流体系结构密码处理器存储系统的研究与设计

朱玉飞,戴紫彬,徐进辉,李功丽
(信息工程大学,河南郑州 450001)

摘 要: 以信息安全设备的密码应用需求为基础,融合流体系结构处理器基本架构,设计出流体系结构密码处理器.文章主要研究和设计影响该处理器性能的瓶颈——流存储系统.此系统针对专用密码处理器的存储特点,并采用可配置化设计,满足密码应用对处理器存储系统灵活高效的要求.同时,该设计将层次化-分布-分体式存储、多数据通道流水并行化访存、流访存调度策略相结合,优化存储系统的访存效率,以提高该处理器的整体性能.研究结果表明,相比于典型密码处理器的存储设计,该设计的访存效率最高可提升约 6 倍.

关键词: 密码处理器; 流体系结构处理器; 流存储系统; 可配置
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2017)12-2957-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.12.018

Research and Design of Memory System of Stream Architecture Cryptography Processor

ZHU Yu-fei, DAI Zi-bin, XU Jin-hui, LI Gong-li
(*Information Engineering University. Zhengzhou, Henan* 450001, *China*)

Abstract: The design of stream architecture cryptography processor bases on the need of cryptography applications for information security equipment and fuses the basic structure of stream architecture processors. The paper basically researches and designs stream memory system which is a bottleneck that affects the processor's performance. The system aims at memory characteristics of the dedicated cryptography processor and takes reconfigurable design to satisfy cryptography applications' flexible and efficient requirements on the processor's memory system. Meanwhile, the design combines hierarchical-distributed-banked memory、parallel stream access of channels and stream access dispatcher strategy together, which optimizes memory access efficiency of the system to improve the whole performance of the processor. Research results demonstrate that comparing with the memory design of typical cryptography processors, memory access efficiency of this design can be highly raised to 6 times.

Key words: cryptography processor; stream architecture processor; stream memory system; reconfigurable

1 引言

目前重要信息的安全保障面临诸多挑战,适用于信息系统的密码处理器,以实现密码算法加/解密信息任务为设计目标,是保障系统信息安全的关键硬件,多方用户对此类密码硬件寄予更高性能的期待.一方面,研究密码算法的可重构实现,设计安全灵活的硬件结构是密码处理器[1]领域近年来持续探讨的要点.另一方面,具有规模化运算资源、高访存带宽特点的流体系结构处理器[2],已成为处理器设计领域努力探索的新方向.在对常用对称密码算法分析研究的基础上,比较密码应用和流应用[3]发现两者有着相似的处理特点.随着用户对密码处理器日渐提高的要求,需要研究人员设计出在芯片资源受限情况下,可发挥更大密码任务处理潜力的芯片架构,流体系结构的可重构密码处理器——可重构密码流处理器(Reconfigurable Cryptography Stream Processor, RCSP)有效融合上述两方面设计思想进行处理器设计.RCSP 拥有适当数量的密码运算资源,用于实现对重要信息集的即时

收稿日期: 2016-08-30;修回日期: 2017-01-13;责任编辑:梅志强
基金项目:国家自然科学基金(No.61302107);国家 863 计划项目(No.2009AA012201)

快捷加密,确保信息集的安全. 但密码处理器运算系统和存储系统的运行速度之间存在差距,对于大批量的密码任务而言,数据访存时间开销[4]占据其整体运行时间之重要比例,要充分发挥出 RCSP 的密码任务处理性能,设计高效、灵活的专用存储系统是解决其"访存瓶颈"的核心部件.

2 相关研究工作

RCSP 访问主设备内存时,面临的"访存瓶颈"问题和通用处理器存在的"存储墙[5]"问题相似. 目前用来缓解"存储墙"的方法对 RCSP 具有参考作用,相关研究如下:

(1)采用 eDRAM 技术[6]:eDRAM(嵌入式 DRAM)技术将存储器资源和处理器逻辑资源内嵌融合,设计实现嵌入式 DRAM,在同一芯片上集成处理器与存储器,使得处理器逻辑部件能够充分开发 DRAM 内部结构的带宽,化解存储器和处理器之间的带宽差距. 但是采用内嵌式 DRAM 替代 Cache 结构,实际是用增加延时为代价来换取存储系统带宽和容量的提升. 而密码处理器作为一种协处理器受设计面积、制造工艺、工作功耗等条件限制,难以集成片内 DRAM 存储器,不适合应用 eDRAM 技术.

(2)采用层次化存储结构[7,8]:处理器采用层次化存储结构,将其存储系统由内而外划分为多层,如寄存器、多级 Cache 及至片外存储器. 同时采用精细存储策略管理利用片内带宽和片内缓冲,以期减少对外存的访问. 密码处理器用于加解密各类信息集,其片内存储系统的容量小,需要频繁访问片外存储资源,不断进行片内外信息交互,单纯采用这样的方法不能满足密码处理器的需要.

