PCIE 扩展 ROM 控制芯片 CH366

硬盘和网络安全隔离卡方案

版本： 1

http://wch.cn

1、概述

安全隔离卡用于将普通计算机分为安全环境（内网）和开放环境（外网），内网和外网使用不同的硬盘并且连接到不同的网络，从而能够避免硬盘中的重要数据通过网络等方式泄露。一般的双网卡方案、多重引导卡或者多用户管理卡只是在逻辑层提供硬盘数据隔离，而硬盘和网络安全隔离卡的特点主要是在物理层提供硬盘数据隔离，确保更高的数据安全性。

现有的技术方案主要是单网卡、双硬盘物理切换隔离，通常都需要在启动时选择内网或者外网，这些选择界面和切换操作通常由扩展 ROM 中的启动程序完成。

2、用户的功能需求分析

① 用户需要在开机后选择将使用内网的安全环境，还是外网的开放环境，所以安全隔离卡应该能够在开机时向用户提供选择界面，而且应该是在 DOS 或者 Windows 等操作系统引导之前。

② 当用户选择完后，安全隔离卡需要执行内外网的环境切换，也就是说，需要在选择界面（软件）与隔离卡切换电路（硬件）之间建立通讯。

③ 当启动时切换选择后，必须确保不能在 Windows 等系统的运行过程中被黑客无意或者恶意的切换，否则将导致硬盘数据不完整以及数据通过外网泄露，所以安全隔离卡需要一个切换锁定装置。当隔离卡在启动时切换完成后，必须锁定防止再被切换，直到关机或者重启才能解除。

④ 美观需求。早期产品是从计算机后壳引出电线接一个电器开关到桌面，由用户随时拨动开关，所以就很难做到美观，也不完全，容易无意中碰到，完全不象一个高科技的 IT 产品。

⑤ 方便性和智能化，体现在软件功能上。新式的隔离卡通常采用扩展 ROM 程序，根据用户的使用习惯提供仿 Windows 中文界面和智能提示，以及个性化的启动图片。

⑥ 方案的统一性和可升级性。同一方案既能支持 PATA 并口硬盘，也能支持 SATA 串口硬盘，便于批量采购和备货，便于简化售后服务。

⑦ 软硬件的兼容性，由所采用的技术方案而定。例如，IDE 接口只用于硬盘和光驱产品，当前的 UDMA133 硬盘工作在 133MHz 高频上,如果通过拦截硬盘 IDE 接口获取扩展 ROM 发出的切换指令，那么就会增加 IDE 接口的负载，对于更高速度的 SATA 接口则问题更严重，很容易产生主板兼容性问题，或者影响硬盘数据的传输速度，好的技术方案应该尽量采用成熟的标准化技术，例如通过 PCI-Express 总线的 I/O 端口获取扩展 ROM 发出的切换指令。

3、我们的技术方案

根据上述分析，可以采用 PCIE 扩展 ROM 专用控制芯片 CH366Q，主要是考虑：

① CH366 具有支持锁定的控制输出引脚，可以实现切换锁定，防止被 WINDOWS 下的黑客应用软件意外切换导致数据泄密。

② CH366 可以预置切换信息，支持在下次开机时或者重新启动时自动加载，方便在 WINDOWS 下进行切换。即先在 WINDOWS 下预置，再在重启时执行切换，防止立即切换导致死机。

③ CH366 支持睡眠和唤醒，可以设定在关机后数秒内自动重新开机，通过关机来清空内存中的数据，避免遗留在内存的的重要数据在切换后被带到外网。

④ CH366 提供 Flash-ROM 闪存，支持在线擦写，便于在用户端远程升级，容量从 64KB 到 1MB，可以记忆用户上次的选择，也可以记忆进入内网时所需的密码，或者保存产品序列号等。

⑤ CH366 支持扩展 ROM，并且可以使用厂家随芯片提供的免费授权使用的 BRM 程序库，基于 BRM 程序库和参考样例，设计出个性化的选择界面将非常容易。

⑥ CH366 具有 I/O 端口读写功能，不需要拦截硬盘数据就可以在标准的 PCIE 总线上获得扩展 ROM 发出的切换指令，用于在合适的时间点实现内外网络环境切换和判断。

