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

杜怡然,南龙梅,戴紫彬,李 伟
(解放军信息工程大学,河南郑州 450000)

摘 要: 针对基于粗粒度可重构阵列结构的分组密码算法映射情况复杂、难以实现统一度量的问题,该文采用多目标决策手段,以性能及功耗参数为决策目标,基于分组密码算法轮运算及粗粒度可重构阵列结构特征约束,提出了一种面向分组密码算法映射的加权度量模型. 同时,采用主客观综合分析法,定义了模型权重参数的计算方式,从而通过配置合理的权重参数,以高能效映射算法实现差异化的映射. 为了降低决策时间,该文进一步提出了基于二进制编码的枚举搜索算法,实现了最优映射结果搜索与映射矩阵建立的并行,使决策的时间复杂度降至 $O(2^n)$. 实验结果表明,该文提出的加权度量模型能实现高效的分组密码算法映射方案决策,单位面积性能提升了约 14.2%,能效提升了约一倍.

关键词: 粗粒度; 分组密码; 映射; 加权度量; 能效
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2019)01-0082-10
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.01.011

Reconfigurable Block Cryptographic Logic Array Weighted Metric Model and High Energy-Efficient Mapping Algorithm

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

Abstract: Aiming at the problem that the block cipher algorithm mapping based on coarse-grained reconfigurable array structure is complex and the evaluation standard is not uniform, this paper adopted a multi-objective decision-making means to evaluate the performance and power consumption parameters, and proposed a weighted metric model for map of block cipher algorithm. At the same time, the method of weighting parameters is defined by comprehensive subjective and objective factors, so as to provide differentiated mapping scheme by configuring reasonable weight parameters. In order to reduce the decision time, this paper introduced the algorithm of enumeration search based on binary coding, and realized the parallelism between the optimal scheme search and the generate mapping matrix, so that the time complexity of decision decrease to $O(2^n)$. The experimental results show that the weighted metric model can achieve efficient block cipher algorithm mapping, and the throughout per chip area has improved about 14.2%, with a 100% improvement in energy efficiency per workload bit.

Key words: coarse-grained; block cipher; mapping; weighted metric; energy efficiency

1 引言

密码算法是信息安全保障的重要手段,其中,分组密码算法是密码算法中的重要组成部分. 课题组在前期对基于超长指令字结构的分组密码算法处理器研究[1,2]的基础上发现,基于指令流的分组密码算法处理器结构因受摩尔定律发展的制约,其单处理器性能已达到瓶颈,难以满足高速安全数据传输需求. 粗粒度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,能有效实现对具有循环结构的算法的加速.

粗粒度可重构阵列丰富的运算资源在实现算法性

收稿日期:2017-10-09; 修回日期:2018-06-07; 责任编辑:李勇锋
基金项目:国家自然科学基金(No.61404175);信息工程大学优青基金(No.2705010304)

能提升的同时也造成了系统功耗的增大. 不同的映射方式将直接影响算法的实现性能及功耗,因此合理的映射方式是充分发挥粗粒度可重构阵列结构优势的关键. 现阶段,基于粗粒度可重构阵列结构的映射技术主要聚焦于算法中循环部分映射的研究. 文献[3]采用Map-Reduce 模型实现了循环部分的并行化映射,由于模型面向局部空间,难以取得全局最优解. 文献[4]建立了基于多面体模型及其仿射变换的粗粒度可重构阵列性能模型,实现了对算法映射的评价;文献[5,6]改进了文献[4]中模型,提出了基于联合仿射变换及多流水线合并的方法,进一步优化算法映射模型,但文献[4~6]均只基于性能参数进行映射优化,度量因素不够全面. 文献[7]针对软件流水中模调度问题,采用启动间隔作为评价的标准,但并未针对粗粒度可重构阵列结构进行优化. 文献[8]采用"聚簇—合并"的映射方式,有效降低了存储带宽及全局互连需求,但缺乏对循环内部算子运算的度量.

上述研究成果能够较好的实现基于粗粒度可重构阵列结构的算法映射,但其研究大多面向多媒体应用领域,算法结构与分组密码算法存在较大差异,具体表现为:分组密码算法不存在复杂的嵌套循环过程,循环间数据依赖性不强;分组密码算法轮运算内部算子类型较多,不同映射方案对应的系统关键路径延迟不同. 在实际应用中,密码算法芯片设计沿着高性能与低功耗两条技术路线发展,因此算法实现性能与系统功耗的限制已成为影响密码算法映射的关键.

本文针对分组密码算法映射及映射算法优劣程度度量等问题,首先研究了分组密码算法及粗粒度可重构阵列结构的特征,提取模型约束参数,分别提出了算法映射的性能及功耗模型,并基于此构建了面向应用的加权度量模型. 最后,提出了面向加权度量模型的高能效映射算法,通过综合主客观因素以配置合理化的权重参数,提供差异化的映射方案,从而满足不同的应用需求.

2　约束条件下的模型参数分析

加权度量模型以性能及功耗为度量标准,以分组密码算法映射方案为模型参数进行建模. 由于分组密码算法映射方案与分组密码算法结构及粗粒度可重构阵列结构直接相关,因此本节针对上述两个因素进行研究,研究不同特征下各参数对加权度量模型建模的影响,从而对模型进行参数化表示.

2.1　基于分组密码算法特征的模型约束研究

分组密码算法采用轮运算的多次循环迭代实现,轮运算映射的优劣直接影响着分组密码算法的实现性能. 因此,对分组密码算法特征的研究即为对分组密码算法轮运算的研究.

