面向分组密码的可重构异构多核并行处理架构

冯 晓[1],李 伟[2],戴紫彬[1],马 超[1],李功丽[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 20123)

摘 要: 现有的可重构分组密码实现结构中,专用指令处理器吞吐率不高,阵列结构资源利用率低、算法映射过程复杂.为此,设计了分组密码可重构异构多核并行处理架构RAMCA(Reconfigurable Asymmetrical Multi-Core Architecture),分析了典型SP(AES-128)、Feistel(SMS4)、L-M(IDEA)及MISTY(KASUMI)结构算法在RAMCA上的映射过程.在65nm CMOS工艺下完成了逻辑综合和功能仿真.实验表明,RAMCA工作频率可达到1GHz,面积约为1.13mm^2,消除工艺影响后,对各分组密码算法的运算速度均高于现有专用指令处理器以及Celator、RCPA和BCORE等阵列结构密码处理系统.

关键词: 分组密码;异构多核;可重构;并行处理;密码处理器
中图分类号: TN492 **文献标识码:** A **文章编号:** 0372-2112 (2017)06-1311-10
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.06.005

Reconfigurable Asymmetrical Multi-core Architecture for Block Cipher

FENG Xiao[1], LI Wei[2,1], DAI Zi-bin[1], MA Chao[1], LI Gong-li[1]
(1. *PLA Information Engineering University, Zhengzhou, Henan* 450000, *China*;
2. *State Key Laboratory of Special Integrated Circuit and System, Fudan University, Shanghai* 20123, *China*)

Abstract: Among the existing reconfigurable block cipher hardware structures, the special instruction processor does not achieve high throughput rate, while resource utilization of the reconfigurable block cipher processing array is low and mapping process is very complicated. Therefore, the reconfigurable asymmetrical multi-core architecture (RAMCA) for block cipher was designed. Mapping processes of typical structures, which were SP (AES-128), Feistel (SMS4), L-M (IDEA) and MISTY (KASUMI), was analyzed. Hardware implementation was designed and synthesized in a 65nm CMOS process. The experimental area is about 1.13sq mm while frequency reaches 1GHz. After the influence of the process is eliminated, the performance of RAMCA is higher than that of other special instruction processors and most of the reconfigurable block cipher processing arrays, such as Celator, RCPA, BCORE, etc.

Key words: block cipher; heterogeneous multi-core; reconfigurable; parallel processing; cipher processor

1 引言

作为保障信息安全的有效手段,分组密码在数据加密、消息鉴别、认证及密钥管理等方面具有广泛的应用.分组密码运算是典型的计算密集型应用,对密码模块的运算速度有极高的要求,而分组密码算法、标准的多样性和不断发展,要求密码模块具备一定的灵活性.可重构计算面向特定应用领域进行优化,运算单元可重构,兼备了高性能与灵活性[1],面向分组密码的可重构架构设计成为密码实现技术的研究热点之一.

分组密码可重构实现技术主要有两条技术路线,一是专用指令处理器结构,一是阵列结构可重构处理系统.专用指令处理器的指令及运算单元面向密码应用进行优化,通过指令编写实现密码算法,具有数据处理位宽大、处理并行性高、控制简单、开发便捷等优点.Lisa Wu等人提出的专用指令处理器CryptoManiac采用4路32-bit的并行超长指令字VLIW(Very Long Instruction Word)结构[2].复旦大学设计了支持多簇扩展的VLIW结构安全处理器SophSEC[3],通过指令组合能够较高效地实现常见的几种密码算法.Bossuet等人系统研究对称密码硬件实现技术后明确指出,多核密码处理器是满足密码灵活性和吞吐率需求的最佳实现方

收稿日期:2015-12-21;修回日期:2016-04-08;责任编辑:覃怀银
基金项目:国家自然科学基金(No. 61404175)

式[4]. Grand 等人提出的可重构密码多核处理器 MCCP 集成了 4 个 32-bit AES 处理核心和 1 个 8-bit 任务调器，能够支持 AES 算法的各种模式，但对其他密码算法的支持较差[5]. 目前密码专用指令处理器结构密码实现吞吐率普遍较低.

阵列结构可重构处理系统为基于数据流驱动的密码运算单元阵列，相比于专用指令处理器实现方式，吞吐率有很大提升. 杨晓辉等人提出的可重构分组密码处理模型 RCPA 能够在横向和纵向上开发分组密码并行特征[6]. 陈韬等人设计的可重构分组密码处理模型 S-RCCPA，构造了基于分级互连的粗粒度可重构分组密码处理阵列结构[7]. Sayilar 和 Chiou 提出的 Cryptoraptor 结构集成了 80 个基本重构单元，极大地提升了许多密码算法的吞吐率，但由于缺少乘法单元，对 IDEA 等算法实现效率较差[8]. 阵列结构的密码运算单元一般设计比较复杂，面积和功耗较大，资源利用率较低，同时，数据流控制非常复杂，算法映射难度很大.

针对现有密码专用指令处理器吞吐率不高，可重构阵列结构资源利用率低、算法映射过程复杂的问题，论文设计了面向分组密码的可重构异构多核并行处理架构 RAMCA（Reconfigurable Asymmetrical Multi-Core Architecture），并以具有较广泛应用的 AES、ARIA、Camellia、SMS4、IDEA 及 KASUMI 等典型算法为例，实现了 SP、Feistel、L-M、MISTY 等分组密码结构在 RAMCA 上分组密码处理上的映射和性能评估.

2 RAMCA-可重构异构多核分组密码处理架构

2.1 RAMCA 总体结构

RAMCA 为异构多核结构，如图 1 所示. RAMCA 集成了 4 个精简型分簇式可重构分组密码处理器 R-RCBCP（Reduced Reconfigurable Clustered Block Cipher Processor）和 1 个共享加速运算处理器 SAC（Shared Accelerator Core）. RAMCA 具有独立的指令传输通路、数据输入通路和数据输出通路，通过共享输入缓存和共享输出缓存与外部交互数据. R-RCBCP 是 RAMCA 的主体运算部件，集成了 32-bit 内的二输入逻辑单元、移位单元、模加/减单元和 4 个并行 8×8 S 盒. SAC 是 RAMCA 的加速运算部件，用来实现模乘、有限域乘法、大位宽移位、置换等 R-RCBCP 实现效率低的密码操作.

