

多核密码处理器中的片上网络互连结构研究

杜怡然¹, 李 伟^{1,2}, 戴紫彬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: 为有效解决目前单核密码处理器性能无法满足高速密码运算处理需求的问题, 研究了片上网络结构的基本特点, 设计并实现了基于共享存储式的簇状片上网络多核密码处理器架构, 分析密码运算特征并完成密码算法的多核适配. 与单核密码处理器性能相比, 本架构有较强的并行性及可扩展性, 能够更好地完成大位宽、细粒度密码算法的支持. 高效的核间数据交互机制大大提升了片上网络多核密码处理器密码处理性能, 能够实现最大 426 Gb/s 的网络数据吞吐量, 与通用多核处理器实现密码算法相比, 性能提升约 5.7%~37.5%.

关键词: 共享存储; 片上网络; 算法适配

中图分类号: TN4

文献标识码: A

文章编号: 1000-7180(2016)01-0010-05

Research and Implementation of Network-on-Chip Interlinkage Structure for Multi-core Cipher Processor

DU Yi-ran¹, LI Wei^{1,2}, DAI Zi-bin¹

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

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

Abstract: In order to solve the problem that a single-core cipher processor cannot satisfy the high speed cryptographic operations' demand, this paper focused on the network-on-chip architecture and proposed a new architecture based on shared memory for multi-core cipher processor. In the proposed architecture, this paper analyzed the characteristic of cryptographic operations and achieved a DES algorithm mapping. Comparing with the single-core cipher processor, the proposed architecture gets a better parallelism and expansibility, to provide a giant bandwidth and fine grit cryptographic algorithm support. An efficient data interaction mechanism is able to improve the performance of multi-core cipher processor, and achieved a maximum throughput for 426 Gb/s. The performance of the proposed architecture improved about 5.7% ~ 37.5% when compared with the general purpose multi-core processor in achieving cryptographic algorithms.

Key words: shared memory; network-on-chip; algorithm mapping

1 引言

近年来, 片上网络的研究大多着眼于通用多核处理器芯片, 在面向某些特定领域的应用中往往表现出核间通信效率不高、对特定应用的指令支持不强等缺陷, 无法充分满足用户高效处理特定任务的期望. 文献[1]在 32 nm 工艺下实现了一款 8 核处理

器, 在 1.35 GHz 下能够实现 172.8×10^9 次的浮点运算; 文献[2-3]分别实现了两款基于 28 nm 工艺 16 核处理器, 能够达到最大 3.0 GHz 及 3.6 GHz 主频. 使用通用处理器完成特定密码运算指令, 往往需要消耗上百条指令, 使通用处理器性能大打折扣. 基于密码运算这一特殊领域, 本文将实验室设计的单核密码协处理器挂接于路由节点之上, 组织形成

片上网络多核结构,通过合理划分密码运算任务,在 65 nm 库工艺下进行仿真验证,4 核片上网络密码处理器甚至能够达到超过单核密码协处理器四倍的性能,对密码运算提供有力支撑.

2 基于数据共享的片上网络拓扑结构

随着处理器性能的提升,传统加密算法已无法应对现阶段高性能计算机的穷举式攻击,因此,新的密码算法朝着大位宽、细粒度的方向发展.通过加大密码算法的数据位宽,虽然能在一定程度上带来更强的安全保障,但也对密码处理器的设计提出了新

的挑战.

针对同一密码算法中密钥等数据的共享及不同算法间数据交互的问题,本文提出了一种基于数据共享的簇状片上网络结构(如图 1 所示),通过路由节点(Router)组织形成一个密码运算处理簇,簇内集成 4 个密码运算核心,通过固定写任意读的方式共享一块存储区域,完成核间数据的交互;路由节点完成簇间互联任务,形成片上网络多核结构.良好的可扩展性确保了更大规模的密码运算核心的集成,以适应用户对不同性能的密码运算处理性能的要求.