⑦ CH366 提供了常用的串行通讯扩展接口，能够方便地与单片机或者 CPLD/FPGA 交换数据，对产品进行加密或者解密。

⑧ CH366 是 CH364 芯片的升级版本，继承了 CH364 的优点并做了改良。

另外，真正的安全性必须是在公开技术方案后仍然保持原来的安全性，基于 CH366Q 设计的安全隔离卡，由于通过 I/O 端口获取切换指令并且采用切换锁定技术，所以，在公开技术方案的情况下，依然能够保持原来的安全性，而不怕任何恶意的黑客程序和病毒。

总之，与通用芯片相比，CH366 在隔离卡应用方面，更加专业、更加安全、综合成本更低。

4、基本原理图

由于 CH366Q 是专用的扩展 ROM 控制芯片，所以除了 CH366 芯片组之外，无需其它任何芯片，只要外加物理切换器件即可，不但提高了性能，而且综合成本更低。

完整的物理切换电路请参考隔离卡评估板的技术资料光盘。

U3 是 CH364F 芯片，用于存放扩展 ROM 程序，支持在线擦写随时升级。由于内外网络切换和锁定指令只需要两条 I/O 指令，加上启动选择界面等部分后，扩展 ROM 程序仍然很小，CH364F 的剩余空间可以用于存放图片界面等，以及用于记忆用户的使用习惯，保存进入内网时的安全密码等，隔离卡厂家也可以用其保存产品序列号、扩展 ROM 的启动模式、工作模式等。CH364F 可以提供 64KB、128KB、256KB 甚至 1MB 的容量，默认为 64KB 容量。

U4 是 24C02 或 24C04 等芯片，该芯片是可选的，用于提供产品信息 ID，并记忆上次关机或者重启前的切换状态，便于下次冷复位、开机电源上电时自动恢复上次的切换状态。由于 EEPROM 芯片的可擦写次数更多，所以比 U3 更适宜存储需要频繁修改的数据，例如记忆当前切换状态。

跳线 J1、J2 是可选器件，由用户根据需要设定跳线，从而使扩展 ROM 卡采用不同的启动模式、工作模式等。当前的 BRM 子程序库默认是使用 GPI2 引脚即 J2 跳线选择启动模式，所以 J2 不宜用于其它用途。而预留的 GPI1 引脚即 J1 跳线可以由应用程序自行定义其用途，默认的隔离卡源程序将插上 J1 定义为临时禁止扩展 ROM 程序，解决调试过程中因为程序失误而无法进入系统的问题。

三级管 T1 是继电器的功率驱动电路，并联的二级管和电容是针对继电器等电感性负载的安全保护和抗干扰措施。如果实际需要切换的网络线和硬盘线比较多，那么可以采用多个双刀双掷的继电器，其驱动控制端并联后由 T1 进行驱动。三极管和二极管的驱动电流都不能小于所有继电器吸合所需驱动电流的总和。由于继电器消耗电流较大，建议实际电路对继电器独立供电。

对于网络信号切换，由于需要电隔离，建议使用继电器。对于硬盘信号切换，除了可以选择两只双刀双掷的继电器之外，也可以将继电器换成高速且低阻的模拟开关芯片，以节约成本。例如含有四只 SPDT 单刀双掷模拟开关的 CH440 芯片。

5、切换的工作原理

开机后，U1 内部自动解锁，隔离卡进入准备状态。U1 的 SW1 引脚被置位为高电平，三极管控制继电器选择内网。

当扩展 ROM 接收到用户的选择后，首先通过 I/O 读取当前切换状态，不匹配则通过 I/O 端口向 U1 发出切换选择，U1 控制 T1，由 T1 控制继电器选择内网或者外网。

当内外网切换和配置参数保存操作完成后，扩展 ROM 程序通过 I/O 端口向 U1 发出锁定指令，U1

的 SW1 引脚输出状态将保持不变直到重新启动，隔离卡进入锁定状态。

在 WINDOWS 下的切换工具也可以向 U1 预置重启后的切换状态，如果未预置，则默认值是仍然保持为当前切换状态。

当计算机重新启动时，PERST#信号线使 U1 自动切换到之前预置的切换状态，并且 U1 内部自动解锁而进入准备状态，从而可以由扩展 ROM 程序验证预置的切换状态或者重新选择网络环境。验证通过后扩展 ROM 程序应该锁定 U1，确保直到重新启动才能再次切换。

锁定操作分为独立的两种，一是锁定切换操作，二是锁定在线编程和配置存取。前者是指锁定后无法再次切换，防止在使用过程中被意外地切换。后者是指锁定后无法在线升级扩展 ROM 程序以及存取配置参数，防止被意外或者恶意改写。