分组密码算法的轮运算主要实现混乱及扩散功能,一般包含以下四种结构:Feistel 结构、SP 结构、L-M 结构和 MISTY 结构,各种轮运算结构及其对应数据依赖图如图 1 所示.

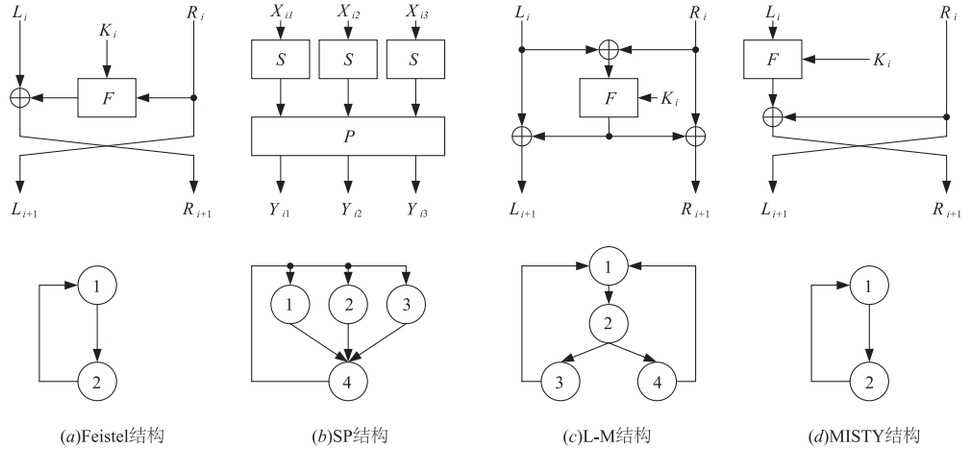

图 1　分组密码算法的轮运算结构及其数据依赖图

由图 1 可得,分组密码算法具有如下三个基本特征.

特征一:轮运算内部结构简单且算子排列有序

对于不同结构的分组密码算法轮运算,其运算由异或运算及 F 函数组成,其中 F 函数包含了诸如加、减、乘、S 盒、移位以及置换等基本运算环节,且 F 函数中一般不存在相同的基本运算环节,各运算环节具有严格的先后次序. 因此在构建映射模型时,需对轮运算

内算子的映射顺序进行约束,同时,对于不同分组密码算法,相同算子间无特定的映射次序.

特征二:轮内数据依赖强烈但轮间无数据依赖

分组密码算法的轮运算数据依赖图可得,第 i 轮运算的输入数据与第 i-1 轮运算的输出数据存在依赖关系,轮运算内部数据仅与当前轮相关,不存在轮间的数据依赖关系. 因此在构建映射模型时,应尽可能在有限的约束范围内完成单轮运算的映射,以避免长跳线使映射过于分散.

特征三:轮内数据单向流动

轮运算内部数据流呈单向流动,不存在数据的倒流、回馈过程,具有潜在流水并行处理的可能性. 因此在构建映射模型时,应充分考虑不同流水级数对性能及功耗的影响.

综上所述,分组密码算法的基本特征决定了加权度量模型的部分构建规则,同时也对算法映射方式进行了约束,为度量评价模型的建立奠定了基础.

2.2 粗粒度可重构阵列结构特征模型及约束

粗粒度可重构阵列作为分组密码算法轮运算映射的载体,能有效实现对算法中循环部分的加速,主要包括主控制器、配置存储器、数据存储器以及运算元素(Processing Element,PE)阵列等. 运算元素阵列是构建分组密码算法数据路径的基础,由大量同构的 PE 互连形成,其中 PE 内部包含的可重构功能单元(Functional Unit,FU),用于映射分组密码算法的不同运算环节.

为了进一步提升粗粒度可重构阵列结构的映射能力,本文对通用结构的运算元素 PE 进行改进. 通过对近几年密码算法征集活动及现有信息安全协议所采纳的分组密码算法的统计分析,将分组密码算法的基本运算类型划分为简单布尔类运算、非线性类运算、S 盒运算、置换类运算以及算数类运算五类,并针对上述基本运算类型分别设计了五类可重构功能单元.

根据分组密码算法的基本特征可得,不同类型的可重构功能单元在映射时并无先后次序,因此本文采用 Crossbar 全互连结构设计了输入及输出互连网络,以实现内部任意 FU 的互连. 由于各 FU 关键路径延迟不同,通过设置可旁路的寄存器实现多 FU 的单周期级联运算,提升映射的灵活性. 面向分组密码算法的粗粒度可重构阵列结构如图 2 所示.

粗粒度可重构阵列丰富的计算及互连资源,在有效实现分组密码算法数据流映射的同时也带来了系统功耗的提升,限制了分组密码算法的映射方案. 由于粗粒度可重构阵列较细粒度阵列的配置过程更为简单,因此可忽略其配置时间消耗. 分组密码算法靠多次迭代实现其安全性与可靠性,大量的数据交互存在于轮运算内部及轮运算间,与运算元素阵列外部的数据存储器交互不频繁,仅在数据输入与输出时产生交互,因此在本文所建立的模型中不考虑与外部存储器交互带来的性能损失.