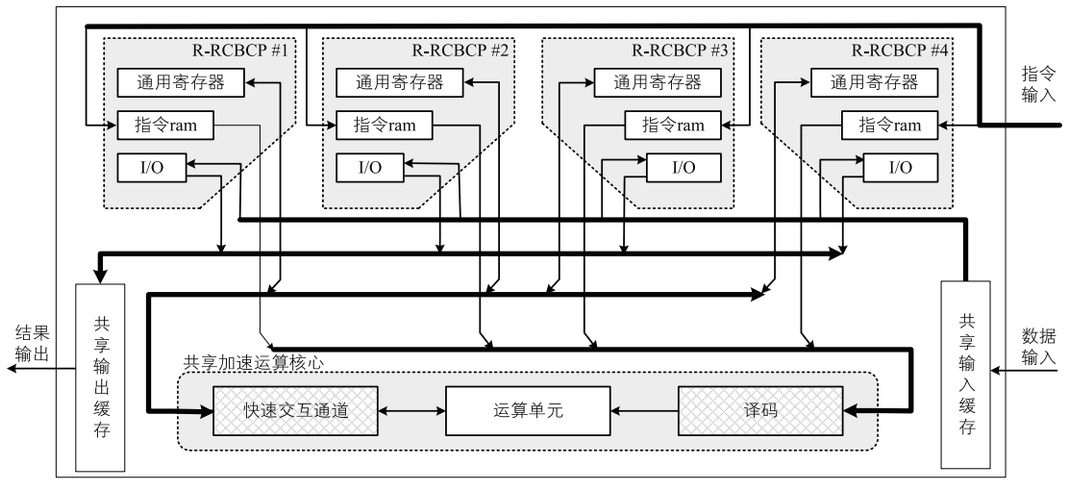


图1 RAMCA整体结构图

在分组密码算法中，模乘、有限域乘法、大位宽移位、置换等单元使用频率不高，但其关键路径长，对处理器工作频率有较大影响. 对这些操作一般有两种处理方式，一是降低处理器工作频率，如 RCBCP 等架构[9]，二是通过其他指令组合实现这些操作，如 Cryptoraptor 等结构[10]. 这两种方式都在一定程度上限制了处理器密码实现性能. RAMCA 有效地解决了上述问题，R-RCBCP 只集成使用频率高且延时小的密码运算单元，SAC 集成实现延时较长和大位宽的密码运算. 异构结构将不同操作特征的密码运算分开处理，既保证了处理器能够在较高的工作频率下运行，又保证了密码操作的实现效率，同时，资源共享机制也大大提升了密码处理器的资源利用率，有效减少了处理器面积.

2.2 精简运算核心 R-RCBCP 结构

R-RCBCP 借鉴了 RCBCP [9]的可重构分簇式设计思想，数据路径可重构为 4 个、2 个和 1 个运算簇，以 VLIW 结构指令驱动处理器各单元，在指令级充分开发了分组密码算法的并行特征. 同时，在详细分析分组密码结构特点和各运算单元延时特征的基础上，对 RCBCP 结构做了进一步改进. 将 4 路 32-bit 并行运算簇更

改为4路8-bit并行运算簇,并精简掉了严重影响系统工作频率的有限域乘法、模乘、大位宽移位和置换等运算单元.在此基础上,重新设计了指令系统、数据路径、控制路径及其他功能模块,结构如图2所示.

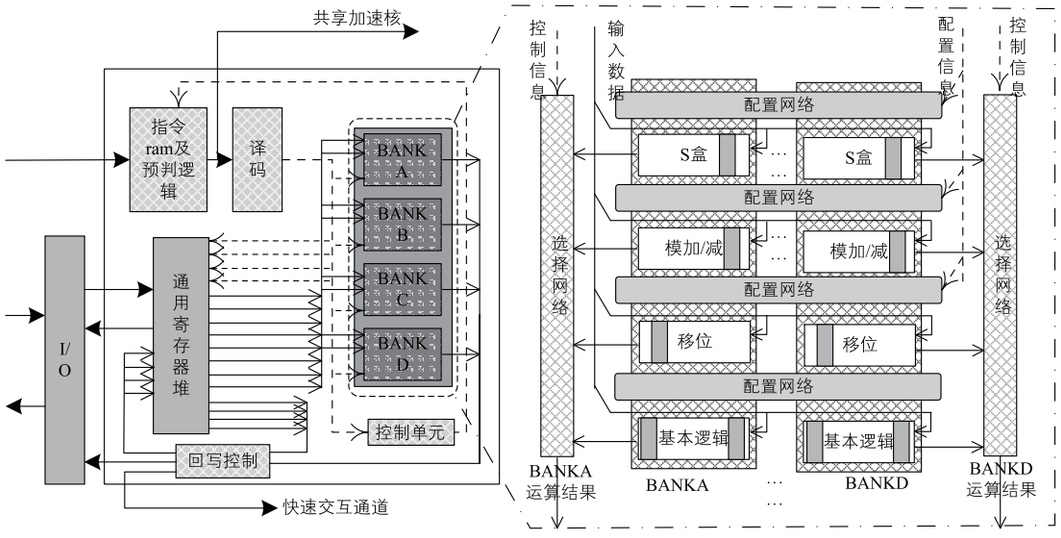


图2　R-RCBCP结构图

R-RCBCP集成的模加/减(32-bit内)、移位(32-bit内)、S盒及二输入基本逻辑操作延时较短,经初步评估,R-RCBCP的关键路径在流水线取指部分.由于分组密码中与、或及异或操作使用频率非常高,根据各操作延迟具体情况,在S盒单元绑定了前处理单元、在模加/减和移位单元绑定了后处理单元、基本逻辑单元绑定了前/后处理单元.前处理单元可对运算单元的源操作数进行与、或及异或的预处理,后处理单元可对运算单元的运算结果进行与、或及异或的后处理.运算单元绑定操作后,延时仍小于取指段延时,不会对系统工作频率产生影响.

R-RCBCP通用寄存器设计为相对任意读、固定写的分簇式结构,根据分组密码运算过程中存储需求,通用寄存器总存储量设计为32×8-bit,被分为4个存储量为8×8-bit的寄存器子块BANKA、BANKB、BANKC和BANKD,分别对应BANKA、BANKB、BANKC和BANKD 4个同构运算单元.每个BANK有1个写端口、2个读端口和1个固定输出端口,BANK内支持任意读写操作.固定输出端口为每个BANK的第5、6号寄存器和第7、8号寄存器,分别作为绑定操作的源操作数.