当内外网的硬盘参数不同时，切换网络环境后必须重新启动。为了防止重启后扩展 ROM 程序再次要求用户进行选择，可以在 U1 中设置一个标志，当重启后扩展 ROM 检测到这个标志则在锁定状态后直接引导操作系统，而不必再出现选择界面。

如果使用 CH366 的 SW1 引脚作为切换控制输出，那么 I/O 端口 CH366_SW_CTRL 的字节数据中：位 1 是当前实时切换状态；位 3 是预置的重启后的切换状态；位 4～位 6 为应用程序可定义的内部标志位，其数据不受重启影响。进入锁定状态后，位 1 将不再接受新写入的数据，但是可以向位 3 写入新的切换状态，该状态只能在重启时才能生效，并且将被重启后的扩展 ROM 程序验证。

I/O 端口 CH366_IO_GPO 的字节数据中：位 3 是在线编程和配置存取的锁定状态，位 4 是切换操作的锁定状态。

6、扩展 ROM 程序设计

以下是与硬件相关的切换和锁定等部分 C 语言程序，IO_BASE_ADDR 由 BRM 提供。

```
ctrl_port = IO_BASE_ADDR + CH366_SW_CTRL;
lock_port = IO_BASE_ADDR + CH366_IO_GPO;
```

① 读取当前切换状态和锁定状态（假定 SW1 高电平时选择内网）

```
s = inportb ( ctrl_port )
if ( s & 0x02 ) { 正在内网 }
else { 正在外网 }
if ( inportb ( lock_port ) & 0x10 ) { 正在锁定状态 }
else { 正在准备状态，没有锁定状态 }
```

② 设定新的切换状态和锁定状态（假定继电器不吸合为外网）

```
if ( 需要选择内网 ) { s = 0x0F; }
else { s = 0x05; }  /* 选择外网 */
outportb ( ctrl_port, s );  /* 设定切换状态 */
if ( 需要锁定状态 ) { outportb ( lock_port, inportb ( lock_port ) | 0x10 ); }
```

③ 读写 I^2C 接口的串行 EEPROM 芯片 24Cxx

请参考 BRM 子程序_CH363_I2C7_BYTE_R 和_CH363_I2C7_BYTE_W 及 CH363_I2C7_BLK_R 等

④ 读写 Flash-ROM 闪存

请参考 BRM 子程序_CH364_FLASH_READ 和_CH364_FLASH_WRITE 及_CH364_FLASH_ERASE 等

为了加速和简化扩展 ROM 程序设计，CH366 还可以提供与之配套的 BRM 应用子程序库，其中包括 800x600x256 色仿 Windows 中英文图形界面程序库、图片显示程序库、硬盘文件读写操作程序库、Boot-ROM 启动程序库、数据解压缩程序库、字符串处理程序库、杂项程序库，这些子程序都能够在 BIOS 环境下运行，无需 DOS 等操作系统，另外，还可以提供与之配套的多国语言字库提取工具等。基于专业的 BRM 程序库设计隔离卡的扩展 ROM 程序将非常简单，可以不需要考虑主板兼容性，不需要考虑硬盘存取、中英文图形显示等各种底层 I/O 操作。相关说明也可参考 CH36x 通过 Boot-ROM 进行

BIOS 扩展的方案。

7、隔离卡评估板

双硬盘隔离卡评估板套件包括：

一块隔离卡样品。

技术资料光盘，包括：隔离卡样板的电路原理图和 PCB 印制板图；
BRM 子程序库 V4.X（支持 800x600x256 色）；
隔离卡扩展 ROM 源程序；
WINDOWS 环境下的切换工具的源程序。

本样品的扩展 ROM 是基于 BRM V4.X 程序库开发，支持 800X600X256 色图形界面。

本样品的 ASM 源程序是 CH366ISL\SOURCE 目录下的 CH366ISL.ASM

CH362BRM 目录是 BRM 程序库，BRM40 是 BRM V4.0，支持 800X600X256 色图形界面。

扩展 ROM 程序开发环境需要 TASM 3.0 和 TLINK 2.0，可以调用批处理程序 BRM40.BAT 进行字库提取、编译、链接、压缩，最终生成 BIN 目标文件，可以直接用在线编程工具 CH364PGM 写入 CH364F 芯片。如果因为程序失误导致无法进入系统，那么可以在跳线 J1 上加短路块使其临时禁止程序，等进入系统后再去掉 J1 及重新编程，但是该功能可以在源程序中被屏蔽掉。

