1. 绪论
   1. 研究背景
      1. 可重构计算概述
      2. 密码算法综述
   2. 国内外研究现状
      1. 可重构密码架构综述
      2. 可重构系统PE概述
   3. 论文研究内容及意义
   4. 论文组织结构
2. 分组密码算法与可重构架构
   1. 分组密码算法概述
   2. 面向分组密码算法可重构系统架构
   3. 本章小结
3. 分组加密算法图模型与算法特征提取
   1. 分组密码算法图模型
   2. 算法特征提取
      1. 算法的关键特征
      2. 算法特征提取方案
      3. 算法特征总结
   3. 本章小结
4. PE初始方案与架构图模型
   1. PE初始设计方案
      1. 设计方法
      2. 阵列拓扑结构
      3. 行间互连
      4. 异构组
      5. 处理单元
      6. 功能单元

* 1. 架构图模型
  2. 本章小结

1. PE初始方案映射分析与优化
   1. 可重构架构映射概述
      1. 问题模型
      2. 研究现状
   2. 基于子图同构的映射方案
      1. 子图同构问题描述
      2. VF2子图同构算法
      3. 基于VF2算法的映射方案
   3. 映射结果分析与PE结构优化
      1. 算法映射结果分析
      2. 基于映射结果的PE优化
   4. 本章小结
2. 优化PE方案的验证与分析
   1. PE实现与性能分析

PE的RTL实现分析，各个单元的面积和延迟，关键路径等分析

* 1. 算法映射结果

使用映射工具对算法集映射的结果

分组加密算法中的有限域乘法

AES

特征多项式：m(x)=x8+x4+x3+x+1

矩阵：

2 3 1 1

1 2 3 1

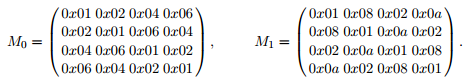
1 1 2 3

3 1 1 2

Clefia

不可约多项式

矩阵： x8 + x4 + x3 + x2 + 1



* 1. 与不同架构的对比

1. 功能单元消耗对比

算法集在不同架构的映射下阵列所需要的功能单元统计

课题中的架构优化的粒度是功能单元，因此这个表能直接说明课题的优化方案达到的效果

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 架构 | 算法 | 功能单元使用 | | | | | |
| AU | SH | PER | LOU | LUT | GFM |
| 本文 | AES |  |  |  |  |  |  |
| DES |  |  |  |  |  |  |
| IDEA |  |  |  |  |  |  |
| BLOWFISH |  |  |  |  |  |  |
| CAMELLIA |  |  |  |  |  |  |
| CAST128 |  |  |  |  |  |  |
| GOST |  |  |  |  |  |  |
| RC5 |  |  |  |  |  |  |
| SEED |  |  |  |  |  |  |
| TWOFISH |  |  |  |  |  |  |
| SM4 |  |  |  |  |  |  |
| RC6 |  |  |  |  |  |  |
| SERPENT |  |  |  |  |  |  |
| TEA |  |  |  |  |  |  |
| 更多算法 |  |  |  |  |  |  |
| 项目中的架构 | AES |  |  |  |  |  |  |
| DES |  |  |  |  |  |  |
| IDEA |  |  |  |  |  |  |
| BLOWFISH |  |  |  |  |  |  |
| CAMELLIA |  |  |  |  |  |  |
| CAST128 |  |  |  |  |  |  |
| GOST |  |  |  |  |  |  |
| RC5 |  |  |  |  |  |  |
| SEED |  |  |  |  |  |  |
| TWOFISH |  |  |  |  |  |  |
| SM4 |  |  |  |  |  |  |
| RC6 |  |  |  |  |  |  |
| SERPENT |  |  |  |  |  |  |
| TEA |  |  |  |  |  |  |
| 更多算法 |  |  |  |  |  |  |
| Cyptoraptor | AES |  |  |  |  |  |  |
| DES |  |  |  |  |  |  |
| IDEA |  |  |  |  |  |  |
| BLOWFISH |  |  |  |  |  |  |
| CAMELLIA |  |  |  |  |  |  |
| CAST128 |  |  |  |  |  |  |
| GOST |  |  |  |  |  |  |
| RC5 |  |  |  |  |  |  |
| SEED |  |  |  |  |  |  |
| TWOFISH |  |  |  |  |  |  |
| SM4 |  |  |  |  |  |  |
| RC6 |  |  |  |  |  |  |
| SERPENT |  |  |  |  |  |  |
| TEA |  |  |  |  |  |  |
| 更多算法 |  |  |  |  |  |  |
| 更多架构 | AES |  |  |  |  |  |  |
| DES |  |  |  |  |  |  |
| IDEA |  |  |  |  |  |  |
| BLOWFISH |  |  |  |  |  |  |
| CAMELLIA |  |  |  |  |  |  |
| CAST128 |  |  |  |  |  |  |
| GOST |  |  |  |  |  |  |
| RC5 |  |  |  |  |  |  |
| SEED |  |  |  |  |  |  |
| TWOFISH |  |  |  |  |  |  |
| SM4 |  |  |  |  |  |  |
| RC6 |  |  |  |  |  |  |
| SERPENT |  |  |  |  |  |  |
| TEA |  |  |  |  |  |  |
| 更多算法 |  |  |  |  |  |  |

