# 系统事件记录

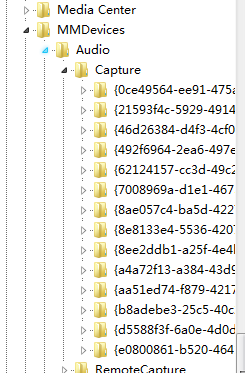
可以使用微软官方的程序ProcessMonitor来记录计算机操作系统各个进程下的事件。但需要注意的是一定要控制进程的数量，仅仅是很少的时间，产生的记录数量可能也会达到100MB+。之后就是大海捞针一样的搜索。



上图是一个设备插入计算机直到播放插入声音开始。

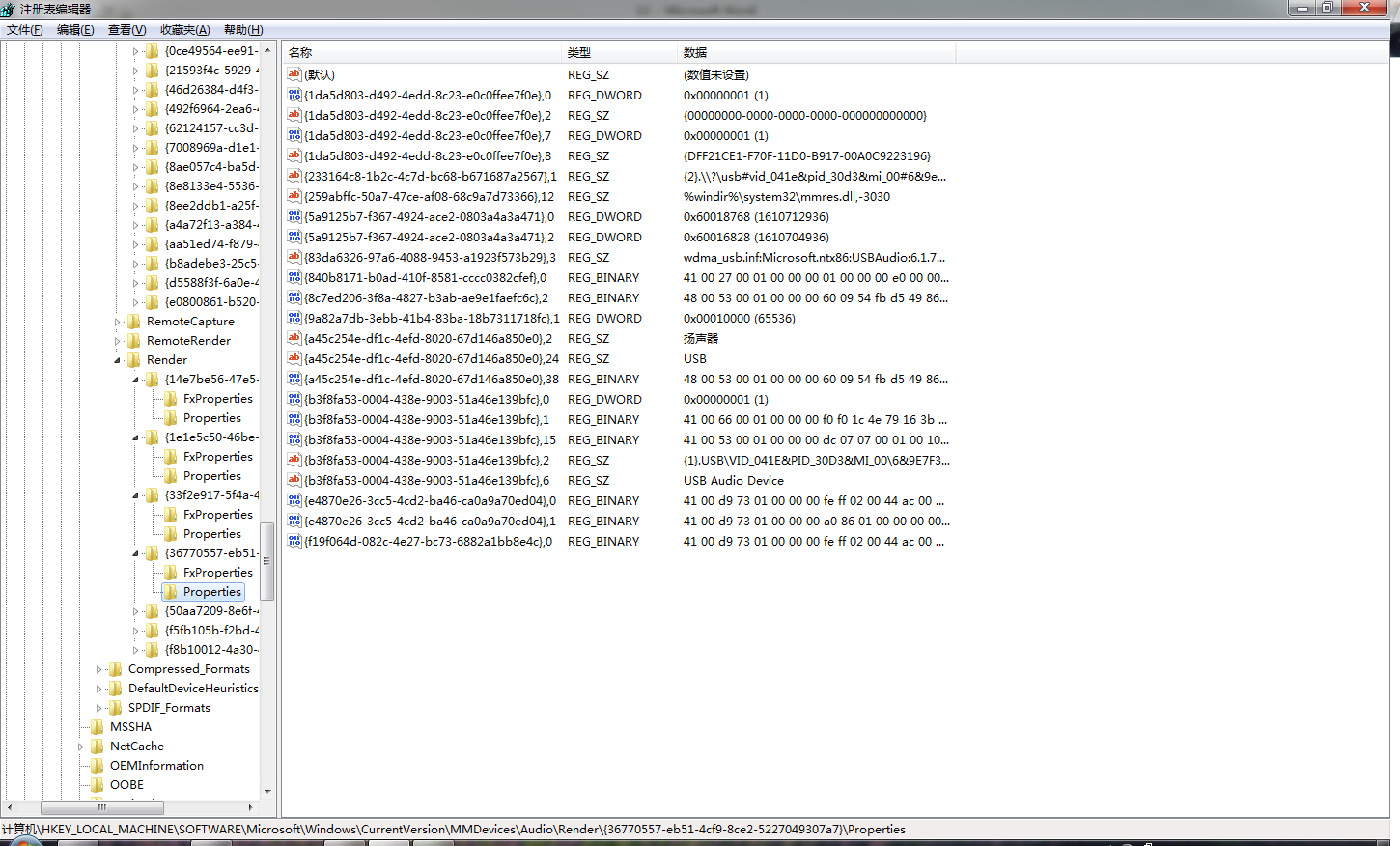


路径很有价值，里面是很多的GUID。



这里的GUID应该代表的是各种设备。

<http://answers.flyppdevportal.com/categories/metro/csharpvb.aspx?ID=02a0ad0c-dbf6-4533-8369-c4174949654e>



