PVHArray:一种流水可伸缩的层次化可重构密码逻辑阵列结构

杜怡然,李 伟,戴紫彬
(解放军信息工程大学,河南郑州 450000)

摘 要: 针对密码算法的高效能实现问题,该文提出了一种基于数据流的粗粒度可重构密码逻辑阵列结构PVHArray.通过研究密码算法运算及控制结构特征,基于可重构阵列结构设计方法,提出了以流水可伸缩的粗粒度可重构运算单元、层次化互连网络和面向周期级的分布式控制网络为主体的粗粒度可重构密码逻辑阵列结构及其参数化模型.为了提升可重构密码逻辑阵列的算法实现效能,该文结合密码算法映射结果,确定模型参数,构建了规模为4×4的高效能PVHArray结构.基于55nm CMOS工艺进行流片验证,芯片面积为12.25mm^2,同时,针对该阵列芯片进行密码算法映射.实验结果表明,该文提出高效能PVHArray结构能够有效支持分组、序列以及杂凑密码算法的映射,在密文分组链接(CBC)模式下,相较于可重构密码逻辑阵列REMUS_LPP结构,其单位面积性能提升了约12.9%,单位功耗性能提升了约13.9%.

关键词: 流水可伸缩;层次化;周期级;高效能;阵列
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2020)04-0781-09
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.04.020

PVHArray:A Pipeline Variable Hierarchical Reconfigurable Cryptographic Logic Array Structure

DU Yi-ran,LI Wei,DAI Zi-bin
(*Zhengzhou Institute of Information Science and Technology*,*Zhengzhou*,*Henan* 450000,*China*)

Abstract: Aiming at the high energy-efficiency implementation of cryptographic algorithm, this paper proposed a coarse-grained reconfigurable cryptographic logic array structure named PVHArray. Based on the research of cryptographic algorithm operation and control structure features, adopted the reconfigurable array structure design method, this paper proposed the coarse-grained reconfigurable cryptographic logic array structure and its parametric model, which is mainly composed of pipeline variable coarse-grained reconfigurable computing units, hierarchical interconnected network and periodic-oriented distributed control network. In order to improve the energy-efficiency of the reconfigurable cryptographic logic array, this paper combined the cryptographic algorithm mapping results to determine the model parameters, and constructed a high energy-efficiency PVHArray structure with a size of 4×4. The chip area of PVHArray is 12.25mm^2 based on 55nm CMOS technology, and at the same time, cryptographic algorithm mapping is performed for PVHArray. The experimental results show that the proposed high-efficiency PVHArray structure can effectively support the mapping of block, stream and hash cipher algorithm. In the cipher block chaining (CBC) mode, compared with state-of-the-art reconfigurable cryptographic logic array REMUS_LPP, the performance per unit area has increased by 12.9% and the performance per unit power has increased by 13.9%.

Key words: pipeline variable;hierarchical;periodic-oriented;high-efficiency;array

1 引言

可重构阵列是一种基于数据流的高效运算结构,它结合了专用集成电路高性能与通用处理器高灵活性的特点,针对算法中的循环结构进行优化,降低控制开销,能有效实现对算法的加速.

收稿日期:2019-03-03;修回日期:2019-07-31;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61404175)

随着通信技术的不断发展,信息安全成为人们关注的重点,作为保障信息安全的重要手段,密码算法能有效防范对信息的窃取与篡改,确保信息传输的安全、可靠.密码算法作为计算密集型应用的典型代表,能充分发挥可重构阵列的结构优势,完成密码算法的高性能实现,因此,针对密码算法设计的可重构密码逻辑阵列成为研究的热点.

CryptoManiac[1]是一种以处理器为主体的密码运算结构,能够支持多种密码算法,但由于其结构是基于AES算法进行了定制优化,因此其它算法的实现性能不高;Cryptonite[2]与CryptoManiac结构类似,均属于指令流驱动的处理器结构,以ALU及LUT作为主要计算资源实现密码算法映射,但受制于指令流体系结构,其算法实现性能不高;COBRA[3]是一种采用VLIW结构的阵列处理器,面向分组密码算法进行设计,以指令流方式进行驱动,但受所研究的分组密码算法集合限制,其内部可重构密码处理元素(Reconfigurable Cryptographic Elements,RCE)中的各类运算模块以固定方式连接,算法映射受到一定制约;Anole[4]是一种高效的动态可重构阵列结构,通过采用分布式控制网络(Distributed Control Network,DCN)实现对阵列的高效精细控制,同时,Anole支持多算法并行映射,提升算法的实现性能以及阵列映射密度,并基于FPGA进行验证;Cryptoraptor[5]以高性能为目标进行设计,通过尽可能缩减运算单元提升系统工作频率,同时,缩减运算单元造成了阵列部分功能缺失,制约了密码算法的映射.上述研究成果主要基于处理器及可重构阵列两种方式实现,根据对文献[1,2]的研究可以得到,处理器结构受指令流"取指—译码"过程的制约,其性能难以实现飞跃式提升,可重构阵列结构的数据流特征使得其天然具有高的算法实现性能.对于可重构阵列结构,其算法实现性能与其规模密切相关,因此不能单纯关注算法实现性能,而应对算法实现进行全面考量.

针对这一问题,本文提出了一种高效能的粗粒度可重构密码逻辑阵列结构PVHArray.通过对密码算法特征的深入研究,构建了流水可伸缩的粗粒度可重构运算单元,同时,采用层次化互连网络有效解决了阵列的灵活性与可扩展性,并通过面向周期级的分布式控制网络,实现了对粗粒度可重构密码逻辑阵列的精细控制.