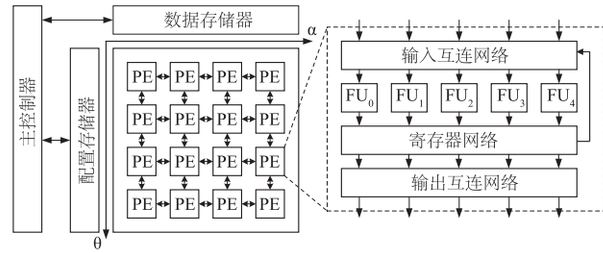

图 2 面向分组密码算法的粗粒度可重构阵列基本结构

如图 2 所示,运算元素阵列分别在 α 及 θ 维度展开,考虑到 PE 运算位宽的限制,若 PE 运算位宽小于分组密码算法分组长度,则分组密码算法沿 α 维度映射,并通过 PE 间的级联实现小位宽到大位宽运算的转换. 运算元素阵列的 θ 维度用于实现分组密码算法不同轮映射的展开,以开发轮运算映射的流水特性,提升分组密码算法实现性能.

3 分组密码算法映射的加权度量模型

分组密码算法映射常采用性能及功耗作为其映射结果的评价指标,但对于不同的应用场景,难以单纯采用某一评价指标去衡量映射的优劣,需全面考虑性能或功耗在当前应用场景下所占的权重,从而以更加高效、合理的方式实现分组密码算法的映射. 通过对分组密码算法基本特征及粗粒度可重构阵列结构的研究,面向分组密码算法的加权度量模型主要包含以下两个部分:(1)聚焦分组密码算法单轮轮运算映射,以性能为衡量指标,在 α 维度实现单轮轮运算的映射;(2)聚焦分组密码算法轮运算展开映射,以功耗为衡量指标,在 θ 维度实现多轮轮运算的映射. 本节将从上述两个方面入手,分别建立分组密码算法映射的性能参数模型及功耗参数模型,并据此建立了统一的映射加权度量模型,通过分析算法映射需求,配置合理的加权度量参数,以评价分组密码算法映射的优劣.

3.1 分组密码算法映射性能及功耗参数模型

对于分组密码算法,其算法的主体为轮运算的循环迭代. 除轮运算外,分组密码算法还常包含初始变换及末尾变化,但均可看做是轮运算的精简,在建模时可忽略其特异性,因此本节首先对分组密码算法的单轮轮运算映射进行模型构建. 为了进一步提升模型的普适性,假设粗粒度可重构阵列内部 PE 包含 n 个异构的 FU($FU_0 \sim FU_{n-1}$),用于映射分组密码算法轮运算中的不同映射环节. 对于第 p 行,第 q 列的 PE 而言,其映射可以表示成一个 $n \times n$ 的映射矩阵 $\Pi_{p,q}$.

$$\boldsymbol{P}_{p,q}=\begin{bmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,n-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n-1,0} & x_{n-1,1} & \cdots & x_{n-1,n-1} \end{bmatrix} \tag{1}$$

其中 $x_{i,j}(0\leqslant i,j\leqslant n-1)$ 表示 FU 的映射情况,取值为 0 或 1,若 $x_{i,j}=1$ 则对应的 FU_j 被占用. 映射矩阵中第 i 行表示第 i 个时间步的映射情况,第 j 列表示 FU_j 在该轮轮运算映射中是否被占用. 显然,对于任意 PE,FU_j 具有唯一性,满足以下约束:

$$\Pi_{p,q}^{\mathrm{T}}\times\overrightarrow{1}\leqslant\overrightarrow{1} \tag{2}$$

由于不同运算环节的复杂度不同,其所对应 FU 的关键路径延迟也不同. 假设 $\mathrm{FU}_0\sim\mathrm{FU}_{n-1}$ 的关键路径延迟分别为 $tcp_0\sim tcp_{n-1}$,则 PE 的关键路径延迟可由映射矩阵 $\Pi_{p,q}$ 表示为:

$$\begin{aligned}(t_{p,q})_{\max}&=\max(\Pi_{p,q}\times\overrightarrow{\mathrm{FU}_{tcp}})\\&=\begin{bmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,n-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n-1,0} & x_{n-1,1} & \cdots & x_{n-1,n-1} \end{bmatrix}\begin{bmatrix} tcp_0 \\ tcp_1 \\ \cdots \\ tcp_{n-1} \end{bmatrix}\end{aligned} \tag{3}$$

若存在:

$$\Pi_{p,q}\times\overrightarrow{1}>\overrightarrow{1} \tag{4}$$

则表示在第 p 行,第 q 列的 PE 映射中,存在多个运算环节合并的情况,由于不同运算环节之间的合并并不会产生额外明显的关键路径延迟增加,因此合并后运算环节的关键路径延迟可视作参与合并的运算环节的关键路径延迟之和.

在粗粒度可重构阵列的 α 维度上,分组密码算法映射主要完成了小位宽扩展大位宽的级联运算,因此对于同一行上的 PE 而言,其关键路径延迟相同. 假设分组密码算法单轮轮运算在阵列 θ 维度上共映射了 k 行,则分组密码算法单轮轮运算的关键路径延迟为:

$$t_{\mathrm{round}}=\sum_{l=0}^{k-1}(t_{p,q+l})_{\max} \tag{5}$$

对于分组密码算法,其各轮运算结构相同,因此可采用任意轮运算的关键路径延迟作为分组密码算法轮运算的关键路径延迟. 假设分组密码算法分组长度为 L,算法共有 N 轮轮运算,每轮轮运算包含 m 个运算环节. 对于单分组数据的加解密运算,分组密码算法实现性能(Total Execute Throughput,TET)可以表示为:

$$\mathrm{TET}=\frac{L}{N\times m\times t_{\mathrm{round}}} \tag{6}$$

分组密码算法及应用中输入的数据长度确定时,式(6)中的分组密码算法分组长度 L 及轮运算轮数 N 由分组密码算法本身决定,因此可以通过减小轮运算中的运算环节数目或降低粗粒度可重构阵列的关键路径延迟来提升分组密码算法实现性能. 假设分组密码算法轮运算映射中各运算环节的关键路径延迟分别为 $tcp_0\sim tcp_{m-1}$,则 $m\times t_{\mathrm{round}}$ 在 $m=1$ 时取得最小值,证明如下:

$m=1$ 时:$m\times t_{\mathrm{round}}=1\times(tcp_0+tcp_1+\cdots+tcp_{n-1})$

$m=2$ 时:

$m\times t_{\mathrm{round}}=2\times\max\{tcp_0+\cdots+tcp_{j-1},tcp_j+\cdots+tcp_{n-1}\}$

$m=3$ 时:

$m\times t_{\mathrm{round}}=3\times\max\{tcp_0+\cdots+tcp_{j-1},\cdots,tcp_p+\cdots+tcp_{n-1}\}$

……

$m=n$ 时:$m\times t_{\mathrm{round}}=n\times\max\{tcp_0,tcp_1,\cdots,tcp_{n-1}\}$

设 $m=k$ 时,$tcp^*=\max\{\sum tcp_0,\sum tcp_1,\cdots,\sum tcp_{k-1}\}$,可以得到:

$$\begin{aligned}m\times t_{\mathrm{round}}&=k\times tcp^*=tcp^*+tcp^*+\cdots+tcp^*\\&\geqslant\sum tcp_0+\sum tcp_1+\cdots+\sum tcp_{k-1}\\&=tcp_0+tcp_1+\cdots+tcp_{n-1}\end{aligned}$$

由上述证明可得,尽可能的合并分组密码算法轮运算映射中的运算环节,可使分组密码算法映射的性能得到提升. 当映射不再局限于算法中的一轮轮运算时,同理可证,分组密码算法在粗粒度可重构阵列上按整数倍轮运算进行完全展开及合并,分组密码算法映射的单分组实现性能均可达到最大.

式(6)中的分组密码算法实现性能是基于单分组数据加解密模式得到的,忽略了分组密码算法映射中潜在的并行流水特性. 对于多分组密码算法映射,可以在 θ 维度上开发分组密码算法映射的并行流水特性,进一步提升分组密码算法的实现性能.

在粗粒度可重构阵列 θ 维度上进行映射意味着需要占用更多的硬件资源,即增大算法运行时所需的功耗. 因此本文对分组密码算法轮运算映射的性能参数模型进行了改进,并结合并行流水映射方式,进行功耗参数模型的建模. 若分组密码算法在粗粒度可重构阵列上共映射了 R 轮运算,则分组密码算法可以按照 $R\times m$ 级流水方式进行展开,如图 3 所示.

当分组密码算法实现 Q 个分组长度数据的加解密时,若按照 R 轮映射进行展开,则性能参数模型可以改写为:

$$\mathrm{TET}=\frac{L\times Q}{\left[\left\lfloor\frac{Q}{R}\right\rfloor\cdot(N\times m+R-1)+\left(Q-\left\lfloor\frac{Q}{R}\right\rfloor\times R\right)\cdot\left(N\times m+Q-\left\lfloor\frac{Q}{R}\right\rfloor\times R-1\right)\right]\times t_{\mathrm{round}}} \tag{7}$$

分组密码算法实现性能仅和参数 R、m 与 t_{round} 相关. 参

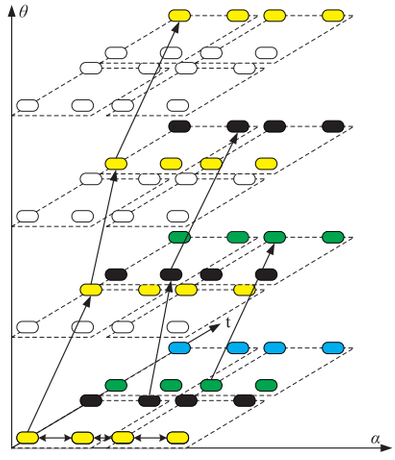

图 3 分组密码算法流水映射方式($R=4$,$m=1$)

数 R 表征了分组密码算法轮运算在粗粒度可重构阵列 θ 维度上映射展开的轮数,展开程度越高,分组密码算法的潜在流水并行性越高.

除了与分组密码算法实现性能相关,参数 R 还直接影响了分组密码算法的实现功耗. 对于粗粒度可重构阵列,映射不同分组密码算法其控制部分及存储部分的功耗变化不大,可视为一常数. 因此,由不同映射方案带来的系统功耗的差别主要存在于 PE 的不同映射方式上. 定义粗粒度可重构阵列执行功耗为(Total Execute Power,TEP)为:

$$\mathrm{TEP}=P_c+P_m+P_s\times N_{\mathrm{sum}}+\sum P_d \tag{8}$$

其中 P_c 及 P_m 分别表示粗粒度可重构阵列主控制器及存储器所产生的功耗,P_s 和 P_d 分别表示 PE 的静态功耗与动态功耗,N_{sum} 为粗粒度可重构阵列中 PE 的总数. 对于同一粗粒度可重构阵列结构,参数 P_c、P_m、P_s 及 N_{sum} 可视为常量参数;P_d 与 PE 内部映射的 FU 类型有关,可表示为映射矩阵 $\Pi_{p,q}$ 及映射所占用 PE 数目的函数.

3.2 加权度量模型建模

对于不同的应用需求,其性能及功耗指标各异,因此无法单独采用式(7)或(8)对基于粗粒度可重构阵列的分组密码算法映射方案进行度量. 同时,受映射展开轮数 R 的影响,式(7)和(8)的单调性相同,因此需要建立统一的度量评价模型对分组密码算法轮运算映射的优劣进行评价.