精简运算单元和寄存器堆容量后,R-RCBCP的指令位宽减少到了128-bit,考虑到密码算法编制需求,指令存储模块容量设计为512×128-bit.指令存储器中存储R-RCBCP指令和SAC指令.执行密码运算时,首先从R-RCBCP指令存储器中读取指令字,若该指令为R-RCBCP指令,则该指令经过R-RCBCP译码单元生成运算单元、存储单元的控制信号,实现密码计算、数据存取以及数据传送等操作,若该指令为SAC指令,则发送到SAC译码单元,由SAC完成后续操作.

2.3　加速核心SAC结构

SAC同样采用VLIW处理结构,主要由译码模块、运算单元、快速交互通道及控制单元组成,可实现1个128-bit、2个64-bit或者4个32-bit的密码运算,如图3所示.SAC接收R-RCBCP发送的SAC指令后进行译码、执行、回写操作,其中,64/128位移位指令为单周期指令,有限域乘法指令和置换指令为2时钟周期指令,模乘指令为3时钟周期指令.SAC完成运算后将结果写入快速交互通道对应地址.快速交互通道为任意读、相对固定写的分簇式寄存器堆,位宽为32-bit,总存储量为16×32-bit,被分为4个存储量为4×32-bit的寄存器子块,分别对应R-RCBCP #1~#4.为指令编写方便,快速交互通道寄存器命名为RSij,i取值范围为0~3,j取值范围为a~d.

R-RCBCP #X中数据只允许写入寄存器RSXj.R-RCBCP与快速交互通路通信位宽为32-bit,RSij对应R-RCBCP中BANKA、BANKB、BANKC和BANKD具有相同地址标号的4个寄存器(数据由高到低组合),例如将R-RCBCP #1中BANKA、BANKB、BANKC和BANKD中的第3号寄存器数据写入RS1a.SAC与快速通道的通信位宽为128-bit,可任意读取/写入RSi(表示RSia|RSib|RSic|RSid)或者RSj(表示RS1j|RS2j|RS3j|RS4j).快速通道不仅能够实现R-RCBCP与SAC间数据的透明传输,而且在置换指令的配合下,能够实现R-RCBCP间数据交互,具有很高的灵活性和传输效率.

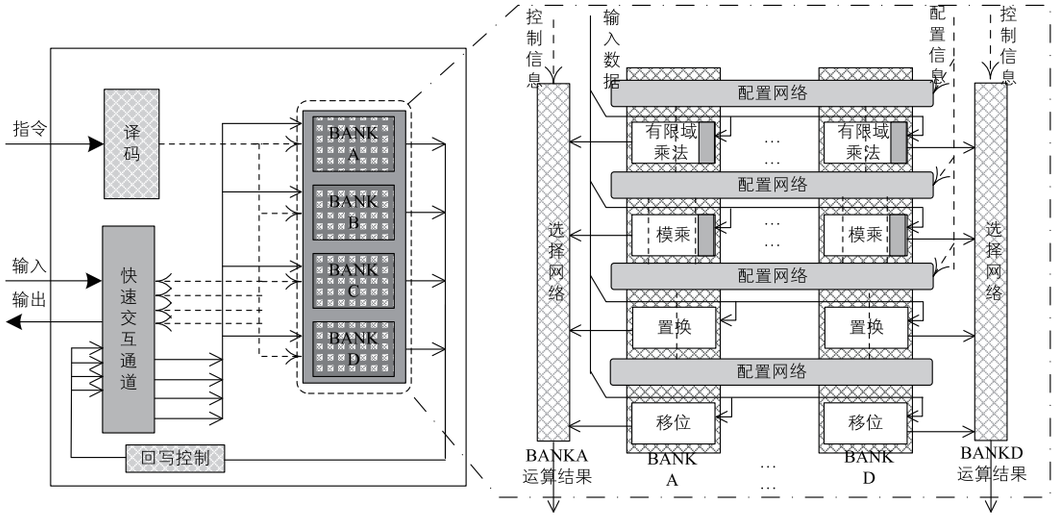


图3 SAC结构图

3 典型分组密码算法映射

本节将以 AES-128[11]、SMS4[12]、IDEA[13]和 KASUMI[14]算法为例,详细讨论 SP、Feistel、L-M 和 MISTY 结构分组密码在 RAMCA 上的映射过程. 上述算法均有比较广泛的应用,基本可以代表当前分组密码的设计特点. 同一算法可以有多种不同的映射结果,文中仅列出性能较优的映射方案,不代表最优映射方案.

3.1 SP 结构-AES 密码算法映射

SP 结构是目前广泛应用的一种分组密码结构,以 AES-128 算法为例进行 SP 结构分组密码映射. AES-128 分组长度及密钥长度为 128-bit,主要由初始轮密钥加、轮变换和末尾变换 3 部分组成,其中,轮变换包括字节代替、行移位、列混合和密钥加,末尾变换包括字节代替、行移位和密钥加. 图 4 所示为 AES-128 算法映射结果,其中图 4(a)为输入单分组的映射结果,图 4(b)为输入 4 个并行分组的映射结果.

