众核构造高性能密码算法协处理器

叶　宾
（保密通信重点实验室，四川 成都 610041）

【摘　要】通过分析 Feistel 结构和 SP 网络结构的分组密码算法的特点与实现结构，说明了分组算法适合可重构实现的机理，提出了以众核方式构造高性能密码算法协处理器的架构思想，在适当降低单核处理性能的情况下，因为能最大化利用芯片的电路容量，实践证明这种架构相比起单核、多核架构重构方式实现分组算法具有较为明显的整体性能优势，最后，也指出了众核带来的编程复杂、资源分配困难等问题和众核架构的核数与整体性能的压线性关系等注意事项。

【关键词】多核；众核；分组密码算法；协处理器
【中图分类号】TN918　　【文献标识码】A　　【文章编号】1002-0802(2013)04-0009-04

High-Performance Crypto Alorgithm with Many-Core Architecture

YE Bin
(State Key Laboratory for Secure Communication, Cengdu Sichuan 610041, China)

【Abstract】Through analyzing some characteristics and implementation strucutres of block cipher algorithm of Feistel structure and SP network, this paper gives the mechanism of block cipher suitable for reconfigurable implementation, and proposes the architecture idea of high-performance crypto algorithm with many-core architecture. The maximal use of chip circuit capacity could be realized at the expense of proper decrease of the single-core processing capability, and the experiment shows that the many-core architecture has more obvious advantage than single-core or multi-core architecture. Finally, some problems and key points are also given, including complex programming, difficult resources allocation, and relationship of cores number and chip performance.

【Key words】multicore; many-core; block cipher; coprocessor

0 引言

随着信息系统的性能的快速增长，以及信息安全事件不断爆发，安全需求呈现爆炸式增长，对数据、信息进行安全保护的最有效措施公认为数据加密，为此，对完成计算密集型任务为主的密码算法实现部件提出了更高的性能要求。出于对投资的保护需求，用户提出了对算法实现的灵活性、可升级变换的迫切愿望。为此，各种算法可重构实现方法如雨后春笋般诞生，当前较为热门的方式是采用 CPU(Central Processing Unit)技术为核心的专用指令集的密码协处理器实现[1]。

从各种文献发现，这些密码协处理器尽管比用通用 CPU 实现性能高出不少，但与 FPGA(Field Programmable Gate Array)重构实现算法还是存在一定性能差距，使得其存在价值、市场空间受到一定质疑，大幅度提高性能成为其迫切需求。

开展高性能密码算法协处理器体系结构研究，目的是通过分析分组算法数据处理流程及工作的特点，组织和构建尽可能的并行工作模式，大幅提升数据并行性能，从而充分实现好空间换时间的合理转换，构造出高性能密码算法协处理器。

收稿日期：2012-11-30。
作者简介：叶　宾（1968-），男，工学硕士，高级工程师，主要研究方向为安全芯片。

1 分组算法分析

分组密码是将定长的明文块转换成等长的密文，这一过程是在密钥的控制之下，使用逆向变换和同一密钥来实现解密。分组密码处理的单位是一

组明文，即将明文消息编码后的数字序列 $m_0,m_1,m_2,\cdots,m_i$ 划分成长为 L 位的组 $m=(m_0,m_1,m_2,\cdots,m_{L-1})$，各个长为 L 的分组分别在密钥 $k=(k_0,k_1,k_2,\cdots,k_{t-1})$（密钥长为 t）的控制下变换成与明文组等长的一组密文输出 $c=(c_0,c_1,c_2,\cdots,c_{L-1})$。$L$ 通常为 64 或 128[2]。

目前分组密码典型代表是以 DES(Data Encryption Standard)为代表的 Feistel 结构（如 CAST-256、DEAL、DFC/E2 等）和以 AES(Advanced Encryption Standard)为代表的 SP 网络（如 Safer+、Serpent 等）。

