

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 Wei¹, LI Yang², CHEN Fan³

(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

1 引言

传统的单核密码处理器已经无法满足新型复杂密码算法日益增长的性能要求和用户日益增长的应用需求. 而密码多核处理器作为多任务密码算法和多密码算法加密协议的理想载体,能够相比于单核密码处理器更加灵活、更加高效地实现密码运算操作. 所以设计高效的密码多核处理器已经成为目前信息安全领域亟待解决的问题,具有重要的现实意义. 与此同时,多核处理器中核间通信机制的设计,是决定多核处理器性能优劣的关键技术之一. 目前,国内外的专家学者对多核处理器核间通信机制进行了大量的研究. 现有核间通信机制主要包括基于共享总线的核间通信机制、基于共享存储的核间通信机制和基于 NoC (system on chip) 数据包传递的核间通信机制^[1-2]. 但是通用多核处理器核间通信机制的设计技术在密码多核处理器上实现时仍存在一定的不足^[3]. 由此本文提出了新的机制和设计方法.

2 密码多核处理中数据核间交互特征分析

通过对大量密码算法特征的分析^[4-5],采用多核结构实现密码算法时,多个处理器核间存在着频繁的数据交互操作,主要表现为三种类型. 分组密码算法中轮运算和子密钥生成操作间的数据通信量基本等于密钥长度,如表 1 所示. 每轮的核间通信量都是一个子圈密钥,如果核间传输一个子圈密钥通过多条指令进行实现,那么将会造成对轮运算过程所需指令周期的增多,需要待子圈密钥全部传输完成后进行相应的下一轮运算. 特别是考虑到分组密码算法普遍具有多轮迭代的特点,将会造成对整体分组密码算法处理性能的下降. 换言之,分组密码算法需要一种快速高效的核间通信方式,且能够满足子密钥的传输位宽需求.

表 1 分组密码算法轮运算与子密钥生成间通信量分析

密码多核处理模式	核间通信量/轮	核间通信总量/bit
AES128	128	$10 \times 128 = 1280$
SM4	32	$32 \times 32 = 1024$
IDEA	32	$52 \times 16 = 832$
DES	64	$16 \times 64 = 1024$
AES256	256	$10 \times 256 = 2560$

序列密码算法中初始化与密钥流生成间的数据通信量基本等于移存器的总长度,如表 2 所示. 初始

化后的核间通信都是将移位寄存器的状态序列传递给相应的处理器核进行后续的密钥流生成操作. 核间通信的总量远小于分组密码算法. 此外由于序列密码算法初始化完成后能够产生大量的密钥流,移存寄存器状态序列通过核间通信传递的效率不会对密钥流的产生速率造成影响,因此序列密码算法对核间通信的效率要求不是很高.

表 2 序列密码算法初始化与密钥流生成间通信量分析

序列密码多核处理模式	核间通信总量/bit
A5	$18 + 21 + 22 = 61$
E0	$25 + 31 + 33 + 39 = 128$
LILI-II	$127 + 128 = 255$
Grain-80	$80 + 80 = 160$
MICKEY128	$128 + 128 = 256$

在密码算法多分支拆分于不同密码处理器的模式中,不同密码算法的核间数据通信量具有很强的差异性,如表 3 所示. 核间的通信量主要依据每个密码算法的处理特征. 例如 SM3 算法每轮仅需 2 个 32 bit,而 SHA-512 算法每轮需要 5 个 64 bit. 基于密码算法多分支拆分方式对核间通信效率的要求具有一致性,即要求能够快速高效地传递核间数据. 主要原因在于核间数据的传递都是由于算法处理过程中的数据相关性引起的,这些核间通信数据直接影响着轮运算的继续计算,所以同样需要一种快速高效地核间通信方式,且能够满足相关性所带来的数据位宽需求.

表 3 密码算法多分支拆分情况下的核间交互通信量分析

密码多核处理模式	核间通信量/轮	核间通信总量/bit
SM3	64	$(32 \times 2) \times 64 = 4096$
SHACAL2	64	$(32 \times 2) \times 64 = 4096$
SHA-256	160	$(32 \times 5) \times 64 = 10240$
SHA-512	320	$(64 \times 5) \times 80 = 25600$

综上所述,需要设计一种面向密码运算的专用核间通信方式,具有高效率、大位宽的数据传递特点. 考虑到 CSIP-I 指令结构中三源两目的的特点,结合上述对密码核间通信量的分析,数据位宽选取为 256 bit 能够确保单条指令即能够完成对核间通信数据的读/写操作,而且能够减少通信过程的时钟周期.