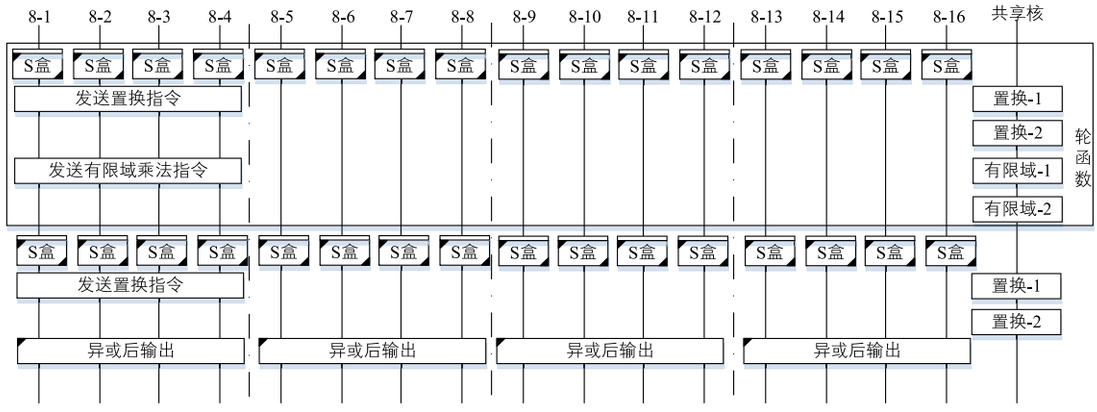
对于单分组,R-RCBCP#1 ~ R-RCBCP#4 由低到高并行实现 16 个 8×8 的 S 盒运算,SAC 以 R-RCBCP 的 S 盒输出结果为源,完成行移位(置换)和列混合(有限域乘法)操作. 由于 R-RCBCP 的 S 盒单元绑定了前处理逻辑,因此初始轮密钥加操作可与第一轮的 S 盒操作使用一条指令完成,而轮函数最后的密钥加操作可与下一轮的 S 盒操作使用一条指令完成. SAC 完成 128 位置换和有限域乘法操作分别需要 2 个时钟周期,分别标记为"置换 - 1"、"置换 - 2"、"有限域 - 1"和"有限域 - 2",因此 RAMCA 共需要 5 个时钟周期完成 AES-128 轮函数. 末尾变换不包括列混合操作,仅需要 4 个时钟周期即可完成. (图中,各操作上/下的阴影块表示绑定前/后逻辑操作,左上角黑三角表示自快速交互通道取数,右下角黑三角表示运算结果写入快速交互通道.)

对于多分组,R-RCBCP#1 ~ R-RCBCP#4 分别处理 1 个分组,各分组在图 4(b)中以不同灰度表示. 由于 R-RCBCP 支持任意读操作,轮函数中的行移位操作可在指令译码/取数阶段隐式完成,因此 R-RCBCP 仅需 6 个时钟周期即可完成一次轮变换. SAC 可以以流水方式实现 R-RCBCP#1 ~ R-RCBCP#4 发送的有限域乘法指令,"有限域-12"表示有限域乘法单元流水执行当前列混合指令第 2 周期操作和下条列混合指令第 1 周期操作. 受限于 SAC 有限域乘法单元,R-RCBCP#1 ~ R-RCBCP#4 处理输入数据时无法完全并行,会损失 3 个时钟周期用于等待共享资源. 当处理分组数量较大时,该损耗可忽略不计.

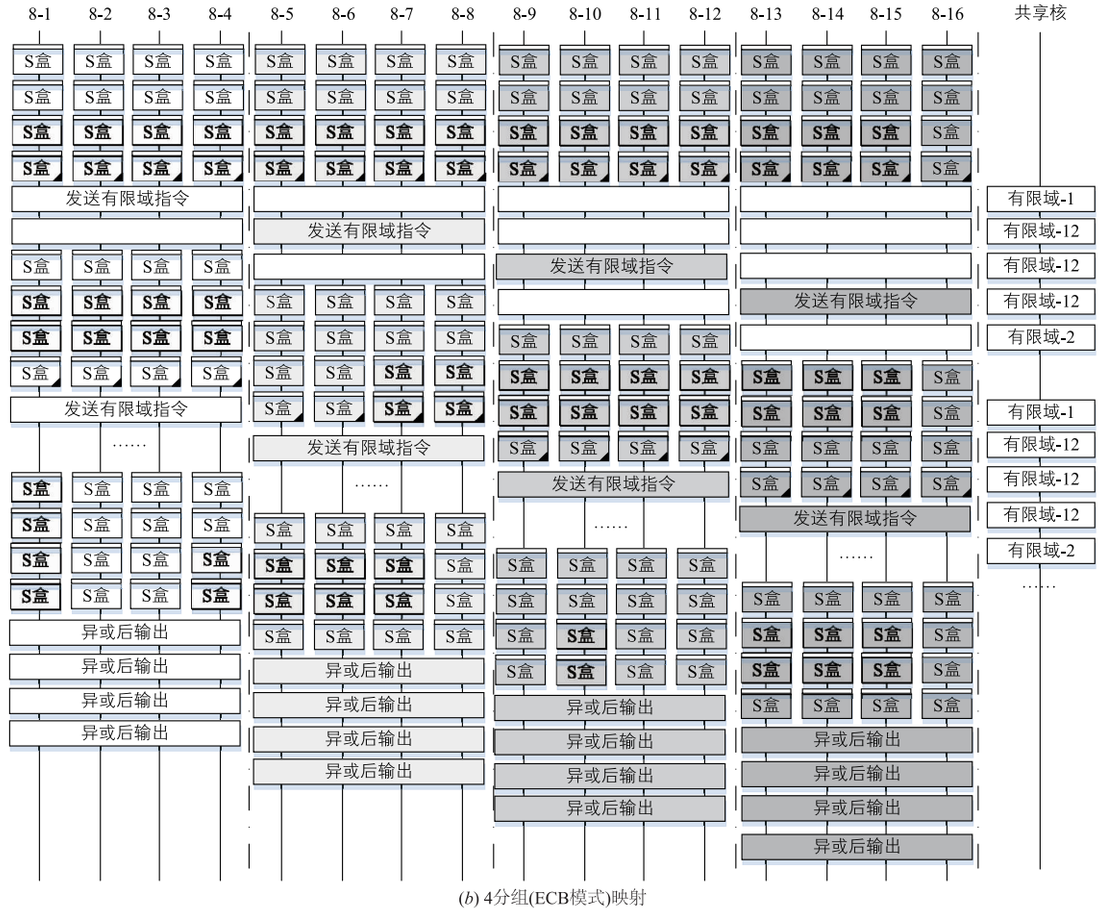
3.2 Feistel 结构-SMS4 密码算法映射

以 SMS4 算法为例进行 Feistel 结构分组密码映射. SMS4 分组长度和密钥长度均为 128-bit,采用 32 轮迭代结构. 设明文输入为(X_0,X_1,X_2,X_3),轮密钥为 rk_i,$i=0,1,\cdots,31$,SMS4 加密变换可表示为:$X_{i+4}=F(X_i,X_{i+1},X_{i+2},X_{i+3},\mathrm{rk}_i)$,密文输出$(Y_0,Y_1,Y_2,Y_3)=(X_{35},X_{34},X_{33},X_{32})$,$F=X_i\oplus B\oplus(B\lll 2)\oplus(B\lll 10)\oplus(B\lll 18)\oplus(B\lll 24)$,其中 $B=S(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus \mathrm{rk}_i)$. 图 5 所示为 SMS4 算法映射结果,其中图 5(a)为输入单分组的映射结果,图 5(b)为输入 4 个并行分组的映射结果.