2 粗粒度可重构密码逻辑阵列研究

粗粒度可重构密码逻辑阵列是一种面向密码运算的高效数据流处理结构,它是粗粒度可重构阵列在密码应用方向上的拓展,因此其设计应遵循粗粒度可重构阵列的设计方法.本节围绕粗粒度可重构密码逻辑阵列可重构运算单元、拓扑互连网络以及控制机制三个方面展开研究.

2.1 流水可伸缩的粗粒度可重构运算单元

可重构运算单元是密码算法实现的基础,应依照密码算法特征进行设计,主要包括可重构运算单元支持的运算类型以及处理粒度.采用统计学方法对现有信息安全协议及密码算法特征进行统计分析,可以得到密码算法特征如下[6~8]:密码算法中基本运算类型多样,包含了诸如与、或、非、异或、移位、置换、S盒替换、算数加/减法、模加/减法、算数乘法、模乘、有限域乘法、非线性布尔函数、反馈移位寄存器等基本运算类型,同时,密码算法中大多为无符号整数运算,不存在浮点及定点类型;同一运算类型运算模式多样,密码算法中各运算类型均存在不止一种的运算模式,不同运算模式使密码算法更加多样化;基本运算处理粒度多样,密码算法中的基本运算处理粒度主要包含了基于字节、半字、字、双字及四字等粒度,与基本运算的运算模式类似,不同的处理粒度在运算方法上并无本质区别,但采用不同的处理粒度将对硬件资源及互连资源造成影响,因此,合理规划基本运算单元的处理粒度至关重要.

综合考虑可重构密码逻辑阵列硬件资源开销及其利用率,以硬件结构相似及实现原理相似为划分原则,本文构建了5种可重构运算单元[9~11],分别为:算数类可重构运算单元(FU_AL)、置换类可重构运算单元(FU_BP)、逻辑类可重构运算单元(FU_LG)、非线性类可重构运算单元(FU_NF)以及查表类可重构运算单元(FU_LT),实现了对基于可重构密码逻辑阵列密码算法映射的支持.

采用细粒度(通常小于4比特)可重构运算单元实现大位宽运算时,需对各可重构运算单元进行级联,提升了单元间互连的复杂度;采用粗粒度(通常大于16比特)可重构运算单元实现小位宽运算时,仅占用了可重构运算单元中的部分硬件资源,造成剩余硬件资源的浪费.因此,可重构运算单元的粒度直接影响了可重构密码逻辑阵列的运算资源的利用率以及互连资源的复杂度,需要针对密码算法特征进行设计,从而达到单元间互连复杂度与单元利用率间的平衡.通过对密码算法进行分析,大部分密码算法以32比特粒度进行运算,因此本文将可重构运算单元的粒度定义为32比特,构建了面向密码运算的粗粒度可重构运算单元.

粗粒度可重构密码逻辑阵列的数据流运算特征使算法的流水映射成为可能,现阶段,面向粗粒度可重构阵列的流水寄存器设计较为简单,常采用固定方式寄存,即可重构运算单元的运算结果通过一级寄存后输出至下一个可重构运算单元.采用这一方式,当粗粒度可重构阵列结构确定后,其最大工作时钟频率即被确定,若流水运算中各可重构运算单元关键路径延迟差异较大,则算法映射性能变差,无法发挥粗粒度可重构

阵列的优势.

针对这一问题,本文提出了一种可配置的流水寄存器结构,通过配置寄存器的寄存与否,平衡流水线中各级长度,从而进一步提升算法的实现性能. 以可重构运算单元的一般结构为例进行研究,图 1(*a*)为典型粗粒度可重构阵列流水寄存器结构,各可重构运算单元的输出均通过一级流水寄存器寄存后输出至输出网络;图 1(*b*)为本文提出的可配置流水寄存器结构,通过增加一级输出配置电路,实现对可重构运算单元输出数据的可选择寄存.

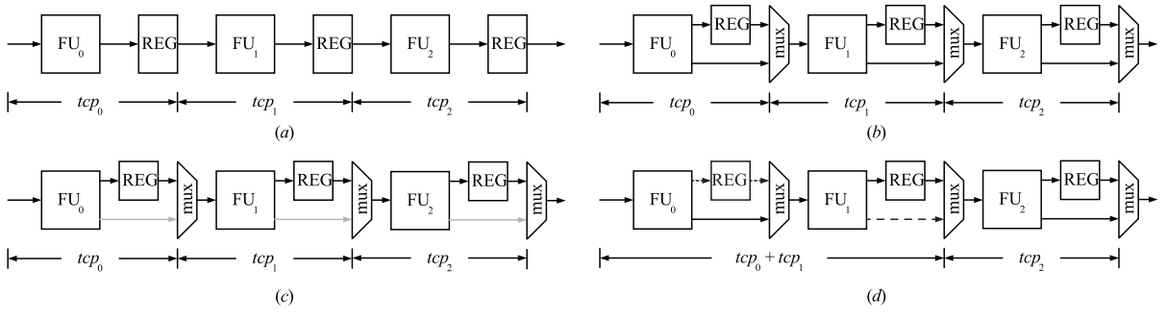

图1　两种粗粒度可重构阵列流水寄存器结构

假设 FU_0、FU_1及 FU_2的关键路径延迟分别为 tcp_0、tcp_1及 tcp_2,则对于如图 1(*a*)所示运算路径,其关键路径延迟为 $\max(tcp_0, tcp_1, tcp_2)$;当图 1(*b*)采用全寄存模式时,其算法路径如图 1(*c*)所示,等价于图 1(*a*)中的算法路径,因此其关键路径延迟仍为 $\max(tcp_0, tcp_1, tcp_2)$;当图 1(*b*)采用部分寄存模式时,其算法路径如图 1(*d*)所示,FU_0的输出不进行寄存直接输出至 FU_1,因此其关键路径延迟为 $\max(tcp_0 + tcp_1, tcp_2)$. 当 $tcp_0 + tcp_1 \leqslant tcp_2$时,有 $\max(tcp_0 + tcp_1, tcp_2) = \max(tcp_0, tcp_1, tcp_2)$.