3 密码多核处理器总体结构

密码多核处理器采用了如图 1 所示的硬件结构,整体结构采用了分簇式结构.一个多核密码处理器簇 Cluster 包含了四个同构的密码处理核心 (PCore0~PCore3)、输入 FIFO、输出 FIFO、输入微程序控制器 (Import Ctrl)、输出微程序控制器 (Export Ctrl) 以及核间共享存储区.外部数据由输入 FIFO 进入簇内,在输入控制器的控制下进入各个密码处理核心,处理完成后的数据在输出控制器的控制下进入输出 FIFO.簇内密码处理核心通过共享存储器进行数据的传递.多个多核密码处理器簇通过路由节点 Router 相连,在空间上构成 2D-Mesh 的 NoC 网络结构^[6].

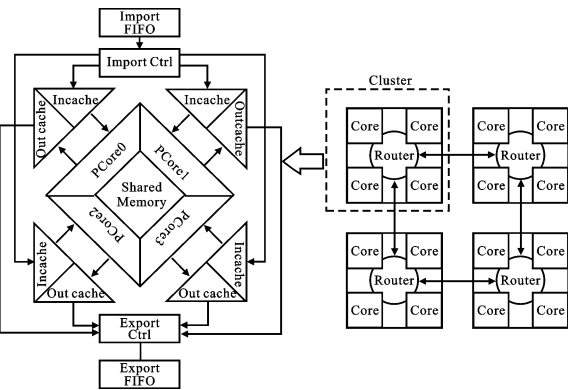


图 1 多核密码处理器总体结构

依托整体的密码多核处理器结构,在具体的密码算法映射过程中,簇内主要承担的是单任务下的密码处理需求,簇间主要承担多任务下的密码处理需求.由于在单任务下的密码数据交互非常频繁,且与通用计算的数据交互特征具有明显的差异性,因此簇内面向密码运算的共享存储器及通信机制设计就凸显的尤为重要,而且核间通信效率直接影响着密码在多核模式下的处理性能.

4 密码多核处理器中共享存储器设计

由本文第 2 节的分析可知,密码多核处理模式中的核间数据通信位宽较大,目前通用多核处理器的核间数据通信位宽大多集中在 32 bit,在密码多核处理器中,如果选择 32 bit 位宽作为通信位宽,则将会导致密码运算中的核间通信数据需要多个时钟周期才能够完成同步,从而核间通信的效率将会严重降低密码多核处理器的密码实现性能.相反,如果选用大位宽进行通信,例如 1024 bit

或更高,则会造成资源的浪费.同时增加硬件开销成本和功耗的提升.因此本文在第 2 节分析的基础上,采用 256 bit 作为通信的最大位宽,主要目的能够实现密码运算过程中的核间数据交互在一个时钟周期内完成,从而不会导致因核间数据交互的延迟造成密码运算执行过程的停顿.与此同时,考虑到不同密码算法在多核处理模式下核间通信数据位宽的不同特点,共享存储器需要支持对不同数据位宽的读写访问操作.

综上所述,本文提出的簇内共享存储器的结构如图 2 所示.簇内共享存储器主要有 16 个存储块 (Block0~Block15) 组成,且每个 Block 由存储区和标记区两部分组成,存储区由 8 个 32 bit 的寄存器组成,主要用于存储核间通信的数据.标记区由 5 个 1 bit 的寄存器组成,主要用于标记每个处理器核心对共享存储区的使用情况.整体共享存储器包含 8 个独立的写端口和 8 个独立的读端口,每个处理器核心 (Pcore0~Pcore3) 的地位是平等的,每个存储区可由任意处理器核心根据通信需求通过选择网络传输 1~8 组的 32 bit 数据.该结构的设计在保证了核间通信大位宽数据传输高效地基础上,又兼顾了对小位宽数据传输的支持.

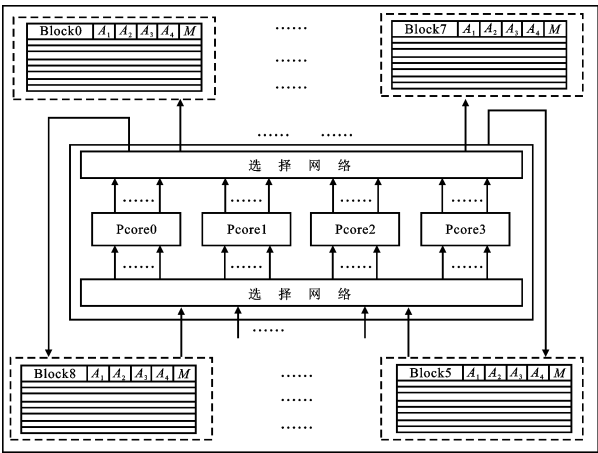


图 2 簇内共享存储器硬件结构

5 密码多核处理器中同步器设计

本文提出的同步器的设计主要解决了两个主要问题,即“锁”与“钥匙”的问题.“锁”对应解决的是存储访问一致性冲突问题,即在多核系统内如果出现多个处理器核同时访问一个存储区时写冲突问题;“钥匙”对应解决的存储区空间的释放问题,即在多核系统中存储区数据被写入后,该数据的接收运算核心何时才能读取该数据的问题.