(3)数据预取/定向技术[9,10]:通过提前启动数据传输,将批量数据预取入处理器的片上存储部件(如片内 Cache),能够减少处理器的本地访存失效,隐藏访存延迟. 它需要大容量的 Cache 以隐藏访存延迟,并要将待处理信息严格规划为连续排列、粒度相同、访存模式规则的数据单元队列. 密码处理器是服务于密码应用的专用处理器,其常见的设计结构中,并不采用该技术所需要的大容量片内 Cache. 密码处理器在对各类信息集进行加解密处理时,将根据信息集所用算法类型、密码算法的工作模式、信息集在密码运算资源上的映射方式等实际条件,进行信息集访存的规划调整,与数据预取/定向技术的要求不符,难以将这种技术运用于密码处理器,来解决密码处理器的"访存瓶颈"问题.

(4)提高外存带宽[11]:提高外存带宽直接有效的方式即提高时钟频率和加大存储器总线位宽. 对于当前的 DRAM 技术来说,这类方法已逼近其制造工艺和生产成本的上限. 想要通过提高存储带宽,来优化密码处理器和外存间的访存性能,受到现有 DRAM 技术发展水平的限制.

3 RCSP 流存储系统的设计

3.1 流存储系统总体结构

目前,RCSP 主要面向于分组类对称密码算法,它采用32bit 密码运算簇[12]为基本运算单位,支持由 32bit 运算簇级联成更大位宽的密码运算核. 具有可重构功能的 RCSP 在适配密码算法时,通过配置信息的作用,可向上兼容大位宽密码运算,保证密码算法选择的多样化,满足用户对信息防护的不同要求. 既能实现多个信息分块在运算簇上的并行处理,也能兼顾几个信息块在运算核上的大位宽运算.

RCSP 中采用层次化-分布-分体式流存储结构,面向密码任务主要特点,设计符合任务需要的流结构存储系统,简记为流存储系统(Stream Memory System, SMS). 应用时将待加/解密信息集划分组织成信息流[13],信息流由记录组成,记录中含有多个信息单元.

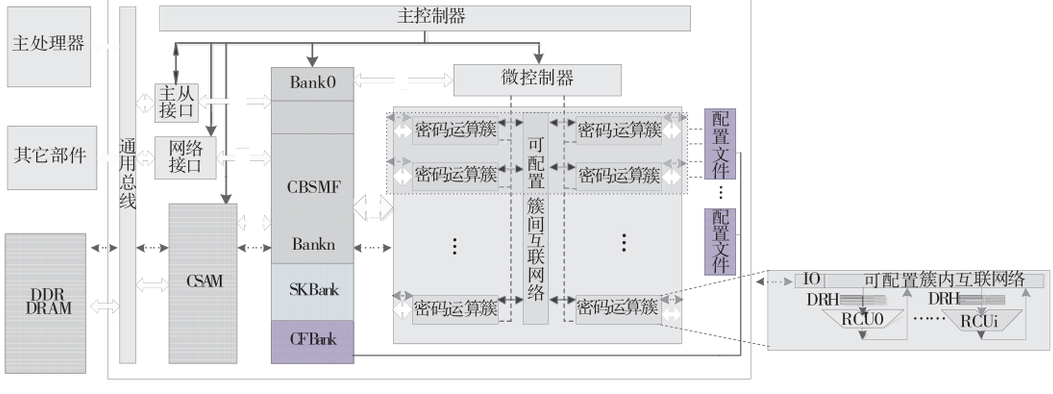

图1 RCSP层次架构图

如上图 1 所示为 RCSP 的层次架构图,该处理器的存储系统分为三层,分别是运算簇内分布式寄存器堆(Distributed Register Heap,DRH)、可配置分体式流存储文件(Configurable Banked Stream Memory File,CBSMF)、经可配置流访存模块(Configurable Stream Access Module,CSAM)连接外部主存,存储系统内的信息流路径如图 1 中双向虚线箭头所示.

3.2　运算簇内分布式寄存器堆

密码运算簇内采用分布式寄存器堆结构,图 2 为运算簇组合工作图. 每个密码运算簇由多个可重构密码运算单元(Reconfigurable Cipher Unit,RCU)构成,用于实现 32bit 及以下位宽数据的基本密码逻辑运算. 每个 RCU 配有 DRH,RCU 的操作数单元、配置需求信息等可暂存于 DRH 中. DRH 中设有一个专用寄存器项用于存放所属 RCU 的配置信号. RCU 从 DRH 中获取操作数,并对其进行相应的密码逻辑运算. DRH 之间利用簇内互联网络联通,分享数据单元. 在控制器作用下,各运算簇和 CBSMF 通过流缓冲可实现多路信息流并行传输.

各密码运算簇在配置信息(来自配置文件集(见下文))作用下,灵活配置运算簇的组合状态、簇内各 RCU 单元的工作状态,以及待处理数据单元在簇内进行密码运算的执行路径. 一个 DRH 中暂存的操作数经其所属 RCU 处理后,送往下个目标 RCU 的 DRH,历经后续 RCU 处理,实现该操作数的密码算法轮运算过程.

