基于流体系结构的高效能分组密码处理器研究

王寿成,严迎建,徐进辉
(解放军信息工程大学,河南郑州 450001)

摘 要: 针对现有密码处理器存在的问题,借鉴流处理器架构,提出了高效能的可重构分组密码流处理器架构.该架构采用层次化设计思想,通过分块式本地寄存器组的数据组织方式和共享拼接使用运算单元机制,实现了软件流水和硬件流水的协同工作,能够挖掘分组内和分组间的指令级并行性并提高功能单元的利用率.在65nm CMOS工艺下对架构进行了综合仿真,并经过了大量算法映射.实验结果证明,该架构在CBC和ECB加密模式下均具有良好的加密性能.与其他密码处理器相比,该架构具有小面积、高效能的特点.

关键词: 分组密码;流处理器;可重构;软件流水;面积能效比
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2017)04-0937-07
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.04.024

Research of High-Efficient Block Cipher Processor Based on Stream Architecture

WANG Shou-cheng, YAN Ying-jian, XU Jin-hui
(*PLA Information Engineering University, Zhengzhou, Henan* 450001, *China*)

Abstract: To solve the existing problem of the cipher processor, high-efficiency reconfigurable block cipher processor based on stream architecture was proposed. Through the efficient data organization and flexible cipher computing units, the processor that adopts the design conception of hierarchy achieves the cooperation of software and hardware pipeline, develops instruction level parallelism in a block and among multiple blocks and improves the utilization rate of functional units. The processor was simulated and synthesized in 65nm CMOS process. The mapping results of typical block cipher algorithms show that it has high encryption performance both in CBC and ECB mode. Compared with other cryptographic processors, this processor has the advantage of small-area and high-efficiency.

Key words: block cipher; stream processor; reconfigurable; software pipeline; area efficiency

1 引言

随着互联网技术的持续发展,信息安全面临的挑战越来越多样化.密码处理器作为一种高效的信息保护手段,在各类信息设备中广泛使用.由于密码算法种类和应用场景众多,通常采用可重构技术来设计密码处理器,使处理器兼具高性能和灵活性.国内外针对分组密码的可重构实现进行了一系列研究.Bo Wang等提出的可重构密码运算阵列RCPC[1],集成了16×32规模的可重构功能单元,该结构能够实现密码算法性能的极大提升,对AES、DES、SMS4等分组密码算法的性能实现都达到了数十Gbps.Gokhan S等提出的可重构密码处理器Cryptoraptor[2],集成了20×4规模的可重构功能单元,具有很高的密码实现性能,其功能单元利用率平均在29%左右.此外MCCP[3]、RCBCP[4]、SophSEC[5]等结构也实现了密码算法处理的高性能和灵活性.但上述结构有一个共同问题就是资源消耗巨大但利用率却不高,尤其是在进行CBC等串行加密模式时大量的资源闲置,造成了极大的浪费.

在密码处理器的实际应用中,如在移动终端内集成密码处理器,需要综合考虑性能、面积及功耗等指标,其应用要求往往是在资源受限的条件下追求性能的最

收稿日期:2016-04-18;修回日期:2016-10-19;责任编辑:马兰英
基金项目:国家自然科学基金(No.61404175)

大化,即达到密码处理的高效能. 本文提出了一种基于层次结构的可重构分组密码流处理架构,该架构具有高效的数据组织方式和灵活的数据加密单元,通过软件流水和硬件流水协同开发指令级并行度,有效提高功能单元的利用率,在资源受限的条件下极大地提高加密性能. 多种密码算法映射结果表明,该架构功能单元利用率能达到50%以上,在CBC加密模式和ECB加密模式下都具有良好的性能优势. 与其余密码处理器架构相比较,该架构在性能方面不存在太大的劣势,而且具有最优的面积能效比.