例如：BRM40 CH366ISL 执行后，如果没有错误提示，则直接产生 BIN 文件。

如果需要插入图片数据，那么参考源程序中的说明，先压缩再用 DEBUG 工具合成。

单硬盘隔离方案主要依赖于硬盘自身安全特性和 BRM 程序库中提供的相关子程序，而其硬件更为简单，当然也可以直接使用双硬盘隔离卡的硬件，单硬盘隔离方案主要包括另外一套扩展 ROM 源程序。

其它技术细节请联系我们的技术支持人员。

8、常见问题解答

使用隔离卡之后，除了每次开机或者重启后需要选择内网或者外网之外，所有的软件安装包括操作系统安装都与未安装隔离卡之前一样。

样品的启动选择菜单中提供了“内网”、“外网”、“设置”三个选项。如果内外网的两个硬盘参数不同，请务必进入“设置”选中“切换后重新启动”的复选框，这样，切换内外网时计算机会自动重启后再进入；如果两个硬盘参数完全相同，可以不必选中该复选框，除非在使用过程中检查出有影响。隔离卡会记忆该控制项和当前选择。

在 CH366ISL\WIN 目录下提供了在 WINDOWS 下控制网络切换的工具程序及其源程序。

如果在菜单下按 ESC 键可以看到说明，再按空格键可以看到图形菜单界面。图形界面与仿 WINDOWS 菜单界面的功能相同，实际产品可以只提供其中一种用户界面。

因为已经连接了两个硬盘，为了防止过载和提高可靠线，请不要将光驱等设备与硬盘连接在同一个 IDE 接口上，实际上目前几乎所有计算机都是将硬盘与光驱分别接在主板的两个 IDE 接口上的。建议将硬盘也就是隔离卡接在主板的第一个 IDE 接口上，而将光驱等设备接在主板的第二个 IDE 接口上。所有 PATA 硬盘线都应该使用 80 芯硬盘线，并且要注意 80 芯硬盘线是有方向的，硬盘端仍然接硬盘，主板端仍然接主板。对于 SATA 硬盘，则全部使用标准 SATA 硬盘线，最好是短线。

如果插卡后没有出现隔离卡的界面。个别主板可能会有这个问题，请在 CMOS 中修改引导控制项“BOOT FROM LAN 或者 NETWORK”，或者“BOOT FROM OTHER DEVICE”，或者“TRY OTHER DEVICE”、或者“FIRST BOOT DEVICE”中选择“SCSI”或者“OTHER”等。

如果插卡后启动不正常，或者找不到硬盘，请尝试在跳线 J2 上加短路块。

如果使用隔离卡后，硬盘数据会出错，请检查硬盘线，或者缩短硬盘信号线，或者检查“高级设置”中的“切换后重新启动”选项是否选中。

如果产品不稳定，挑主板、挑 PCIE 和 PCI 插槽、挑硬盘，那么可能与 PCB 布线有关。PCB 布线的设计要点如下：

① 除非规范有特殊的长度要求，否则所有信号线都必须尽可能地短。过长的走线有可能导致不稳定等兼容性问题或者数据传输速度下降。
② 主要信号线上的过孔 VIA 必须尽可能地少，尤其是 PCIE 和 SATA 的成对信号线。
③ 要避免信号线互相缠绕，避免锐角和直角走线。
④ PCIE、SATA、PATA 等硬盘信号线布线时必须考虑阻抗匹配问题。
⑤ PCIE 信号线是成对的高频信号，应该参考 PCIE 规范和 PCIE_PCB.PDF 布线。SATA 硬盘信号线也是成对的高频信号，应该参考 SATA 规范布线。高频信号周边及背面尽量用地平面保护，附近不宜有频繁变化的其它信号线。
⑥ PCI 时钟线 CLK 和 PATA 硬盘控制信号线 IOR/IOW 以及数据线也需要考虑与周边信号的相互干扰问题。
⑦ 关键信号线两侧可以用 GND 地平面保护，以减少对外的干扰和来自外部的干扰。
⑧ 应该保留足够的 GND 地平面铺铜，GND 上多加 VIA 过孔连接。
⑨ 考虑到最好的效果，也可以将硬盘信号线的切换单独做成一块板，放置在主板和硬盘之间，从而能够将硬盘信号线更大程度的缩短。如果购买的硬盘线较长，可以将其截短。

第一次使用隔离卡时，因为有些数据区域未使用过，所以会出现内部数据无效的提示，隔离卡程序会自动进行初始化，有可能会有一些正常提示。