1. 面积、性能对比

这个对比是一般论文都会有的对比，也是杨博在汇报时提的要求。和论文中的对比会出现工艺对齐的问题，这些论文中都给出了阵列的门数，面积的对比有一定的参考意义。但是不同的工艺下性能是没有可比性的。

杨博只要求和清华目前的PE进行对比，这个是可以做到的，到时可以使用相同的工艺库进行综合。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 架构 | 本文 | | | 项目中的架构 | | | Cyptoraptor | | |
| 工艺/nm |  | | |  | | |  | | |
| 主频/MHz |  | | |  | | |  | | |
|  | 算法映射面积/Mgates | 性能/Gbps | 性能面积比**/(Gbps/Mgates)** | 算法映射面积 | 性能 | 性能面积比 | 算法映射面积 | 性能 | 性能面积比 |
| AES |  |  |  |  |  |  |  |  |  |
| DES |  |  |  |  |  |  |  |  |  |
| IDEA |  |  |  |  |  |  |  |  |  |
| BLOWFISH |  |  |  |  |  |  |  |  |  |
| CAMELLIA |  |  |  |  |  |  |  |  |  |
| CAST128 |  |  |  |  |  |  |  |  |  |
| GOST |  |  |  |  |  |  |  |  |  |
| RC5 |  |  |  |  |  |  |  |  |  |
| SEED |  |  |  |  |  |  |  |  |  |
| TWOFISH |  |  |  |  |  |  |  |  |  |
| SM4 |  |  |  |  |  |  |  |  |  |
| RC6 |  |  |  |  |  |  |  |  |  |
| SERPENT |  |  |  |  |  |  |  |  |  |
| TEA |  |  |  |  |  |  |  |  |  |
| XTEA |  |  |  |  |  |  |  |  |  |
| SKIPJECT |  |  |  |  |  |  |  |  |  |
| SPECK |  |  |  |  |  |  |  |  |  |
| SIMON |  |  |  |  |  |  |  |  |  |
| LUCIFER |  |  |  |  |  |  |  |  |  |
| 更多算法 |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 架构 | ProDFA | | | RCPA | | | CORBA等更多架构 | | |
| 工艺/nm |  | | |  | | |  | | |
| 主频/MHz |  | | |  | | |  | | |
|  | 算法映射面积/Mgates | 性能/Gbps | 性能面积比**/(Gbps/Mgates)** | 算法映射面积 | 性能 | 性能面积比 | 算法映射面积 | 性能 | 性能面积比 |
| AES |  |  |  |  |  |  |  |  |  |
| DES |  |  |  |  |  |  |  |  |  |
| IDEA |  |  |  |  |  |  |  |  |  |
| BLOWFISH |  |  |  |  |  |  |  |  |  |
| CAMELLIA |  |  |  |  |  |  |  |  |  |
| CAST128 |  |  |  |  |  |  |  |  |  |
| GOST |  |  |  |  |  |  |  |  |  |
| RC5 |  |  |  |  |  |  |  |  |  |
| SEED |  |  |  |  |  |  |  |  |  |
| TWOFISH |  |  |  |  |  |  |  |  |  |
| SM4 |  |  |  |  |  |  |  |  |  |
| RC6 |  |  |  |  |  |  |  |  |  |
| SERPENT |  |  |  |  |  |  |  |  |  |
| TEA |  |  |  |  |  |  |  |  |  |
| XTEA |  |  |  |  |  |  |  |  |  |
| SKIPJECT |  |  |  |  |  |  |  |  |  |
| SPECK |  |  |  |  |  |  |  |  |  |
| SIMON |  |  |  |  |  |  |  |  |  |
| LUCIFER |  |  |  |  |  |  |  |  |  |
| 更多算法 |  |  |  |  |  |  |  |  |  |

* 1. 本章小结

1. 总结与展望

Hütter, Markus, Johann Großschädl, and Guy-Armand Kamendje. "A versatile and scalable digit-serial/parallel multiplier architecture for finite fields GF (2 m)."*Information Technology: Coding and Computing [Computers and Communications], 2003. Proceedings. ITCC 2003. International Conference on*. IEEE, 2003.

Cordella, Luigi P., et al. "A (sub) graph isomorphism algorithm for matching large graphs." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 26.10 (2004): 1367-1372.