* 简要介绍课题的问题背景、目标、解决思路和方法。

问题背景：

可重构密码处理器处理单元设计方案如表1所示，表1简要列出了当前领域中处理单元设计常见的几种方案，以及这几种方案的特征、优缺点。

**表1 现有的几种PE结构及其优缺点分析**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 方案 | 方案特征 | 文献 | 优点 | 缺点 |
| 功能单元串行设计 | 将所有需要的功能放在一条串行的路径上，通过配置选择功能开关。 | [2][3]  [4] | 可以有更多的功能级联，在一个PE里面可以做更多的工作。 | 单个PE的延迟很大，而且功能串行的需求在不同的算法中有不同的表现很难兼顾所有算法。在迭代架构中有优势但是不适合阵列的多级流水架构。 |
| 功能单元的内部连接可按需配置设计 | PE内部的功能模块的串并连接可以通过配置进行动态组合。 | [10] | PE内部各个功能单元的利用率提高，可以在一个PE里实现更多的功能。 | 更加复杂的PE内部互连、配置。增加了面积和延迟。与串行的问题一样，如果不插寄存器那么PE的延迟就是所有功能单元的和，如果插寄存器解决延迟就要引入多周期。 |
| 功能单元并行设计 | 将所有需要的功能并行地放在不同的路径上，通过配置选择某一条路径完成某一个功能。 | [6][7] | 在保证PE功能完整的同时可以使PE的主频变得很高。 | PE中某一时刻只有一个功能单元在工作，功能单元利用率低。 |
| 功能单元串行和并行混合设计 | 通过对不同的模块进行延迟分析，结合算法的功能特征，功能模块先串行组合再并行组合。 | [4][5]  [6][9] | 平衡不同的功能单元的延迟，提供了简单功能单元的串行并且和功能并行结构具有相近的高主频 | 功能串行是算法相关的，很难兼顾所有算法 |

在表1的几种设计方案中，功能串行和可配置连接的设计方案，单个PE的功能十分强大，对应的延迟也很高，这种设计大多出现在迭代的架构中。为了追求更高的吞吐率，可重构密码处理器正在向阵列化发展，通过将算法进行迭代展开，在可重构阵列上进行十几级甚至几十级的流水线设计，基本达到一个周期完成一个完整加密过程，达到几十Gbps的吞吐率。功能并行和串并混合方案就是针对可重构密码阵列提出的，功能并行方案将算法所需要的各种功能都被并行地放置在一个PE中，纵向上的功能组合通过多个PE行来实现，这种设计方案可以极大地提高整个阵列的主频。串并混合方案通过对不同的模块进行延迟分析，结合算法的功能特征，功能模块先串行组合再并行组合，这样做在没有增加路径的延迟的同时丰富了处理单元纵向上的功能组合，可以有效降低阵列的规模，提高面积效率。

从上面的分析可以发现，在进行可重构密码处理器阵列设计时，最合适的处理单元设计方案是功能单元串行和并行混合设计方案，但是当前的设计方案仍然存在明显的缺陷：

* 经验的、简单的功能组合

现有架构的功能组合的标准是在延迟不够的并行路径上加上一个延迟小的功能来平衡不同路径的延迟，比较多的情况是加抑或逻辑[8]、字节置换[3][4]和移位[3][8]。这些延迟平衡的组合缺少足够的算法分析，这些组合到底是不是最佳的，被使用的频率是多少，都缺乏必要的证据，而且很多架构在进行功能单元设计时关注点集中在几个常见的算法上，有很大的算法倾向性。

* 只关注单个PE设计，没有考虑功能单元之间的拓扑关系

在当前的功能单元设计中，考虑的是算法中使用了哪些功能单元以及这些功能单元的简单组合，然后将这些功能单元堆砌在同一个PE中，形成一个同构的阵列架构。这样做的好处是在算法需要某个功能时，对应位置的PE就能提供所需的功能，其它位置的PE中这些功能单元就会被闲置。比如对于AES算法，假设映射时算法的一个轮函数被映射到3行中，如果一行中有4个PE，那么就有3x4=12个PE；AES算法中查表的操作会被映射到4个PE中，那么其它的8个PE中的查表单元就会被闲置，对于其他的功能单元也会有类似的闲置发生，而且闲置的单元数目会远远多于被使用的数目。在有些时候，为了兼顾多种算法，闲置是不可避免的，但是通过研究足够多的算法的功能单元拓扑结构，从中找出这些算法拓扑之间的共性，可以在某种程度上减少闲置的发生。

目标：

针对当前项目中和学术论文中的架构，新的PE设计方案在整体的性能面积比上有30%以上的提升。

解决思路：

本课题提出的PE设计方案，在优化PE内部功能单元设计的同时对各个功能单元在阵列中出现的拓扑关系进行了布局，减少在算法映射时闲置的发生，提高了功能单元的利用率，从而有效地提升了整个架构的面积效率。