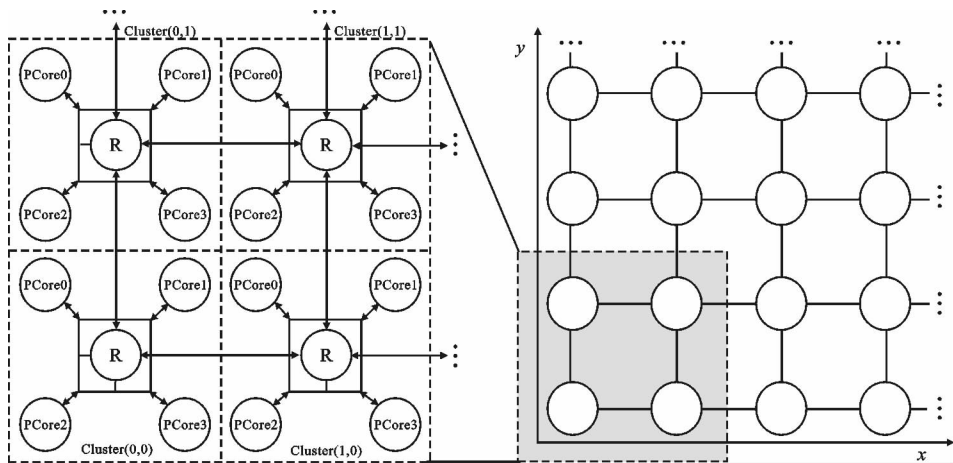


图 1 共享存储式簇状片上网络多核处理器拓扑结构

片上网络多核架构在整体上遵循 2D-Mesh 进行组织,保证了良好的可扩展性与可移植性,同时,簇内以星型结构组织互联,减少了密码运算核心间数据交互的跳数,从而提高该架构下多核处理器的密码运算处理能力.在相同规模密码运算核心下(16 核),本文提出的架构在网络直径及平均跳数上等参数上相比于传统片上网络拓扑结构带来的提升如表 1 所示.

表 1 常见片上网络拓扑结构性能比较

拓扑结构	网络直径	平均跳数	路由节点规模	可扩展性
2D-Mesh	6	2.5	小	高
2D-Tours	4	2	较小	低
Binary-Tree	7	5.19	较大	较低
本文	2	1.18	大	较高

在路由节点规模可接受的条件下,本文提出的基于数据共享的簇状片上网络在网络直径与平均跳数的优化上有显著提升,同时该架构可扩展性良好,便于硬件升级与性能提升.

路由节点规模与其互联的路由节点数目及处理器核心数目呈近似平方级增长,采用通用路由节点模型进行建模,其中路由节点中的主要资源消耗存在于数据缓存单元、仲裁器、路由选择单元以及内部全互连网络.假设星型结构的路由节点上挂接 n 个处理器核心,并同时与周围 m 个路由节点互联,则该路由节点的逻辑资源消耗(Logic Consume)为

$$LC = \sum_{m+n} (B + A + C + I).$$

式中, B 为数据缓存单元消耗, A 为仲裁器消耗, C 为路由选择单元消耗, I 为内部互连网络消耗.数据缓存单元由 FIFO 构成,其余模块均为简单与非门电路,结合具体电路设计,采用同一化处理后路由节点的逻辑资源消耗为

$$\begin{aligned} LC &= (2l + 0.3l + 0.2l)(m + n) + (m + n)^{(m+n)} 0.2l; \\ LC &= 2.5l(m + n) + (m + n)^{(m+n)} 0.2l; \\ LC &= l[2.5(m + n) + 0.2(m + n)^{(m+n)}]. \end{aligned}$$

集中的处理器核心互联结构能够大大减少核间

通信带来的通信消耗,因此在可承受的资源消耗下,片上网络中处理器核心数目总量一定时,单个路由节点上连接的处理器核心数目及与其互联的路由节点数目越多,多核处理器性能越高.