SMS4 轮函数有两种实现方案,一是由 SAC 使用 1 条 128 位移位指令计算($B\lll 2$)、($B\lll 10$)、($B\lll 18$)和($B\lll 24$),然后使用异或指令实现其他操作,一是由 R-RCBCP 使用移位绑定后异或操作实现. 第一种方式比第二种方式节省1个时钟周期,但是



(*a*)单分组映射



(*b*) 4分组(ECB模式)映射

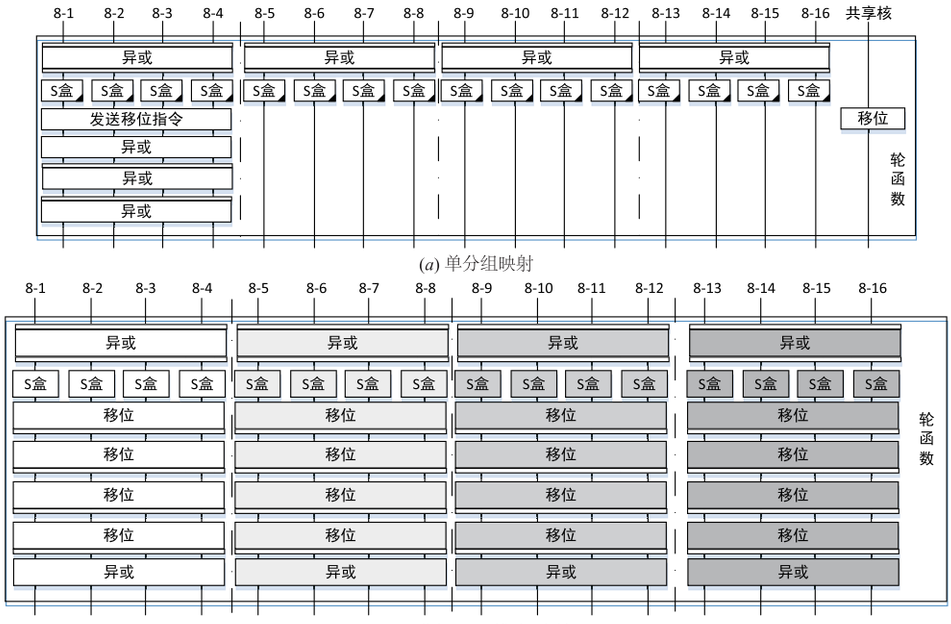
图4　AES算法在RAMCA上的映射

需要其他 3 个 R-RCBCP 进行重复计算. 在单分组映射中,采用第一种映射方式,在多分组映射中,采用第二种映射方案. RAMCA 寄存器位宽为 8-bit,不需要额外指令实现反序变换,因此,单分组映射时轮函数需 6 条指令实现,多分组映射时轮函数需要 7 条指令实现.

3.3　L-M 结构-IDEA 密码算法映射

以 IDEA 算法为例进行 L-M 结构分组密码映射. IDEA 的分组长度为 64-bit,密钥长度为 128-bit,由 8 轮轮变换和一个输出变换组成. 图 6 所示为 RAMCA 对 IDEA 算法的映射结果,其中图 6(*a*)为输入单分组的映射结果,图 6(*b*)为输入 4 个并行分组的映射结果.

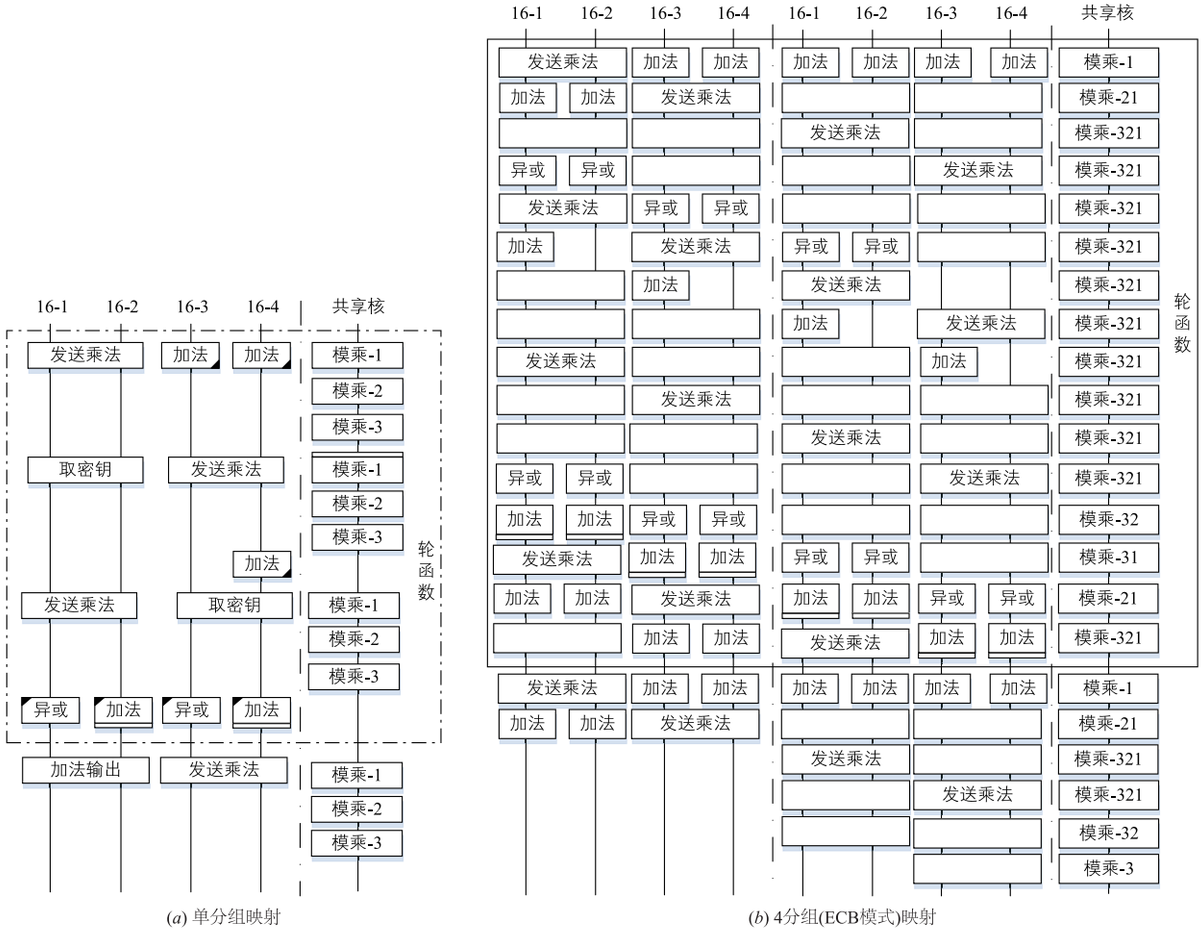
IDEA 轮变换中包括 4 个模 $2^{16}+1$ 乘法操作、4 个模 $2^{16}+1$ 加操作和 6 个异或操作,各操作间前后依赖关系紧密,只有2个$2^{16}+1$乘法操作及最后的加法/异