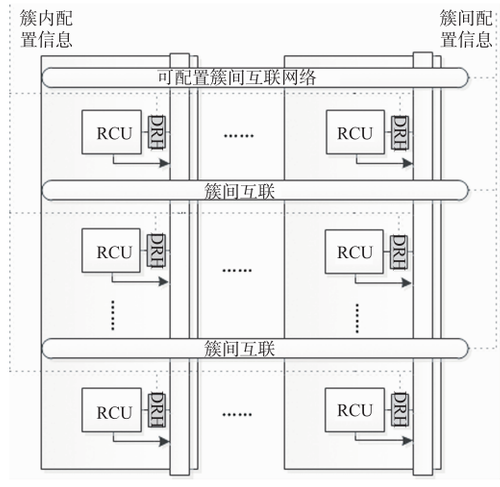

图2　密码运算簇组合工作图

正是因为分布式寄存器堆的作用,使得密码运算部件可以凭借其拥有的规模化运算资源,在控制信号和配置信息的作用下,使用多个簇组合成运算核,实现多报文块在各运算组合上的并行加/解密操作. 同时,采用流水化的思想可在单运算簇内实现报文单元级的流水化并行处理.

3.3　可配置分体式流存储文件

如图 3 所示,CBSMF 作为该处理器各功能部件的共享暂存空间. 它由三个部分构成,分别是通用存储文件集、子密钥存储文件集、配置文件集.

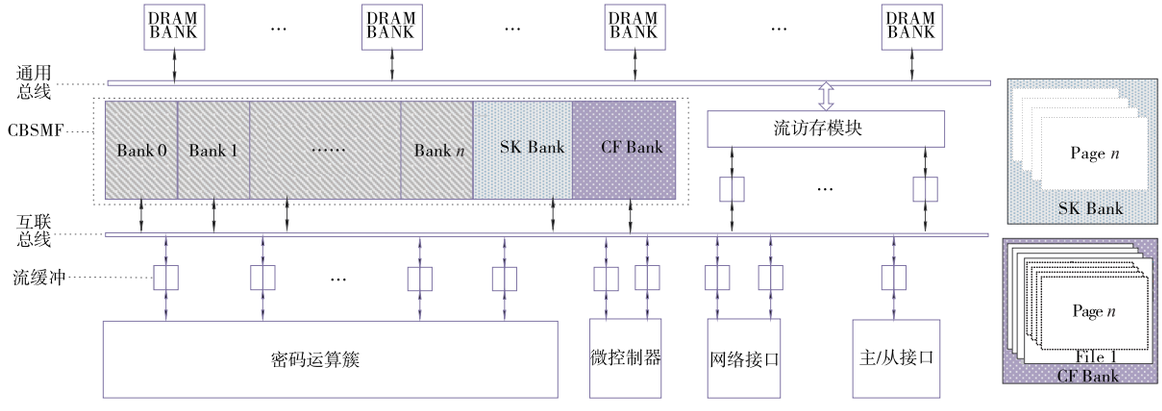

图3　可配置分体式流存储文件

CBSMF 与流访存模块、网络接口、主从接口、微控制器、密码运算簇模块间通过流缓冲并行通信,连接关系可通过主控制器配置信号改变,使其传输性能满足执行批量密码任务所需的访存带宽.

通用存储文件集:用于存放已加载待处理的明文/密文数据块、处理完成待输出的明文/密文数据块、存储部件与控制部件的交互信息、密码处理器与主处理器的交互信息、密码处理器和其他部件的交互信息等. 通用存储文件采用多分体(Bank)的形式构成. 其中分体的数量对应于密码运算部件所包含的运算簇个数,每个分体具有自己的通信端口,可以通过配属的流缓冲与相应密码运算簇直接通信,能满足规模化运算部件所需要的存储性能,其中流缓冲器采用双缓冲的结构,可同时进行数据的传输与加载. 另外,根据片上相应功能部件的需要,各分体可通过文件互联总线实现分体间的信息交互.

子密钥存储文件集(Sub Key Bank,SK Bank):用于保存整个密码运算部件产生的子密钥信息流,以包含密码运算簇的运算核为单位生成子密钥流,将密码运算核预先生成的子密钥流存放在 SK Bank 中. SK Bank 由多个子密钥文件页构成,每个子密钥文件页对应一个密码运算核,在主密钥变更时,刷新 SK Bank 中的子密钥信息流. 对于密码处理过程中所需要的常数/向量等数据,在使用方式上与子密钥数据类似,可以作为子密钥信息流进行存储.

配置文件集(Configuration File Bank,CF Bank):RCSP 从主系统将配置信息流加载到配置文件集中,为后续重构操作做准备. 配置文件集包含多个独立的文件,每个文件对应一个密码运算核,每个文件中又包含多个配置页,对应于运算核中的各密码运算簇. 运算簇在配置页包含的配置信息作用下,按需配置运算簇的组合状态、簇内各 RCU 的启用状态、待加/解密数据在簇内历经相应 RCU 的轮运算路径.