从表 2 看出,当处理器核心数目与互联路由节点数目之和大于 9 时,继续提升带来的逻辑资源消耗过大,综合考虑片上网络结构的规整性,本文提出的单簇四核四向的星型结构能够在较低逻辑资源消耗下实现高性能密码运算任务.

表 2 连接不同节点数目下路由节点的逻辑资源消耗

LC	互联路由节点数目 m						
	1	2	3	4	5	6	7
处理器核心数目 n	1	5.8	9.3	13.2	17.5	22.2	27.3
	2	9.3	13.2	17.5	22.2	27.3	32.8
	3	13.2	17.5	22.2	27.3	32.8	38.7
	4	17.5	22.2	27.3	32.8	38.7	45
	5	22.2	27.3	32.8	38.7	45	51.7
	6	27.3	32.8	38.7	45	51.7	58.8
	7	32.8	38.7	45	51.7	58.8	66.3
	8	38.7	45	51.7	58.8	66.3	74.2

3 片上网络的数据交互分析及密码算法映射

密码算法中的数据交互不仅存在于相同算法中的子密钥共享、逻辑运算单元间数据的相互调用,也存在于不同算法运算结果间的关联. 基于密码运算的这一特点,本文设计的数据共享式簇状片上网络结构可以较好地解决密码运算中的数据交互问题,从而实现高性能密码运算.

3.1 基于片上网络的簇内数据共享机制

本文设计的多核密码处理器以簇为基本单元,簇内呈星型结构,集成四核密码运算核心,通过共享数据存储空间完成簇内各个处理器核的数据交互,共享数据存储空间划分为四个子存储空间,分别对应簇内不同处理器核,处理器核对共享数据存储空间采用固定写任意读的方式进行操作,不仅避免了数据的写入冲突,同时各处理器核拥有一块独立的私有写存储区,便于用户实现数据的有效管理与维护.

共享存储区主要应用于相同密码算法间任务级并行的子密钥共享,基于片上网络的簇内数据共享流程如下所示.

Step1:密码运算核心 PCore0 接收外部注入的初始密钥 Key;

Step2:密码运算核心 PCore0 完成子密钥 Sub-key 扩展,并将子密钥存储于其对应的数据共享存储区;

Step3:密码运算核心 PCore0 向其他密码运算核心 PCore1-3 发送子密钥运算完成消息;

Step4:密码运算核心 PCore0-3 读取数据共享存储区中子密钥,开始运算.

3.2 基于片上网络的簇间数据交互过程

片上网络多核密码处理器整体上以 2D-Mesh 拓扑结构进行组织,簇间数据交互通过路由节点路由实现,以图 1 中簇(0,0)中的密码运算核心 PCore0 向簇(1,1)中的密码运算核心 PCore0 数据传送过程为例,基于片上网络的簇间数据交互流程如下.

Step1:簇(0,0)中密码运算核心 PCore0 将需要传输的数据传送至簇(0,0)的路由节点;

Step2:经路由算法计算路由路径,即数据按簇(0,0)至簇(0,1)最后传送至簇(1,1)的路由节点;

Step3:簇(1,1)解析数据包头,将数据分发至目的密码运算核心 PCore0;

Step4:簇(1,1)中的密码运算核心 PCore0 接收数据,完成对数据的处理.

当片上网络中集成的密码处理器较多时,需要充分考虑路由算法对性能带来的影响,固定路由算法如 XY 路由算法实现简单,无死锁活锁,但当网络中某一路由节点发生拥塞时,易造成整个网络的阻塞,从而降低多核密码处理器性能. 适应性路由算法通过侦测临近路由节点状态,选择合适的路由路径,能有效避免长时间拥塞带来的性能上的下降,但死锁及活锁的出现,会造成数据的不可达.

