计算机键盘电磁信息泄漏及其防护研究

王利涛，郁　滨
（解放军信息工程大学 电子技术学院，郑州 450004）

摘　要： 在研究 PS/2 键盘控制模块的时钟与数据信号接口电路结构特征的基础上，利用电路等效的方法研究了键盘电磁泄漏发射与信息还原机理，通过测试实验验证了该方法的有效性；进一步提出了两种电磁泄漏防护方式，具体设计了一种电磁泄漏防护方案。实验测试结果表明，该方案能够有效抑制键盘的电磁发射，防止按键信息通过电磁发射被还原。

关键词： 电磁信息泄漏；信息安全；下降沿；安全防护
中图分类号： TP309.7　　**文献标志码：** A　　**文章编号：** 1001-3695(2012)07-2708-04
doi:10.3969/j.issn.1001-3695.2012.07.084

Study on electromagnetic compromising emanations of computer keyboard and its protection

WANG Li-tao, YU Bin
(*Institute of Electronic Technology, The PLA Information Engineering University, Zhengzhou* 450004, *China*)

Abstract: This paper studied the circuit structure characteristic of data and clock signal interface in the PS/2 keyboard's control module. On this basis, it used the method of equivalent circuit to research the electromagnetic compromising emanations and its information recovery mechanism, the effectiveness of which was test and verified by a later measurement experiment. Furthermore, it proposed two different ways of security protection, and designed a shielding protection method against compromising emanations of keyboard. It is demonstrated by the result of the experiment that electromagnetic emission of keyboard is suppressed effectively and good protection effect against keystroke recovery is reached.

Key words: electromagnetic compromising emanations; information security; falling edge; security protection

0　引言

近年来，网络安全问题日益突出，病毒、木马及各种形式的网络攻击已经成为人们广泛关注的信息安全问题。然而电磁信息泄漏伴随信息设备的运行一直存在，时刻威胁着各类电子设备的信息安全，但由于其隐蔽性而未得到人们广泛的认识。事实上，电磁信息泄漏已成为信息安全的短板，并已形成了严重的安全隐患。

电磁信息泄漏指电子信息设备因电磁发射而引起的信息安全保密问题[1]。自 20 世纪 80 年代 Eck[2] 还原 CRT 显示器画面的公开实验开始，不断有国内外学者开展计算机视频信息的电磁发射分析还原及安全防护研究[3~7]。尤其是剑桥大学 Kuhn[4,5] 对显示设备电磁发射的系列研究，成功恢复还原了 CRT 显示器以及 LCD 等平板显示器显示的图像信息，从工程和技术层面验证了计算机视频设备存在的电磁信息安全威胁，并提出了基于软件方法进行电磁窃密和防护的 Soft-Tempest 技术。日本学者 Tosaka 等人[8,9] 对激光打印机的电磁发射进行了实验研究，通过接收打印机输出端产生的电磁发射，还原了打印内容，证实了激光打印机的电磁信息泄漏风险。Smulder[10] 对早期通过 RS-232 协议进行信号传输时的电磁发射强度与特性进行了研究，使用改造的收音机接收并成功还原了线路中传输的数据，表明有特征的数字信号可以通过电磁发射被精确地接收还原。

对常用的计算机键盘而言，无论是 PS/2、USB 或是笔记本键盘，都是检测击键位置并进行编码，然后将按键编码传送给主机。阵列扫描与编码传输都存在电磁发射，这些发射与按键（位置或编码）信息相关，有可能通过分析检测还原出键盘输入信息。针对计算机键盘的电磁发射，20 世纪末就有研究者进行了测试分析[3]，由于技术水平特别是测试仪器的灵敏度和精度的限制，按键的信息还原一直都没有取得突破性进展。直到近几年，瑞士学者 Vuagnoux 等人[11,12] 对键盘的电磁发射进行了研究，通过获取键盘全频段的电磁发射原始信号并进行后期处理，成功还原了键盘的击键信息。张静勤[13] 在其硕士论文中描述了对键盘电磁泄漏的研究，重点比较分析了不同测量距离下天线接收到的键盘电磁发射信号，并对 PS/2 键盘按键输入信息的还原进行了研究。但是，Vuagnoux 和张静勤没有分析 PS/2 键盘产生特殊电磁发射的根源及信息泄漏的机理，且均未给出有效的电磁泄漏防护方案。