如图 4(*a*)所示,簇内分布式寄存器堆(DHR)暂存即将用到的操作数(明/密文单元),DHR 中操作数经历算法需要的运算过程,被来自于流缓冲的新操作数替换. 流缓冲的半缓冲与 DHR 进行传输时,另一半缓冲可同时与 CBSMF 进行信息传输,将已经过加解/密处理需要输出的数据传送到 CBSMF 中,并从 CBSMF 中加载新的报文数据覆盖已处理数据.

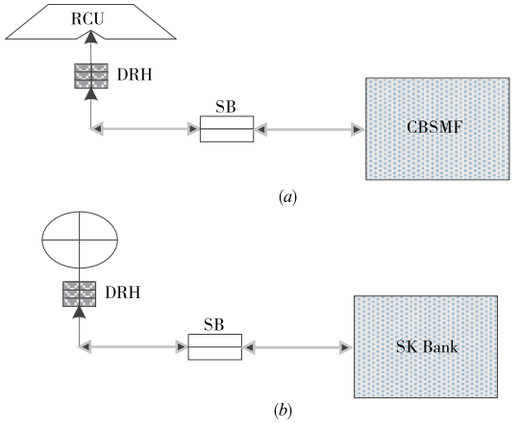

图4 CBSMF与密码运算簇信息传输示意图

如图 4(*b*)所示,对于密钥数据的使用,在对称类算法中密钥数据主要用于和报文数据进行异或操作. 运算簇中异或运算单元的 DHR 里保存即将用到的密钥(根据算法密钥长度决定临时存放的密钥数量),运算核对应的流缓冲中预备需要使用的子密钥页,该 DHR 半侧寄存器中的密钥使用过后被流缓冲中后续子密钥替换,流缓冲中的子密钥页预先从 SK BANK 中查找加载. 信息传输时,报文数据与密钥数据的传输错开,不产生重叠.

如图 5 所示,以分组密码算法的两种常用加解密模式为例:ECB 模式和 CBC 模式. 若 RCSP 的每个运算核包含四个运算簇,为简化起见,图中各画出一个运算核.

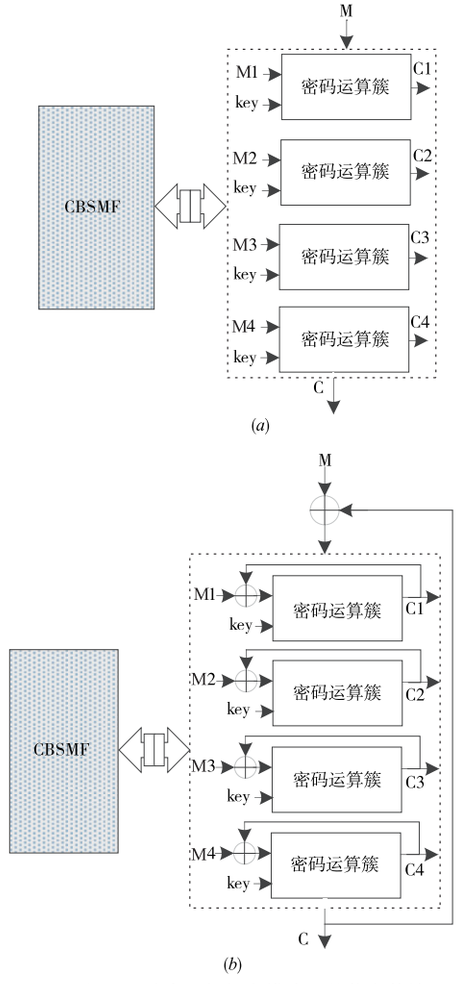

图5 两种常用加解密模式下的信息传输

如图 5(*a*)所示,采用 ECB 模式时:CBSMF 的多分体存储文件搭配对应流缓冲,实现与各运算核的报文并行传输. 流存储文件将待处理报文块以分组的形式传送给各运算核对应的流缓冲,各流缓冲将同一批次的报文组发送给各运算核并行处理. 每个报文组顺序拆分成独立报文单元暂存在各簇内某 RCU(对应于目标算法初始运算操作)的 DHR 中. 根据具体算法的轮运算操作步骤,有序安排加载不同批次的报文组单元,在运算核中的各运算簇内可实现多批次报文单元的流水化并行加解密. 遍历算法运算过程后,将处理完毕的同批报文单元经流缓冲有序返回 CBSMF 的对应分体中.

如图 5(*b*)所示,采用 CBC 模式时:各运算核对相互独立的报文块(或单个报文块允许被分成多个独立

部分)同期处理. 从 CBSMF 的分体文件中,加载相互独立的报文块信息,供不同运算核处理. 每个报文块包含多个报文组,经流缓冲与对应运算核进行传输. 报文组顺序分为相同大小的报文单元发送给对应运算簇,暂存在簇内某 RCU(对应于算法初始运算)的 DHR 中. 簇内报文单元遍历算法操作后,将处理完成的同一批结果输出给 CBSMF 的对应文件,并且将这一批新生成的结果单元与新一批输入报文单元异或,再对异或后的单元进行算法轮运算. 例如,第一批报文组为 M1、M2、M3、M4,第一批生成的密文组为 C1、C2、C3、C4. 第二批报文组为 M5、M6、M7、M8. M5 与 C1、M6 与 C2、M7 与 C3、M8 与 C4 的对应单元异或后再进行相应的密码运算. 同理,该模式下的后续处理过程相似,这里不再赘述.

