3. (1) 位0 (V)：有效位(Valid)。如果为1，表示条目有效可访问。如果为0则无效

位1 (R)：读权限(Read)。如果为1，可读取该页内容。如果为0表示不可读取

位2 (W)：写权限(Write)。如果为1，可写入该页内容。如果为0不可写入

位3 (X)：执行权限(Execute)。如果为1，表示可执行该页内容。如果为0表示不可执行

位4 (U)：用户/特权位(User/Supervisor)。如果为1，表示用户态可访问该条目。如果为0，只有特权态可访问

位5 (G)：全局(Global)如果为1，表示该页可以在多个地址空间共享。如果为0，则只能在当前地址空间使用

位6 (A)：访问记录(Accessed)：如果为1表示被访问过，否则为0

位7 (D)：修改记录(Dirty)：如果为1，表示被修改过，否则为0

(2) 会导致：

(2.1) 安全问题：用户进程可能修改自己的页表，打破系统安全性

(2.2) 可靠性问题：用户进程修改了自己的页表，导致页面不一致，可能出现内存泄漏或崩溃等问题。

(2.3) 性能问题：用户进程修改自己页表，破坏原有映射关系，导致程序出错，降低程序性能

(3) 表不能被读写、执行。

4. (1) PMP控制寄存器的X/W/R位用于进一步细化对物理内存域的访问权限控制。具体作用如下：

(1.1) X位：指定该物理内存区域是否允许执行指令。如果为1允许执行，为0反之

(1.2) W位：用于指定该物理内存区域是否允许写入数据。如果为1，允许写入，为0反之

(1.3) R位：用于指定该物理内存区域是否允许读取数据，如果为1，允许读取，为0反之

这些位可以与页表目中的X/W/R位进行交叉验证，以对物理内存访问权限进行更严格控制

(2) (2.1) L位：用于指示该PMP配置寄存器是否被锁定。如果L位为1，表明设置是锁定，不可修改；如果为0可修改

(2.2) A位：用于指定该PMP配置寄存器是否与物理地址匹配。如果A为1，表该PMP配置寄存器与物理地址进行匹配。为0反之，

通过设置L位，可保证PMP配置寄存器设置不被篡改，提高安全性。

通过设置A位，可选是否对物理地址进行匹配，如果不进行匹配，则该PMP配置寄存器的权限设置将应用于整个物理内存空间

5. (1) 对一个完整64位的虚似空间，需管理2^{64}个字节的虚拟地址，即$2^{64}/4KB = 2^{52}$个页面，需$2^{52}\times 8 = 2^{55}$字节空间来存储页表。这个大小约为4PB，不适合现代计算机系统

(2) $(2^{48}/2^{12})\cdot 2^8 = 2^{44}$个字节

(3) 虚拟地址区域被分为多个较小区域，每个区域对应一个级别的页表。这样，只有实际使用部分需分配页表条目，节省存储空间。也通过把不常用条目放级别较低的页面，减少频繁访问的页表条目数目