由于 TET 及 TEP 运算结果的量纲不同,分别为 Gbps 和 mW,无法直接进行运算. 因此,本文首先采用线性归一化方法,对式(7)、(8)进行归一化处理[9],可以得到:

$$\mathrm{TET}^*=\frac{\mathrm{TET}-\mathrm{TET}_{\min}}{\mathrm{TET}_{\max}-\mathrm{TET}_{\min}} \tag{9}$$

$$\mathrm{TEP}^*=\frac{\mathrm{TEP}_{\max}-\mathrm{TEP}}{\mathrm{TEP}_{\max}-\mathrm{TEP}_{\min}} \tag{10}$$

其中 TET^* 及 TEP^* 表示归一化处理后的分组密码算法实现性能和粗粒度可重构阵列执行功耗,$\mathrm{TET}_{\max}$、$\mathrm{TET}_{\min}$、$\mathrm{TEP}_{\max}$ 及 $\mathrm{TEP}_{\min}$ 分别表示 TET 和 TEP 的最值,可在搜索合法映射矩阵的过程中计算得到.

为了更好的评价分组密码算法在特定应用场景下映射的优劣程度,本文定义了映射评价函数(Mapping Evaluate Function,MEF)作为评价映射的标准,函数定义如下:

$$\mathrm{MEF}=\omega_t\cdot\mathrm{TET}^*+\omega_p\cdot\mathrm{TEP}^* \tag{11}$$

其中参数 ω_t 为性能参数权重,参数 ω_p 为功耗参数权重. 依据应用对性能及功耗的不同需求,配置合理的权重参数,从而搜索最优的分组密码算法映射方案.

4 加权度量模型高能效映射算法研究

根据式(11)可知,性能及功耗参数 ω_t 及 ω_p 直接影响着分组密码算法的映射方案,因此本文基于文献[10]提出的一种多目标决策指标权重计算方法,结合分组密码算法应用需求进行差异化映射.

根据前一节所建立的分组密码算法映射的性能及功耗参数模型可知,其归一化处理后的分组密码算法实现性能和粗粒度可重构阵列执行功耗包含了对应映射方案性能及功耗的信息. 从性能及功耗指标的差异上分析,指标差异程度越大,则信息熵越小,该指标提供的信息量越大. 因此,通过计算分组密码算法映射性能及功耗的熵值,确定该指标的客观权重. 计算步骤如下:

Step1 假设有 m 种待评价的映射方案,对于不同映射方案,均采用 TET 及 TEP 作为映射评价指标,定量地取得各方案关于上述两个指标的评价矩阵,并进行归一化处理:

$$\boldsymbol{X}=\begin{bmatrix}\mathrm{TET}_1^* & \mathrm{TEP}_1^*\\ \mathrm{TET}_2^* & \mathrm{TEP}_2^*\\ \vdots & \vdots\\ \mathrm{TET}_m^* & \mathrm{TEP}_m^*\end{bmatrix} \tag{12}$$

Step2 计算第 i 个方案下,评价指标 TET 及 TEP 的比重 p_{ti}、p_{pi}:

$$p_{ti}=\mathrm{TET}_i^*/\sum_{i=1}^{m}\mathrm{TET}_i^*,\quad p_{pi}=\mathrm{TEP}_i^*/\sum_{i=1}^{m}\mathrm{TEP}_i^* \tag{13}$$

Step3 计算评价指标 TET 及 TEP 的熵值 e_t、e_p:

$$e_t=-\frac{1}{\ln m}\sum_{i=1}^{m}p_{ti}\ln p_{ti},\quad e_p=-\frac{1}{\ln m}\sum_{i=1}^{m}p_{pi}\ln p_{pi} \tag{14}$$

Step4 计算各评价指标的熵权 α_t、α_p:

$$\alpha_t=(1-e_t)/(2-e_t-e_p)$$

$$\alpha_p = (1 - e_p)/(2 - e_t - e_p) \tag{15}$$

由于熵权表示各指标提供信息的多寡程度,完全依靠客观数据计算得到,当客观数据较为特殊时,权重会与实际情况相差较大. 同时,基于粗粒度可重构阵列的分组密码算法映射是一种面向需求型的应用,即其映射方案会根据对性能或功耗的不同需求有较大差异,需根据应用目标需求确定该指标的主观权重.

Step5　根据需求目标确定主观权重 θ_t、θ_p:

$$\begin{aligned}\theta_t &= f_1(\mathrm{TET}_{\mathrm{demand}}, \mathrm{TEP}_{\mathrm{demand}}, \mathrm{TET}_{\max}, \mathrm{TET}_{\min})\\ \theta_p &= f_2(\mathrm{TEP}_{\mathrm{demand}}, \mathrm{TET}_{\mathrm{demand}}, \mathrm{TEP}_{\max}, \mathrm{TEP}_{\min})\end{aligned} \tag{16}$$

Step6　计算主客观综合权重 ω_t、ω_p:

$$\begin{aligned}\omega_t &= \alpha_t\theta_t/(\alpha_t\theta_t + \alpha_p\theta_p)\\ \omega_p &= \alpha_p\theta_p/(\alpha_t\theta_t + \alpha_p\theta_p)\end{aligned} \tag{17}$$

采用这一方式能有效排除客观数据过于集中带来的权重计算的误差,同时将主观需求目标作为评价权重的重要组成,能更好的对映射方案进行筛选,从而得到最优的分组密码算法映射方案. 与文献[10]相比,本文结合分组密码算法应用需求特征,将性能及功耗需求参数引入了主观权重的计算过程之中,削弱了由错误经验导致的主观权重计算偏差. 同时,采用线性叠加的方式能有效提升主客观权重的计算速度,提升分组密码算法映射的评价效率.