3.4　可配置流访存模块

RCSP 是面向于密码任务的协处理器,根据密码处理器的常规设计结构[14],主要芯片面积被其运算模块、控制模块、联接模块等占用. 且出于芯片低功耗设计[15]的需要,对 RCSP 的片上存储部件大小有限制,只用于缓存局部时域内的少量待处理信息.

因而设计 CSAM 用于实现 RCSP 对片外主存的高效访存,它采用多数据通道流水化并行传输与流访存调度策略相结合的设计思想,以优化 RCSP 对片外主存的访存效率.

CSAM 的设计出于如下考虑:当前主流 DDR 存储器主要采用 4/8 个独立 Bank,在实际应用时会将 RCSP 应用于多种类型的设备,难以保证各型设备都采用相同分体的外存. 另外,结合外部存储器的 Bank 数,用户可以将待执行报文任务有序拆分为大小相等的报文块,分别存放于各 Bank 中. 各报文块执行密码运算时为互相独立的关系. Bank 中的分块又包含多个报文段,根据具体算法的需要来划分报文段的长度,同一个报文块内的报文段在执行密码运算时为前后相关或互相独立的关系. 可利用上述报文缓存方式,配合完成 SMS 的流水化并行访存.

如图 6 所示,图中上下两行虚线间为流访存模块的设计. 流访存模块用于 RCSP 和片外存储器之间的数据传输,该访存模块的内部单元主要包括:重排序缓冲(ROB,Reorder Buffer)、流地址产生器(SAG,Stream Address Generator)、流访存局域控制器(SALC,Stream Access Local Controller)、可配置访存体(CMB,Configurable Memory Bank)、请求/数据线构成.

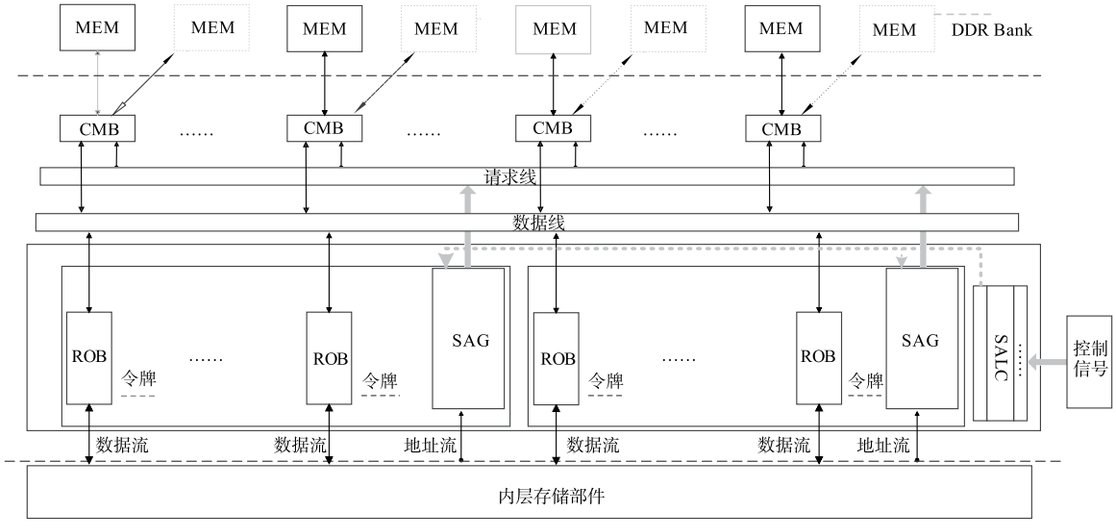

图6　可配置流访存模块设计

流访存模块访问外存时,主控制器同时启动两套访存路径,根据待处理报文集容量和实际采用的外存分体数,访存体工作状态由主控制器的配置信号确定,启用偶数个(不超过 8 个)访存体工作,同时启动对应 ROB,两者协同构成多条并行传输通道. 为保证传输通道和 SAG 的工作协调,在每套访存路径中都使用了一组令牌环机制:各传输通道拥有附带标识的令牌,配置传输通道的启用数量,令牌总量会成相应倍数增长. SAG 每产生 1 个新地址会消耗 ROB 提供的 1 个令牌. ROB 每传输 1 次数据,便发送给 SAG 一个令牌. SAG 只要仍拥有令牌,它就能接着产生新地址,采用令牌环匹配的机制,保证传输通道和 SAG 的互相协调.

ROB 用于暂存来自上游存储模块的数据单元,按数据组成流记录的顺序将其规整排列,为各单元的后续传输做准备.

