面向分组加密算法的可重构阵列处理单元优化与设计

摘要

随着科技水平不断发展，人们生活的需求越来越复杂，各种新型应用层出不穷。它们普遍具有运算复杂度高、处理数据量大等特点。在这种背景之下，可重构计算技术应运而生。可重构计算同时兼顾了通用处理器与 ASIC 的优点，既保留了通用处理器的灵活性，也具有 ASIC 的高效性，能够比较好地满足众多复杂应用的计算需求。与此同时，随着计算机技术和网络通信技术的发展，信息安全问题也逐渐成为人们关注的社会问题，密码技术是保证信息的可用性、机密性和安全性等安全要求的基本手段。密码算法是各种安全应用的基础，也是信息系统安全性的根本所在，高效灵活的密码算法是各种高性能信息系统的重要指标和基本保障，因此成为信息安全领域的重要课题。密码算法应用常常需要处理较大的信息量，或具有较大的计算强度，往往是各种通信系统中计算密集型环节，影响整个系统的吞吐率。可重构计算技术在处理此类应用上表现出巨大的优势，既保证了系统的高性能又具备应用必须的高灵活性。近年来，可重构密码处理器已成为研究热点，为了适应密码算法应用不断提升的性能需求，可重构阵列规模也在逐渐增加，阵列架构内功能单元冗余数量多、利用率低的问题日益凸显，严重影响了整个系统的面积效率（性能面积比）。

本文针对可重构阵列架构功能单元冗余数量多，利用率低，整体面积效率不高的问题，通过算法算子次序特征和算法映射反馈设计两方面消除密码可重构 PE 阵列中的冗余功能单元，提高算法映射时的功能单元利用率，从而提升整个系统的面积效率。整个研究过程分为四个主要阶段：第一阶段为算法特征分析，提取分组密码算的设计特征，为后续架构设计提供依据，第二阶段为初始架构设计，第三阶段为架构建模，第四阶段为基于算法映射的反馈优化。

第一阶段：算法特征分析，选取 36 种比较常用分组密码算法作为算法研究对象，为分组密码算法建立了统一的有向图节点网络图模型，其中图中的顶点表示算法中的运算，边表示算法中各个运算间的数据依赖。基于这个图模型采用图关键路径算法提取了与架构设计相关的算法算子模式特征、组合特征和次序特征，这些算法算子特征为本文后续的架构设计提供依据；

第二阶段：确定初始架构，根据提取的算法算子模式特征、组合特征和次序特征分别确定 PE 初始设计中的功能单元设计、功能组合设计和功能拓扑分布设计，进而确定整个 PE 阵列的拓扑结构，PE 组结构，PE 结构、互连结构以及六类功能单元结构。其中次序特征通过算子在密码算法轮函数表现出来的整体位置信息指导阵列中功能单元的分布设计，这种按需分布的设计方式减少了部分功能单元在 PE 阵列中的数量，与同构架构相比，一个 PE 组中减少了 8 个 S 盒单元，8 个有限乘法单元和 8 个置换单元。第二阶段确定的初始架构同时也作为后续算法映射反馈优化设计的基础模板架构；

第三阶段：架构建模，对可重构阵列架构建立有向节点网络图建模，其中图中的顶点表示架构中的 PE，包含 PE 在架构中的位置信息和功能信息，图中的边则模拟架构中的互连单元，同时架构中的功能单元和互连单元被参数化，这样可以很方便地完成架构的调整，便于后续的架构探索。这个架构图模型一方面作为一个超图，算法图可以这个超图中完成匹配映射，另一方面，参数化的功能和互连模型可以很方便地对架构调整验证，完成架构后续的探索优化。

第四阶段：基于算法映射的反馈优化，在第一阶段和第三阶段分别完成了对算法和架构的有向节点网络图建模，使算法和架构有了一个统一的图分析模型，因此可以很方便地使用图论中的匹配算法来对架构设计进行探索。本文通过分析算法在可重构 PE 阵列上映射的问题模型，将算法映射问题归纳为类似子图同构问题，通过对 VF2 子图同构算法中双射条件的修正，成功将该算法应用到算法图到架构图的映射中，完成目标算法集合中的算法图到架构超图的映射。本文对多种算法在初始架构中的映射结果进行了统计分析，总结了 PE 阵列中各个功能单元的利用率，找出冗余功能单元和低利用率单元，对于冗余单元，直接将其在 PE 阵列中消除，对于低利用率单元则进行消除验证实验，去除了 PE 阵列中部分低利用率的功能单元。相对初始 PE 阵列方案，映射反馈消除了初始架构中的 5 个算术单元，5 个移位单元，6 个逻辑单元和 1 个置换单元，加上第二阶段中根据次序特征减少的 8 个 S 盒单元，8 个有限乘法单元和 8 个置换单元，和同构的架构相比，各类功能单元优化比例在 41.7%~75%之间，总体优化比例为 56.9%。

在确定了最优的 PE 阵列结构设计后，本文对该设计进行了电路实现，使用 Verilog HDL 语言描述了该 PE 阵列，使用 Synopsys 公司的 Verilog Complier Simulator（VCS）工具进行功能和时序仿真，通过设计的功能验证。基于 TSMC 40nm CMOS 工艺标准单元库对 PE 设计进行逻辑综合，生成面积、时序等参数。对架构进行了算法映射分析，完成了 30 个比较常用的分组密码算法的映射分析，根据映射的结果计算出这些算法在 PE 阵列上的性能、面积和面积效率。

最后，将本文设计的 PE 阵列结构与同类型的分组密码可重构架构 Cyptor、RCPA、COBRA 和 RPU 进行了对比，分别对比了多种密码算法在这些架构上映射后的功能单元利用率和整体面积效率。本文设计的 PE 阵列结构算法平均功能单元利用率为 25.5%，平均面积效率为 171.7Gbps/mm^2。与其它面向分组密码算法的可重构阵列架构相比，平均功能单元利用率提高了 83.2%~168.5%，平均面积效率提高了 57.1%~643.5%。

关键词：可重构系统，分组密码算法，冗余优化，子图同构，算法映射