由于本文将分组密码算法映射限定在单个轮运算内,即不同轮的轮运算映射方式相同,因此,分组密码算法的映射方案被压缩至有限集合. 若轮运算内包含 n 个运算步骤,则分组密码算法映射方案的解空间为 $O(2^n)$,由于计算归一化的性能及功耗指标时需要求得其最值,因此必须采用枚举搜索的方式遍历所有可行方案. 考虑到分组密码算法轮运算中,前后算子间的连接只可能存在“独立”或“合并”两种关系,分别对应二进制编码的“0”或“1”,因此在枚举搜素时,可按照二进制编码顺序生成映射矩阵,同步矩阵生成与最优解搜索过程,能有效减少枚举遍历次数,从而更加快速的确定分组密码算法的最优映射方案.

5　实验与分析

本节基于实验室设计的粗粒度可重构密码逻辑阵列平台,对提出的分组密码算法映射加权度量模型的正确性与合理性进行分析,平台基本结构如图 2 所示. 选取 6 种典型分组密码算法 Blowfish[11]、SM4、AES、DES、IDEA[12] 及 MISTY[13] 进行算法映射,对比各映射方案的优劣.

首先选取典型分组密码算法 AES,采用加权度量模型对其映射进行评价. AES 轮运算内包含字节代替、行移位、列混合以及轮密钥加四步,可分别映射至 S 盒运算单元、置换类运算单元以及算数类运算单元(带后异或),定义输入数据包长度为 1MB,则映射方案及其结果如表 1.

表 1　AES 密码算法映射方案及其结果

展开轮数	1				2				3			
映射方案	1	2	3	4	1	2	3	4	1	2	3	4
TET	1.51	1.88	1.52	2.06	2.94	3.57	2.90	3.74	4.27	5.12	4.15	5.14
TEP	420	420	420	420	475	475	475	475	529	529	529	529
TET*	0	0.037	0.001	0.056	0.148	0.214	0.143	0.232	0.287	0.375	0.274	0.378
TEP*	1	1	1	1	0.857	0.857	0.857	0.857	0.714	0.714	0.714	0.714
展开轮数	4				5				6			
映射方案	1	2	3	4	1	2	3	4	1	2	3	4
TET	5.52	6.53	5.29	6.33	6.70	7.82	6.33	7.35	7.81	9.01	7.30	8.23
TEP	584	584	584	584	639	639	639	639	693	693	693	693
TET*	0.417	0.522	0.393	0.501	0.539	0.656	0.501	0.607	0.655	0.780	0.602	0.699
TEP*	0.571	0.571	0.571	0.571	0.429	0.429	0.429	0.429	0.286	0.286	0.286	0.286
展开轮数	7				8							
映射方案	1	2	3	4	1	2	3	4				
TET	8.86	10.11	8.19	9.00	9.85	11.12	9.01	9.68				
TEP	749	749	749	749	803	803	803	803				
TET*	0.764	0.894	0.694	0.779	0.867	1	0.780	0.850				
TEP*	0.143	0.143	0.143	0.143	0	0	0	0				

表1中的映射方案1为字节代替、行移位、列混合+轮密钥加;方案2为字节代替+行移位、列混合+轮密钥加;方案3为字节代替、行移位+列混合+轮密钥加;方案4为字节代替+行移位+列混合+轮密钥加,其中"+"代表操作间的合并. 对于相同的展开轮数,不同映射方案所占用的PE及FU数目相同,因此其映射结果中的TEP也相同. 根据表1可以计算出TET及TEP的比重分别为:

表2 AES密码算法映射性能及功耗比重

单位:10^{-2}

展开轮数	1				2				3			
映射方案	1	2	3	4	1	2	3	4	1	2	3	4
p_{ti}	0	0.24	0.01	0.36	0.95	1.37	0.92	1.48	1.83	2.40	1.75	2.41
p_{pi}	6.25	6.25	6.25	6.25	5.36	5.36	5.36	5.36	4.46	4.46	4.46	4.46
展开轮数	4				5				6			
映射方案	1	2	3	4	1	2	3	4	1	2	3	4
p_{ti}	2.66	3.33	2.51	3.20	3.45	4.19	3.21	3.88	4.19	4.99	3.85	4.47
p_{pi}	3.57	3.57	3.57	3.57	2.68	2.68	2.68	2.68	1.79	1.79	1.79	1.79
展开轮数	7				8							
映射方案	1	2	3	4	1	2	3	4				
p_{ti}	4.88	5.72	4.44	4.98	5.54	6.39	4.99	5.43				
p_{pi}	0.89	0.89	0.89	0.89	0	0	0	0				

因此TET及TEP的熵权分别为:0.440和0.560. 对于AES密码算法映射,性能指标要求其多分组实现性能大于2.5Gbps,单分组实现性能大于1Gbps,功耗小于800mW. 同时,根据表1可知,多分组模式下,AES密码算法映射TET的最大值为11.12Gbps,最小值为1.51Gbps;TEP的最大值为803mW,最小值为420mW. 因此TET及TEP的主观权重分别为:0.823和0.177,从而可以得到TET及TEP的主客观综合权重分别为:0.785和0.215,根据这一权重值,可以得到如表3所示的映射评价函数值.