SALC 受主控制器的作用,在相应指令作用下更新 SAG 内控制寄存器的信息,控制 SAG 的地址流生成.

为了提升 SAG 工作效率,使它可负载多路传输通

道,在设计中 SAG 只用于生成各记录的首单元地址. 且将该地址用作记录请求的整体地址,记录中后续访存单元的请求地址,将在其整体地址的基础上依次递增而来.

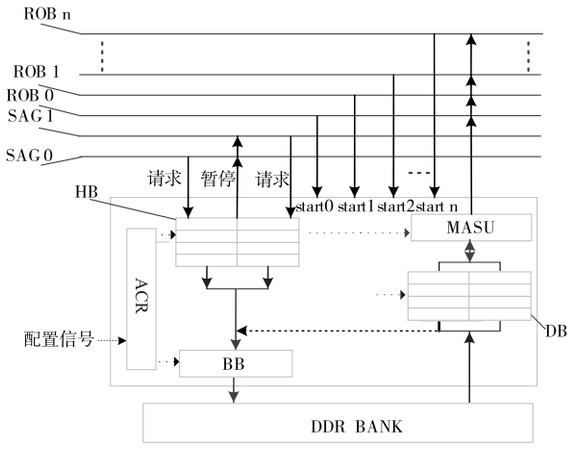

图7 可配置访存体内部结构

图 7 为 CMB 内部结构图,访存体主要由请求保持缓冲(HB,Holding Buffer)、体缓冲(BB,Bank Buffer)、返回缓冲(DB,Data-back Buffer)、访存选控单元(MASU,Memory Access Selection Unit)、访存调配寄存器(ACR,Access Controller Register)构成. HB 暂存需要等待访存资源的访存请求,其内部采用表格的形式暂存,它保存请求直到其等待的资源空闲可用;BB 临时保存即将发送给外存的访存请求队列,确定各记录访存请求的先后顺序,按顺序将访存请求送往外存;DB 具有和 HB 相同的存储形式,用于暂存已完成访存操作、等待送往重排序缓冲的访存结果,或者是已经过 RCSP 处理、等待送出至外存的报文信息单元;MASU 用于选择和访存体进行数据传输的 ROB;ACR 在主控制器配置信号的作用下,确定 MASU 和相应 ROB 的连接关系、根据待处理报文集适用的流记录长度配置该访存体中 HB 和 DB 缓存空间的对称划分、调整体缓冲中访存请求队列的容纳个数.

4 流存储系统工作过程概述

RCSP 的流存储系统充分利用外存(主流 DDR 存储器)分体独立,可支持突发传输[16]的功能. 只要确定突发传输长度和访存起始地址,外存将自动对后续相应个数的存储单元执行连续读/写,无需接连提供访存请求的地址. 且当待加/解密数据连续存储时,只需控制好两次突发传输的请求间隔周期,进而可实现多次连续执行的突发传输. 因而,可采用流访存调度策略,按照适当规律将报文集内的数据信息划分组织,采用硬件和软件相结合的方式动态组织信息单元,优化信息访存的规律性,尽量采用以记录为传输单位的数据形式,实现多信息单元的连续传输,降低访存请求的次数,减少访存周期数,以提高访存效率.

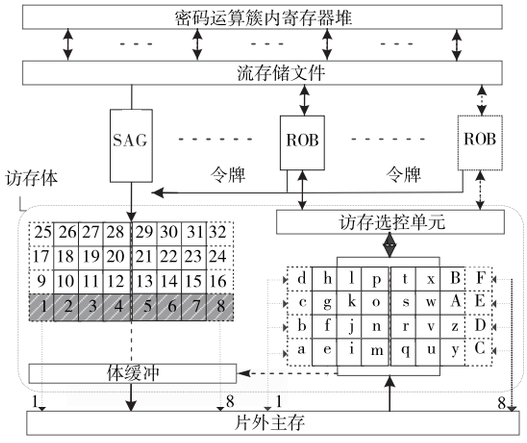

图8 流存储系统工作过程

如图 8 所示,以待处理报文集的流记录传输长度取 4 个单元为例,为便于说明 SMS 工作过程,示意图内只画出了一个传输通道的访存过程. 访存体中的 DB 和 HB 被配置划分为左右两块,可同时进行记录的传输与加载. 每块横向为 4 个单位,纵向为 4 个单位,即每个 HB 中暂存 8 个记录的访存请求,每个 DB 中暂存 8 个记录. 流存储系统的访存过程简述如下:

流存储系统读入过程:由控制信号作用,SAG 模块将新生成的流记录请求送给相应访存体,并组织存放于 HB 内. 如图 8 内细虚线箭头所示,当 HB 分块填充完成后,HB 经由体缓冲传送访存请求. 先向外存传送记录 1 对应着的请求首地址,外存将会连续返回 a、b、c、d 这四个数据单元给 DB. 这四个数据各自对应于 HB 内记录 1 的请求(1、9、17、25 号单元),随后陆续执行记录 2、3、4 的访存请求. 在此期间,另一 HB 分块,可继续接收 SAG 新生成的记录请求,并将新请求顺序存放在记录 5 到 8 的请求列中. 后续访存过程相似,直到记录 8 的请求首地址传送至外存,外存将 C,D,E,F 四个数据单元返回 DB,这样使得 HB 内的访存请求和 DB 内的数据单元逐一对应,后经 MASU 选中的 ROB 将记录方便高效的组织成信息流,送往流存储文件,根据 ROB(传输通道)的令牌标识,确定将信息流存放在 CBSMF 的哪个分体中. CBSMF 各分体再将信息流分批有序的传入相应密码运算簇的寄存器堆中.