Feistel 结构是由于 DES 的公布而广为人知，已被许多分组密码所采用。Feistel 结构示意图如图 1 所示，在 Feistel 型密码中，明文被分成相等的两个子分组，每一轮通过一个非线性函数转换一个子分组，然后与另一个子分组模 2 加。Feistel 结构的最大优点是解密和加密具有相同的结构，这给硬件加密带来很大的方便，其缺点是扩散速度较慢，需要较多的轮数。

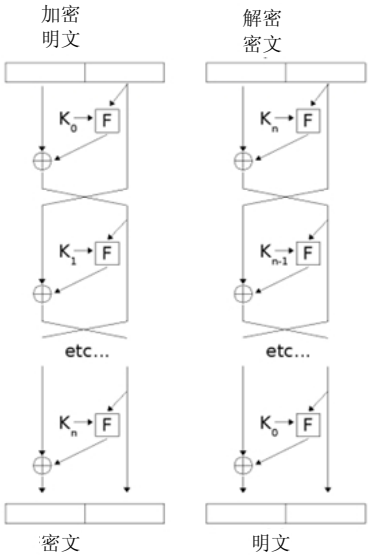

图 1[2] Feistel 结构示意

SP 网络是因 AES 而广为人知，SP 网络示意图如图 2 所示，它采用在整个数据分组上进行并行非线性处理的轮函数，这种方法的优点是高度并行，而这种并行性对高速实现十分有利。此外，SP 网络的扩散特性比较好。

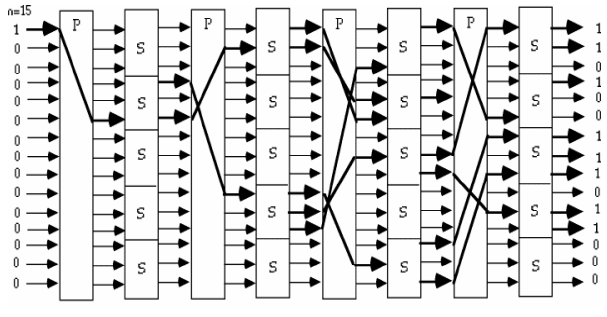

图 2 SP 网络示意

通过对众多业界公开的基于 SP 网络和 Feistel 结构算法分析可知，迭代轮结构是其突出共性特点，迭代轮结构涉及的轮函数通常由 S 盒变换、异或、移位、置换、模加、模减、模乘、逻辑与、逻辑或、逻辑非等基本函数组成[3]。进一步分析可以发现，分组算法具有相同或相似的基本操作元素，算法操作元素相对收敛或者说同一基本操作元素在不同算法中出现的频率很高[4]。那么这些基本操作元素所对应的硬件资源就可以被多种不同的算法所共用，因此就存在以较小的电路规模实现各种分组算法的可行性---即分组算法可重构实现可行。

2 协处理器架构分析

采用什么协处理器架构实现分组算法呢？我们先看看最成熟、最灵活的 CPU。在过去几十年里，微处理器的设计主要是针对冯·诺伊曼结构开发指令集并行，将大量的晶体管主要用于深度流水线控制和大容量的高速缓存以降低数据访问的平均延时，满足各种应用的需求，CPU 适用于办公、网络、数据处理、多媒体应用等。这种设计思想导致计算资源所占的芯片比例相对较低，因此，当用通用处理器（微处理器、微控制器、数字信号处理器等）处理计算密集度很高的密码函数任务时，通用指令没法针对密码运算进行优化，因此，除了异或运算、逻辑与运算、逻辑或运算、逻辑非运算和一部分移位运算外，其余基本密码函数都要用很多条指令（基本逻辑函数）构成，这就是密码算法软件实现的性能远远落后于硬件实现的原因。

2002 年 IBM 推出的 POWER4 多核处理器开始，把我们推到了多核时代，多核处理器从那时起就不断涌现，逐步成为了处理器潮流，从基于 ARM 架构的嵌入式到台式机桌面，如今的手机芯片、电脑芯片市场上形成了全是多核处理器的事实。众多通用多核处理器适合处理密码运算吗？答案是否定的，原因是多核通用处理器的设计思想依然没有改变，适合密码运算的晶体管占的比例并没有提高，也没有专门开发密码运算的指令集。