在子键中有更加详细的内容，比如说接口类型，还有Friendly Name。

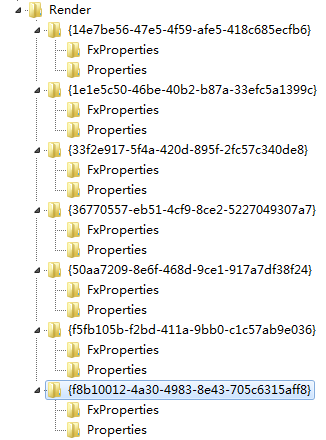
可以看到以下的键值存储的是USB多媒体设备的生产生信息。





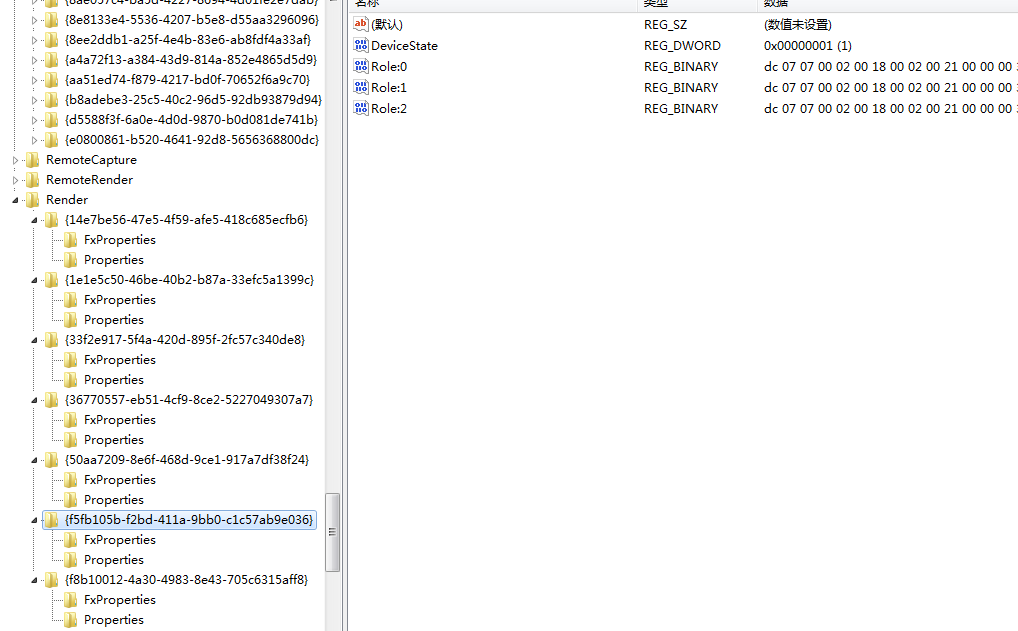
两个设备有所不同，分别对应的是不同的USB声卡。

可以看到注册表中，一共有

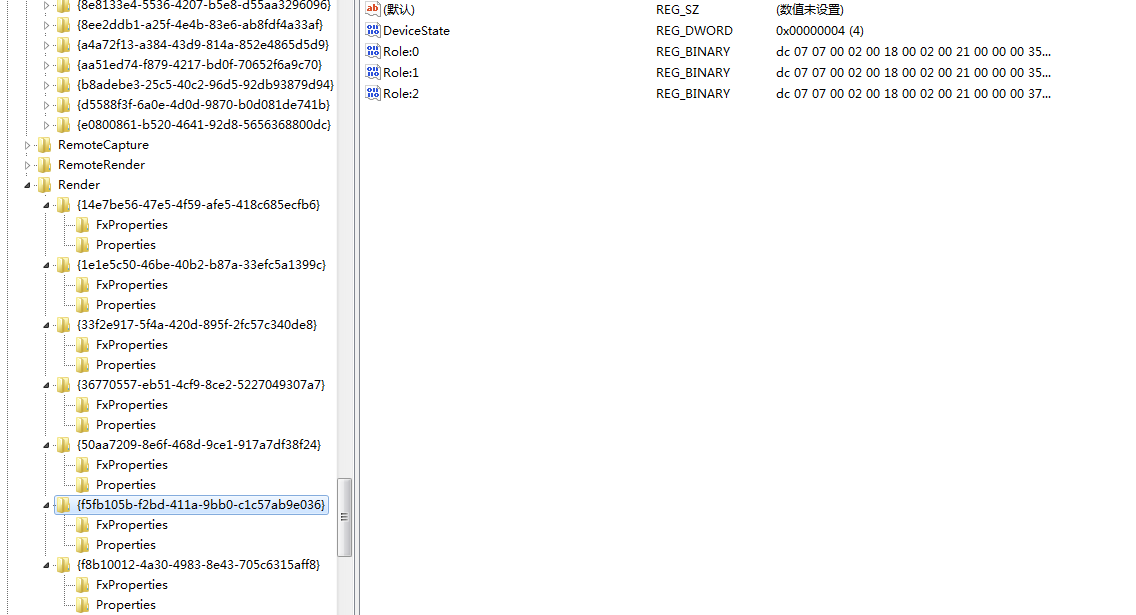