2 可重构分组密码流处理器

2.1 总体架构

结合分组密码算法的特征,立足提高密码处理单元的利用率、开发分组密码的流水特性与并行性,本文提出了一种基于层次的可重构分组密码流处理器(Reconfigurable Block Cipher Stream Processor,RBCSP). RBCSP的结构图如图1所示,其硬件结构采用层次化设计,分别为主从接口层、流级控制层、核级控制层、数据组织层和密码运算层五个层级.

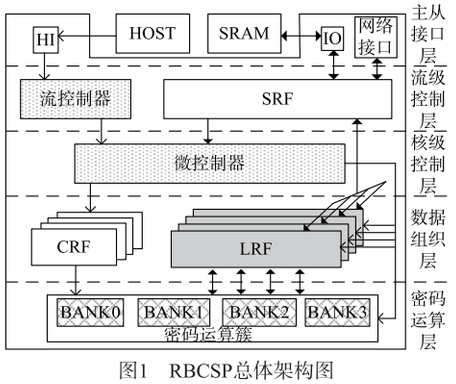


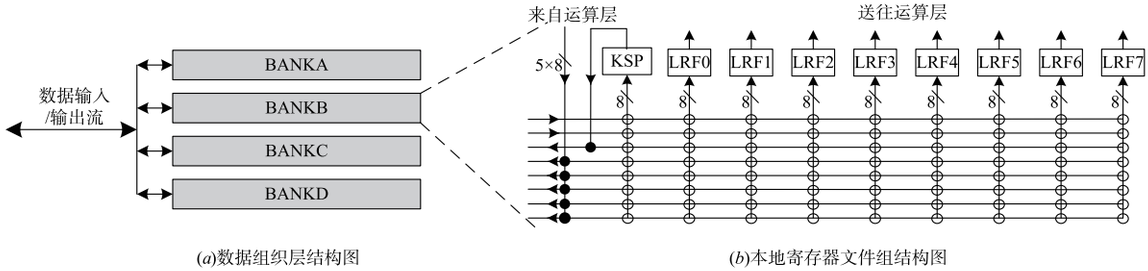
图1 RBCSP总体架构图

主从接口层包括网络接口、主/从接口和外设接口,作用是增加RBCSP的通用性和可扩展性. 网络接口能够实现RBCSP的多核系统,实现ECB加密性能的提升. 主/从接口和外设接口使得RBCSP可以作为通用设备挂载在片上总线上,实现在SoC内的集成. 流级控制层包括流控制器和流寄存器文件(Stream Register File,SRF),流控制器通过流级指令完成数据流的访存、密码运算核心的加载和启动等功能,是控制逻辑的核心. SRF的存储容量为16×32 bit,主要完成输入/输出数据的缓存和加载调度. 核级控制层主要指微控制器,其作用是完成对加/解密微代码的发射,控制数据组织层和密码运算层完成对应的密码操作. 数据组织层包括配置寄存器文件(Configure Register File,CRF)和本地寄存器文件(Local Register File,LRF),CRF通过配置信息完成对可重构密码单元和互连网络的配置. LRF通过灵活的数据组织方式为密码运算层提供源数据并暂存中间结果. 密码运算层专注于密码运算的执行,能够进行多种位宽的密码操作,是实现密码算法的关键. 下文重点对数据组织层和密码运算层进行阐述.

2.2 数据组织层

通过对大量密码算法的分析发现,密码算法的运算粒度通常是8 bit、16 bit、32 bit、64 bit或128 bit. 而绝大多数密码处理器的数据位宽为32 bit,这样在实现细粒度运算时就需要频繁地进行异或和移位操作来完成小位宽数据的组织,这就造成加密周期数急剧增长,使得密码处理性能直线下降. 基于此考虑,RBCSP采用了如图2所示的数据组织结构,该结构能够更加灵活高效地进行数据调度,从而保证密码操作的高效快速执行.