在算法实现性能方面,常采用吞吐率作为其性能评价的重要指标. 算法吞吐率反比于算法执行周期数与系统最大路径延迟之积. 对于图 1(*b*)结构,当采用全寄存方式时则等价于图 1(*a*)结构;当采用部分寄存方式时,其算法执行周期数减少,系统最大路径延迟增加或者保持不变. 依据算法映射所对应的可重构运算单元类型对流水寄存器进行相应配置,在最差的情况下可配置为全寄存模式,使算法映射性能与固定寄存流水线的算法映射性能相当. 综上所述,采用图 1(*b*)结构可以获得不小于图 1(*a*)结构的算法吞吐率.

2.2　层次化互连网络结构

粗粒度可重构密码逻辑阵列丰富的运算资源为其高性能计算的实现提供了基础,然而,相较于运算资源,粗粒度可重构密码逻辑阵列的互连资源则较为贫乏,往往成为算法映射及性能实现的瓶颈. 针对这一问题,本节对粗粒度可重构密码逻辑阵列的拓扑互连结构展开研究.

良好的可扩展性与灵活性是粗粒度可重构密码逻辑阵列的重要特征,其中,规则的拓扑互连结构是实现粗粒度可重构密码逻辑阵列可拓展性的关键,与此同时,规则的拓扑互连结构能有效降低后端布局布线的风险及难度,提升芯片的可靠性.

Mesh 互连结构以二维网格方式实现对粗粒度可重构运算单元的互连,若粗粒度可重构密码逻辑阵列中共包含 n 种处理位宽为 m 的可重构密码运算单元 $FU_0 \sim FU_{n-1}$,则基于 Mesh 的粗粒度可重构密码逻辑阵列可表示为如图 2 所示结构.

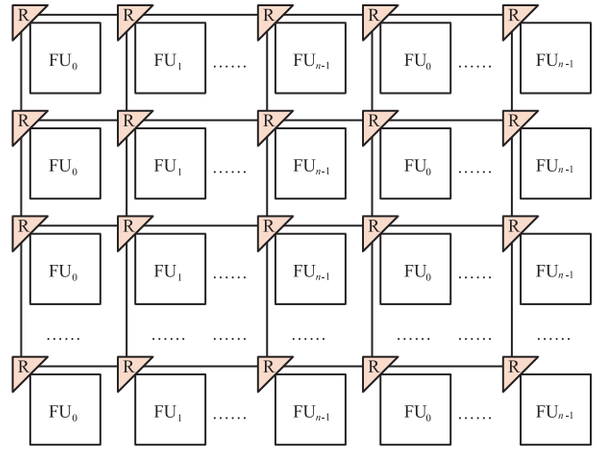

图2　基于Mesh结构的粗粒度可重构密码逻辑阵列

图 2 中“R”表示数据路由模块,负责各 FU 间数据的交互. 一般的,数据路由模块主要以以下两种方式实现:(1)FPGA 结构中的连接器;(2)片上网络互连结构中的路由节点. 其中,连接器的实现方式主要通过构建双向数据选择器进行实现,传输效率较高但缺乏容错机制;路由节点的实现方式主要通过构建较为复杂的路由缓存结构,并采用特定路由算法实现对数据的传输,数据传输正确率高但硬件资源消耗较大且路由过程中存在时钟周期损耗,降低了算法实现性能.

考虑到密码运算中算子间交互频繁,因此采用路

由节点的实现方式将严重制约粗粒度可重构密码逻辑阵列的算法实现性能. 同时,路由缓存结构对密码算法的安全性造成一定威胁,使攻击者能够针对路由节点发起攻击,从而获得密码运算中的关键信息. 综上所述,本文采用连接器结构实现各 FU 间数据的交互.

$FU_0 \sim FU_{n-1}$分别代表不同可重构密码运算单元,由于密码算法中使用的运算类型及运算次序不定,因此采用图 2 所示的互连拓扑结构极易造成互连资源不足,从而导致密码算法映射失败. Crossbar 网络是一种基于数据选择器实现的全互连结构,能够实现任意方式的数据互连,是一种最灵活的互连结构. 然而,Crossbar 互连结构所消耗的硬件资源随其连接的节点数目呈平方级数增长,因此采用 Crossbar 网络实现粗粒度可重构密码逻辑阵列中全部可重构运算单元的互连是不可行的. 基于以上分析,本文构建了一种如图 3 所示的层次化互连网络结构,其中 CB(Connect Box)、SB(Switch Box)为前文所述连接器结构,PE(Processing Element)为包含 n 个可重构密码运算单元的集合.

粗粒度可重构密码逻辑阵列的第一层互连网络为面向 PE 的 Mesh 互连网络结构,第二层互连网络为面向 FU 的 Crossbar 互连网络结构. 采用层次化的互连网络结构能有效克服单一网络结构的缺陷,使粗粒度可重构密码逻辑阵列具有良好可扩展性的同时兼顾可重构密码运算单元互连的灵活性,确保密码算法的成功映射.