七个播放设备，其中只有前两个的State键值为1，推测应该是启用的意思，剩下的设备的State全部都是4。

现在实验测试插入声卡之后，默认设备改变的情况下，看State键值会变成什么样子。



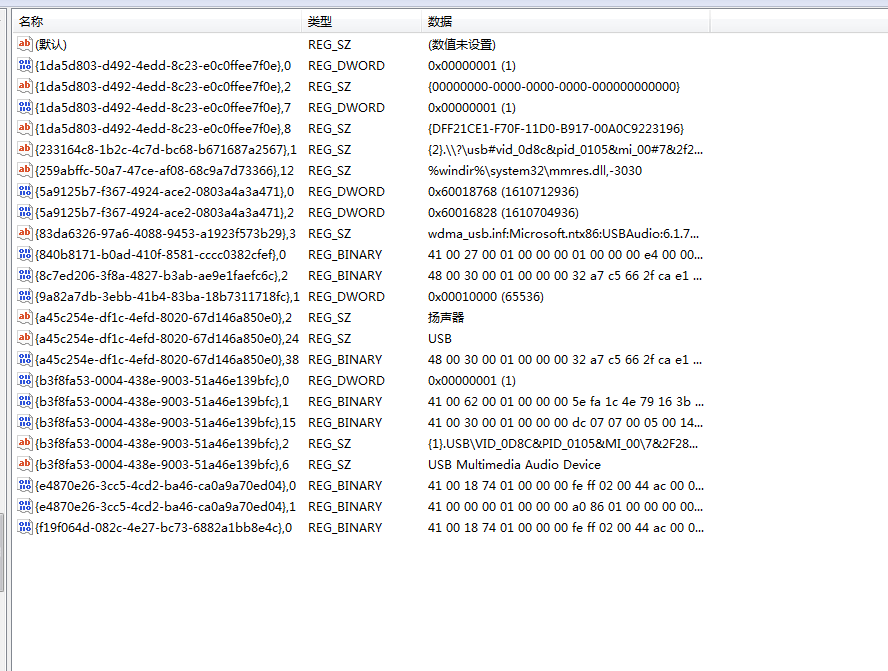
设备的State键值变为了1，其他的没有变化。再移除设备查看。

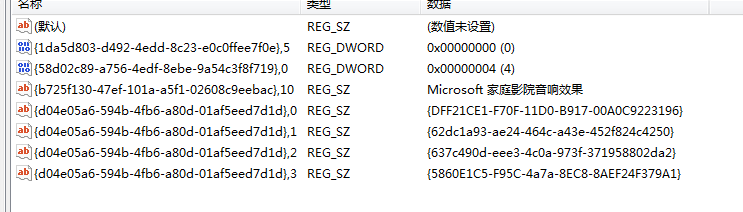


有变回了4。

之后查看调整Level带来的结果。

其子键情况如图所示：





