复旦大学微电子学院

2021~2022　学年第 二 学期期末考试试卷

☑A 卷 ☐　B 卷☐　C 卷

课程名称： 嵌入式处理器与芯片系统设计 **课程代码：** MICR130006，MICR130006.h

开课院系： 微电子学院 **考试形式：** 线上/线下考试（开卷）

姓名：_____ **学号：**_____ **专业：**_____

提示：请同学们秉持诚实守信宗旨，谨守考试纪律，摒弃考试作弊。学生如有违反学校考试纪律的行为，学校将按《复旦大学学生纪律处分条例》规定予以严肃处理。

（装订线内不要答题）

题号	1	2	3	4	5	6	7	8	总分
得分									

（以下为试卷正文）

一、简述题（48 分，共 6 小题，每小题 8 分）

1)　什么是指令集？简述 CISC 和 RISC 指令集的起源、发展和优缺点。

2) 简述近年来我国处理器领域的代表性成果，并简要分析学好集成电路知识能够为我国处理器相关产业的发展做出何种贡献。

3) 简述主要的处理器流水线冲突类型，并分别分析其产生原因。

4) 简述磁盘冗余阵列（RAID）的主要作用及 RAID0～RAID6 各个等级的主要特点。

5) 有一个处理器实现的 RISC-V 指令集为 RV64IMAFD，请解释 64 以及 I、M、A、F、D 具体代表什么含义。

6) 简述为什么流水线技术能够带来处理器性能的提升，并讨论是否可以通过不断加深流水线来获得更多的性能提升。

二、编程题（22 分，共 2 小题，第 1 小题 10 分，第 2 小题 12 分）

1) 已知等式如下图，其中 p、q、r 为指针，a、b、c 以及指针指向的数据都为 integer 类型变量，请基于 RISC-V 64 位指令集编写汇编代码实现等式右边的表达式（勿使用伪指令）。假定参数 p，q，r 分别存放在通用寄存器 x13，x14，x15，而 a，b，c 分别存放在通用寄存器 x6，x17，x16。

$$f = (-a + *p) \times \frac{(b - *q)}{(-c + *r)}$$

2) 若 C 程序中定义一函数 f 实现上一题中表达式的运算功能

```
int f(int *p, int *q, int *r, int a, int b, int c)
```

并通过上层母函数 wrapper 对这一子函数 f 进行调用

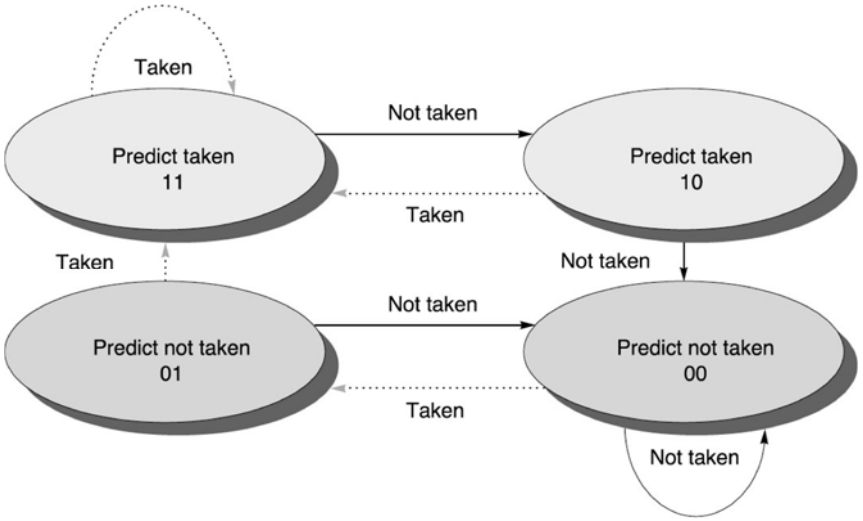
```
int wrapper(int *p, int *q, int *r, int a, int b, int c) {
    int aa, bb, cc, qq, pp, rr;
    aa = a + 1;
    bb = b + 1;
    cc = c + 1;
    qq = *q + 1;
    rr = *r + 1;
    pp = *p + 1;
    return f(&pp, &qq, &rr, aa, bb, cc);
}
```