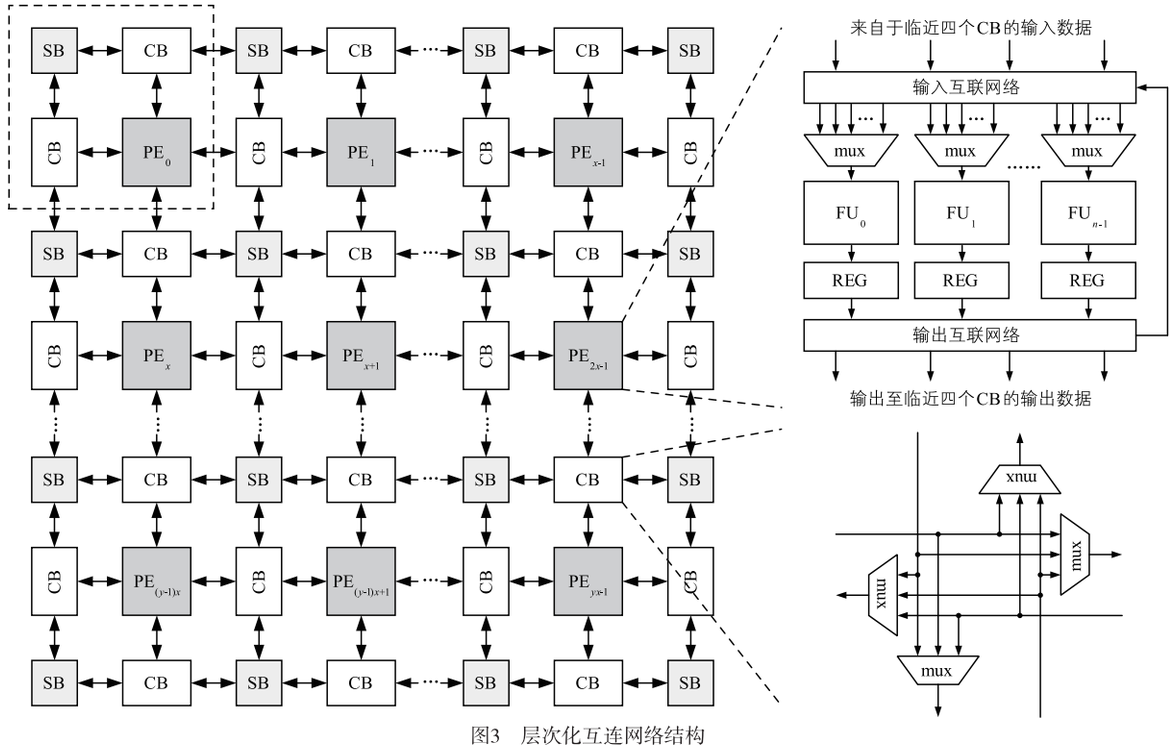

图3 层次化互连网络结构

2.3 面向周期级的分布式控制网络

粗粒度可重构运算单元是密码算法映射的载体,而粗粒度可重构密码逻辑阵列中的控制结构是确保密码算法正确映射的关键. 对于密码算法,其运算过程具有严格的时序特征,控制网络主要完成寄存器使能信号的产生、配置页面的切换以及关键标志信号的产生,当密码算法类型被确定后,上述控制信号也随之被确定. 因此,控制网络以周期级进行精细控制.

对于粗粒度可重构密码逻辑阵列,其可重构运算单元以层次化互连网络连接,呈分布式排列. 若采用集中式控制则会造成状态信号过多、状态跳转过于复杂的情况. 同时,集中式的控制方式制约了粗粒度可重构密码逻辑阵列的可扩展性,因此,本文采用分布式控制网络结构,构建了控制网络模块(Control Element,CE),以实现对各 PE 的精细控制.

增大粗粒度可重构运算单元的数目,有利于提升密码算法映射的流水深度,从而提升密码算法的映射性能. 因此,应尽可能降低控制网络结构的硬件资源开销,从而使粗粒度可重构运算单元占有更多的硬件资源. 基于以上原因,本文提出了一种面向周期级的分布式控制结构,并通过级联以传递各分布式控制结构所产生的控制信号,实现了对密码算法映射的控制. 其中,面向周期级的分布式控制结构如图 4 所示,主要包括计数比较模块、布尔运算模块以及可旁路寄存器模块.

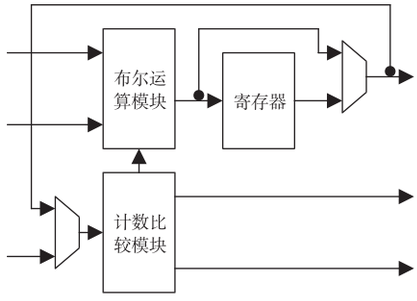

图4　面向周期级的分布式控制结构

(1)计数比较模块

计数比较模块采用可配置计数器和比较器实现,其计数方式与溢出值可配置,负责实现控制中的计数及比较操作,从而灵活的生成控制信号.

通过对密码算法控制流结构的研究,密码算法控制流主要包括计数、比较,用于实现对算法运算阶段的切换. 为了提升控制的灵活性,本文所设计的级联计数模块中计数方式包括连续计数与触发计数两种,连续计数在获得计数起始信号后连续计数至溢出,主要用于完成控制逻辑中的加法及乘法操作;触发计数在获得一次计数信号后进行一次计数,当计数信号无效时不进行计数,主要用于完成条件计数功能. 同时,各 CE 内部的计数比较模块可采用级联的方式,构成控制信号传递链,以实现算法并行部分的同步控制.

(2)布尔运算模块

布尔运算模块主要用于实现控制网络中的简单布尔函数操作,采用查找表的方式实现. 对于 n 输入的查找表,能够实现 2^{2^n} 种不同函数,由于控制网络中所需的布尔函数较少,因此采用 2 输入查找表进行控制网络设计,以降低控制网络的硬件资源消耗.

(3)可旁路寄存器模块

控制网络中的可旁路寄存器主要用于平衡数据流与控制流的周期,以实现更精确的周期控制. 同时,在控制流中可旁路寄存器能够替代使用 1 比特计数器计数的场景,从而节省了计数器资源消耗.