针对 PS/2 键盘，本文对其结构组成、控制电路工作原理以及 PS/2 协议过程进行了深入研究，分析了电磁发射与按键信息存在关联的原因，研究了依据信号跳变沿的发射来还原击键信息的可行性，利用等效电路方法分析了时钟与数据信号接口的 NPN 型三极管电路结构，通过键盘电磁发射接收信号确定

收稿日期： 2011-12-03；**修回日期：** 2012-01-17

作者简介： 王利涛（1983-），男，河南许昌人，博士研究生，主要研究方向为信息安全、电磁信息泄漏与防护（tor.3769@163.com）；郁滨（1964-），男，教授，博导，博士，主要研究方向为网络安全、视觉密码等.

时钟与数据的电平序列,恢复了传输的按键扫描码。依据泄漏机理的分析,对电磁信息泄漏防护的措施与方式进行了研究,提出了一种易于实施的屏蔽式防护方案。

1　电磁信息泄漏机理

PS/2 键盘接口能更好地支持计算机底层硬件,在计算机故障时具有更好的兼容性,依然是应用最广泛的一类键盘。本文即针对 PS/2 键盘进行研究,其按键编码采用第二套扫描码表[14]。键盘产生电磁泄漏发射需满足三个方面的条件,即与按键输入关联的发射源、天线效应部件以及允许电磁波通过的介质。键盘电子器件和金属部件均可作为天线发射电磁波,本文重点研究泄漏发射源。

1.1　泄漏发射源确定

PS/2 键盘采用双向同步串行协议,控制电路的数据与时钟信号输出均采用集电极开路方式,其电路结构如图 1 所示。数据与时钟信号常态为高电平,即在没有信号传输时保持 +5 V高电平;当主机发送键盘控制命令时,微控制器通过 A、B 端口读取;当向主机输出按键编码时,在端口 D、C 写入逻辑 1 可将数据或时钟信号拉低。尽管此电路已在一些 PS/2 键盘中以集成电路方式实现,但这种集电极开路的基本电路结构依然存在,相应的电路特征也被保持下来。

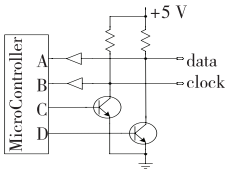

图1　键盘输出的集电极开路电路

电路的动作过程是:当数据或时钟信号由逻辑 1 变为 0 时,在 D 或 C 端口写入 1,基极电压达到导通门限,NPN 型的双极型三极管(BJT)进入集射极导通状态,集电极电流疾速上升,即在数据或时钟的下降沿处产生瞬态冲击电流,信号具有极短的下降沿时间;而当数据或时钟信号由逻辑 0 变为 1 时,端口 D、C 被写入 0,此时集射极截止,集电极电流减小为 0,该过程数字信号的上升沿较缓。

由天线发射原理、键盘内各天线效应部件的有限尺寸决定 PS/2 键盘对高频信号或信号高频分量具有较强的辐射能力,而对低频部分则辐射很弱。同时,由实际梯形数字信号的傅里叶变换分析得知,影响数字信号高频频谱分量的关键参数是上升沿和下降沿持续时间,跳变沿时间短的信号具有更丰富的高频分量。由此可见,PS/2 键盘跳变沿持续时间短的信号下降沿位置将产生更强的电磁发射;相应地,从时域接收角度分析,将更多地接收到陡峭跳变沿位置的发射信号。因此,PS/2 键盘存在从电磁发射的时域接收信号中区分跳变沿位置的可能,亦即键盘控制模块 NPN 型 BJT 电路所生成的数字信号经由天线效应部件产生的电磁发射与按键输入信息相关,控制模块成为 PS/2 键盘电磁泄漏的一个重要发射源。