如图2(*a*)所示,本地寄存器文件组被分为4个子块BANKA、BANKB、BANKC和BANKD,在微指令控制下,能够单独或协同与密码运算层进行数据交互. 每个BANK的结构如图2(*b*)所示,由8个LRF、1个密钥便签寄存器(Key Scratch pad,KSP)和交叉互连网络(也称为结果总线)组成,BANK内的数据位宽均为8 bit. 每个LRF的容量为4×8 bit,密码分组进行运算时,只在数据输入和最终结果写回时访问SRF,其间所有的源操作数和中间结果都缓存在LRF中. LRF支持写穿透操作,即在1个时钟周期内完成交叉互连网络向密码运算层的数据传输. 一个时钟周期内,单BANK的LRF最多能够为密码运算层提供8个8 bit源数据,密码运算层最多能够向LRF传输5个8 bit运算结果. KSP的存储容量为64×8 bit,支持基变址寻址方式,用于子密钥和中间结果的存储. 32 bit的子密钥存储在4个BANK中KSP



(*a*)数据组织层结构图 (*b*)本地寄存器文件组结构图

图2 本地寄存器文件组结构

的相同地址中,微控制器以一条微指令广播到四个BANK,即可取出子密钥参与运算.

RBCSP 与传统密码处理器最大的区别体现在数据组织上. 例如进行 32 bit 的密码操作,传统的运算过程是将一个 32 bit 数据写入 32 位寄存器的一个地址中,然后从该地址读取数据,进行相应的操作后写回到 32 位寄存器的另一个地址中;而 RBCSP 的运算过程是将 32 bit 的数据分割写入 4 个 BANK 中 LRF 的同一个地址中,然后向四个 LRF 广播一条读数据指令,将此数据读出并进行相应的操作,再将写数据指令广播给 4 个 BANK,将运算结果写入另 4 个 LRF 的一个相同地址. 此外,还可以通过向一个或两个 BANK 发射数据读写指令,完成 8 bit 或 16 bit 数据的读写操作. RBCSP 灵活高效的数据组织方式省去了细粒度运算中利用操作组织数据的琐碎过程,是保证密码运算快速执行的关键,是实现功能单元指令级并行性的重要基础.

2.3　密码运算层

考虑到 RBCSP 处理器资源受限,密码运算层只集成了一组最大运算位宽为 32 bit 的可重构功能单元(Reconfigurable cipher processing Unit,RCU)和一个 128 bit 的比特置换单元. 密码运算层的结构如图 3 所示,RCU 分布在 4 个子块 BANK0,BANK1,BANK2 和 BANK3 中,每个 BANK 内的数据位宽和运算粒度为 8 bit,不同 BANK 间通过共享拼接使用 RCU 完成 16 bit 或 32 bit 的操作. 比特置换单元完成 128 比特内的置换操作和移位操作,同时还完成 BANK 间的数据通信. 单 BANK 内,比特置换最多能读取对应数据组织层 BANK 内四个 LRF 的数据,其余 RCU 最多能读取两个 LRF 的数据. 通过超长指令字(Very Large Instruction Word,VLIW)的控制方式,RCU 能够实现指令级并行,最多支持 5 个 RCU 同时进行密码操作,极大提高了功能单元的利用效率,同时也为软件流水技术的实现提供了重要硬件基础.

RBCSP 中,延迟最大的 RCU 决定着处理器的关键路径. 本文对所有 RCU 都进行了结构优化,有效减少了 RCU 的关键路径,优化后关键路径最长的功能单元是置换单元,其延迟为 1.58 ns. 此外采用操作绑定能够有效减少执行周期数. 由于异或操作与 S 盒替代操作连续进行的频率较高且都不是关键路径,本文对 S 盒进行前/后异或绑定,使得 S 盒单元在单周期内最多能够完成两个操作,有效减少执行周期数.

3　软硬件流水协同技术

分组密码算法大多采用迭代型结构,通过多次调用轮函数实现数据的混乱和扩散,进而达到隐蔽数据的目的. 软件流水技术[6]能够开发轮函数的指令级并行度,加速轮函数的执行效率. 硬件流水线通过划分指令执行的不同阶段,实现多条指令不同阶段的并行执行,能够有效提高吞吐率. 本文将软件流水技术和硬件流水技术相结合,从而大幅度提高密码处理器的运算速度和性能价格比.

