

计算机电磁信息泄漏与防护技术

张灵振 刘直承 南秀华



当前,计算机的应用范围十分广泛,在科学研究、军事部门、财贸系统、工业自动化、办公室自动化、教学现代化等方面都有普遍的应用。计算机是高速运行的数据处理系统,它象其他电子设备一样能产生电磁辐射,而且向外辐射大量有用的电磁信息,对于国家机要部门、军事部门来说,这些信息一旦被非法截获、破译,就会造成严重的失泄密,在战争环境下甚至会危及国家的安全。在海湾战争中美国发射了一种间谍卫星,其中就采用了一种最先进的技术截获了伊拉克及海湾地区的政治、军事、经济情报,导致了伊拉克的惨重损失。本文将简述计算机电磁信息泄漏机理、防护技术以及防信息泄漏计算机的发展概况。

一、计算机电磁信息辐射机理

计算机是一个机电一体化设备,装有各种电子电气和磁性元件,计算机内部采用了大量数字集成电路和模拟集成电路,数字集成电路一般工作在低电压、大电流的高速开关状态。模拟集成电路是由电阻、电容、晶体管等非线性元件集成的。计算机主要由以下部件组成:以微处理器和主存储器为核心,CRT、键盘、打印机为人机接口,模-数、数-模变换器和数字输入输出传感器输入输出,还有联系其他系统的通讯接口。

计算机内主要有以下工作信号:晶体振荡器、各种时钟信号和各种指令信息(包括控制、数据、地址、像素等信号)。随着计算机速度的提高,晶振和时钟频率越来越高,现在一般台式计算机可达133MHz。晶振是连续波,其频谱是单根谱线,时钟是一串周期脉冲信号,其频谱是线谱,包络具有 Sinx/x 的形状,指令信号是准周期脉冲信号,其频谱是由频率轴任意位置上无规

则离散谱线所组成,周期信号和准周期信号都是由无穷多谱线分量组成。现在计算机日趋小型化和高功能化,要求电路器件高密度、高速度、宽带域工作。这就给计算机带来潜在的危害而增加相互干扰。如:在相距很近的印刷线条中有高频成分的高速开关电流通过,尤其是在相邻的平行多根信号线的数据总线中。在地址信息和输入输出数据被送到总线和从总线取出时,由于多支电流在相应的位线中同时发生急剧变化,这就很容易发生串扰,同时由于信号线和负载阻抗不匹配,印刷线粗细不均匀等引起反射,或通过公共阻抗产生寄生耦合。根据电磁感应定律,任何系统中只要有电流通过则在其周围空间产生电磁场,电磁场的强弱与通过的电流大小和变化速率有关。计算机工作时是在低电压、大电流的状态,所以可形成较强的电磁场。这些信号在长波和短波段可沿着导线传播,在超高频段主要通过空间辐射,这种辐射大部分是经过接地线、电源线、机壳、信号连线和元器件等向外辐射。可见计算机的电磁辐射频谱很复杂。

显示适配卡和CRT是不可缺少的组成和主要的人机界面,它们辐射的信号(如视频)具有能直接解调判读的特点,被截获后可很容易地复现,所以显卡和CRT是主要的信息泄漏部件。

实验中发现:关闭CRT电源(主机电源仍打开)后,接收机的显示器上仍然有图像显示,而从显卡输出插头拔掉输出电缆,图像就没有了。说明显卡的确存在信息泄漏,而且应该说从计算机主板到I/O输出接口板都程度不同地产生电磁辐射。经过对显示卡的频谱特性分析,发现由于显示卡中D触发器的调制作用,只要有D触发器高速工作的电路就会有信号辐射。普通的黑白电视机稍加修改,就可在一定距离内进行接收。

目前大多数 CRT 都采用逐行扫描制式,从驱动输入级到视放驱动级间的电路结构大多为二值处理电路. 在视频驱动级,工作电压设计到了百伏特的数量级,尤其对高分辨率的显示器. 由于行、场频率的提高,工作电压更高. 其次,受到视频调制的电子束,在几千伏高压作用下轰击显像管荧屏,这种高速电子流也必然产生辐射. 另外,诸如电源线、连接导线以及其他分布参数形成谐振电路也都能产生电磁辐射,而且频率越高,辐射强度越大. 由此可见,视频电路和显像管为主要辐射源.

二、信息泄漏的防护技术

当前一般把计算机辐射的电磁信号分为红信号和黑信号,红信号是指被接收到后能够被破译,并复现出有用信息的信号;而黑信号是指那些即使被接收到,也不能复现出有用信息的信号. 衰减量高于 RED 线的区域为绝对安全区,一般定义为红区,满足红区条件的信息设备不会有信息泄漏的危险. 衰减量在 RED 与 BLACK 线之间的区域为过渡安全区,一般定义为黑区,衰减量低于 BLACK 线的区域为危险区,如图 1. 采取防护措施就是使辐射信号的衰减量达到限值,满足红区标准.

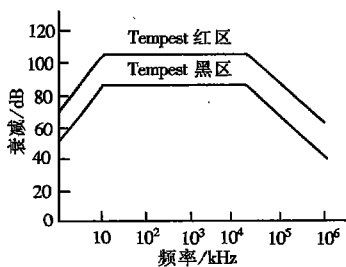


图1 Tempest POC. VDE辐射限值曲线

计算机电磁信息泄漏的防护技术可采取抑源法和包容法. 抑源法主要是减少电磁信息辐射的能量,包容法主要是防止电磁信息泄漏出来而采取的屏蔽滤波等技术.