方法：

1. 算法建模：建立了一个图模型来描述所有的分组加密算法，选取一定量的算法进行图建模，这些算法的图模型会作为后面算法特征提取算法和映射算法的输入。
2. 算法特征提取：涉及到算法中的算子类别、算子组合特征和算子拓扑特征；算子类别决定处理单元所需的功能单元种类和对应的功能，算子组合特征用来指导PE内部的功能组合设计，算子拓扑特征用来指导功能单元在阵列上的拓扑设计。
3. PE设计方案：根据提取的算法特征，进行功能单元设计，组合设计，拓扑设计。
4. 架构建模：建立了一个图模型来描述阵列架构，这个阵列架构的图模型会作为映射验证算法的输入。
5. 映射验证和进一步优化：将建模的算法图模型集合映射到阵列架构图模型上，分析映射结果，对架构中可能存在的闲置单元进行进一步优化。
6. 设计实现：RTL实现最终方案，仿真、综合。
7. 结果对比：与项目中、学术论文中的架构进行对比。

* 明确列出对比对象、对比目标的指标和代价、对比方案、对比条件以及对比结果。

对比对象的目标水平为工业界当前一流水平或学术界2年前一流水平。自行复现的对比对象需要验证正确性。

对比目标在指标和代价上必须量化，局部的间接指标必须能够反映到系统指标。

对比方案描述仿真验证或真实系统测试的基本思路和步骤。

对比条件描述仿真模型或真实系统的配置和参数设置，以及测试输入向量（仿真或真实数据）。

对比结果通过图表方式展示，有分析结论。

表2 不同架构实现算法所需功能单元对比

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 本文 | AU | SH | PER | LOU | 4\*LUT256\*8 | GFM |
| AES | 12 | 12 | 4 | 12 | 4 | 4 |
| DES | 12 | 12 | 4 | 12 | 4 | 4 |
| SM4 | 12 | 12 | 4 | 12 | 4 | 4 |
| TWOFISH | 24 | 24 | 8 | 24 | 8 | 8 |
| RC5 | 16 | 16 | 5.3 | 16 | 5.3 | 5.3 |
| BLOWFISH | 12 | 12 | 4 | 12 | 4 | 4 |
|  |  |  |  |  |  |  |
| TH |  |  |  |  |  |  |
| AES | 8(67%) | 8(67%) | 4(100%) | 48(400%) | 16(400%) | 0(0%) |
| DES | 16(133%) | 16(133%) | 8(200%) | 96(800%) | 32(800%) | 0(0%) |
| SM4 | 16 | 16 | 8 | 96 | 32 | 0 |
| TWOFISH | 24 | 24 | 12 | 144 | 48 | 0 |
| RC5 | 16 | 16 | 8 | 96 | 32 | 0 |
| BLOWFISH | 16 | 16 | 8 | 96 | 32 | 0 |
|  |  |  |  |  |  |  |
| Cyptoraptor |  |  |  |  |  |  |
| AES | 8 | 8 | 8 | 8 | 56 | 0 |
| DES | 12 | 12 | 12 | 12 | 84 | 0 |
| SM4 | 16 | 16 | 16 | 16 | 112 | 0 |
| TWOFISH | 20 | 20 | 20 | 20 | 140 | 0 |
| RC5 | 16 | 16 | 16 | 16 | 112 | 0 |
| BLOWFISH | 12 | 12 | 12 | 12 | 84 | 0 |
|  |  |  |  |  |  |  |
| RCPA |  |  |  |  |  |  |
| AES | 8 | 8 | 8 | 16 | 16 | 8 |
| DES | 12 | 12 | 12 | 24 | 24 | 12 |
| SM4 | 16 | 16 | 16 | 32 | 32 | 16 |
| TWOFISH | 20 | 20 | 20 | 40 | 40 | 20 |
| RC5 | 16 | 16 | 16 | 32 | 32 | 16 |
| BLOWFISH | 12 | 12 | 12 | 24 | 24 | 12 |

表3 不同架构实现算法的性能面积比

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 架构 | 工艺 | 主频 | 算法 | 映射面积(mm^2) | 面积减少 | 算法性能 | 性能面积比 | 性能面积比对比 |
| 本文 |  |  | AES | 0.1929094 |  |  |  |  |
| DES | 0.1929094 |  |  |  |
| SM4 | 0.1929094 |  |  |  |
| TWOFISH | 0.3858188 |  |  |  |
| RC5 | 0.2572125 |  |  |  |
| BLOWFISH | 0.1929094 |  |  |  |
| 清华项目中的架构 |  |  | AES | 0.407476 | 53% |  |  |  |
| DES | 0.814952 | 76% |  |  |  |
| SM4 | 0.814952 | 76% |  |  |  |
| TWOFISH | 1.222428 | 68% |  |  |  |
| RC5 | 0.814952 | 68% |  |  |  |
| BLOWFISH | 0.814952 | 76% |  |  |  |
| Cyptoraptor |  |  | AES | 0.873618 | 78% |  |  |  |
| DES | 1.310427 | 85% |  |  |  |
| SM4 | 1.747236 | 89% |  |  |  |
| TWOFISH | 2.184045 | 82% |  |  |  |
| RC5 | 1.747236 | 85% |  |  |  |
| BLOWFISH | 1.310427 | 85% |  |  |  |
| RCPA |  |  | AES | 0.3670776 | 47% |  |  |  |
| DES | 0.5506164 | 65% |  |  |  |
| SM4 | 0.7341552 | 74% |  |  |  |
| TWOFISH | 0.917694 | 58% |  |  |  |
| RC5 | 0.7341552 | 65% |  |  |  |
| BLOWFISH | 0.5506164 | 65% |  |  |  |