1.2　信息还原机理分析

信号下降沿位置丰富的高频分量决定其产生更强的电磁辐射,相应地可接收的电磁发射就高于上升沿。如果从天线和仪器接收的电磁发射时域信号中不能分辨信号下降沿的发射,也将无法区分出上升沿发射,无助于键盘信息恢复,不作讨论。不妨假设可从中分辨出信号下降沿位置的电磁发射,则根据信号上升沿电磁发射可否从时域接收信号中与背景电磁噪声相区别,分以下两种情况进行分析:

a)可以从时域接收信号中分辨出上升沿的电磁发射。不失一般性,依据 PS/2 协议数据与时钟信号的时序关系,给出按键‘M’按下时的时序及电磁发射,如图 2 所示。时钟序列由周期性间隔相同的方波组成,其跳变沿的位置间隔相同,因此容易从发射信号中分辨出来。根据图 2,数据的下降沿与紧接着的时钟下降沿将形成两个连续的较高脉冲,而数据上升沿与紧接着的时钟下降沿形成两个连续的较低能量脉冲发射,其他情形无连续的发射脉冲,因而可以根据发射的脉冲序列还原出时钟与数据信号的电平状态变化,从而还原所传输的按键扫描码。

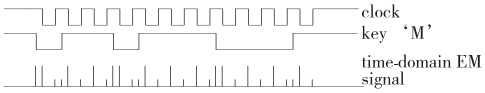

图 2　按键的跳变沿时域发射信号

b)不能从电磁噪声中分辨出信号上升沿对应的电磁发射。此时的发射接收信号与图 2 的分析相似,但仅有信号下降沿位置的尖脉冲。数据信号允许出现连续的高电平,两下降沿之间可能存在不同位置或数量的上升沿,因此,同一个下降沿序列可与多个不同的按键编码相对应。例如按键‘M’和‘X’具有相同的下降沿序列,时序如图 3 所示。

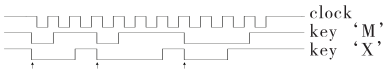

图 3　不同按键的扫描码具有相同的下降沿

尽管从电磁发射信号中仅有下降沿位置不能唯一地确定输入的按键,但可大大减少攻击猜测集合。例如在通过分析还原得到与‘M’相同的下降沿序列后,只需要从按键集{‘B’,‘D’,‘H’,‘J’,‘M’,‘X’}中进行猜测。而在实际的分析中,可进一步参考按键统计规律及输入内容的上下文信息,从而大大提高按键还原的成功率。

1.3　等效电路模型及分析

分析图 1 的双 BJT 集电极开路电路结构,研究数据与时钟信号在不同状态下的电流关联关系,将有助于找出电磁发射存在的区别,有利于信号的还原。在图 1 电路中,NPN 型 BJT 起流控开关的作用,即通过控制基极电流,使 BJT 在截止状态与饱和状态之间变换,切换集射极间断开或闭合状态,因此可将 BJT 看做是受控的开关。将实际 +5 V 电源等效为电压源与电阻的串联,记等效电压源电压为 U 和内阻为 r,据此对图 1 的电路进行等效转换,并记上拉电阻阻值为 R,则得到等效电路如图 4 所示。

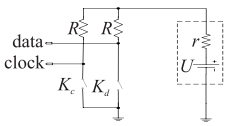

图4　数据时钟集电极开路的等效电路

当 K_d(K_c)断开时,对应输出的 data(clock)为高电平,反之信号为低电平,在开关闭合时信号产生下降沿。对 data 和 clock 信号而言,两者不可能同时出现下降沿,因此针对一个信号下降沿分析时,按另一信号所处的电平状态分情况进行讨论。由于 data 与 clock 信号具有对称性,不妨针对 clock 信号进行分析。

a)当 data 为高电平(即开关 K_d 为断开)时,开关 K_c 闭合前支路电流为 $I_0=0$,闭合后该支路的电流为 $I_1=\frac{U}{R+r}$,即闭合前后的电流变化量为

$$\Delta I_1=\frac{U}{R+r}$$

b)当 data 为低电平(即开关 K_d 为接通)时,开关 K_c 闭合前支路电流为 $I_0=0$,闭合并稳定后两支路电流相等,两上拉电阻的并联等效阻值为$\frac{R}{2}$,因此闭合完成后支路电流为 $I_2=\frac{U}{2(\frac{R}{2}+r)}=\frac{U}{R+2r}$,电流变化量为

$$\Delta I_2=\frac{U}{R+2r}$$

由于电阻的阻值为正值,故有 $\Delta I_1>\Delta I_2$。根据 BJT 开关特性,集射极导通过程时间极其短暂,导通后集电极和发射极间近似短路。因此数据处于高电平时,时钟下降沿产生更大的瞬变电流,即数据高电平状态下时钟下降沿将产生更强的电磁发射。