本文提出了一种自选锁的邮箱同步机制,该机制与通用同步机制的不同在于该机制的实现由存储区上的标记位与邮箱同步单元两部分配合完成.其中存储区的标记位主要解决同步过程的“上锁”问题,邮箱同步单元主要解决同步过程中“钥匙”的传递问题.“锁”的建立是通过在每个共享存储区上设计一个标记位.当有运算核心向共享存储区中写入数据后,将标记位置数,即给该块存储区上锁,避免任一运算核心再一次写入数据而覆盖之前的数据.每个 Block 上设计的标记区如图 3 所示.

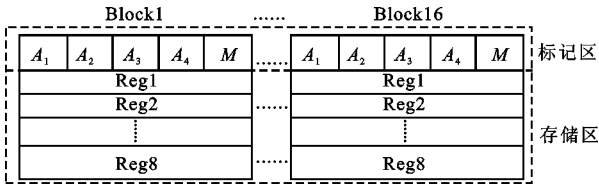


图 3 Block 中的标记区

标记区中的每 1 bit 对应该存储区内数据的一个流向.标记位中的 $A_1 \sim A_4$ 分别对应簇内四个处理器核心, M 对应着簇间传输.当某个 Block 的标记位 A_i 为“1”时,标识当前 Block 有向对应处理器核心的待通信任务;“ M ”位 A_i 为“1”时,标识当前 Block 中有需要通过簇间高速通道传输的数据.当且仅当 Block 的标志区为 5 bit 全“0”状态时,该 Block 才能被运算核心写入数据,否则标志着该 Block 已被占用,直到 Block 内数据的目的运算核心读取该数据后清除标记位,该 Block 的存储空间才能被释放.

在同步过程中,存储区被“上锁”之后,本次通信的接收方需要得到“钥匙”才能对存储区的数据进行“解锁”并读取.因此本文提出在各运算核心中设计一个独立的邮箱单元,负责接收通信发起方传递来的钥匙.在接收方得到钥匙后,读取共享存储区的数据同时将“锁”打开,以释放存储空间.簇中运算核心检测到存储区的“锁”打开后,便可开始新一轮的同步操作.本文提出了一种硬件结构简单且同步高效地邮箱同步单元.每个处理器核包含一个邮箱同步单元,处理器核 0 所对应的邮箱同步单元的结构如图 4 所示.一共包含了 6 个 8 bit 专用寄存器,每两个寄存器分为一组,主要目的在于能够支持同步中的乒乓操作,即 (Mreg20、Mreg21)、(Mreg30、Mreg31)、(Mreg40、Mreg41),且分别对应本簇内其余三个运算核心.

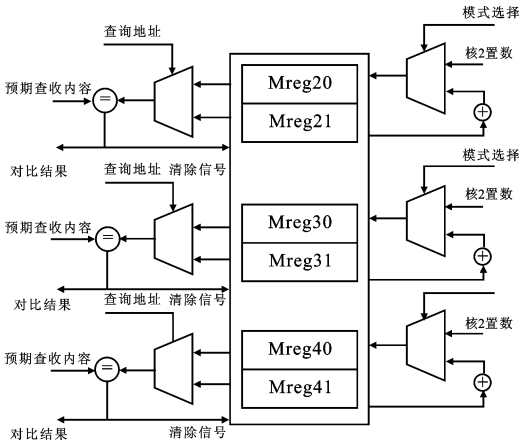


图 4 邮箱同步器结构

每个邮箱寄存器支持置数与自加 1 两种模式.对于自加 1 模式,主要应用于对于同一类型数据的多次核间通信过程中.例如,PCore1 完成子密钥生成运算,PCore2 完成轮运算加密,PCore2 每轮运算都需要 Pcore1 提供子密钥,此时 PCore1 每完成一个子密钥的核间通信后,发送邮件进行一次“自加一”,Pcore2 则针对邮箱进行检测 Pcore1 所对应的邮箱数值,完成对应的轮运算,否则继续查询.对于置数模式,主要应用于不同类型数据的核间通信过程中,在核间通信中可约定通信内容用固定代码表示,例如邮箱中数值“1”表示当前同步数据为“IV 向量”、数值“2”表示该数据为“密钥”等约定,以此在同步过程中告知目的运算核心接收数据的用途.

6 性能分析

本文以一次完整的簇内通信过程为例说明本文设计的基于自旋锁的邮箱同步机制的处理流程.该处理过程如图 5 所示.该通信过程中,第一步先由通信发起方对通信信道即共享存储单元进行可用性检测.当共享存储单元存储区可用时,第二步再由发送方将数据写入该存储单元并对该存储单元标记位上锁.第三步发送方通过同步单元将存储区的“钥匙”发送至接收方.第四步接收根据“钥匙”指示,读取通信数据.