3.3 基于片上网络的多核算法映射方案

基于本文设计的数据共享式簇状片上网络结构,密码算法主要按完整密码算法映射及基本逻辑单元映射两种方式映射至片上网络多核密码处理器中. 以 DES 密码算法为例,两种映射方式在单簇上的映射如图 2 所示.

完整密码算法映射将完整的 DES 加密逻辑配置于单个密码运算核心之中,运算过程中,首先由密码处理核心 PCore0 计算子密钥并存储于其对应共享存储区域内,同时发送子密钥运算完成消息至其余密码处理核心,当各个核心接收到该消息后,启动 DES 加密运算,处理事先划分好的数据分组,计算

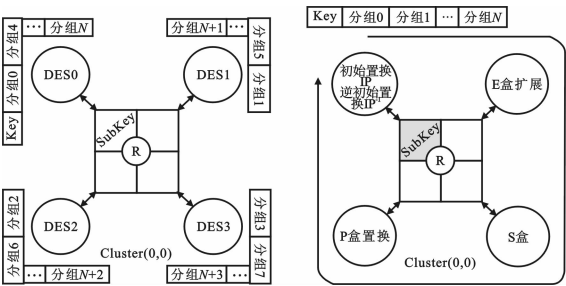


图 2 DES 算法在单簇上的两种映射方式

完成后输出各个分组,形成完整的加密数据。

基本逻辑单元映射是将完整的 DES 加密逻辑拆分为基本的运算逻辑——初始及逆初始置换、E 盒扩展、S 盒、P 盒置换,通过屏蔽不必要的运算逻辑,降低密码运算过程中的功耗损失。同时,更加简单的运算逻辑能够有效提升整个密码运算处理器的时钟频率,从而提升密码算法的吞吐率。运算过程中,首先生成子密钥并存放至共享存储区内,然后依次对各个分组进行加密处理,计算完成后,输出形成完整的加密数据。

两种映射方式均能有效提升密码算法的处理性能,基本逻辑单元映射能够有效降低密码运算过程中不必要的功耗损失,但过多的数据交互也将对密码运算效率产生影响,当核间数据交互所需的时钟周期数目大于密码算法运算的时钟周期时,甚至会造成性能的降低。因此,合理划分逻辑单元在各个核的映射对多核处理器整体性能的提升有至关重要的影响。

4 片上网络多核密码处理器性能分析

为了验证设计的合理性,对本文设计的共享存储式片上网络进行验证实现。构建 4 簇 16 核片上网络互连结构。在 SMIC COMS 65 nm 工艺下经 DC 综合,本文提出的片上网络单簇路由节点占据 $0.46\ \mu\text{m}^2$ 的芯片面积,其中组合逻辑占用面积仅为 $0.19\ \mu\text{m}^2$ 。

片上网络数据吞吐率定义如下:

$$DT = \frac{D \times f_{\max}}{T_{\text{clk}}}$$

式中,DT 为片上网络数据吞吐率,D 为网络传输数据总量, $f_{\max}$ 为片上网络能够工作的最大时钟频率, T_{clk} 表示数据传输所需的时间。

由于本文提出的片上网络多核结构的是以四核四向方式进行连接,即在理想的情况下,每条数据通路上都能够存在数据流动,且数据位宽为 32 比特,16 核处理器结构中共有 40 条数据通路,在不发生阻塞的情况下,最大片上网络数据吞吐率为

$$DT = \frac{D \times f_{\max}}{T_{\text{clk}}} = \frac{(32\ \text{bit} \times 40) \times 333\ \text{MHz}}{1} = 426.24\ \text{Gb/s}.$$

考虑到实际应用中,数据分发往往会存在同向性,即一对处理器核占用一条数据通路后,其他核无法再占用该路径进行通信,且当发生阻塞时,片上网络的数据吞吐率会大打折扣。设计数据传输模型并进行仿真,随机性数据传输能够达到的最大片上网络吞吐率为 138.53 Gb/s。

