Project题目

设计一款MIPS处理器设计并用AES-128加密算法验证其设计

Project实验报告提交截止时间2022年6月17日，占总分25%

FPGA实验室地点：电工电子中心EDA实验室-西主楼4区209室 （电话62771932）
FPGA实验时间：第11周（5月6日）—第14周（5月27日），每周五第四大节（共4次）（3：20—17：50）ktq18@mails.tsinghua.edu.cn

一、 实现一个5级流水MIPS处理器，要求如下：

1. 支持的指令：

（1）访存指令：lw，sw 指令，必选。

（2）算术逻辑指令： add，addi，addiu，sub，and，or，xor，andi，ori，xori，lui， slt，sll，srl指令，必选。

（3） 转移指令：beq，bne，j，jal， jr 指令，必选。

（4） 附件《mips32v2指令集.pdf》里有说明的其他指令，可选。

2. 支持的功能：

（1）支持数据相关检测处理（forwarding or bypass），必选；

（2）支持转移冒险处理（流水线冲刷），可选。（如不支持此项，在汇编时遇到转移指令必须手动插入空泡，保证程序正确执行）。

（3）异常和中断处理，可选。

(4) 课件或教参里面提及的其他功能，可选。

二、用自己的指令集完成一个AES-128加密算法(包含密钥扩展算法)的汇编，要求如下：

1. 功能：

要求编译和汇编完成后的指令能完整实现AES在128密钥长度下一个block的

加密功能（包含计算密钥扩展），AES相关文档见附件。

2. 参考测试向量：

明文：32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34

密钥：2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

密文：39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32

3. S盒的处理：

S盒采用查表实现，预先将附件《aes_sbox.txt》里面提供的S盒存在dcache里面，计算时根据地址查找。

三、将硬件代码和指令下载到FPGA开发板上测试：

1. 使用quartusII 综合、绑定管脚、下载：

将第二部分得到的指令放在icache.v中，将加密数据、密钥、S盒放到dcache.v中，结合第一部分代码，使用quartusII进行综合，绑定管脚并下载到开发板，具体流程参考《MIPS上机指导.pdf》。

2. 使用Signal Tap观测实际上板测试结果。

四、完成实验报告：

1. 提交5 级流水线的数据通路和控制通路结构图。
2. 提交实现的verilog 源码及其注释。
3. 提交AES汇编程序以及仿真测试结果，计算AES运算时钟周期数。
4. 交微处理器在FPGA的时延报告、资源报告、以及执行结果。

具体是在FPGA Quartus_II的Signal Tap AES执行结果相关寄存器的观测截图，及FPGA综合的时延报告、资源使用情况报告。

五、其他说明：

1. project限单人完成。
2. 请不要将任务拖到最后。