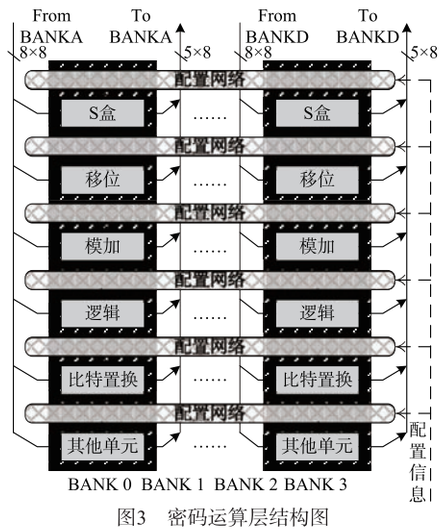


图3　密码运算层结构图

3.1　软件流水研究

轮函数是分组密码算法加解密过程中耗费时间最多的部分,通过挖掘轮函数中不同操作间的指令级并行度能够有效提高轮函数的执行效率. 软件流水技术是一种重组轮函数的技术,通过并行执行轮函数中多个加密迭代,产生一种周期模式的并行调度,使得相邻迭代的加密操作尽可能地重叠执行,来提高功能单元的利用率并加快轮函数的执行速度. 在软件流水中,一个迭代启动于上一迭代结束之前,相邻两个迭代的启动时刻差称为启动间距(Initiation Interval,II).

启动间距 II 是衡量软件流水效率的重要指标,决定了新的轮函数的大小,从而决定了软件流水的效果. II 的下界称为最小启动间隔(Minimum Initiation Interval,MII). MII 的大小由两方面的因素决定:一是操作的资源占用情况,二是循环中操作间的相关限制关系. 它们分别决定一个 II 下界:ResMII 和 RecMII. MII = Max(ResMII,RecMII). 如式(1)、(2)所示:

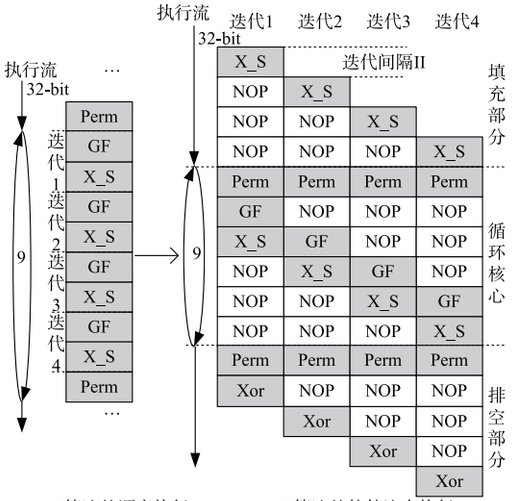
$$\mathrm{ResMII}=\max_{\forall\text{资源类型}r}\frac{r\text{类资源的操时延之和}}{r\text{类资源的总数}} \tag{1}$$

$$\mathrm{RecMII}=\max_{\forall\text{任一回路}c}\frac{\delta(C)}{d(C)} \tag{2}$$

II 必须是整数,如果 MII 是分数,就需要向上取整. MII 是由资源限制的 ResMII 和相关限制的 RecMII 共同决定的,因此在计算展开因子时主要考虑这 2 个因素. 在 RBCSP 中,若以资源限制为主,其中置换单元(Perm)资源是关键资源,由于置换单元的处理位宽是 128 bit,相当于 4 个 32 比特的处理单元,此时 ResMII = 4/4 = 1. 若以相关限制为主,$d(C)$ 是相关限制最严重

的回路上所有相关距离之和,则 $\delta(C)$ 是该回路上所有相关延迟之和,由于 RBCSP 能够将功能单元组成任意的流水线型密码运算链,故 $d(C)$ 是确定的,其值为 1. 故需减小 $\delta(C)$ 的值,最小的值是 1,而 $\delta(C)$ 的值取决于回路上的数据相关性,由硬件流水线结构来确定的,其值的讨论在 3.2 节进行.

