FPGA和基于FPGA的HPC平台

——国防科大2020年高性能评测与优化课程小组讨论

报告人： 王翊鹏 齐新新

指导：龚春叶、甘新标、杨博

日期： 2020.03.30

目 录

需求分析

- **FPGA (Field Programmable Gate Array)**
  - FPGA是可重构器件的典型代表，开始是作为ASIC（特殊应用集成电路）的一种半定制电路而出现，现在已成为一种新兴的算法加速部件，通过利用FPGA提供的并行性加速各种算法的执行。

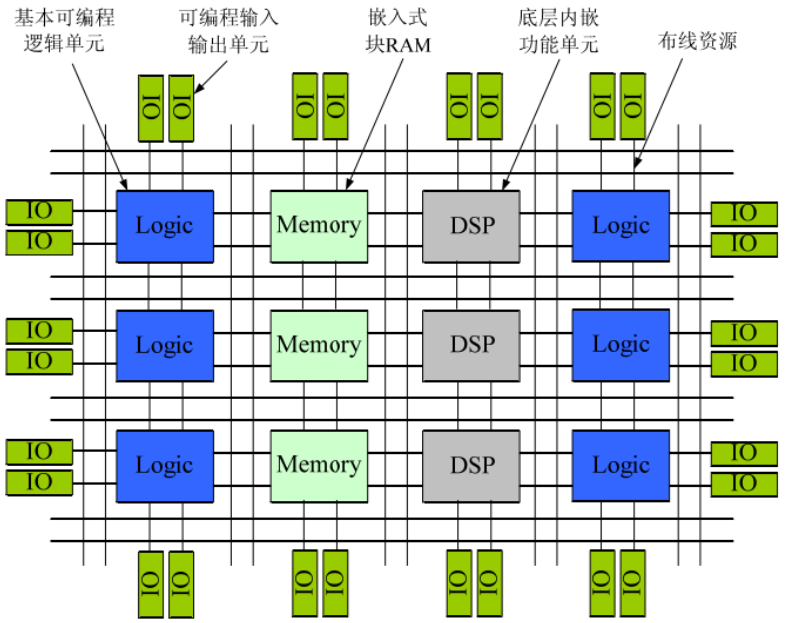

Fig1. FPGA器件的内部结构

需求分析

- **FPGA的基本特点**
  - 采用FPGA设计ASIC电路，用户不需要投片生产，就能得到合用的芯片。
  - FPGA可做其它全定制或半定制ASIC电路的中试样片。
  - FPGA内部有丰富的触发器和I / O引脚。
  - FPGA是ASIC电路中设计周期最短、开发费用最低、风险最小的器件之一
  - FPGA采用高速CHMOS工艺，功耗低，可以与CMOS、TTL电平兼容。

需求分析

- **FPGA 的优点**
  - FPGA可以实现乘法器、寄存器、地址发生器等硬件电路。
  - FPGA可通过使用框图或者Verilog HDL来设计，降低了设计难度
  - FPGA可无限地重新编程，加载一个新的设计方案只需几百毫秒，利用重配置可以减少硬件的开销。
  - FPGA的工作频率由FPGA芯片以及设计决定，可以通过修改设计或者更换更快的芯片来达到某些苛刻的要求

动机

- **FPGA应用于HPC加速**
  - FPCA计算平台的功耗较低，且具有灵活的可编程性。
  - FPGA提供了根据算法描述配置硬件构建块的灵活性。
  - 现代的FPGA提供了专用的算术模块、大量的逻辑资源和存储资源，以及外部存储器接口、网络接口和其它外围接口，可以参与构建高性能计算系统。
  - FPGA的能耗很低，通常情况下，FPGA开发板能耗的峰值小于30W。