表3 不同映射方案下映射评价函数值

单位:10^{-1}

展开轮数	1				2				3			
映射方案	1	2	3	4	1	2	3	4	1	2	3	4
MET	2.140	2.433	2.141	2.582	2.997	3.517	2.961	3.654	3.781	4.475	3.679	4.496
展开轮数	4				5				6			
映射方案	1	2	3	4	1	2	3	4	1	2	3	4
MET	4.499	5.323	4.308	5.162	5.157	6.074	4.858	5.689	5.759	6.741	0.534	6.105
展开轮数	7				8							
映射方案	1	2	3	4	1	2	3	4				
MET	6.312	7.334	5.762	6.432	6.818	7.860	6.130	6.683				

综上所述,根据性能指标约束,分组密码算法AES的最佳映射方案为轮运算内字节代替与行移位合并,然后进行列混合与轮密钥加,并流水展开为7轮,其最大映射评价函数值为0.733,对应算法实现性能为10.11Gbps、算法实现功耗为749mW. 采用相同方式对6种典型分组密码算法进行映射,映射结果如表4.

表4 基于加权度量模型的典型分组密码算法映射

分组密码算法	轮运算结构	轮运算映射方案	展开轮数	最优MET
Blowfish	Feistel结构	异或,S盒,模2^{16}加法(异或)	8	0.795
SM4	Feistel结构	异或,S盒(异或)+移位(异或)	8	0.812
AES	SP结构	字节代替+行移位,列混合(轮密钥加)	7	0.733
DES	SP结构	E盒扩展+S盒+P盒置换	4	0.561
IDEA	L-M结构	模$2^{16}+1$乘法(异或),模$2^{16}+1$乘法,模2^{16}加法(异或)	2	0.429
MISTY	MISTY结构	9*{异或+S盒(异或)}	1	0.684

展开轮数除了受系统功耗的影响,还受粗粒度可重构阵列硬件资源的限制. 若轮运算内部存在相同运算类型的算子,则必须映射至阵列的不同行中,从而限制了算法的展开轮数. 上述 6 种典型分组密码算法的映射结果如图 4 所示.

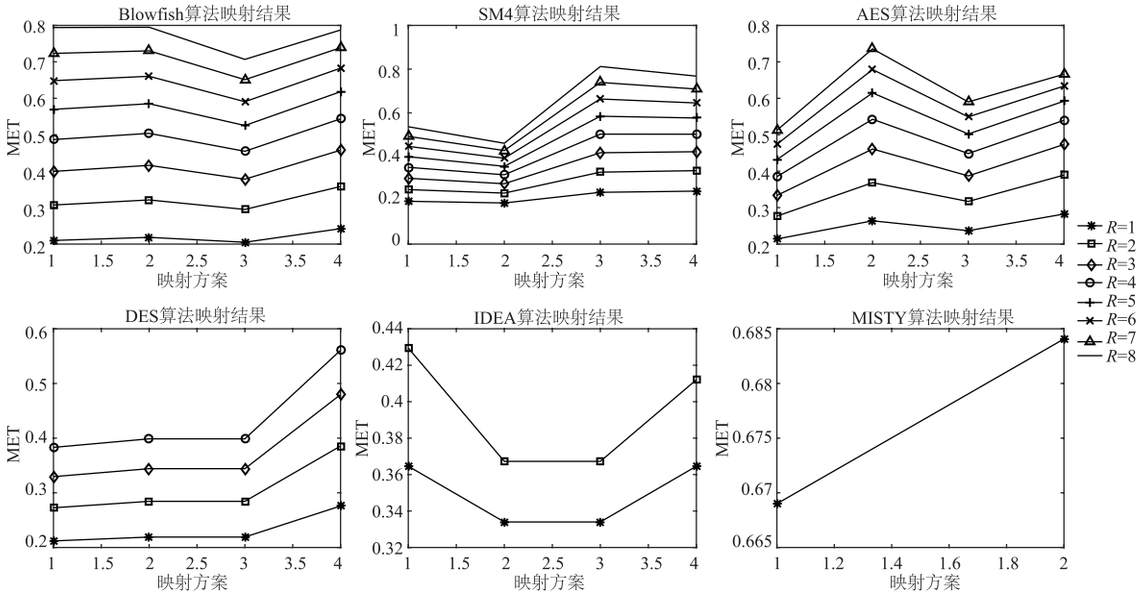

图 4　典型分组密码算法映射结果

由于大部分文献[14 ~ 18]所实现的粗粒度可重构阵列结构无源码支持,采用本文提出的加权度量模型进行映射难以取得可信算法性能. 因此,假定各文献所列的分组密码算法实现性能为最优映射下的性能,将本文映射结构与 PipeRench[14]、RHCA[15]、CryptoManiac[16]、REPROC[17]及 Cryptoraptor[18]等结构进行了比较,结果如表 5.

表 5　分组密码算法处理性能对比

可重构阵列结构	工艺(nm)	面积(mm^2)	功耗(mW)	分组密码算法处理性能(Mbps)		
				AES	DES	IDEA
PipeRench	250	50	NA	NA	NA	126. 6
RCHA	130	17. 96	NA	829. 6	690. 4	412. 4
CryptoManiac	250	1. 93	606. 37	64	NA	26
REPROC	65	4. 28	584	2160	2720	NA
Cryptoraptor	45	6. 32	6207	6400	2670	NA
本文	55	9. 25	803	11120	10353	6337

由于不同可重构阵列结构所采用的工艺水平不同,因此无法直接进行对比,参照文献[19]中不同工艺下芯片指标的换算方法,对表 5 中各指标进行换算,结果如表 6 所示.