AES 算法在 RBCSP 的顺序执行过程如图 4(a)所示,将列混合变换、异或、字节代替变换和行移位变换组成的轮函数映射到 RBCSP,即执行 4 次由运算粒度为 32bit 的有限域乘法(GF)和绑定前异或的 S 盒操作(Xor_Substitution,X_S)组成的迭代及 1 次 128bit 的比特置换操作(Permutation). 由于 RBCSP 能够将 RCU 组织成一条密码运算链,若将迭代内的操作也相应划分为独立的段,每段使用不同的 RCU,由于不同的操作位于不同的段且使用不同的 RCU,使得硬件能够实现不同迭代上多个操作在执行时间上的重叠,实现 AES 算法的软件流水执行,从而有效提高加密效率.



(a)AES算法的顺序执行 (b)AES算法的软件流水执行

图4 AES算法的顺序执行和软件流水执行对比

AES 算法的软件流水执行过程如图 4(b)所示,在填充阶段,每经过 II 间隔启动一轮新的加密迭代去填充软件流水线,由于比特置换操作需要在四次迭代都完成后才能启动,故在前 3 轮迭代 S 盒操作完成后插入 NOP 来填充流水线. 在循环核心阶段,软件流水线以其最大生产能力并行执行四种操作,而在等待周期内均需要插入 NOP. 最高效情况下循环核心段能够在一个时钟周期内遍历所有的操作,即同一时钟周期完成四个迭代的不同操作. 在排空阶段,循环核心段循环执行 9 轮后软件流水线开始“排水”,此时不再启动新的迭代,继续完成尚未完成的迭代. 软件流水把不同加密迭代间的操作交织在一起执行,而单个加密迭代中的操作依然是串行执行的,这样,即保证了加密迭代中数据的相关依赖关系,又提高了指令级并行性.

如图 4 所示,AES 算法在 RBCSP 中顺序执行的加密周期 $Ne=(9\times9\times II+9\times II)=90\times II$,而采用软件流水技术后的加密周期 $Ne=(6\times9\times II+9\times II)=63\times II$. 显然,采用软件流水技术调度执行密码算法可以极大地提高加密效率,相较于顺序执行其加密周期大幅缩短. 此外在 ECB 加密模式下,软件流水技术还可以并行执行相邻分组的加密操作,开发分组并行数,从而提高密码处理性能.

3.2 硬件流水线设计

在 RBCSP 中,核级控制层、数据组织层和密码运算层协同工作,以 SIMD 或 MIMD 的方式共同执行 VLIW 指令来完成密码运算. 指令执行的硬件流水线如图 5 所示.

核级控制层完成硬件流水线的前两栈——取指栈和指令译码分派栈. 在取指栈中,微控制器根据模式选择信息按 SIMD 或 MIMD 的发射方式从 SRAM 中取出一条或两条 VLIW. 在指令译码分派栈中,指令分析单元接收到 VLIW 后,首先进行指令分析,若为配置指令,则将其发射到配置路径进行功能单元的配置;若为执行指令,先将指令进行初步译码,将微控制域指令发送到微控制器的相应部件,同时将数据组织层域和密码运算层域指令分派给相应部件.

数据组织层完成硬件流水线的第三栈和第五栈——取操作数栈和写回栈. 在取操作数栈,对数据组织层域和密码运算层域指令进行完全译码,同时将操作数地址发送到相应 LRF 中读取操作数;此外这一栈还完成了 S 盒外其余功能单元的配置操作. 在写回栈,数据完成运算之后,根据指令将数据写回到 LRF 或 IO 单元中.