(*a*) 单分组映射

(*b*) 4分组(ECB模式)映射

图5 SMS4算法在RAMCA上的映射



(*a*) 单分组映射

(*b*) 4分组(ECB模式)映射

图6 IDEA算法在RAMCA上的映射

或操作可以并行执行. R-RCBCP 中没有模乘单元,模 $2^{16}+1$ 乘指令必须由 SAC 执行,执行周期为 3 个时钟周期. 单分组映射时,IDEA 算法轮函数共需 11 条指令实现. IDEA 算法采用 64-bit 映射方案对处理器资源利用很低,因此在多分组映射中,采用 32-bit 映射方案. R-RCBCP#1 ~ R-RCBCP#4 分别独立执行一个数据分组,SAC 流水处理 R-RCBCP#1 ~ R-RCBCP#4 发送的模乘操作请求,因此,IDEA 4 分组映射每轮轮变换共需 13 条指令,同时会损失 6 个时钟周期用于 SAC 流水执行. 当处理分组数量较大时,该损耗可忽略不计.

3.4　MISTY 结构-KASUMI 密码算法映射

以 KASUMI 算法为例进行 MISTY 结构分组密码映射. KASUMI 分组长度为 64-bit,密钥长度为 128-bit,轮函数迭代 8 轮. 轮函数分为内外两层轮变换,外层轮变换是 32-bit 的 3 轮 MISTY 型,记做 FO 函数,内层变换是 16-bit 的 MISTY 型,记做 FI 函数. FI 函数使用了 7×7 和 9×9 两种不同规模的 S 盒. 图 7 所示为 KASUMI 算法 1 个分组的映射结果. KASUMI 算法实现的难点在于 9×9 S 盒. 根据 RAMCA 结构特点,采用控制路径与数据路径相结合的方式,通过 4 个并行 8×8 S 盒分别计算 $x_8=0$ 时 $y_0 \sim y_7$、y_8 和 $x_8=1$ 时 $y_0 \sim y_7$、y_8,结合位测试(控制指令),根据 x_8 取值跳转至正确分支. 在实际运算中,RAMCA 仅需执行 2 条指令即可完成 9×9 S 盒变换. RAMCA 可并行执行两个分组,在此不再赘述映射过程.

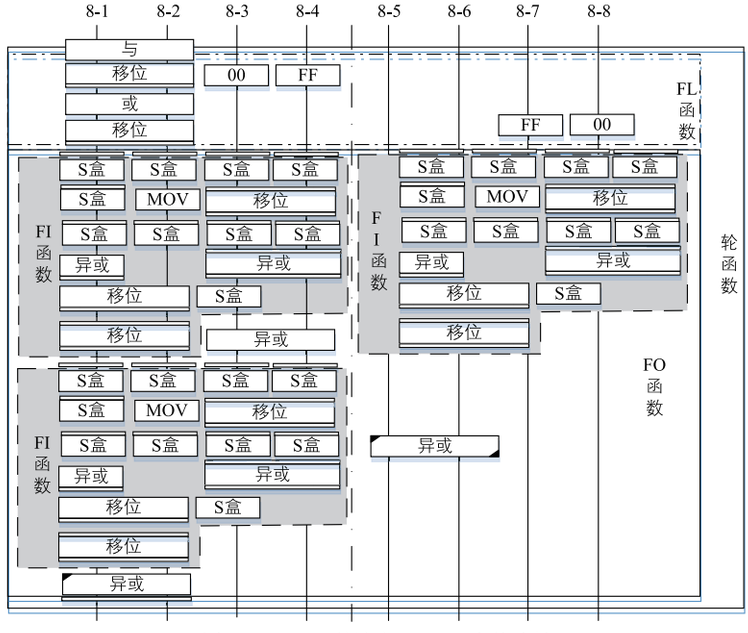


图7　KASUMI算法在RAMCA上的映射

4　实现验证与性能分析

采用 Verilog 语言对 RAMCA 进行描述,采用 65nm CMOS 工艺标准单元库及相应负载模型对 RAMCA 原型进行逻辑综合. 根据仿真结果,RAMCA 关键路径长度为 0.96ns,为保证工作稳定性,将 RAMCA 工作频率选定为 1GHz,此时 RAMCA 仿真面积为 1126260.8μm^2,约 78.2 万等效门. RAMCA 及部分关键单元实现结果如表 1 所示.

由综合结果可知,SAC 面积约为 RAMCA 总体面积的 8.68%,R-RCBCP 面积约为 RAMCA 总体面积的 86.65%,指令 ram 是 RAMCA 的主要面积开销,大约占总面积的 54.22%. 对比表 1 中模乘、有限域乘法、置换等运算单元加入单元内流水前后关键路径延迟情况,加入单元内流水后 RAMCA 运算单元关键路径延时由 1.41ns 降低到了 0.83ns,运算单元工作频率可获得 69.9% 的提升. 由于 SAC 为共享结构且不包含指令 ram,提高了资源利用率,节约了硬件成本,面积开销降低了 26.0% 左右.