流存储系统输出过程:由控制信号作用,SAG 生成新的记录请求送往相应访存体,并组织存放于 HB 内. 同一时期,内层存储部件的数据传入重排序缓冲,以记录的形式排列组织,接着把多个记录依次送往 DB 中. 如图 8 内加粗虚线箭头所示,在 HB 和 DB 分块填充完成后,将 HB

中预备写回记录的首地址、DB 中对应的记录首单元(数据)合并生成请求包送入体缓冲,暂存于体缓冲的记录请求队列里,并将记录的后续数据单元和递增的单元地址合并成新的访存请求包,有序存放于同一请求队列中. 这样,HB 和 DB 经由体缓冲向外部主存逐次传送各记录请求队列首包,且连续传输突发长度个数据单元到各条记录首地址指向的外存数据段内.

5　性能分析评估

使用 Verilog 语言对 RCSP 进行 RTL 级描述,为准确评估其流存储系统的实现性能,使用实验室现有的逻辑综合工具,采用 65nm CMOS 工艺标准单元库及相应负载模型进行逻辑综合,RCSP 的流存储系统综合结果如表 1 所示.

表 1　流存储系统综合结果

综合部件	关键路径延迟(ns)	面积(μm^2)	等效门数(万门)
流存储系统	0.91	992356	68.9

并使用 XILINX Virtex-7 FPGA 平台进行流存储系统性能验证. 片外存储器采用目前主流的 DDR 存储器,DDR 存储器安置在 FPGA 平台的 DDR 插槽内,它包含 8 个独立 DRAM BANK,突发长度为 4 和 8 两种.

实验使用典型分组密码算法——AES 算法,对大小确定的报文信息集进行多分组并行方式的加密/解密实验,在待处理报文集大小相同的条件下,统计 RCSP 流存储系统在多种组合状态时的访存传输周期数,以观察其访存性能. 并与数据包 DMA 访存、主处理器管控访存,这两类常见密码处理器存储系统的访存方式进行比较. 数据包 DMA 访存即外存和密码处理器的内部存储部件直接传输连续数据包的方式;主处理器管控访存即在主处理器程序管控下,密码处理器核作为协处理器进行受控访存的方式.

SMS 在待处理报文信息集容量为 16KB 时,两种配置状态下的访存传输周期数,如表 2 和表 3 所示.

在待处理报文信息集为 16KB 时,两种典型密码处理器访存方式所需要的访存传输周期数,如下表 4 所示.

表 2　4 路传输通道流水化并行访存

SMS 访存方式	DDR 突发长度	流记录长度		
		2	4	8
跨步模式	4	5520	**4426**	4529
	8	6353	5278	**3375**
索引模式	4	6028	**4534**	4656
	8	7252	5342	**3552**

表 3　8 路传输通道流水化并行访存

SMS 访存方式	DDR 突发长度	流记录长度		
		2	4	8
跨步模式	4	4352	**2794**	3265
	8	5568	3396	**1768**
索引模式	4	4506	**2902**	2738
	8	5734	3685	**1872**

表 4　典型密码处理器访存

典型密码处理器访存	访存传输周期数
数据包 DMA 访存	10572
主处理器管控访存	76090

观察 SMS 的实验访存周期数,分别选用表 2 和表 3 里 8 个记录长度和突发长度相同的访存传输周期数取样点. 取样点的含义:(传输通道个数,突发长度,流记录长度),比较 SMS 在两种配置状态时,完成相同大小报文信息集的访存传输周期数,如下图 9 所示.

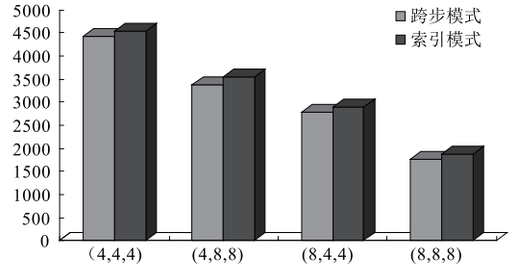

图9　访存传输周期数取样图

观察分析取样点数据可知,对于每种配置状态,当突发长度和流记录长度相同时,SMS 在跨步和索引两种模式下的访存传输周期数较少并且相似,即其访存效率相近. 其中又以跨步模式的访存传输周期个数更少,这与采用跨步模式时,访存流记录的位置相对集中有关. 此外,通过比较表 2、3、4 中数据可以发现:SMS 的设计相比于数据包 DMA 访存和主处理器管控访存的访存传输周期数大幅减少,访存性能显著提高,最大提升约 6 倍.