根据粗粒度可重构密码逻辑阵列控制需要,图 4 所示的面向周期级的分布式控制结构能够实现以下六种基本控制功能,分别为:(a)带溢出值计数;(b)两输入布尔函数;(c)布尔运算驱动计数;(d)计数溢出值作为布尔运算参数;(e)带溢出值与比较值的计数器;(f)计数器与布尔运算独立使用.

综上所述,本文设计并实现了一种面向周期级的分布式控制网络结构,以轻量级硬件结构降低阵列整体硬件资源开销,并能够实现精确的周期级控制.

2.4　高效能 PVHArray 结构

流水可伸缩的粗粒度可重构运算单元、层次化互连网络以及面向周期级的分布式控制网络共同构成了 PVHArray(Pipeline Variable Hierarchical Reconfigurable Cryptographic Logic Array)的整体结构. 粗粒度可重构密码逻辑阵列的数据流运算特征使得密码算法能够进行流水展开映射,算法的流水展开级数与粗粒度可重构密码逻辑阵列规模呈正相关. 与此同时,粗粒度可重构密码逻辑阵列的效能也随之改变. 因此,本节首先根据前文的研究成果构建了粗粒度可重构密码逻辑阵列的参数化模型,并依据密码算法结构特征,设计并实现了高效能的 PVHArray 结构.

假设粗粒度可重构密码逻辑阵列中 PE 以 m 行 n 列形式展开,同时,PE 内部的各 FU 所占的比例分别为 x_0、x_1、x_2、x_3、x_4,则粗粒度可重构密码逻辑阵列可以表示为 PVHArray(m,n,x_0,x_1,x_2,x_3,x_4).

对于不同密码算法,其算法内部的算子类型及先后次序存在差异,同时对于密码算法集合,各运算类型的使用频次不同,因此笼统的采用等比例设置各类型可重构运算单元将造成硬件资源映射不均衡、部分可重构运算单元利用率低等问题. 针对这一问题,对密码算法中各类算子的统计学特征展开研究,构建了 FU 的统计学模型,通过对密码算法集合的统计及模型拟合,确定参数 x_0、x_1、x_2、x_3、x_4 取值. 粗粒度可重构密码逻辑阵列可重构运算单元统计模型如式(1):

$$\begin{aligned} & x_0 : x_1 : x_2 : x_3 : x_4 \\ & = \sum_{\text{algroithm}} cnt_{\text{FU\_AL}} : \sum_{\text{algroithm}} cnt_{\text{FU\_BP}} : \\ & \quad \sum_{\text{algroithm}} cnt_{\text{FU\_LG}} : \sum_{\text{algroithm}} cnt_{\text{FU\_NF}} : \sum_{\text{algroithm}} cnt_{\text{FU\_LT}} \end{aligned} \tag{1}$$

其中 $x_0 \sim x_4$ 分别代表 5 种可重构运算单元的比例,依据典型密码算法的拟合结果,可以得到 5 种可重构运算单元的统计学比例为 2∶1∶5∶1∶1. 其中逻辑类可重构运算单元所占比例明显高于其它类型可重构运算单元,通过对密码算法的进一步分析可得,逻辑类运算单元大多用于实现算法中的异或操作,考虑到可重构运算单元的资源利用率以及密码算法的映射密度,在算数类可重构运算单元、置换类可重构运算单元、非线性类可重构运算单元以及查表类可重构运算单元的输出部分增加后异或结构. 因此,剔除样本空间中的异或操作对典型密码算法进行再拟合,则 5 种可重构运算单元的统计学比例为 2∶1∶1∶1∶1,依照该比例对 PE 中的各类 FU 进行设置.

增大粗粒度可重构密码逻辑阵列的规模势必带来其面积及功耗的增加,假设规模为 $m \times n$ 的粗粒度可重构密码逻辑阵列面积为 $S(m,n)$,系统功耗为 $P(m,n)$. 以分组密码算法为例,分组密码算法常采用分组间并行的

方式提升算法的实现性能,对于分组长度为 k、算法位宽为 W 的分组密码算法,其最大组间并行度为$\frac{W}{k}$,因此当粗粒度可重构密码逻辑阵列的列数 $n \geqslant \frac{W}{k}$时,无法通过提升阵列横向上的并行性提升密码算法实现性能.

分组密码算法常采用轮运算循环迭代的方式实现,因此粗粒度可重构密码逻辑阵列纵向上的规模 m 直接影响了密码算法映射的流水深度 R. 依据文献[12]可知,分组密码算法以单轮轮运算作为整体进行流水展开,其算法实现性能最大. 假设分组密码算法共包含 N 轮轮运算,同时,实现一级轮运算共需要消耗 s 个 PE,因此,在部分流水情况下,实现 Q 个 W 比特数据加解密所能得到的算法总执行性能 TET(Total Execute Throughput)可以表示为:

$$\mathrm{TET}=\frac{W\times Q}{\left[\left\lfloor\frac{Q}{R}\right\rfloor\cdot(N+R-1)+\left(Q-\left\lfloor\frac{Q}{R}\right\rfloor\times R\right)\cdot\left(N+Q-\left\lfloor\frac{Q}{R}\right\rfloor\times R-1\right)\right]\times t_{\max}} \tag{2}$$

其中 $R=\left\lfloor\frac{m\times n}{s}\right\rfloor$,为分组密码算法在粗粒度可重构密码逻辑阵列中所能映射的最大流水深度,$t_{\max}$ 为算法映射时的最大关键路径延迟.