为全面评估 RAMCA 性能,在节 3 列出算法的基础上,增加了韩国标准 ARIA 算法[15](SP 结构)和设计特色较为突出的 Camellia 算法[16](Feistel 结构)进行实现. RAMCA 与其他可重构结构性能对比情况如表 2 所示. 其中,Cryptonite[17]、CCProc[18] 和 RCBCP[9] 为专用指令密码处理器,SophSEC 为多簇并行的安全专用处理器,Celator[19]、RCPA[6]、S-RCCPA[7] 和 Cryptoraptor[8] 为阵列结构可重构密码处理结构,BCORE[20] 为面向 AES 的粗粒度可重构阵列结构. 由于各硬件结构的实现工艺存在较大差距,为减少工艺影响,根据文献[21]不同工艺下面积、频率等效关系,将各结构的面积和吞吐率

均按照65nm CMOS工艺进行了换算.

表1 RAMCA架构ASIC实现结果

单元		关键路径延迟(ns)	面积(μm^2)	所占比例(%)	
SAC	模2^{32}乘(32 -bit)	1.41/0.73	6765.6	0.60	8.68
	模修正(16 -bit)	1.19/0.83	1700.2	0.15	
	有限域乘法(32 -bit)	1.22/0.69	18090	1.61	
	移位(128 -bit)	0.79	5575	与置换单元复用	
	比特置换(128 -bit)	1.58/0.8	11150	0.99	
	快速交互通道	0.41	34325	3.05	
	其他	--	20482	1.82	
R-RCBCP	S盒(8 -bit)	0.55	11217.9	1.00*16	86.65
	两输入逻辑(8 -bit)	0.32	115	0.01*36	
	模加/减(8/16/32 -bit)	0.5	1354.6	0.12*16	
	移位(32-bit)	0.61	998	0.09*16	
	通用寄存器堆	0.43	17163	1.52*4	
	指令ram	0.67	152657.6	13.55*4	
	其他	--	44945	3.99	
其他	--	--	52540	4.67	
RAMCA	--	1.00	1126260.8	100	

表2 不同架构典型密码算法实现性能对比

结构名称	工艺(nm)	面积(mm^2)	时钟频率(MHz)	吞吐率(Gbps)(单分组/多组并行)	映射算法	等效面积	等效吞吐率
Cryptonite	180	--	400	0.73 0.57	AES IDEA	--	2.02 1.58
CCProc	130	5.3	250	0.41	AES	1.33	0.82
RCBCP	180	--	312.5	0.67 0.42	AES IDEA	--	1.86 1.16
SophSEC(SOC)	130	25	200	0.56 0.21	AES SMS4	6.25	1.12 0.42
Celator	130	0.1	190	0.05	AES	0.03	0.1
RCPA	180	14.9	180	/0.79 /0.4	AES IDEA	1.94	/2.18 /1.11
S-RCCPA	180	13.4	243.9	0.47/2.8 0.13/1.6	AES IDEA	1.75	1.3/7.7 0.36/4.43
Cryptoraptor	45	6.32	1000	6.4/128 3.2/64 1/16	AES Camellia KASUMI	13.19	4.43/88.62 2.22/44.31 0.69/11.1
BCORE	65	50	100	0.15/2.33	AES	50	0.15/2.33
RAMCA	65	1.13	1000	2.61/7.88 1.19/1.36 2.13/8.25 0.67/2.29 0.70/2.27 0.49/0.97	AES ARIA Camellia SMS4 IDEA KASUMI	1.13	2.61/7.88 1.19/1.36 2.13/8.25 0.67/2.29 0.70/2.27 0.49/0.97

仿真结果表明,RAMCA 可以高效处理各种结构的分组密码算法. 通过性能对比,RAMCA 对分组密码的吞吐率明显高于其他专用指令处理器. 与阵列结构可重构密码处理架构比较,RAMCA 对 AES 算法和单分组 IDEA 的吞吐率仍明显高于 Celator、RCPA、S-RCCPA 和 BCORE 处理架构. 由此可见,RAMCA 获得了与当前阵列结构可重构密码处理架构相当的密码处理速度. RAMCA 对多分组并行模式下 IDEA 算法吞吐率低于 S-RCCPA,对 AES、Camellia 和 KASUMI 算法吞吐率均低于 Cryptoraptor 结构. Cryptoraptor 结构未设计乘法单元,对使用范围较广的 IDEA 算法支持效果差,Cryptoraptor 作者在吞吐率对比中回避了 IDEA 算法,因此无法做出比较. S-RCCPA 未列举 MISTY 结构分组密码算法的吞吐率,对比范围有限. 同时,S-RCCPA 和 Cryptoraptor 的资源消耗分别是 RAMCA 的 1.6 倍和 12 倍左右,且开发难度较大.

5　结束语

本文设计并实现了面向分组密码的可重构异构多核并行处理架构 RAMCA,详细分析了典型 SP 结构(AES-128)、Feistel 结构(SMS4)、L-M 结构(IDEA)及 MISTY 结构(KASUMI)分组密码在 RAMCA 上的映射过程,在 65nm CMOS 工艺下对 RAMCA 进行了逻辑综合和功能仿真. RAMCA 算法映射过程灵活便捷,对 AES、ARIA、Camellia、SMS4、IDEA 及 KASUMI 等典型分组密码算法的吞吐率(单分组/ECB 模式)分别达到了 2.61/7.88Gbps、1.19/1.36 Gbps、2.13/8.25 Gbps、0.67/2.29 Gbps、0.70/2.27 Gbps 和 0.49/0.97Gbps. RAMCA 资源开销较小、吞吐率高、实现灵活、开发简单,具有很好的应用前景.

参考文献

[1] COMPTON K, HAUCK S. Reconfigurable computing: a survey of systems and software[J]. ACM Computing Surveys, 2002, 34(2): 171 – 210.

[2] WU L, WEAVER C, AUSTINT. CryptoManiac: A fast flexible architecture for secure communication[J]. Computer Architecture: Proceedings Annual International Symposium 2001, 29(2): 110 – 119.

[3] 黄伟. 面向云计算的性能与功耗可配置安全终端技术研究[D]. 上海:复旦大学,2011.