密码运算层完成硬件流水线的第四栈——执行栈. 此时 RCU 根据指令完成相应的密码操作. 在执行栈的后半个周期,将 RCU 的结果输入互连开关,根据指令选择下一路径. 若选择路径 d,下一栈进行写回栈;若选择路径 c,则将数据发送到下一 RCU 进行执行栈,即完成了下一条指令的取数同时不进行写回,此时将 RCU 组织成一条流水线型的密码运算链.

由 3.1 节可知,迭代内/间的数据相关性决定着软件流水的效率高低,为解决数据相关性问题,缩短操作延迟,提高流水线效率,本文在硬件流水中采用定向技术减少数据冲突引起的停顿,如图 5 虚线所示的数据回路 c,数据能够在 RCU 间连续运算,有效解决了数据相关性问题. AES 算法在软件流水技术下加密时,若迭代内采用流水线(d),需要在写回之后再进行取数才能进行下一操作,此时 $\delta(C)=3$,即 $II=3$;若数据相关限制严重的执行回路采用流水线(c),则数据能在功能单元间连续运算,此时 $\delta(C)=1$,即 $II=1$.

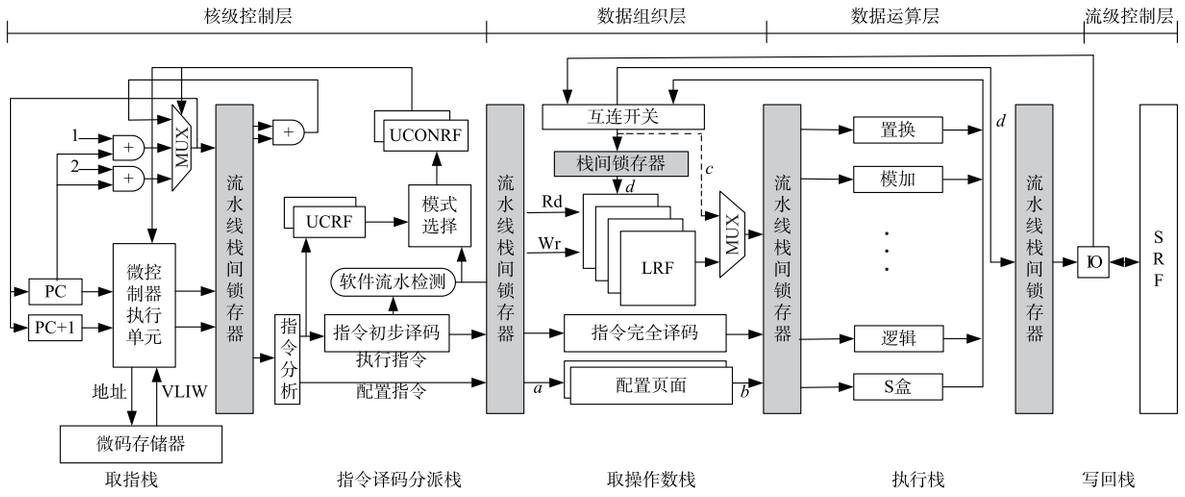


图5　RBCSP的硬件流水线

RBCSP 架构中,软件流水技术与硬件流水线能够协同工作,AES 算法的加密周期 Ne 仅为 63 个时钟周期,有效缩短了加密周期. 图 6 所示为 AES 算法循环核心的软硬件流水协同执行过程,通过开发指令间并行度,能够有效提高功能单元的利用率,使得多个功能单元能够在同一时刻并行处理不同迭代的数据,从而缩短加密时钟周期并提高密码处理性能.

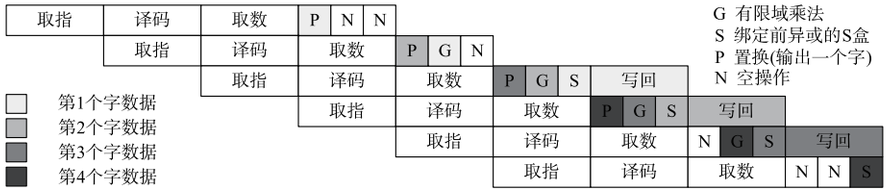


图6　AES算法循环核心的软硬件流水协同执行

4　性能评测

本文采用 Verilog 语言对 RBCSP 进行了描述,并利用综合工具基于65nm CMOS 工艺单元库综合获取了硬件资源信息. 综合结果如表 1 所示,RBCSP 的面积为 0.68mm^2,工作频率可达到 500MHz.