综上所述,为了更加合理的评价粗粒度可重构密码逻辑阵列结构,本文构建了以单位面积实现性能和单位功耗实现性能为指标的评价体系,如式(3)所定义:

$$\Delta S=\frac{S(m,n)}{\mathrm{TET}}$$
$$\Delta P=\frac{P(m,n)}{\mathrm{TET}} \tag{3}$$

对于不同的密码算法,其算法特征参数 $W,R,N,k,s,t_{\max}$ 均不相同. 为了构建统一的高效能 PVHArray 结构,结合典型密码算法,对算法特征参数范围进行设置,同时,采用 Design Compiler 综合工具,基于 55nm CMOS 工艺库对设计进行综合,获取粗粒度可重构密码逻辑阵列的面积及功耗参数,结果如图 5 所示.

可以得到,对于 PVHArray 的吞吐率参数仿真结果,PVHArray 的吞吐率随其规模的增大而增大,当 $m\times n$ 小于 4 时,受阵列规模影响,算法实现性能较低;当 $m\times n$ 等于 4 时,算法能一次展开为 128 比特并行结构,因此其算法实现性能增长迅速;当 $m\times n$ 等于 9 及 16 时,算法的实现性能分别又出现较大提升;当 $m\times n$ 大于 16 时,算法实现性能增长不明显. 对于 PVHArray 阵列面积,由于其采用同构的 PE 构成,因此其面积近似为线性增长,图 5 中虚线表示 PVHArray 的单位面积吞吐率,当 $m\times n$ 等于 16 时取得最大值,此时 PVHArray 的单位面积吞吐率最大. 对于 PVHArray 的功耗参数仿真结果,其功耗正比于所包含的 PE 数目,因此表现为近似的线性增长,虚线表示 PVHArray 的单位功耗吞吐率,当 $m\times n$ 等于 16 时取得最大值,此时 PVHArray 的单位功耗吞吐率最大.

综上所述,当 $m\times n$ 为 16 时,粗粒度可重构密码逻辑阵列取得最佳效能. 考虑到高效能 PVHArray 结构的规整性以及其在密码算法分组间的并行特性,因此将

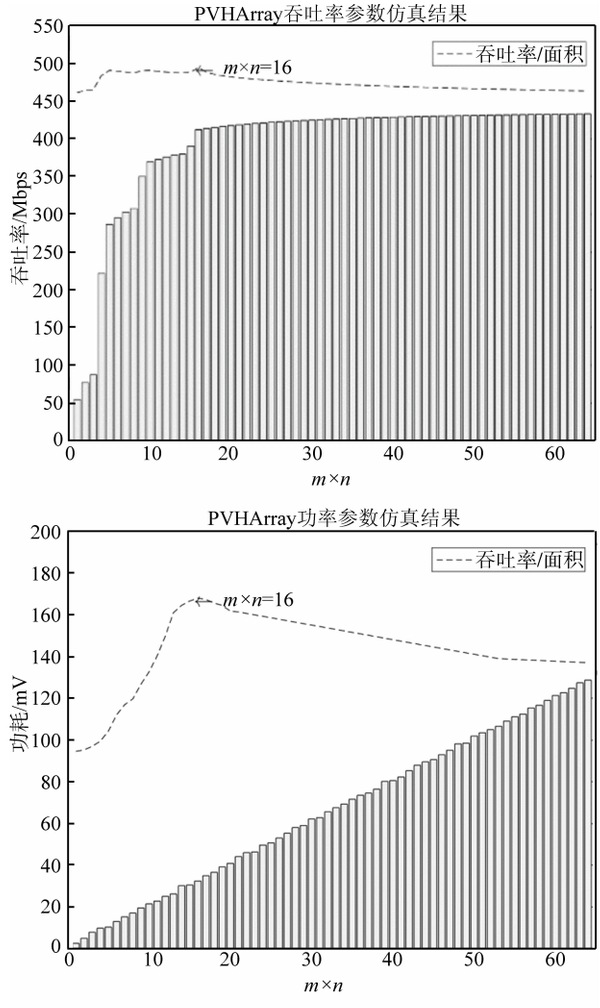

图5 粗粒度可重构密码逻辑阵列结构评价体系

高效能 PVHArray 在横向上展开为 4 列,在纵向上展开为 4 行,构建了如图 6 所示的高效能 PVHArray 结构.

3 实验与验证

基于 55nm CMOS 工艺对本文所设计的高效能 PVHArray 进行流片,芯片面积为 $3.5\times3.5\mathrm{mm}^2$. 同时,搭建如图 7 所示的高效能 PVHArray 芯片验证平台,并

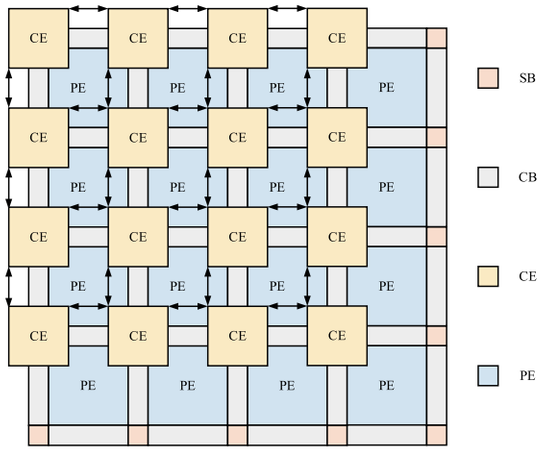

图6　高效能PVHArray结构

对典型密码算法进行映射,结果如表 1 所示.