动机

- **应用FPGA加速的HPC系统**
  - Maxwell-FPGA
  - Janus2
  - Cray XD 1

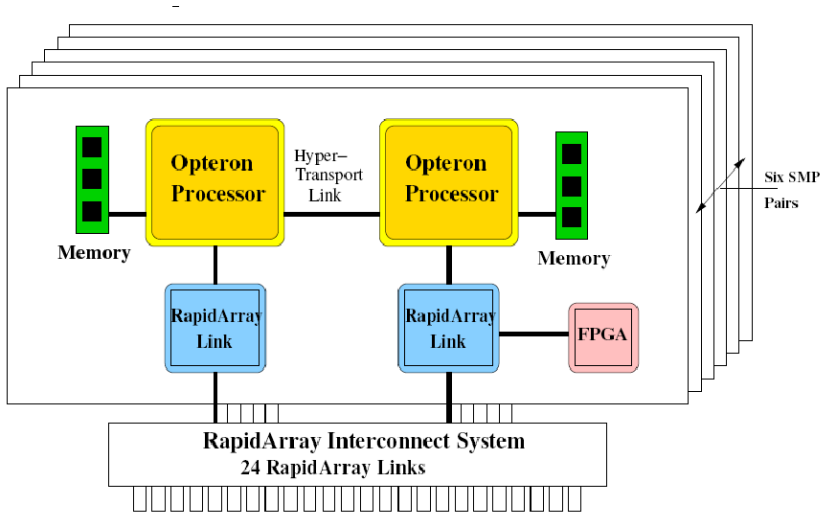

Fig2. Cray XD1系统结构

动机

- **示例——FPGA应用于AES算法的密码分析**
  - 密码分析研究的是如何在密钥未知的情况下恢复明文，由于其**包含大量并行计算**。然而，现实情况是，由于**通用CPU的设计需要权衡性能、功耗、体积、通用性等诸多因素，其计算能力很难满足此类新兴应用的需求**。
  - FPGA作为一种有前途的解决方案，可以**进一步提高计算速度**，从而解决这一问题。
  - 一个定制的HPC平台由多个FPGA组成，其中计算分布在多个FPGA之间，以实现所需的处理能力。

设计方案

高级加密标准(AES)算法

- 具有128位密钥的AES算法对排列在4×4字节阵列中的128位明文执行10轮相同的操作。第1-9轮包括替换字节、移位行、混合列和添加轮键操作，而最后一轮仅包括替换字节、移位行和添加轮键操作
- 对于解密，使用以相反顺序应用的轮密钥来执行相同的操作集。

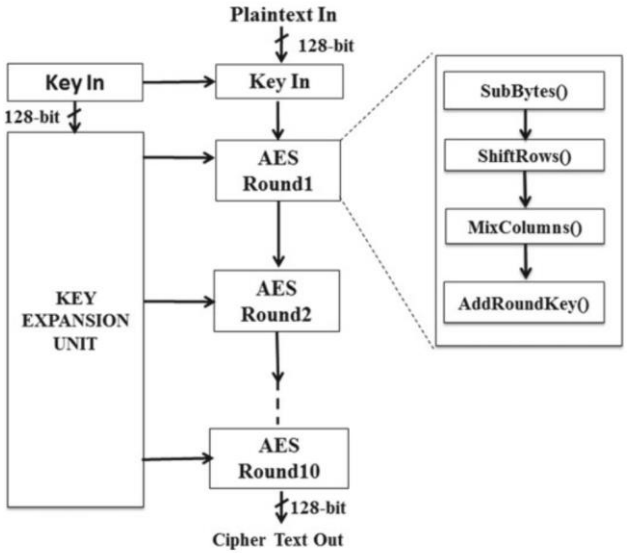

Fig4. AES加密算法

设计方案

- **FPGA-based HPC平台设计**
  - HPC平台由**四个Spartan6（XC6SLX150）FPGA**器件组成，它们以mesh（网状）拓扑连接。
  - 图中所示的HPC平台HPC平台包括使用PEX8311芯片的PCI-Express接口，用做主机PC和目标设备之间的接口。Spartan6（xc6slx150-2fgg900）FPGAs具有低成本，低功耗的特点，提供高达150k的逻辑单元，与主机接口需要集成的PCI-Express块。

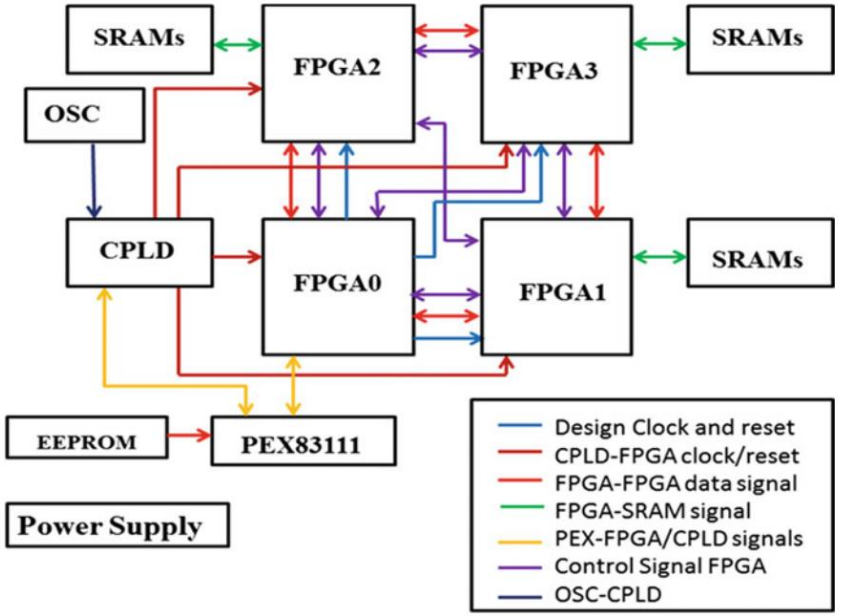

Fig3. HPC平台设计

设计方案

AES密码分析的行为体系结构设计

- 在缺乏数学突破的情况下，穷举或暴力搜索密钥是唯一有效的密码分析技术。暴力攻击指计算所有可能的密钥，直到找到正确的密钥。AES算法的密钥长度为128位，**暴力搜索需要2^128次计算**。
- 为了满足计算量大的要求，提出了一种**并行可扩展的AES密码分析体系结构**。该体系结构由四个AES密钥搜索引擎组成，分别在4个FPGA中实现。