表 1　ASIC 综合结果

约束 (ns)	面积 (μm^2)	等效门数 (万门)	Slack	工作频率 (MHz)
2.0	684194.5	47.51	0.02	500

为全面地评估 RBCSP 的算法适配能力和算法实现性能,本文还进行了 AES、SMS4、IDEA、DES、Camellia 和 RC6 算法在 RBCSP 上的 CBC 和 ECB 映射,并与其他可重构密码处理结构进行了面积、频率、吞吐率和面积能效比的对比,对比情况如表 2 所示. 与其他处理器的性能相比较,RBCSP 具有小面积、高性能的特点,此外还具有最优的面积能效比. 性能评估结果相较于其他可重构密码处理器具有明显优势,在个别性能指标上甚至超过了专用密码处理器.

表 2　性能指标对比结果

结构	发表时间	工艺 (nm)	面积 (mm^2)	频率 (MHz)	映射算法	CBC 吞吐率 (Gbps)	CBC 面积能效比 (Gbps/ mm^2)	ECB 吞吐率 (Gbps)	ECB 面积能效比 (Gbps/ mm^2)
文献 1	2015	65	4.28	400	AES	– –	– –	2.16	0.50
					SMS4	– –	– –	6.30	1.47
					DES	– –	– –	2.72	0.64
					Camellia	– –	– –	3.59	0.84
文献 7	2014	180	13.38	243.9	AES	0.47	0.04	2.80	0.21
					IDEA	0.13	0.01	1.60	0.12
					DES	0.11	0.01	0.91	0.07

续表

结构	发表时间	工艺（nm）	面积（mm^2）	频率（MHz）	映射算法	CBC 吞吐率（Gbps）	CBC 面积能效比（Gbps/ mm^2）	ECB 吞吐率（Gbps）	ECB 面积能效比（Gbps/ mm^2）
文献 8	2013	65	6.63	1210	AES	1.02	0.15	– –	– –
文献 9	2015	65	50	100	AES	0.19	0.004	2.33	0.05
文献 10	2008	130	5.3	250	AES RC6	0.41 0.13	0.03 0.02	– – – –	– – – –
文献 11	2009	180	14.9	180	AES IDEA DES RC6	0.79 0.10 0.12 0.19	0.05 0.007 0.008 0.01	0.79 0.40 0.46 0.38	0.05 0.03 0.03 0.03
文献 12	2014	130	8.75	238	AES IDEA DES	0.39 – – – –	0.04 – – – –	2.87 1.46 1.44	0.33 0.17 0.16
本文	2016	65	0.68	500	AES SMS4 IDEA DES Camellia RC6	1.00 0.39 0.54 0.38 0.44 0.44	1.47 0.58 0.80 0.56 0.64 0.64	1.51 0.66 1.78 0.95 0.72 0.78	2.21 0.98 2.61 1.40 1.06 1.11

从上表可以看出，在 CBC 加密模式下 RBCSP 在进行密码算法时吞吐率在 0.40 Gbps 左右，面积能效比在 0.60 Gbps/mm^2 左右，其中进行 AES 算法时性能最高，吞吐率可达到 1.00 Gbps，面积能效比高达 1.47 Gbps/mm^2. 与其他处理器结构相比较，本文提出的 RBCSP 具有最高的 CBC 加密性能和最优的面积能效比，CBC 加密吞吐率约为其他结构的 2 ~ 4 倍，面积能效比约为其他结构的 10 ~ 100 倍. 在 ECB 加密模式下，RBCSP 在进行密码算法时吞吐率在 0.80 Gbps 左右，面积能效比在 1.00 Gbps/mm^2 左右，其中进行 IDEA 算法时性能最高，吞吐率可达到 1.78 Gbps，面积能效比高达 2.61 Gbps/mm^2. 与其他处理器结构相比较，本文提出的 RBCSP 具有较高的 CBC 加密性能和最优的面积能效比，ECB 加密吞吐率与其他结构差距较小，面积能效比约为其他结构的 10 ~ 30 倍.