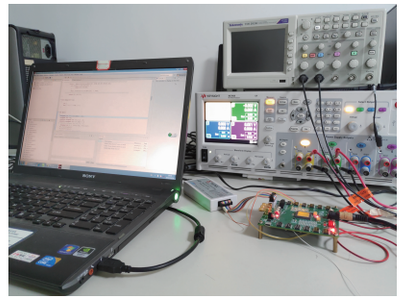

图7　高效能PVHArray芯片验证平台

表 1　典型密码算法映射性能

算法名称		时钟频率/Mhz	吞吐率/Mbps	阵列面积/mm^2	功耗/mW
分组密码算法	AES-128	110	440	12. 25	28
	DES	130	245		32
	SM4	100	200		36
	IDEA	110	176		38
序列密码算法	RC4	120	120		39
	ZUC	125	125		40
杂凑密码算法	SHA256	120	384		30

考虑到密码算法的并行流水映射性能(ECB 模式)并不能直接反映粗粒度可重构密码逻辑阵列的优劣,同时,在密码应用中也常采用 CBC 模式提升密码运算的安全性,因此表 1 中的算法映射结果均基于 CBC 模式实现,即单任务的密码算法吞吐率.

为了进一步验证本文提出的 PVHArray 阵列结构的效能,基于不同硬件平台对上述四种算法进行映射实现. 同时,为了增加实验结果的可信程度,本文选择经流片验证后的密码处理结构进行对比.

表 2 为各密码算法在不同硬件平台下的单位面积性能. 同样的,表 3 为各密码算法在不同硬件平台下的单位功耗性能.

表 2　不同密码运算结构单位面积性能对比(Mbps/mm^2)

运算结构	工艺/nm	面积/mm^2	AES-128	DES	SM4	IDEA	RC4	ZUC	SHA256
CryptoManiac[1]	250	1. 93	240. 41	74. 61	–	103. 63	165. 8	–	–
SophSEC[13]	130	25	22. 56	–	8. 48	–	–	–	–
Celator[14]	180	0. 1	460	260	–	–	–	–	–
PipeRench[15]	250	100	–	–	–	1. 27	–	–	–
REMUS_LPP[16]	65	44. 85 *	63. 32	28. 54	–	–	–	–	–
PVHArray	55	12. 25	39. 52	20	16. 33	14. 37	9. 8	10. 2	31. 35

* 文献[16]中标注的面积为算法核心单元面积,考虑到性能对比到公平性,此处采用文献中的芯片面积进行计算

表 3　不同密码运算结构单位功耗性能对比(Mbps/mW)

运算结构	工艺/nm	功耗/mW	AES-128	DES	SM4	IDEA	RC4	ZUC	SHA256
CryptoManiac[1]	250	606. 37	0. 77	0. 24	–	0. 33	0. 53	–	–
SophSEC[13]	130	325	1. 74	–	0. 65	–	–	–	–
Celator[14]	180	–	–	–	–	–	–	–	–
PipeRench[15]	250	–	–	–	–	–	–	–	–
REMUS_LPP[16]	65	103	27. 57	12. 43	–	–	–	–	–
PVHArray	55	35 *	15. 71	7. 66	5. 56	4. 63	3. 08	3. 13	12. 8

* 对于不同的密码算法,功耗略有差别,该值为标称典型功耗值

经对比可得,采用阵列结构实现的密码算法其单位面积性能及单位功耗性能均优于处理器结构,这是

由于阵列结构基于数据流结构设计并针对密码算法进行了单元优化,从而得到了更佳的运算效能. 同时,由表 2 及表 3 结果可知,各硬件平台对 AES-128 算法映射所能得到的效能最优,因此以 AES-128 算法为基准进行对比,结果如表 4 所示.

表 4 AES-128 算法效能对比

运算结构	工艺/nm	单位面积性能	提升比例	单位功耗性能	提升比例
CryptoManiac[1]	250	240.41	–	0.77	19.4 ×
SophSEC[13]	130	22.56	59.2%	1.74	8.0 ×
Celator[14]	180	460	–	–	–
PipeRench[15]	250	–	–	–	–
REMUS_LPP[16]	65	31.81 *	12.9%	13.79 *	13.9%
PVHArray	55	35.92	–	15.71	–

* 等效 CBC 模式下效能指标

实验结果表明,CryptoManiac 及 Celator 结构在 AES-128 算法的单位面积实现性能上要远高于其它结构,这是由于上述两种结构针对 AES-128 算法进行了优化,其密码运算单元结构简单,仅支持若干种密码算法类型,故其芯片实现面积较小,从而大大提升了该结构芯片的单位面积性能. 相比于 SophSEC 结构,本文提出的 PVHArray 在面积性能方面提升了约 59.2%. REMUS_LPP 结构采用流水并行展开的方式进行算法映射,因此其算法实现性能大于 CBC 模式下的算法实现性能,由于引入流水并行的算法映射方法,假设流水级数及并行度均大于等于 2,则其 CBC 模式下的算法实现性能不高于 ECB 模式下的一半,故 REMUS_LPP 结构在 CBC 模式下的单位面积性能不高于 31.81 Mbps/mm^2,因此相较于该结构,本文提出的 PVHArray 单位面积性能提升了约 12.9%.

在单位功耗性能方面,由于 Celator 及 PipeRench 结构未提供芯片功耗数据,因此无法对比. 相比于 CryptoManiac 及 SophSEC 结构,本文提出的 PVHArray 结构在单位功耗性能方面分别提升了约 19.4 倍及 8 倍. 同样的,由于 REMUS_LPP 结构采用流水并行展开的方式进行算法映射,其 CBC 模式下的单位功耗性能不高于 13.79Mbps/mW,因此相较于该结构,本文提出的 PVHArray 单位功耗性能提升了约 13.9%.

综上所述,本文提出的 PVHArray 结构能够实现较高的单位面积性能以及单位功耗性能,同时由于 PVHArray 的可重构运算单元基于大量密码算法进行设计,其支持的密码算法映射数目相比于其它结构有明显提升,因此具有更高的灵活性.