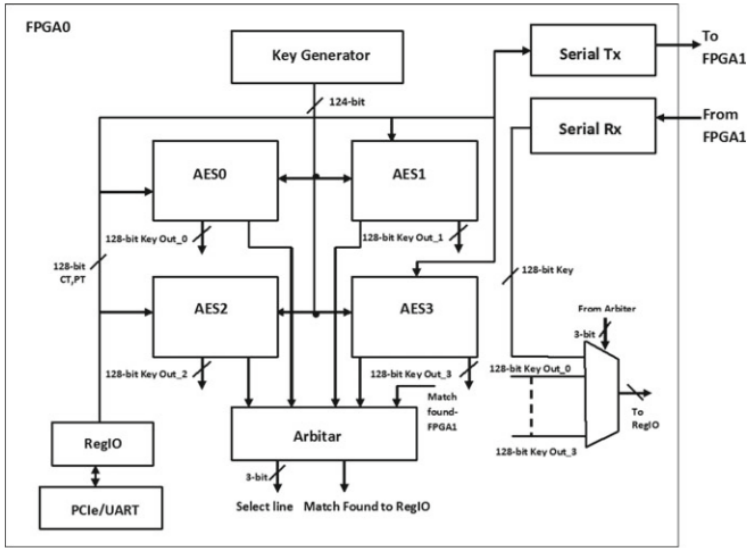

Fig4. AES密码分析的行为体系结构设计

效果

- **AES暴力攻击复杂度降低**
  - 128位密钥的上两位用作设备ID以选择板上四个FPGA中的一个。接下来的两位用于选择密钥搜索引擎的四个实例之一。下124位表示每个密钥搜索引擎要执行的计算范围。
  - 这种格式实际上是将整个2^128密钥空间划分为16个子空间，**每个子空间执行2^124次计算**，从而使得暴力攻击的计算复杂度从2^128减少到2^124.随着计算复杂度的降低，探索密钥空间所需的时间也减少，从而减少了进行密码分析的时间。

Bit numbers		
127 126	125 124	123 0
Device Id	No. of Instances	Bits representing Computational complexity
2-bits	2-bits	124-bits

Fig5. 密钥生成器的帧结构

分析

- **FPGA的局限性**
  - FPGA与主机的通信开销较大
  - FPGA编程与调试困难
  - FPGA缺乏高性能科学计算软件库
  - 软件库nvGraph以及集群通信软件库NCCI等虽然在FPGA上均有实现，但各实现的数据表示、计算过程和性能优化存在较大差异

分析

- **目前开发基于FPGA的算法加速器存在的问题**
  - 开发新的算法加速器仍然沿用传统寄存器传输(RTL)级硬件设计方法，效率不高
  - 以应用为中心，相互隔离，缺乏统一方法和工具，难以实现算法加速器资源共享与复用
  - 硬件结构的优化不好

下一步研究方向

- 降低FPGA与主机的通信开销
- 提高其可编程性
- 完善FPGA上基本的高性能计算软件库

参考文献

1. 贾迅,钱磊,邬贵明,吴东,谢向辉.FPGA应用于高性能计算的研究现状和未来挑战[J].计算机科学,2019,46(11):11-19.
2. 倪时策. 面向密码应用FPGA高级综合关键技术研究[D].国防科学技术大学,2014.
3. 邬贵明. FPGA矩阵计算并行算法与结构[D].国防科学技术大学,2011.
4. Baxter R , Booth S , Bull M , et al. Maxwell - a 64 FPGA Supercomputer[C]// Nasa/esa Conference on Adaptive Hardware & Systems. IEEE Computer Society, 2007.
5. Thomas Steinke, Estela Suarez, Taisuke Boku, Nalini Kumar, and David E. Martin.Using FPGAs to Accelerate HPC and Data Analytics on Intel-Based Systems
6. Harshali Zodpe and Ashok Sapkal. FPGA-Based High-Performance Computing Platform for Cryptanalysis of AES Algorithm
7. The Janus Collaboration.Janus2: an FPGA-based Supercomputer for Spin Glass Simulations.
8. Wang, C., Lou, W., Gong, L., Jin, L., Tan, L., Hu, Y., Li, X., Zhou, X.: Reconfigurable hardware accelerators: opportunities, trends, and challenges (2017). arXiv preprint arXiv:1712.04771 .
9. Todman, T.J., et al., Reconfigurable computing: architectures and design methods. IEE Proceedings-Computers and Digital Techniques, 2005. 152(2): p. 193-207.

感谢观看！