为改变通用处理器不擅长处理密码运算的问题，业界诞生了众多的专用指令加速机制的密码协处理器，结合通用处理器的编程机制，通过一些专用指令调用硬件加速实现的算法函数模块，从而提高算法实现性能。具体为：用户在实现算法时，使用一系列通用和专用指令的序列构成整个算法。

从各种文献可见，目前国内比较典型的密码算法协处理器较多都采用了基于超长指令字 VLIW（Very Long Instruction Word）的体系结构处理器，之所以采用 VLIW，根本原因还是希望尽可能实现并行。这些 VLIW 算法协处理器同时也存在内核的

译码逻辑、指令发射逻辑、数据通路及旁路机制比较复杂，规模、面积开销大的问题，在一定程度上限制了芯片上密码运算函数单元可容纳的个数。特别是随着密码应用需求的迅猛增长，控制功能单元也在增加。

从目前已知的这些密码算法协处理表现的性能来看，基本满足中低速数据加解密的需求，但面对日益迫切的高速应用需求，显得力不从心，因此，迫切需要提高密码算法的协处理器性能。提高性能有两条路可走，一是挖掘处理器的潜力，构造更为强大的处理器（比如尽可能单周期直接支持大数据、宽位宽的复杂运算），从而提高处理能力；另一条路是适当降低单个处理器性能，尽可能减小单核面积占用，用众核并行的方式提供芯片整体吞吐性能的大幅提升。到底采用哪种好呢？我们认真分析可以发现，直接提高协处理器性能遇到的问题较为麻烦，主要表现在功耗和互连线延时。提升处理器性能最直接、最方便的手段是提高工作频率，这直接导致晶体管翻转加速,也导致能量上升、芯片发热，这就是业界通常高频芯片多数背上一个风扇或散热片的原因。随着高工艺的采纳，晶体管越来越小，越来越快，互连线的延迟问题也会日益突出，这些因素制约着直接提升处理器核性能的潜能挖掘。

面对高工艺带来的一个芯片上可容纳的晶体管数越来越多，但是却因为功耗和互连线的限制并不能直接提供很高的性能，那么怎么办呢？办法就是众核实现。具体来讲就是尽可能挖掘晶体管数多的潜力，充分把尽可能多的晶体管用上，而每个处理器核适当裁剪其功能，特别是占用面积的如宽位乘法、表等，适当牺牲单核的性能换取面积的减小，从而获得单位面积性能保证，用众多个核实现芯片整体性能的提高。因为从架构上来看，分组算法具有很高的计算密集性和数据并行性，对大量数据元素同时进行相同的运算，并且控制流程较为简单。而设备对芯片的高性能关注点是在处理数据的宏观吞吐量上，因此将架构设计目标定为在满足有限单线程性能需求的基础上，大大提高多线程加解密性能，众核架构十分适合。

3 众核

众核定位如图 3 所示，它处于超细粒度的 FPGA 和多核处理中间，FPGA、众核结构和多核结构的逻辑单元粒度如图 3 所示[5]。

FPGA 由极细粒度逻辑单元组成，通过可配置网络连线将逻辑门和查找表连在一起，可以使用硬件描述语言对所构想结构进行寄存器传输级描述，通过编译综合工具将其转换为由基本逻辑门组成的网表，FPGA 芯片根据网表对片上互连网络进行配置，实现不同逻辑门之间的连接。多核处理器则处于另一个极端，每一个处理器核通常都是高度复杂的极强的任务处理能力，但是面向的是串行程序指令级并行性开发，在微结构上引入许多复杂机制，如分支预测、超流水、乱序执行和线程级推测执行等，最适合的使用方式是多任务并行，且对每个任务的响应时间有较高要求。众核处理器处于两者之间，不同于 FPGA，众核结构中每个处理器核都具有独立计算的能力，不需要程序员从最基本逻辑门进行构建目标结构;同时，由于每个处理器相对简单，一般是顺序发射结构，因此也不适合对单任务性能要求较高的应用[5]。