5 结束语

本文提出了基于层次结构的可重构密码流处理器 RBCSP. RBCSP 在进行密码算法映射时有两个主要的优势：(1)能够利用软件流水技术和硬件流水技术协同开发指令级并行性，从而减小加密周期、提高功能单元利用率和开发分组并行数；(2)在进行 32 bit 内运算粒度操作时，能够避免数据组织时间，还可以并行利用多 BANK 资源开发分组并行数. 实验结果证明，该架构具有最优的面积能效比，在个别性能指标上甚至超过了专用密码处理器，符合移动终端等资源受限应用场景需求. 由于 RBCSP 未集成支持序列密码和公钥密码算法的功能单元，导致其无法进行这两类算法，下一步可有选择地将相关功能单元集成到 RBCSP 内，增强其密码运算功能，使其更加实用化.

参考文献

[1] WANG Bo, LIU Leibo. A flexible and energy-efficient reconfigurable architecture for symmetric cipher processing [A]. Proceedings of IEEE International Symposium on Circuits and Systems [C]. New York: IEEE, 2015: 1182 – 1185.

[2] GOKHAN S, DEREK C. Cryptoraptor: high throughput reconfigurable cryptographic processor [A]. Proceedings of IEEE/ACM International Conference on Computer-Aided Design [C]. New York: ACM, 2014. 154 – 161.

[3] MICHAEL G, LILIAN B, GUY G, et al. Design and implementation of a muli-core crypto-processor for software defined radios [A]. Proceedings of International Symposium on Reconfigurable Computing Architectures, Tools and Applications [C]. New York: IEEE, 2011. 29 – 40.

[4] 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,2009,31(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)

[5] HUANG Wei, HAN Jun, WANG Shuai. A low-complexity heterogeneous multi-core platform for security SoC[A]. Proceedings of IEEE Asian Solid-State Circuits Conference[C]. New York: IEEE, 2010. 1 – 4.

[6] IQBAL N, SIDDIQUE M A, HENKEL J. RMOT: recursion in model order for task execution time estimation in a software pipeline[A]. Proceedings of IEEE Design, Automation & Test in Europe Conference & Exhibition Dresden[C]. New York: IEEE, 2010. 953 – 956.

[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, 2014,36(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, 2014, 36(12): 3027 – 3034. (in Chinese)

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

[9] 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(9):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(9): 1 – 5. (in Chinese)

[10] DIMITRIS T, ALEXANDROS S, DIONISIS P. CCproc: an efficient cryptography coprocessor[A]. Proceedings of 16th IFIP/IEEE International Conference on Very Large Scale Integration[C]. New York: IEEE, 2008. 160 – 163.

[11] 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)

[12] 李校南,王雪瑞,戴紫彬,等. 可重构分簇式分组密码处理架构[J]. 计算机应用与软件, 2014, 31(1): 315 – 318.
LI Xiao-nan, WANG Xue-rui, DAI Zi-bin, et al. Reconfigurable clustered block cipher processing architecture[J]. Computer Applications and Software, 2014, 31(1): 315 – 318. (in Chinese)

作者简介

王寿成(通信作者)　男,1992 年生于甘肃金昌. 解放军信息工程大学硕士研究生. 从事可重构计算、信息安全方面的有关研究.
E-mail: jeremy_419@163.com

严迎建　男,1973 年生于河南扶沟. 教授、硕士生导师. 主要从事芯片安全防护、专用芯片设计和密码芯片能量攻击等方面的研究工作.