考虑到实际密码应用需求,本文在片上网络架构中挂接了由信息工程大学设计的单核分组密码协处理器,经 DC 综合后,所挂接的分组密码协处理器可以达到的最大时钟频率为 310 MHz。通过任务级并行方式在片上网络中实现典型密码算法的映射,同时,向各个处理器核发送 1 Mb 大小的数据包,经 VCS 仿真验证,不同算法的片上网络数据实测吞吐率如表 3 所示。

表 3 片上网络多核实现密码算法性能

算法分类	密码算法	单核数据吞吐率/(Mb/s)	片上网络数据吞吐率/(Gb/s)
分组密码算法	DES	313	4.76
	AES	969	13.95
	IDEA	47	0.720
	SM4	27	0.400
序列密码算法	SNOW	61.5	0.880
杂凑密码算法	SM3	376	6.72
	SHA256	320	4.83

仿真结果显示,当映射 AES 算法时,片上网络多核密码处理器能实现最大的吞吐率,但该吞吐率与随机性数据传输得到的理论值有一定差距。因此,片上网络总是处于一种空闲的状态,从而能够支持更大量的密码运算操作。

采用文献[1-4]中的通用处理器实现密码算法,其性能如表 4 所示。

表 4 不同处理器下密码算法性能

处理器	工艺/nm	处理器数/个	DES/(Gb/s)	SM4/(Mb/s)	SHA256/(Gb/s)
文献[1]	32	8	2.86	335	2.93
文献[2]	28	16	5.02	603	5.11
文献[3]	28	16	5.53	611	5.58
文献[4]	65	24	3.53	173	3.55
本文	65	16	4.76	400	4.83

考虑工艺提升对处理器性能带来的影响,本文

设计的片上网络多核密码处理器在性能上较文献[1-4]分别提升了约 5.7%~37.5%，能够提供更高速的密码运算支持.

5 结束语

通过对密码算法运算特征进行分析^[5],提出了共享数据的簇状片上网络多核密码处理器架构. 并在该架构的基础上研究了簇内、簇间数据交互及密码算法的多核映射问题,充分开发了密码算法在多核处理器中的并行性. 通过不同密码算法在网络中的仿真实现,16 核完成 AES 算法能够达到最大 13.95 Gb/s 的数据吞吐率. 与通用处理器实现密码算法相比,本文提出的结构性能提升约 5.7%~37.5%. 因此,本文提出的基于共享存储式的片上网络结构能提供更高的密码运算性能与有效的信息安全保障.

参考文献:

[1] Hu Weiwu, Zhang Yifu, Yang Liang, Godson-3B1500: A 32nm 1.35GHz 40w 172.8GFLOPS 8Core processor[C]// Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2013 IEEE International. San Francisco,2013:54-55.

[2] Ryuji Kan, Tomohiro Tanaka, Go Sugizaki. A 10th

Generation 16-Core SPARC64 processor for mission_Critical UNIX server[C]// Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2013 IEEE International. San Francisco,2013:32-40.

[3] Jason Hart, Steve Butler, Hoyeol Cho, A 3.6GHz 16-Core SPARC SoC processor in 28nm[C]// Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2013 IEEE International. San Francisco, 2013: 48-49.

[4] Ou Peng,Zhang Jiajie,Quan Heng. A 65nm39GOPS/W 24-Core processor with 11Tb/s/W packet-controlled circuit-switched double-layer network-on-chip and heterogeneous execution array[C]// Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2013 IEEE International. San Francisco,2013:56-57.

[5] Sao Jie Chen,Lan Yingcherng. Reconfigurable networks-on-chip[M]. New York:Springer-Verlag, 2011.

作者简介:

杜怡然 男,(1991-),硕士研究生. 研究方向为安全专用芯片设计. E-mail:420197028@qq.com

李 伟 男,(1983-),博士研究生,讲师. 研究方向为专用集成电路设计.

戴紫彬 男,(1966-),博士,教授. 研究方向为专用集成电路设计、芯片可重构设计.