假定参数 p，q，r 分别存放在通用寄存器 x13，x14，x15，而 a，b，c 分别存放在通用寄存器 x6，x17，x16，试将函数 wrapper 翻译为 RISC-V 64 位指令集编写的汇编代码（勿使用伪指令）。

三、综合题（30 分，共 2 小题，第 1 小题 12 分，第 2 小题 18 分）

1) 一个分支跳转（branch）成立和不成立的结果可以用“1”和“0”来表征，那么其一定时间内的若干次执行的结果就可以表示为如“111…000….111”一样的二值序列。

1. 考虑一个分支代码结构 if condition then S1 else S2。如果在代码运行过程中条件表达式 condition 为真和假的情况以交替的方式出现，那么请问 1-bit 分支预测器和 2-bit 分支预测器的预测准确率分别为多少？
2. 假设一个 2-bit 分支预测器的状态跳转图如下。



请你设计一个分支转移的二值序列使得 1-bit 分支预测器的准确度为 50%，而 2-bit 分支预测器的准确率在稳定状态下为 0。设想什么样的程序模式下会导致这样的二值序列？

3. 修改 2-bit 分支预测器的状态转移图使其针对你在第二个问题中设计的二值序列在稳定状态下能够达到 50%的准确率。
4. 请你设计一个分支转移的二值序列使得你在第三个问题中修改得到的 2-bit 分支预测器在稳定状态下的准确率为 0。设想什么样的程序模式下会导致这样的二值序列？

2) 处理器对内存的访问时间与各级缓存的命中情况密切相关，在一类基于“时间测量”的侧信道攻击中，攻击者程序可以通过监视共享缓存的命中状态来推断受害者程序曾访问过哪些缓存块，并因此得知受害者程序的访存地址。如果该地址依赖于秘密数据，将会造成严重的数据泄露。考虑如下的受害者程序的 C 代码片段：

```
char* array = (char*)0x40;
int sum = 0;
int secret = somevalue;
for(int i=0;i<64;i++){
    if(secret==0 && (i%11)==0) sum+=array[i%32];
    else if(secret==1 && (i%13)==0) sum+=array[i%32];
}
```

1. 考虑一个总容量 32 字节、直接映射、块大小 4 字节的 L1 缓存，缓存初始为空，程序基于物理地址进行访存操作。由程序代码可见，数组 array 的起始地址为 0x40，假定局部变量 sum、secret 和 i 均存放在通用寄存器内，若 secret 值为 0，则执行上述程序片段会访问哪些缓存块？缓存命中率为多少？
2. 现有一个与上述受害者程序共享同一个 L1 缓存的攻击程序，攻击流程为：第一阶段，攻击者先通过内存访问用地址 0xA0~0xBF 中的数据填满缓存。第二阶段，执行上述受害者程序。第三阶段，攻击者程序再次对某些内存地址进行访问，测量得以下地址的命中信息：

地址	是否命中？
0xAC	否
0xB8	否
0xBC	是

   根据上述命中信息和攻击流程，推断 secret 的值为多少并说明原因。
3. 改用一个总容量和块大小不变的 2 路组相联缓存，攻击的第一阶段和第二阶段保持不变。在第三阶段，如果攻击者仅能从 0xA0、0xA4、0xA8、0xAC、0xB0、0xB4、0xB8、0xBC 这几个内存地址中选择 2 个进行内存访问并测量命中情况，则选择哪 2 个地址可以让攻击者准确推断 secret 的值？请说明原因（假设缓存替换策略会优先驱逐被受害者程序占据的块，如果候选块来自同一程序则发生随机替换）。
4. 若改用全相联缓存，攻击者在第三阶段能否通过构造适当的内存访问地址推断 secret 的值？请说明原因。