通过信息还原机理的分析,根据电磁发射信号可以提取与 PS/2 键盘编码相关的信息,但在仅有信号下降沿发射时难于准确地恢复键盘信息。利用等效电路方法作进一步分析,推导结论表明,时钟下降沿发射强度上存在差异,利用这种差异可以恢复出数据信号电平状态,从而可以精确地还原出键盘输入的按键信息。

2　电磁泄漏防护

在未采取屏蔽的办公环境中,电磁信号通过辐射方式向外传播,如果这些电磁发射被有意接收,将造成键盘输入信息的泄密。为防止键盘的电磁信息泄漏,分别从发射源和传输路径两方面进行研究,给出两种电磁泄漏防护方式。

从发射源上消除电磁发射与信息的关联是解决电磁信息泄漏问题的根本方法。对于 PS/2 键盘而言,就是从时钟与数据的信号特征着手,研究阻止产生数字信号相关电磁发射的技术方法。改进图 1 所示的电路结构,适当延长时钟与数据的跳变沿持续时间,降低信号的高频分量,从而减弱相关电磁发射,如在三极管与时钟/数据输出端之间设置功能器件抑制电平的快速变化。

电磁泄漏防护的另一种有效途径是通过屏蔽发射源和天线效应部件,阻断传输路径,使信息相关的电磁发射不被接收。一些计算机键盘已采用屏蔽线缆、键盘下设置金属层等电磁兼容性防护措施,但作为泄漏发射源的键盘控制模块并未实施屏蔽。对键盘实施更全面有效的屏蔽,将可以达到电磁泄漏防护的目的。

在上述两种防护方式中,修改电路、增加元器件,适合在产品研制过程中实施;对于现有键盘,针对控制模块及天线效应部件采取屏蔽则是一种可行的解决方案。

本文防护方案思路是:对传输线缆已屏蔽的计算机键盘,针对控制电路模块进行独立屏蔽。PS/2 键盘控制模块与按键阵列之间的接口多采用 8 行 16 列并排连线形式,触脚叠合并以螺丝固定相接。方案实施时先将控制模块卸下,用并排导线制作延长线连接控制模块与扫描矩阵的行列线,以绝缘胶带与夹子固定。在屏蔽材料中铝箔纸具有应用方便、易于实施等优点,方案采用能够满足泄漏防护需求的铝箔材料。根据实验测试结果计算电磁屏蔽需求,选择合适的屏蔽材料,具体描述防护方案细节,并对屏蔽后的电磁泄漏防护效果进行测试。

3　实验与结果分析

为验证键盘的电磁信息泄漏,本文设计实施了电磁接收测试实验,根据测试结果计算屏蔽防护要求,具体实现并测试了电磁泄漏防护方案。

3.1　实验环境

在半电波暗室中对商用屏蔽 PS/2 键盘(型号 SK-9270)进行测试,采用 EMI 接收机 R&S ESU40 测量频域发射,Tektronix TDS5054B 示波器用于时域测试分析。键盘与屏蔽机柜中的主机连接,被测键盘与接收天线组相距 1.5 m 远。根据文献的研究[12],设置 20 ~ 300 MHz 频段作为键盘电磁发射分析范围,以双锥天线作为主要的测量接收天线,暗室内的实际测试环境如图 5 所示。

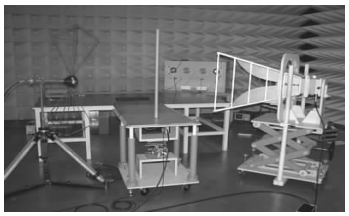

图 5　键盘电磁泄漏的实验测试环境

3.2　频域测试与特性分析

用 EMI 接收机进行频域测试的过程如下:

a)只开启主机设备而不连接键盘,对背景电磁发射进行测试,EMI 接收机的测试结果如图 6 所示。

b)连接键盘,重新对预先设定频率范围的电磁发射情况进行测量,测量结果如图 7 所示。

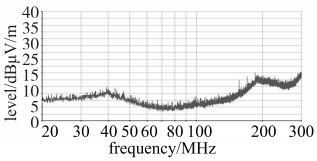

图6　无键盘连接时的背景电磁发射

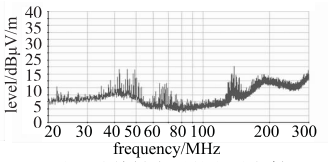

图7　连接键盘后的电磁发射

c)对于有键盘敲击时的电磁发射,采用连续敲击同一按键来测试该键输入时的频域特性。图 8 为连续敲击某一按键时测得的结果。

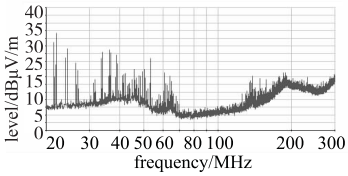

图8　在键盘上连续键入时的电磁发射

与图 6 的背景发射频谱相比,图 7 显示了键盘连接后的一些基本电磁发射信号。当键按下时(如图 8),在许多频点上接收到了明显的电磁发射。敲击多个不同按键进行比较发现,所有按键输入都有类似的测试结果,由此可确定,击键输入操作引起的键盘电路动作与信号传输过程产生了明显的电磁发射,即使是传输线缆已屏蔽的键盘在按键输入时仍产生了较强的电磁发射。

3.3　时域测试与信号还原

利用示波器对键盘电磁发射的时域信号进行测量,示波器

探头 1、2 分别连接键盘的数据信号、时钟信号,将双锥天线输出信号线与示波器的探头 3 相连。设定示波器的触发电平、触发方式、采样率及检波方式等参数,测量敲击键盘按键输入字符时的三路信号变化。为清楚地展现信号跳变沿时间,截取其中时钟与数据信号细节如图 9 所示。微调示波器参数,得到按键输入时的稳定测试结果。图 10 为按键‘V’输入时的时域信号。图中信号 1、2 的高电平幅度约为 5 V,天线接收信号的最大值约为 4 mV。

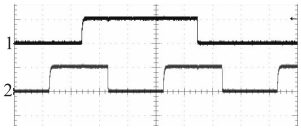

图9　时钟与数据信号沿细节

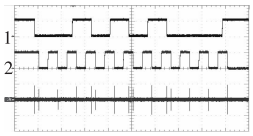

图10　按键‘V’按下时的时域信号

a)从图 9 可直观地看到,与上升沿相比,数据与时钟的下降沿明显更为陡峭。由图 10 电磁发射接收信号可以看出,在时钟和数据下降沿处都接收到对应的明显的脉冲,该结果与信息泄漏机理中 NPN 型三极管电路分析的第二种情况一致,即键盘的电磁信息泄漏与时钟和数据信号相关。

b)比较三路信号不难发现,时钟下降沿对应的电磁脉冲幅度与当时数据信号的电平状态存在关联:当数据信号为高电平时,电磁发射脉冲的电平幅度更高(分析 Vuagnoux 及张静勤的实验测试,其时域测试结果也同样具有该特性)。这一电磁发射特性验证了控制模块电路等效的分析结论。

c)对按键信息进行还原。按键扫描码通码(make code)以 11 bit 串行发送,包括 1 bit 低电平的起始位,8 bit 低位在前的数据位,1 bit 奇校验校验位,1 bit 的高电平停止位,在扫描码发送前时钟与数据均为高电平。据此,先提取等间隔的 11 个脉冲,恢复同步时钟信号。由于数据电平状态在时钟下降沿读取,故时钟下降沿电磁发射的幅度可得到数据信号状态,较高幅度的脉冲对应数据信号为逻辑 1,反之为 0。于是得到 11 bit 数据为 00101010001,按数据格式提取扫描码二进制数据为 00101010,十六进制为 0x2A,查找扫描码表即还原出输入的按键为‘V’。至此,成功恢复键盘的按键输入信息。

3.4　防护效果测试

为了达到良好的电磁屏蔽防护效果,要求防护实施后发射不高于背景电磁噪声。由时域测量结果(图 9)可知,电磁发射信号与噪声的电平比约为 10/1,最低的屏蔽效能要求为 20lg10 = 20 dB;而键盘发射的频域接收信号(图 8)峰值与噪声信号相比,电磁发射峰值约为 32 dBμV/m,噪声谷值约为 5 dBμV/m,故屏蔽效能至少达到 27 dB。因此,理论上在 20 ~ 300 MHz 范围施加屏蔽效能至少为 30 dB 的防护措施,方可将键盘的电磁发射降至低于周围电磁噪声水平。根据 Tosaka 的研究,厚度为 0.012 mm 的铝箔在该频段可提供 40 dB 以上的有效屏蔽,选择 0.012 mm 铝箔作为方案的屏蔽材料。按方案设计进行控制模块的独立屏蔽,为避免引起短路,采用泡沫和胶带等绝缘材料进行包裹固定,然后在外层施加铝箔屏蔽。铝箔间缝隙用导电胶带粘合,屏蔽完成后将铝箔连接传输线的屏蔽层。对防护后的 PS/2 键盘在连续敲击按键时进行实验测试,频域分析结果如图 11 所示。