6　结束语

存储系统是影响专用密码处理器性能的关键部件,本文设计的 RCSP 流存储系统,由分布式寄存器堆、可配置分体式流存储文件、可配置流访存模块构成,文中详细设计和分析了 SMS 所包含的主要部件. 通过对 RCSP 进行 AES 算法加/解密报文集实验,统计结果表明与典型密码处理器的访存设计相比,本设计的访存传输周期数大幅降低,访存效率最高提升约 6 倍,实验检验了 SMS 的访存性能,证明该设计能够满足 RCSP 对

存储系统的性能要求.后续工作将继续优化 SMS 的内部结构,使它能适应新兴外存,为实现更高性能的密码处理器构建坚实基础.

参考文献

[1] WANG B, LIU LB. Dynamically reconfigurable architecture for symmetric ciphers[J]. Science China-Information Science, 2016, 59(4): 3410 – 3425.

[2] B K Khailany. A programmable 512 GOPS stream processor for signal, image, and video processing[J]. IEEE Journal Solid-State Circuits, 2008; 43(1): 202 – 213.

[3] CHEN SK, HUNG CY, CHEN CC, et al. Parallelizing complex streaming applications on distributed scratchpad memory multicore architecture[J]. International Journal of Parallel Programming, 2014, 42(6): 875 – 899.

[4] HU JT, XUE CJ, TSENG WC, et al. Memory access schedule minimization for embedded systems[J]. Journal of Systems Architecture, 2012, 58(1): 48 – 59.

[5] DAVID Padua. Encyclopedia of Parallel Computing[M]. US: Springer International Publishing, 2011. 1110 – 1118.

[6] MATICK RE, SCHUSTER SE. Logic-based eDRAM: origins and rationale for use[J]. IBM Journal of Research & Development, 2009, 49(1): 145 – 165.

[7] ISURU Nawinne, HARIS Javaid, RSOHAN Ragel. Exploring multilevel cache hierarchies in application specific MPSoCs [A]. IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems[C]. India: IEEE, 2015. 1991 – 2003.

[8] 郭振华,等. 面向类仿射型数组下标应用的参数化并行存储结构模板[J]. 电子学报,2016,44(8):1956 – 1961.
GUO Zhen-hua, et al. A parameterized parallelism memory template for affine array subscript application[J]. Acta Electronica Sinica, 2016, 44(8): 1956 – 1961. (in Chinese)

[9] 亨尼西,帕特森. 计算机体系结构:量化研究方法(5 版)[M]. 贾洪峰,译. 北京:人民邮电出版社,2013. 56 – 75.

[10] 党向磊,等. 面向按序执行处理器的预执行指导的数据预取方法[J]. 电子学报,2012,40(11):2145 – 2151.
X L Dang, et al. Pre-execution directed prefetching for in-order processors[J]. Acta Electronica Sinica, 2012, 40(11): 2145 – 2151. (in Chinese)

[11] WANG David. Modern DRAM Memory Systems: Performance Analysis and Scheduling Algorithm[D]. US: University of Maryland, 2009.

[12] TIM Güneysu, GREGOR Leander, AMIR Moradi. Lightweight Cryptography for Security and Privacy[M]. Berlin, Germany: Springer Berlin Heidelberg, 2015. 58 – 130.

[13] VOLOS Stavros, PICOREL Javier. BuMP: bulk memory access prediction and streaming[A]. 47th Annual IEEE/ACM International Symposium on Microarchitecture[C]. England: IEEE, 2014. 545 – 557.

[14] NATTI Rajitha. Implementations of secure reconfigurable cryptoprocessor a survey[A]. 3rd International Conference on Information System Design and Intelligent Applications[C]. India: Springer, 2016. 433 – 435.

[15] LEONARDO Steinfeld, MARCUS Ritt, et al. Low-Power Processors Require Effective Memory Partitioning[M]. Berlin: Springer Berlin Heidelberg, 2013. 73 – 81.

[16] KIM Chulwoo, SONG Junyoung, LEE Hyun-Woo. An I/O Line Configuration and Organization of DRAM[M]. Germany: Springer International Publishing, 2014. 13 – 23.

作者简介

朱玉飞(通信作者) 男,1990 年生于江苏淮安,信息工程大学硕士,主要研究方向为专用芯片设计,SOC 与协处理器设计.
E-mail:876635782@qq.com

戴紫彬 男,1966 年生于河南商丘,信息工程大学专用芯片设计教研室主任,博士生导师,研究方向为安全协处理器设计,VLSI 设计等.

徐进辉 男,1978 年生于江西宁都,博士,讲师,研究方向为计算机体系结构、可重构计算等.

李功丽 女,1981 年生于河南新乡,博士,讲师,研究方向为可重构计算等.