基于 65 nm CMOS 工艺标准单元库,本文对所设计的共享存储器和同步器进行综合实现,得到的综合结果如表 4 所示.共享存储器和同步器的时钟频率可以达到 1 GHz,能够满足高性能密码多核处理器的核间通信需求.

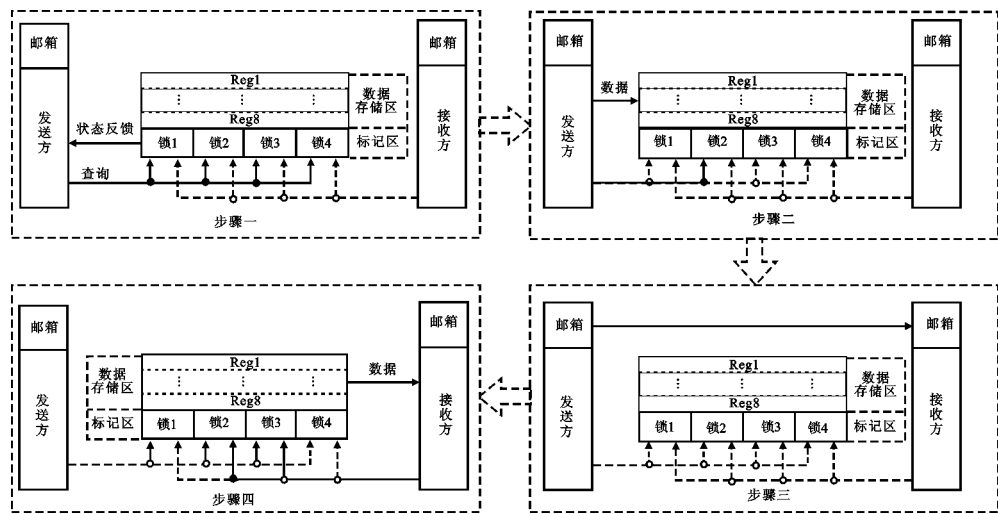


图 5 基于自旋锁的邮箱同步机制的处理流程

表 4 ASIC 综合结果

模块	约束/ns	面积/ μm^2	Slack/ ns	工作频率/ GHz
共享存储器	1	32 034	+0.00	1
同步器	1	1 628	+0.01	1

为了进一步分析本文提出的基于核间通信的效率,本文将文献[7]提出的自旋锁和旗语方案,以及文献[2]提出的邮箱同步方案分别进行了实现,由表 5 可以看出,本文设计的同步器,相较于传统自旋锁和旗语同步方式具有较短的同步硬件开销.此外,本文设计的同步器中同步过程仅需要 2 个时钟周期即可完成.相比自旋锁和旗语方案具有明显的优势.

表 5 核间通信同步效率对比

同步方式	自旋锁 ^[7]	邮箱同步 ^[2]	本文方案
面积/ μm^2	3 413	1 436	1 628
面积增加千分比/%	0.480	0.202	0.229
通信机制	共享存储	共享存储	共享存储
支持同步方式	置数	置数	置数、加 1、乒乓同步
同步所需指令周期数	≥ 3	≥ 3	2
最大同步处理器核数	2	2	4

7 结束语

综上所述,本设计提出的同步器设计具有较小的硬件开销,不仅支持的同步功能丰富,更加贴近密码多核处理的特征,而且同步的效率,缩小了因核间通信对密码处理性能的影响.从而更加满足密码多核的处理需求.

参考文献:

[1] 杨国芳. 多核处理器核间通信技术研究[D]. 哈尔滨:

哈尔滨工程大学, 2011.
[2] Yu Z, You K, Xiao R, et al. An 800MHz 320mW 16-core processor with message-passing and shared-memory inter-core communication mechanisms[C]// Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2012 IEEE International. USA, San Francisco, IEEE, 2012: 64-66.
[3] Bin Liu, Bevan M Baas. Parallel AES encryption engines for many-core processor arrays[J]. IEEE Transactions on Computers, 2013, 62(3):536-547.
[4] 金晨辉, 张少武, 胡斌, 等. 密码学[M]. 北京: 高等教育出版社, 2007.
[5] Delfs H, Knebl H, 肖国镇, 等. 密码学导引: 原理与应用[M]. 北京: 清华大学出版社, 2008.
[6] Dally W J, Towles B P. Principles and practices of interconnection networks [M]. Burlington Massachusetts, Morgan Kaufmann, 2004.
[7] Hu W, Wang R, Chen Y, et al. Godson-3B: A 1GHz 40W 8-core 128GFlops processor in 65nm CMOS[C]// Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2011 IEEE International. USA, San Francisco, IEEE, 2011: 76-78.

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.