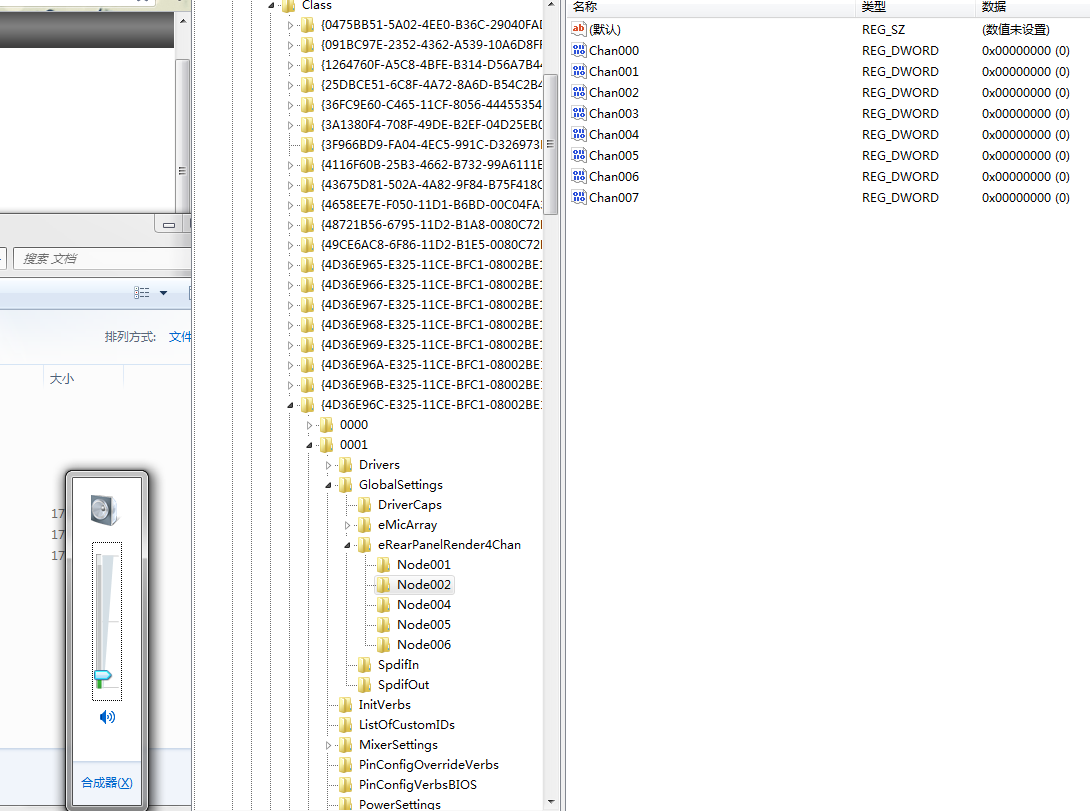
关于Device的Role可以参考网站：

<http://msdn.microsoft.com/en-us/library/windows/desktop/dd316556(v=vs.85).aspx>

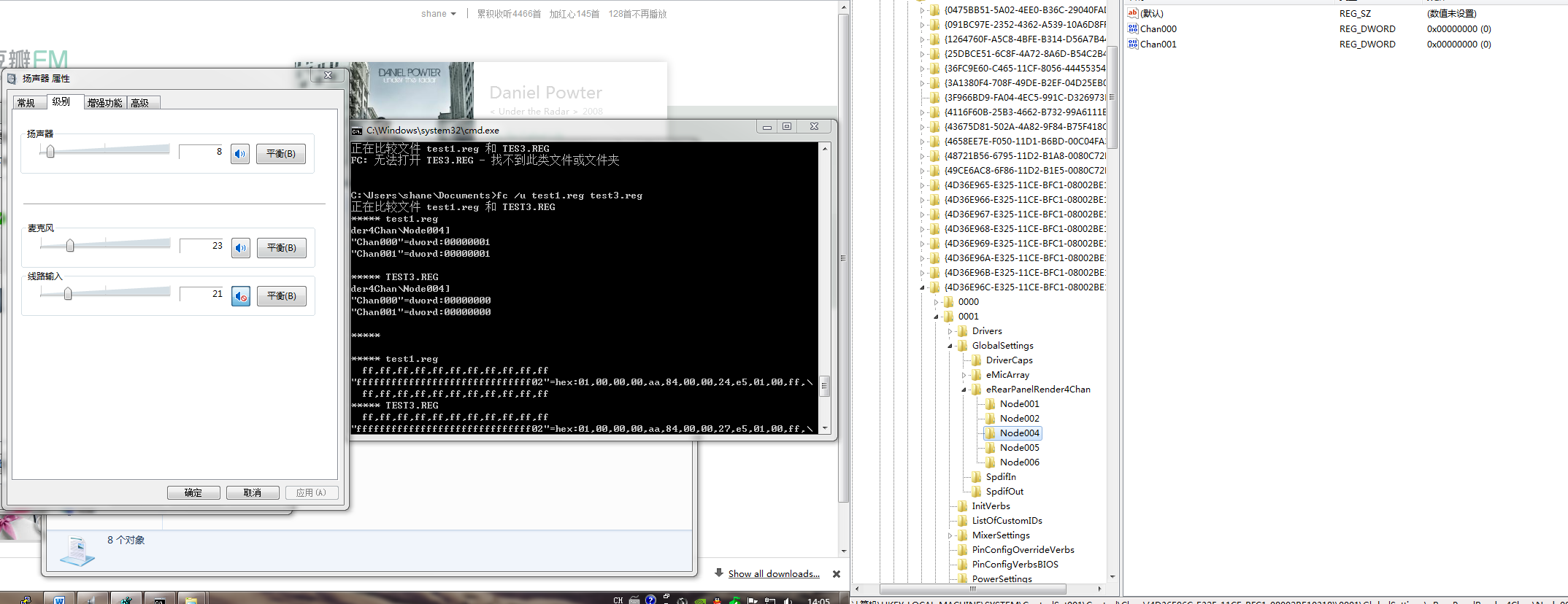
<http://msdn.microsoft.com/en-us/library/windows/desktop/dd370813(v=vs.85).aspx>

