA: IEEE, 2008 : 587-593.

作者简介:

陈晓钢 男, (1991-), 硕士研究生. 研究方向为 SoC 与微处理器设计.

李伟 男, (1983-), 博士研究生. 研究方向为多核密码处理器设计.

徐金甫(通讯作者) 男, (1965-), 博士, 副教授. 研究方向为专用集成电路设计. E-mail: edward. s. chen0401@qq. com.