将屏蔽后的频域测试结果与原测得的频谱(图 8)进行比较可见,大部分频点上的电磁发射已经得到抑制,而电磁发射时域信号也已看不到明显的脉冲,即针对控制模块的屏蔽起到了较好的防护效果,这也表明键盘的控制模块是进行电磁信息泄漏防护研究的重点。

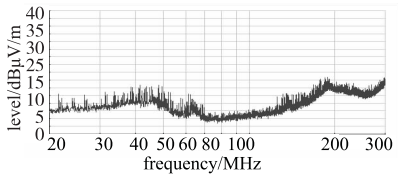

图11　采用屏蔽后点击按键时的发射频谱

4　结束语

电子信息设备的电磁泄漏问题是危及信息安全的一大隐患,本文针对 PS/2 键盘的电磁泄漏问题,确定了键盘的主要泄漏发射源,建立了数据与时钟输出电路 NPN 三极管结构的等效电路,并在此基础上分析了电磁泄漏发射与信息还原的机理。在随后的电磁发射测试中,依据电磁发射的时域接收信号还原了输入按键扫描码编码。针对键盘泄漏发射源控制电路模块,提出了两种防护方式,并设计了一种易于实施的屏蔽防护方案。根据本文的研究,除传输线缆屏蔽,键盘的电磁安全防护重点在于对控制模块进行电路结构改造和电磁发射抑制。

参考文献:

[1] YOUNG J. NSA tempest documents[EB/OL]. (2008-06-14)[2010-09-30]. http://cryptome.info/0001/nsa-tempest.htm.

[2] Van ECK W. Electromagnetic radiation from video display units: an eavesdropping risk? [J]. Computers & Security, 1985,4(4):269-286.

[3] 韩放. 计算机信息电磁泄漏与防护[M]. 北京:科学出版社,1993.

[4] KUHN M G. Compromising emanations: eavesdropping risks of computer displays[EB/OL]. [2010-11-27]. http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-577.pdf.

[5] KUHN M. G. Security limits for compromising emanations[C]//Lecture Notes in Computer Science, vol. 3659. Berlin: Springer, 2005: 265-279.

[6] 董士伟,许家栋. CRT 显示器信息电磁泄漏保熵性研究[J]. 电子与信息学报,2004,26(3):405-409.

[7] 张洪欣,吕英华,贺鹏飞,等. 计算机电磁信息泄漏文字再现[J]. 西南交通大学学报,2007, 42(6):453-458.

[8] TOSAKA T,TAIRA K,YAMANAKA Y,*et al*. Electromagnetic security for electromagnetic disturbance that contains information[C]//Proc of the 2nd Workshop on WAVE. 2006.

[9] TOSAKA T,TAIRA K,YAMANAKA Y,*et al*. Feasibility study for reconstruction of information from near field observations of the magnetic field of a laser printer[C]//Proc of the 17th International Symposium on EMC. 2006:630-633.

[10] SMULDER S P. The threat of information theft by reception of electromagnetic radiation from RS-232 cables[J]. Computers & Security, 1990,9(1):53-58.

[11] VUAGNOUX M,PASINI S. Compromising electromagnetic emanations of wired and wireless keyboards[C]//Proc of the 18th USENIX Security Symposium. 2009:1-16.

[12] VUAGNOUX M,PASINI S. An improved technique to discover compromising electromagnetic emanations[C]//Proc of the 21st International Symposium on EMC. 2010:121-126.

[13] 张静勤. 键盘电磁泄漏发射信息还原关键技术研究[D]. 北京:北京交通大学, 2010.

[14] CHAPWESKE A. The PS/2 mouse/keyboard protocol[EB/OL]. (2002-02-24)[2010-09-29]. http://www.computer-engineering.org/ps2protocol.

[15] 刘杰. 泄漏发射的信息重建与防御对策[D]. 杭州:浙江大学, 2004.