4 结束语

结合密码算法运算特征,本文针对粗粒度可重构密码逻辑阵列中的运算、互连以及控制结构展开研究,构建了流水可伸缩的粗粒度可重构运算单元、层次化互连网络和面向周期级的分布式控制网络结构,并基于此实现了粗粒度可重构密码逻辑阵列的参数化模型. 以高效能映射为目标,基于统计模型及高效能评价体系,确定阵列模型参数,从而构建了规模为 4 × 4 的高效能 PVHArray 结构. 最后,基于高效能 PVHArray 阵列样片进行密码算法映射,实验结果表明,该结构能够实现较高的单位面积性能以及单位功耗性能. 下一步,将结合高效能 PVHArray 结构,对密码算法的优化映射算法展开研究.

参考文献

[1] LISA WU, CHRIS WEAVER, TODD AUSTIN. CryptoManiac: A fast flexible architecture for secure communication [A]. Proceedings. 28th Annual International Symposium on Computer Architecture [C]. Sweden: IEEE, 2001. 110 – 119.

[2] RAINER BUCHTY. Cryptonite-a programmable crypto processor architecture for high-bandwidth applications [A]. International Conference on Architecture of Computing Systems [C]. Berlin, Heidelberg: Springer, 2004. DOI:10.1007/978-3-540-24714-2_15.

[3] ELBIRTADAM J, CHRISTOF PAAR. An instruction-level distributed processor for symmetric-key cryptography [J]. IEEE Transactions on Parallel and Distributed Systems, 2005, 16(5): 468 – 480.

[4] LIU Leibo, WANG Bo, DENG Chenchen. Anole: A highly efficient dynamically reconfigurable crypto-processor for symmetric-key algorithms [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, PP(99): 1 – 1.

[5] GOKHAN SAYILAR, DEREK CHIOU. Cryptoraptor: High throughput reconfigurable cryptographic processor [A]. International Conference on Computer-Aided Design [C]. San Jose: IEEE, 2014. 155 – 161.

[6] LI Wei,ZENG Xiaoyang,NAN Longmei,et al. A reconfigurable block cryptographic processor based on VLIW architecture[J]. China Communications,2016,13(1):91 -99.
[7] SHAN Weiwei, FU Xingyuan, XU Zhipeng. A secure reconfigurable crypto IC with countermeasures against SPA,DPA,and EMA[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,2015,34(7):1201 -1205.
[8] SHAN Weiwei,XU Zhipeng,FU Xingyuan,et al. VLSI design of a reconfigurable S-box based on memory sharing method[J]. IEICE Electronics Express,2014,11(1):1 -6.
[9] 冯晓,李伟,戴紫彬. 面向分组密码的可重构异构多核并行处理架构[J]. 电子学报,2017,45(6):1311 -1320.
FENG Xiao,LI Wei,DAI Zi-bin. Reconfigurable asymmetrical multi-core architecture for block cipher[J]. Acta Electronica Sinica,2017,45(6):1311 -1320. (in Chinese)
[10] 马超,李伟,戴紫彬. 新型可重构移位-置换单元研究与设计[J]. 电子学报,2017,45(5):1025 -1034.
MA Chao,LI Wei,DAI Zi-bin. A novel reconfigurable rotation-permutation unit research and implementation[J]. Acta Electronica Sinica,2017,45(5):1025 -1034. (in Chinese)
[11] TIAN Chaoxuan,ZHU Jialiang,SHAN Weiwei,et al. VLSI design of reconfigurable cipher coprocessor supporting both symmetric and asymmetric cryptographic algorithms [A]. International Conference on Computer Science and Information Technology[C]. China:Kunming,2014. 299 -307.
[12] 杜怡然,南龙梅,戴紫彬. 可重构分组密码逻辑阵列加权度量模型及高能效映射算法[J]. 电子学报,2019,47(1):82 -91.
DU Yi-ran,NAN Long-mei,DAI Zi-bin. Reconfigurable block cryptographic logic array weighted metric model and high energy-efficient mapping algorithm[J]. Acta Electronica Sinica,2019,47(1):82 -91. (in Chinese)
[13] 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.
HUANG Wei. Research on Cloud Computing Performance and Power Consumption Configurable Secure Terminal Technology[D]. Shanghai:Fudan University,2011. (in Chinese)
[14] FRONTE D,PEREZ A,PAYRAT E. Celator:A multi-algorithm cryptographic co-processor[A]. The International Conference on Reconfigurable Computing and FPGAs [C]. Cancun,Mexico:IEEE,2008. 438 -443.
[15] SETH COPEN GOLDSTEIN,HERMAN SCHMIT,HARI CADAMBI. PipeRench:A reconfigurable architecture and compiler[J]. Computer,2000,33(4):70 -77.
[16] LIU Leibo,WANG Dong,ZHU Min,et al. An energy-efficient coarse-grained reconfigurable processing unit for multiple-standard video decoding[J]. IEEE Transactions on Multimedia,2015,17(10):1 -1.

作者简介

杜怡然　男. 1991 年 4 月出生,河南郑州人. 解放军信息工程大学计算机科学与技术专业博士研究生,从事安全专用芯片设计等有关研究.
E-mail:yrdu_ieu@163.com

李　伟(通信作者)　男. 1983 年 11 月出生,天津人. 解放军信息工程大学副教授,从事体系结构、安全芯片设计、集成电路技术等有关研究.

戴紫彬　男. 1966 年 5 月出生,河南商丘人. 解放军信息工程大学教授,博士生导师,从事专用集成电路设计、芯片安全防护、信息安全芯片技术等有关研究.