在系统中可以使用fc /u进行注册表的比对。

可以通过对比得出

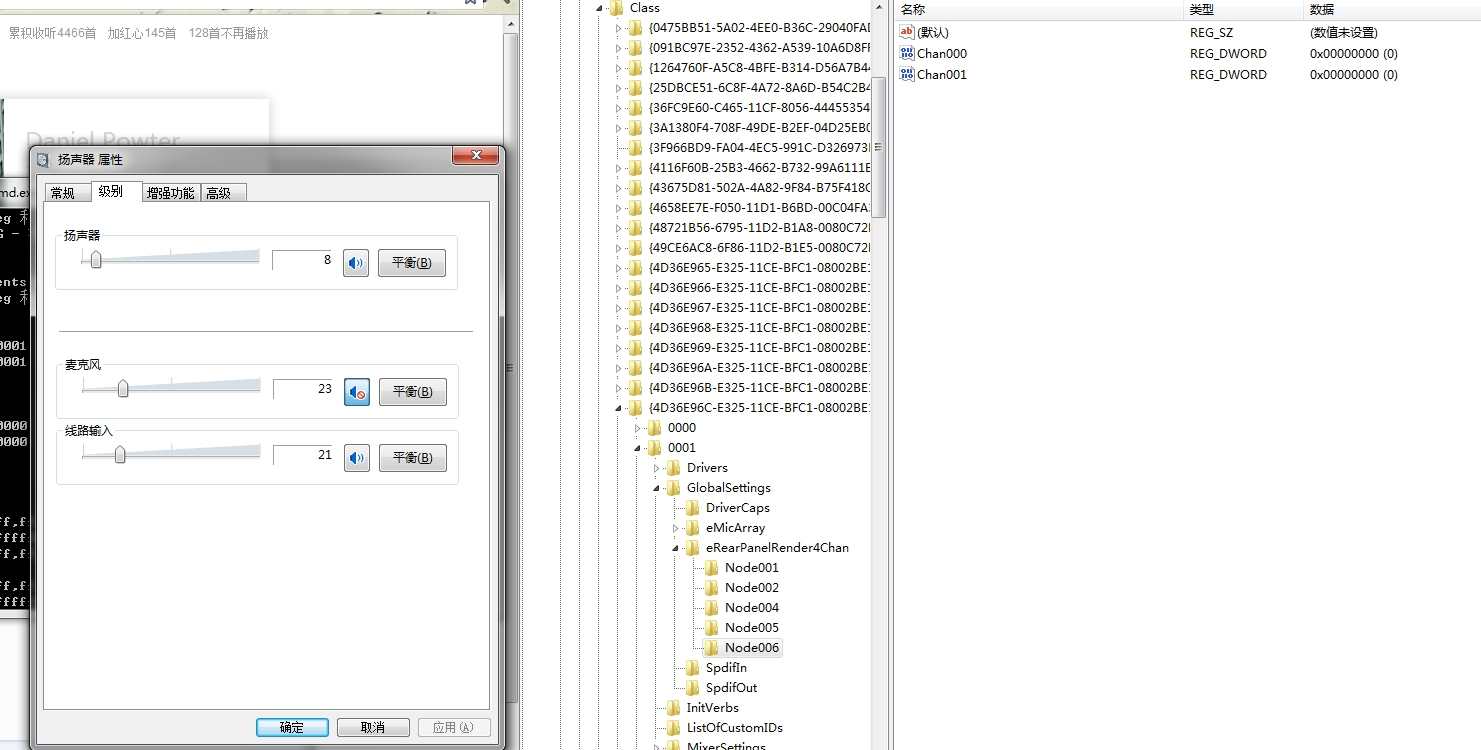


以上的节点对声音的控制有关系。



开关有关项。

线路对应



已经麦克风分别对应不同的选项。

