考核指标

PE结构

分组密码算法中的的运算可以分为以下几种

|  |  |
| --- | --- |
| 运算种类 | 在算法中出现的频率 |
| 逻辑 | 97.56% |
| 查找表 | 73.17% |
| 移位、循环移位 | 85.36% |
| 模运算 | 48.78% |
| 置换 | 24.39% |
| 模乘 | 17.07% |
| 有限域乘 | 17.07% |

根据所需要的算法特征选择必要的运算加入到PE。

运算种类：PE在广度上的功能，决定支持算法的种类

运算级联：PE在深度上的功能

运算种类和运算级联共同决定了PE最终能够组合成的运算组合的数目

延迟：PE作为整个阵列的主要功能单元往往会成为整个架构的关键路劲，因此提高性能的一个关键点就是降低PE的关键路径。而且虽然运算级联能够为PE提供更多的运算功能，但是运算级联越大关键路径延迟也越大，这里有一个折衷的选择。

阵列的主要面积来自存储和PE，因此虽然可以往PE上并行地堆砌更多的运算单元，但是必然带来更多的面积和功耗开销。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 架构名称 | 运算种类 | 位宽 | 运算级联 | 运算组合 | 工艺/nm | 延迟/ns | 面积 |
| celator | 逻辑、移位、置换、模运算 | 8 | 1 | 4 | 180 | 5.26 |  |
| COARX | 循环移位、逻辑、模运算 | 32 | 2 | 5 | 90 | 1.43 |  |
| COBRA | 逻辑、模运算、查找表、模乘、移位、循环移位、有限域乘法 | 32 | 10 | >100 | 350 | 9.81 | 117080gates |
| cryptoraptor | 模运算、查找表、逻辑、移位、循环移位、置换 | 32 | 2 | 9 | 45 | 0.63/1.00 | 0.0344mm^2 |
| ProDFA | 逻辑、模运算、查找表、移位、置换、模乘 | 32 | 5 | 48 | 130 | 2.50 |  |
| RCPA | 逻辑、移位、置换、查找表、模运算、模乘、有限域乘法 | 32 | 3 | 28 | 180 | 5.55 |  |
| 目前我们的架构 | 模运算、逻辑运算 | 8 | 2 | 4 | 45 | 1.69 |  |

算法支持：

算法的支持范围越大意味着PE的功能也越多，PE需要提供更多的运算支持来支持这些算法，因此算法支持是对PE功能广度的一个度量。

可以根据它的算子推出来它支持的算法，但是不好预测性能。

|  |  |  |  |
| --- | --- | --- | --- |
| 架构名称 | 块密码算法 | 流密码算法 | Hash算法 |
| celator | 实现的是AES和DES | 不支持 | 实现的是SHA256 |
| COARX | 不支持 | 不支持 | 5 |
| COBRA | 40种 | 不支持 | 不支持 |
| cryptoraptor | 84.38% | 96.15% | 86.49% |
| ProDFA | 实现了五种 | 不支持 | 不支持 |
| RCPA | 实现了DES和AES | 不支持 | 不支持 |
| 目前我们的架构 |  | 不支持 | 不支持 |

整体性能：

对比面积和性能面积比时需要统一工艺。

周期数决定了CBC模式的吞吐率，但是针对CBC和EBC这两种模式的设计思路是完全不同的，因此一种架构只需要选择其中一个模式进行设计。

我们的架构是一个多核阵列，因此设计的重点在于EBC模式。

性能对比选择不同的分组规模，不同的循环规模的算法进行性能的测试对比。不同点分组规模对应的是阵列中每行总位宽的大小选择，而循环轮数则对应的是阵列行数规模已经每一个PE功能的复杂性。

AES128分组

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 架构名称 | 工艺/nm | 主频 | 周期数 | 吞吐率/MbPs | 面积mm^2 | 吞吐率/面积 |
| celator | 130 | 190 | 524 | 46(CBC) | 0.1 |  |
| COBRA | 350 | 102 | 90 | 1450(EBC) | 2.5Mgates |  |
| cryptoraptor | 45 | 1000 | 20 | 6400(CBC)  128000(CTR) | 6.3244 |  |
| ProDFA | 130 | 203.8 | 147 | 4163(EBC) | 0.72 |  |
| RCPA | 180 | 400 | 48 | 4767(EBC) | 14.9/1.49Mgate |  |
| 目前我们的架构 | 45 | 500 |  | 64000(EBC) |  |  |

DES64分组

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 架构名称 | 工艺/nm | 主频 | 周期数 | 吞吐率 | 面积 | 吞吐率/面积 |
| celator | 130 | 190 | 476 | 26(CBC) | 0.1 |  |
| cryptoraptor | 45 | 1000 | 48 | CBC:2670  CTR:42670 | 6.3244 |  |
| ProDFA | 130 | 203.8 | 91 | 4491(EBC) | 0.72 |  |
| RCPA | 180 | 400 | 83 | 2764.8(EBC) | 14.9/1.49Mgate |  |
| 目前我们的架构 | 45 | 500 |  |  |  |  |