表 6　分组密码算法处理性能对比(工艺换算后)

可重构阵列结构	工艺(nm)	换算后工艺(nm)	换算后性能/面积(Mbps/mm^2)			换算后功耗/性能(nJ/bit)		
			AES	DES	IDEA	AES	DES	IDEA
PipeRench	250	55	NA	NA	52. 314	NA	NA	NA
RCHA	130	55	258. 062	214. 761	128. 284	NA	NA	NA
CryptoManiac	250	55	685. 137	NA	278. 337	2. 084	NA	5. 131
REPROC	65	55	940	980	NA	0. 229	0. 182	NA
Cryptoraptor	45	55	1012. 65	422. 46	NA	1. 931	3. 052	NA
本文	55	55	1202. 16	1119. 24	685. 08	0. 072	0. 078	0. 127

在55nm相同工艺水平下,相比于文献[14~18],本文实验所采用的结构在性能最优映射下实现的单位面积性能提升了约14.2%,能效提升了约一倍.综上所述,本文提出的分组密码算法映射的加权度量模型能够高效的实现分组密码算法不同映射方案的度量,使决策时间降至$O(2^n)$,为基于粗粒度可重构阵列的分组密码算法映射提供指导.

6 结束语

为了充分发挥粗粒度可重构阵列对密码算法中轮运算的加速作用,提升密码算法映射效率,本文在对分组密码算法轮运算及粗粒度可重构阵列结构特征研究的基础上,提出了一种面向分组密码算法映射的加权度量模型.以算法映射的性能及功耗为综合优化目标,综合主客观因素,计算合理化权重参数,提供差异化的映射方案.采用基于二进制编码的枚举搜索算法,在搜索最优映射方案的同时构建映射矩阵,从而降低整体决策的时间复杂度.本文主要考虑分组密码算法在运算元素阵列上的数据路径映射,下一步将结合控制路径映射提供更为精确的度量模型.

参考文献

[1] 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.

[2] 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 Zibin. Reconfigurable asymmetrical multi-core architecture for block cipher[J]. Acta Electronica Sinica,2017,45(6):1311-1320.(in Chinese)

[3] SHAO Shengjia,YIN Shouyi,LIU Leibo,et al. Map-reduce inspired loop parallelization on CGRA[A]. IEEE International Symposium on Circuits and Systems[C]. Melbourne,2014. 1231-1234.

[4] LIU Dajiang,YIN Shouyi,LIU Leibo,et al. Polyhedral model based mapping optimization of loop nests for CGRAs[A]. Design Automation Conference[C]. Austin,2013. 1-8.

[5] LIU Dajiang,YIN Shouyi,PENG Yu,et al. Optimizing spatial mapping of nested loop for coarse-grained reconfigurable architectures[J]. IEEE Transactions on Very Large Scale Integration Systems,2014,23(11):1-1.

[6] YIN Shouyi,LIU Dajiang,PENG Yu,et al. Improvingnested loop pipelining on coarse-grained reconfigurable architectures[J]. IEEE Transactions on Very Large Scale Integration Systems,2015,24(2):1-1.

[7] WARTER-PEREZ,NANCY J,PARTAMIAN N. Modulo scheduling with multiple initiation intervals[A]. International Symposium on Microarchitecture[C]. Michigan,1995. 111-118.

[8] LEE JONG EUN,CHOI K,et al. An algorithm for mapping loops onto coarse-grained reconfigurable architectures[J]. ACM SIGPLAN Notices,2003,38(7):183-188.

[9] AKSOY,SELIM. Feature normalization and likelihood-based similarity measures for image retrieval[J]. Pattern Recognition Letters,2001,22(5):563-582.

[10] 郭金维,蒲绪强,高祥.一种改进的多目标决策指标权重计算方法[J].西安电子科技大学学报,2014,41(6):118-125.
GUO Jinwei,PU Xuqiang,GAO Xiang. Improved method on weights determination of indexes in multi-objective decision[J]. Journal of Xidian University,2014,41(6):118-125.(in Chinese)

[11] CANNIERE,CHRISTOPHE DE. Blowfish[J]. Encyclopedia of Cryptography & Security,2005:48-49.

[12] 金晨辉,郑浩然.密码学[M].北京:高等教育出版社,2009. 146-231.
JIN Chenhui,ZHENG Haoran. Cryptography[M]. Beijing:Higher Education Press,2009. 146-231.(in Chinese)

[13] MATSUI,MITSURU. New block encryption algorithm MISTY[J]. Lecture Notes in Computer Science,1997,1267(1267):54-68.

[14] GOLDSTEIN S C,SCHMIT H,Budiu M,et al. PipeRench:A reconfigurable architecture and compiler[J]. Computer,2000,33(4):70-77.

[15] 姜晶菲.可重构密码处理结构的研究与设计[D].国防科学技术大学,2004.
JIANG jingfei. The Research and Design of Reconfigurable Cipher Processing Architecture[D]. National University of Defense Technology,2004.(in Chinese)

[16] LISA WU,CHRIS WEAVER,TODD AUSTIN. CryptoManiac:A fast flexible architecture for secure communication[A]. International Symposium on Computer Architecture[C]. Sweden,2001. 110-119.

[17] WANG Bo,LIU Leibo. Dynamically reconfigurable architecture for symmetric ciphers[J]. ScienceChina Information Sciences,2016,59(4):042403.

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

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

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 SoC 与可重构设计、安全专用芯片设计等有关研究.
E-mail:yrdu_ieu@163.com

南龙梅　女. 1981 年 11 月出生,陕西乾县人. 解放军信息工程大学讲师,从事安全芯片设计、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.

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.