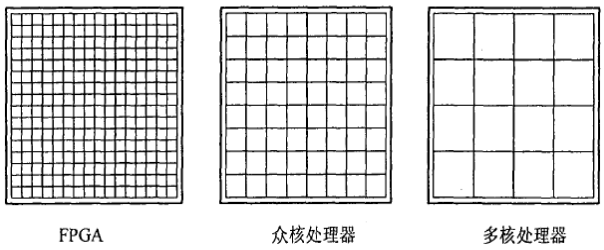

图 3 逻辑单元粒度

通常的众核架构的协处理器结构如图 4 所示。

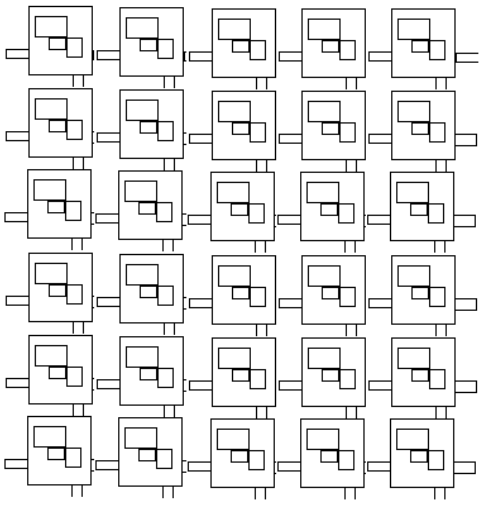

图 4 众核架构的协处理器结构

每个核由基于 VLIW 指令的处理单元、存储单元、互联控制单元构成。

数个物理核可构成逻辑核，如图 5 所示，每组逻辑核尽可能相对独立地工作可实现线程级并行，尽可能将算法轮函数甚至轮内函数用多个逻辑核并行流水甚至超流水工作可进一步提升性能，每个处理器采用 VLIW 指令，提供了指令级并行机制。在三个层面上挖掘潜力，均可提高协处理器整体性能。

采用这种设计思想，我们用在复杂运算局部，将一个大位宽的乘法器在 FPGA 上模拟实现，先用单核思想实现，然后用和双核模式实现，大约取得了 1.8 倍的性能提升，改用众多小位宽的乘法器单元来实现，实现了约 10 倍的性能提升。

在实现AES分组密码算法方面，业界有众多用分别基于多核的 CPU 和众核的 GPU（Graphics Processing Units）实现 AES 算法结果表明，众核取得了数倍的性能优势[6-7]。

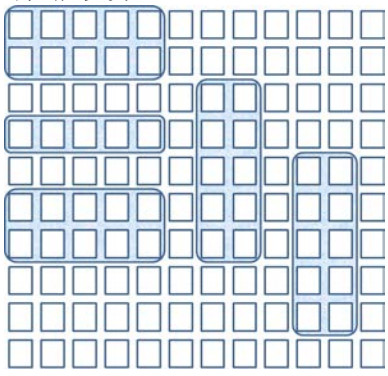

图 5 逻辑核

当然，单纯从性能看众核取得了性能回报，但众核依然存在许多不足。突出表现在编程、资源管理等方面。在多个处理器核组成的芯片上，并行是其核心思想，任务必须进行有效切分并分布到各个处理器核上并行执行，编程和调试均很困难，特别是专用协处理器的相关开发工具成熟度无法与通用处理器开发工具相比的情况下，更需要软件人员深度熟悉硬件架构。在处理器设计进入众核时代以后，丰富的片上资源也对如何高效利用资源提出了很高要求，比如：如何将多个物理核藕合成粗粒度逻辑核来处理比较复杂的密码算法函数运算，如何最大化配置资源来进行并行运行？逻辑核动态配置等等，均很复杂和麻烦。众核架构下，核间通信呈现网络状态，路径安排也很讲究。

