



step2 如果当前进程时间片用完，则阻塞进程并寻找RUNNABLE的进程切换。如果当前进程被exit或阻塞则另找RUNNABLE的进程切换；

step3 如果需要切换，则用提供的代码进行进程切换。

### 3. kernel/kernel/irqHandle.c 中 void syscallFork() 函数

step1 代码段（pcb物理地址中内容）与数据段（pcb的stack中内容）拷贝；

step2 定义与父进程无关的stackTop、prevStackTop、state、timeCount、sleep-Time与pid等参数；

step3 保存父进程上下文，将regs中除eax的寄存器直接复制父进程的值；

step4 返回值放在寄存器eax中。此时父进程返回值（初值为-1）为子进程pid、子进程为0。

### 4. kernel/kernel/irqHandle.c 中 void syscallSleep() 函数

注意判断传入时间应大于零。

### 5. kernel/kernel/irqHandle.c 中 void syscallExit() 函数

### 6. kernel/kernel/irqHandle.c 中 void syscallExec() 函数

step1 根据syscallPrint()函数获得文件名存储在tmp字符串中；

step2 调用loadElf将文件加载至空闲内存；

step3 加载失败则return，成功则eip = entry。

### 7. kernel/kernel/kvm.c 中 void loadElf()函数

通过阅读loadUMain()函数，将程序头等初值赋0物理内存地址设为传入参数。在readInode函数执行中根据返回值判断是否读取文件成功，失败则返回-1。最终将entry的值赋值为uMainEntry返回0表示加载成功。

## 四、实验中遇到的问题以及解决方法

1. 在切换进程时，current应更新为 (current + i) % MAX\_PCB\_NUM。错误更新写成i导致切换进程错误。

2. 出现只打印父进程的情况。syscallFork中子进程返回值未设为0。

## 六、实验心得

通过对代码结构的理解，读懂每一个程序的含义及其起到的作用是顺利完成实验的关键。实验中需要对实验指南进行研读，并能积极的对一些功能进行实践，保持良好学习心态。这是健康的学习成长经历。