[4] BOSSUET L, GRAND M, GASPAR L, et al. Architectures of flexible symmetric key crypto engines-a survey: from hardware coprocessor to multi-crypto-processor system on chip[J]. ACM Computing Surveys, 2013, 45(4): 115 – 123.

[5] GRAND M, BOSSUET L, GAL B L, et al. Design and implementation of a multi-core crypto-processor for software defined radios[A]. Andreas Koch. Reconfigurable Computing: Architectures, Tools and Applications[C]. Berlin: Springer Berlin Heidelberg, 2011. 29 – 40.

[6] 杨晓辉,戴紫彬,张永福. 可重构分组密码处理结构模型研究与设计[J]. 计算机研究与发展,2009,46(6):962 – 967.
YANG Xiao-hui, DAI Zi-bin, ZHANG Yong-fu. Research and design of reconfigurable computing targeted at block cipher processing[J]. Journal of Computer Research and Development, 2009, 46(6): 962 – 967. (in Chinese)

[7] 陈韬,罗兴国,李校南,等. 一种基于流处理框架的可重构分簇式分组密码处理结构模型[J]. 电子与信息学报,2014,12(12):3027 – 3034.
CHEN Tao, LUO Xing-guo, LI Xiao-nan, et al. An architecture of stream based reconfigurable clustered block cipher processing array[J]. Journal of Electronics & Information Technology, 36(12): 3027 – 3034. (in Chinese)

[8] SAYILAR G, CHIOU D. Cryptoraptor: high throughput reconfigurable cryptographic processor[A]. Marculescu D. The IEEE/ACM International Conference on. Computer-Aided Design [C]. San Jose, CA: IEEE, 2014. 155 – 161.

[9] 孟涛,戴紫彬. 分组密码处理器的可重构分簇式架构[J]. 电子与信息学报,2009,2(2):453 – 456.
MENG Tao DAI Zi-bin. Reconfigurable clustered architecture of block cipher processor[J]. Journal of Electronics & Information Technology, 2009, 31(2): 453 – 456. (in Chinese)

[10] SAYILAR G. Cryptoraptor: High Throughput Reconfigurable Cryptographic Processor for Symmetric Key Encryption and Cryptographic Hash Functions[D]. Texas: The University of Texas at Austin, 2014.

[11] 夏辉,贾智平,张峰,李新,陈仁海,EdwinH. -M. Sha. AES 专用指令处理器的研究与实现[J]. 计算机研究与发展,2011,48(08):1554 – 1562.
XIA Hui, JIA Zhiping, ZHANG Feng, et al. The research and application of a specific instruction processor for AES [J]. Journal of Computer Research and Development, 2011, 48(08): 1554 – 1562. (in Chinese)

[12] LI R, Sun B, LI C, et al. Differential fault analysis on sms4 using a single fault[J]. Information Processing Letters, 2011, 111(4): 156 – 163.

[13] BIHAM E, DUNKELMAN O, KELLER N, et al. New attacks on IDEA with at least 6 rounds[J]. Journal of Cryptology, 2015, 28(2): 209 – 239.

[14] DUNKELMAN O, KELLER N, SHAMIR A. A practical-

time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephone[J]. Journal of Cryptology,2014,27(4):824 – 849.

[15] 李曼曼,陈少真. 对 ARIA 算法中间相遇攻击的改进[J]. 通信学报,2015,36(3):277 – 282.
LI Man-man, CHEN Shao-zhen. Improved meet-in-the-middle attack on ARIA cipher[J]. Journal on Communications,2015,36(3):277 – 282. (in Chinese)

[16] SUGIO N,AONO H,SEKINO K,et al. A new higher order differential of Camellia[A]. Kasai K. The International Symposium on Information Theory and Its Applications (ISITA)[C]. Melbourne Australia: IEEE, 2014. 478 – 482.

[17] BUCHTY R. CRYPTONITE-A Programmable Crypto Processor Architecture for High-bandwidth Applications [D]. Munchen: Institut fur Informatik der Technischen Universitat Munchen,2002.

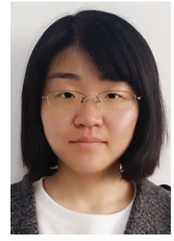
[18] THEODOROPOULOS D,PAPAEFSTATHIOU I,PNEVMATIKATOS D. N. CCproc: An efficient cryptographic coprocessor[A]. Torres L. The 16th IFIP/IEEE International Conference on Very Large Scale Integration [C]. Montpellier France: IEEE,2008. 160 – 163.

[19] FRONTE D,PEREZ A,PAYRAT E. Celator: A multi-algorithm cryptographic co-processor[A]. Cumplido R. The International Conference on Reconfigurable Computing and FPGAs[C]. Cancun, Mexico: IEEE, 2008: 438 – 443.

[20] 郭岩松,刘雷波. 一种面向分组密码的粗粒度可重构阵列及 AES 算法映射[J]. 微电子学与计算机,2015,32(09):1 – 5.
GUO Yan-song, LIU Lei-bo. A block cipher oriented coarse-grained reconfigurable array and AES algorithm mapping [J]. Microelectronics & Computer, 2015, 32(09):1 – 5. (in Chinese)

[21] LIU B. BAAS B M. Parallel AES encryption engines for many-core processor arrays [J]. IEEE Transactions on Computers,2013,62(3):536 – 547.

作者简介

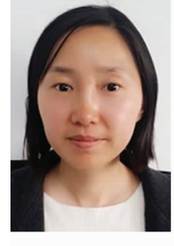


冯 晓 女,1987 年生于河北衡水. 信息工程大学博士生. 研究方向为多核处理器、密码专用芯片设计.
E-mail: fengxiaoisl@163.com

李 伟(通信作者) 男,1983 年生于天津. 信息工程大学副教授,现为复旦大学国家集成电路重点实验室博士生. 研究方向为密码处理器设计,ASIC 专用芯片设计.
E-mail: liwei12@fudan.edu.cn

戴紫彬 男,1966 年生于河南商丘. 信息工程大学教授,博士生导师. 研究方向为专用芯片设计、可重构芯片、可重构 SoC 设计.

马 超 男,1988 年生于陕西西安. 信息工程大学博士生. 研究方向为多核处理器、密码专用芯片设计.



李功丽 女,1981 年生于信阳. 信息工程大学博士生. 研究方向为多核处理器、密码专用芯片设计.