4 结语

到底是用少数几个强大的单核，还是众多简单的核来实现算法协处理器？是否众核架构核越多越好呢？单个处理核很强大时，其单线程性能较高，但芯片的总体性能并不太高；众核架构下如果每个核太过简单，单线程的性能太低，整体性能也会相当低。对于大部分是必需串行执行的算法（如序列算法），那么一个强大的单核是理想的方案，并行行比较好的如众多的规则的SP网络的分组算法[8]，那么使用更多的较简单的核好些。众核中，是否核越多越好呢？笔者就用同一个适合众核实现的算法做简单的试验发现，性能与核的多少大致呈现出准正态分布的关系，即随着核的增多，性能大幅提升，但太多的核也会反而导致性能急剧下降！原因是单个核性能低到一定程度后，支撑众核设计指导思想的单位面积性能优势被完全抵消，因此，我们进行核的数量设计时，必须充分根据算法函数特点规划好单个核中运算函数的粒度大小、多个核构成的逻辑核的性能。

参考文献

[1] 曲英杰.可重组密码逻辑的设计原理[D].北京：北京科技大学，2002.

[2] 宋震 等编著 密码学[M]北京:中国水利水电出版社，2002:52-53.

[3] 许萍,程代伟,龙束媛.分组算法模块的 VHDL 和 VERILOG 实现及其比较研究[J].通信技术,2008,41(12):1353-354,357.

[4] 杨晓辉.面向分组密码处理的可重构设计技术研究[D].河南：解放军信息工程大学,2007

[5] 任永清.逻辑核动态可重构的众核处理器体系结构[D].安徽：中国科技大学,2010

[6] Luken B P,Ouyang M,Desoky A H.AES and DES Encryption with GPU[C]// Proceedings of ISCA PDCCS. [s.l.]:ISCA PDCCS, 2009:67-70.

[7] Kipper M, Slavkin J,Denisenko D.Implementing AES on GPU Final Report[D]. Toronto: University of Toronto,2009.

[8] 胡永进,向楠,赵俭.分组密码算法的三种硬件实现结构及性能分析[J].通信技术,2008,41(05):113-115.

（上接第 8 页）

[9] JOLLIFFE, I. Discarding Variables in a Principal Component Analysis. I: Artificial Data[J]. Appl. Stat. 1972,21(02):160－173.

[10] MILLER, BRADLEY N,ALBERT I, et al. MovieLens Unplugged: Experiences with an Occasionally Connected Recommender System. Proceedings of the 8th international conference on Intelligent user interfaces[C]//[s.l.]:ACM,2003:263-266.

[11] 张圣.一种混合式协作过滤服务推荐算法[J].通信技术,2011,44(07):118-119,122.

[12] 胡明,刘嘉勇,刘亮.一种基于代码特征的网页木马改良模型研究[J].通信技术,2010,43(08):155-157.

[13] 刘涛,薛质,唐正军,等.基于数据挖掘的大规模分布式入侵检测系统的设计[J].信息安全与通信保密,2004(05):31-33.

众核构造高性能密码算法协处理器

作者：叶宾
作者单位：保密通信重点实验室,四川 成都 610041
刊名：通信技术
英文刊名：Communications Technology
年，卷(期)：2013(4)

参考文献(8条)

1. 曲英杰 可重组密码逻辑的设计原理 2002

2. 宋震 密码学 2002

3. 许萍;程代伟;龙束媛 分组算法模块的VHDL和VERILOG实现及其比较研究 2008(12)

4. 杨晓辉 面向分组密码处理的可重构设计技术研究 2007

5. 任永清 逻辑核动态可重构的众核处理器体系结构 2010

6. Luken B P;Ouyang M;Desoky A H AES and DES Encryption with GPU 2009

7. Kipper M;Slavkin J;Denisenko D Implementing AES on GPU Final Report 2009

8. 胡永进;向楠;赵俭 分组密码算法的三种硬件实现结构及性能分析 2008(05)