Report

范逍宇 2019013273

一、分支预测器的设计。

分支预测器包括两部分，分别是两位饱和分支预测器，用来预测是否跳转，以及目标地址缓冲器，用来保存每个 pc 对应的跳转目标地址。另外设置了记录 11 位历史信息的全局历史寄存器，根据历史跳转的 pattern 选择 PHT Entry。

每次判断是否跳转时，根据 GHR 查找 PHT，如果 PHT_Counter 的值为 0 或 1 ，则不发生跳转，预测地址为下一条指令的 Pc 地址。如果 PHT_Counter 的值为 2 或 3，则发生跳转，在 BTB 中查找当前 PC 对应的跳转地址，如果没有找到，则默认预测地址为下一条指令的 PC 地址。

在更新时，先根据是否跳转更新 GHR，如果不发生跳转，则将对应的 PHT_Counter 减一，如果发生跳转，则将对应的 PHT_Counter 加一，同时更新 BTB，如果在 BTB 中找到了当前 PC，则更新其目标地址，否则，新增 BTB_Entry，替换策略为先入先出。

PHT 和 BTB 各占一半储存空间（忽略 GHR 占用的地址空间），因为程序具有空间的局部性，大部分情况下跳转的距离不会太长，因此 BTB 中只存储 pc 的后 16 位。

二、测试用例说明。

考虑到编写的测试程序应该接近真实场景的应用程序，应该具有一般程序的特性，而不应该随机地进行跳转，所以这里实现了快速排序算法，对 100 个整数进行排序和输出到命令行，因为实际的程序中会经常用到排序算法或者打印信息的功能。这 100 个整数为使用线性同余生成的随机数，程序一共执行了 2001 次分支指令。

三、问答题。

（1）比较ARM A64指令集和你熟悉的一种指令集，说明两者各自的优势和不足。

与 RISC-V 进行比较。
在寻址方面，RISC-V 只有一种寻址方式，而ARM A64 有五种寻址方式，寻址更加灵活。
RISC-V 指令集更加简单，指令更容易通过硬件实现，但同时对编译器提出了更高的要求，需要编译器具有较强的优化能力。

（4）请阅读Nailgun攻击论文第III节，说明为何ARM调试架构是不安全的。

对于非入侵式调试模式，运行在低特权级的程序可以通过PMU和ETM获得高特权级的信息。
对于入侵式调试模式，低特权级的处理器可以通过 ECT 令处于任意特权级的处理器进入调试模式；目标处理器在执行指令以及获取资源时，不会考虑调试器的特权级；dcps 指令可以让处于调试模式的目标处理器进入任何高优先级，它就能访问高优先级的资源，并将敏感资源泄露给调试器。

（6）Linux内核模块与用户进程的数据交互方式有哪些？请介绍三种以上的方法。

系统调用：系统调用时内核提供给应用程序的接口。应用程序发出系统调用请求进入内核态，在内核态处理完请求后返回用户态，实现内核与用户的数据交互。
Netlink：netlink是一种在内核与用户应用间进行双向数据传输的异步通信方式。
sysctl：通过sysctl，用户应用可以在内核运行时来改变内核的配置参数，也可以在任何时候获得内核的配置参数。