* 简要介绍课题的问题背景、目标、解决思路和方法。

问题背景：

可重构处理器发展趋势：

迭代架构-处理器阵列

更高的主频更高的吞吐率

可重构处理器阵列通过轮函数流水展开，实现单周期完成一组数据加密，实现高吞吐率。但同时也是整个处理器的面积变得很大，其中可重构处理器阵列部分占据主要部分。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 架构 | 架构特点 | 工艺nm | 芯片面积m2 | 处理单元面积m2 |
| ProDFA | 迭代 | 130 | 0.72 |  |
| cryptoraptor | 处理单元阵列 | 45 | 6.32 | 4.54 |
| RCPA | 处理单元阵列 | 80 | 14.9 |  |
| 清华项目 | 处理单元阵列 | 40 |  |  |

导致可重构处理器阵列面积过大的原因分析：

每一个PE包含了所有算法的所有功能，这些功能单元的利用率很低，存在很大的冗余，下图列出了阵列架构中基本运算单元的利用率。从表中可以看出这些单元的利用率很低，存在很大的优化空间。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| TH | AU | SH | PER | LOU | 4\*LUT256\*8 | GFM |
| AES | 0% | 0% | 0% | 8% | 25% |  |
| DES | 0% | 0% | 25% | 2% | 6% |  |
| SM4 | 0% | 25% | 0% | 4% | 3% |  |
| TWOFISH | 17% | 4% | 0% | 4% | 4% |  |
| RC5 | 13% | 13% | 0% | 2% | 0% |  |
| BLOWFISH | 19% | 0% | 0% | 3% | 3% |  |
|  |  |  |  |  |  |  |
| Cyptoraptor |  |  |  |  |  |  |
| AES | 0% | 0% | 0% | 50% | 7% |  |
| DES | 0% | 0% | 17% | 17% | 2% |  |
| SM4 | 0% | 25% | 0% | 25% | 1% |  |
| TWOFISH | 20% | 5% | 0% | 30% | 1% |  |
| RC5 | 13% | 13% | 0% | 13% | 0% |  |
| BLOWFISH | 25% | 0% | 0% | 25% | 1% |  |
|  |  |  |  |  |  |  |
| RCPA |  |  |  |  |  |  |
| AES | 0% | 0% | 0% | 25% | 25% | 50% |
| DES | 0% | 0% | 17% | 8% | 8% | 0% |
| SM4 | 0% | 25% | 0% | 13% | 3% | 0% |
| TWOFISH | 20% | 5% | 0% | 15% | 5% | 10% |
| RC5 | 13% | 13% | 0% | 6% | 0% | 0% |
| BLOWFISH | 25% | 0% | 0% | 13% | 4% | 0% |

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，减少在算法映射时冗余的发生，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aoe加模、特征提取：建立了一个图模型来描述所有的分组加密算法，提取算法特征。主要涉及三列特征参数特征、组合特征、拓扑特征
2. 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。
3. 算法aov建模、架构建模：建立了一个图模型来描述阵列架构和算法，这个算法模aov型和阵列架构的图模型会作为映射验证算法的输入。
4. 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。
5. 设计实现：RTL实现最终方案，仿真、综合。
6. 结果对比：与项目中、学术论文中的架构进行对比。



1. 算法aoe加模、特征提取

* 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% |  |  |  |