抑源法措施包括:选用多层印制板,以减少高频振荡;把振荡器、时钟、高重复频率信号(地址、锁存、读写控制等)埋入电源层和地线层之间,保护关键电路;选用有电磁干扰模拟的 PCB 软件对电路板上的器件布局、电路走线等进行设

计,以减少电磁干扰及辐射;对个别辐射量较大的地方可进行局部屏蔽,如晶振外壳接地, CRT 中的行频场频有关电路用金属小盒子包起来等,减少辐射. 此外,还有电源去耦、端接、接地等措施.

包容法措施包括:机箱、连接器和电缆的选择. 机箱一般采用有一定厚度(3—5mm)的铝金属机箱,铝与其他金属材料相比屏蔽较好,重量较轻,容易加工,价格适宜等. 对塑料机壳可进行电涂,或在设备与机壳之间做一个较薄的金属壳夹在两层中间,提高屏蔽效果. 此外,机箱与盖板之间应有良好的电气接触,机箱的散热窗口需装通风波导,还要防止缝隙泄漏. 连接器和电缆应作为一个整体而不是单独的元器件要同时考虑,尤其在高频时,要求他们的屏蔽性能越好.

滤波措施就是采用滤波器可以把不需要的传输能量减小到使系统能满足工作的电平上,可根据需要进行选择设计低通滤波器、高通滤波器、带通滤波器、带阻滤波器等. 微机电源一般是开关电源,工作频率约在 20kHz 以上,有电磁能量通过电源线辐射出去,因此在电源输入处应串高性能滤波器.

三、防信息泄漏技术的发展概况

“信息泄漏的威胁”是由瑞典人在 1983 年首次报道,并在 1985 年 Van Eck 论文的论证和发表后,再次引起人们的注意. 此后随着信息泄漏威胁的日益严重,各国军方和机要保密部门均投入巨额资金研究,防信息泄漏 (TEMPEST) 计算机也随之得到广泛发展. 在此之前若干年, TEMPEST 截获和防护技术研究在有关国家悄悄地进行并高速发展着.

美国是防信息泄漏计算机发展最早的国家之一. 1970 年美国国家安全局发表了 NACSIM5100 测试技术标准,到 1982 年期间,美国包容式 TEMPEST 计算机占主导地位. 所谓包容是以屏蔽、滤波、吸收原理为基础,以金属结构为主体,限制电磁能量发射的一种屏蔽结构. 其特点是体积大、重量重、设计难、成本高. 相当于我国的低辐射计算机.

高压静电场在酿造品生产中的应用

蒋耀庭



酒、醋和酱油是人们喜爱的三种酿造品。在他们的色、香、味形成的过程中，要经历一系列复杂的物理和生物化学的变化。实验研究表明，高压静电场可以加速他们的物理变化，还可以对有关的生物化学反应起到催化作用。

在酒和食醋生产中，刚蒸馏出的新酒或新醋，往往都具有暴辣、冲鼻、刺激性大等特点，同时带有杂味。要酿出酯香、优雅、协调和绵软的酒和食醋，生产工艺中都规定了一定时间的陈酿贮存期。对酒来讲，陈酿期少则半年、一年，多则数十年。对食醋来讲，也需要一到六个月的陈酿贮存期。因此生产厂家必须备有大的贮存库和容器。资金不能周转。这对于一些中、小型企业来讲，带来一定的困难，因此，传统的自然老熟方法限制了酒和食醋的大量生产。为此，国内曾有人利用高压静电场，对酒和食醋进行人工老熟。图1是人工老熟实验装置示意图。它由高压静电发生器、控制器、电晕线以及

特制的盛酒或盛醋容器组成。被处理样品与容器一道，置于电场中。这样，在样品存在的空间，存在大量的负离子、臭氧等。

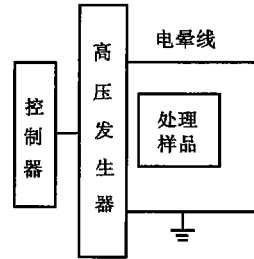


图1 实验装置示意图

目前，用高压静电场对酒类的人工老熟，主要对象是白酒和葡萄酒。辽宁大学关效圣教授对白酒的人工老熟，所采用的电场变化范围是 $2\text{kV}/M-400\text{kV}/M$ ，处理时间为1分—16小时。白酒中含有多种微量成分，其中丙烯醛是新酒呈现辛辣味的主要成分，异戊醇是具有刺舌的涩味，杂醇油具有刺激性味，经过静电处理后，三种成分均有所下降。乙缩醛、乙酸乙酯、总酯是白酒香气的主要成分，经静电处理后，均

海军航空工程学院基础部 山东烟台 264001

1982年前后美国国家安全局发布 NACSIM 5200 标准及“Guidelines for Facility Design and Red/Black Installation”，标志着红黑分离式 TEMPEST 计算机开始替代包容式 TEMPEST 计算机。同年北约集团也公布了 AMSG720 泄密辐射实验室标准。红黑隔离设计使用板级隔离、系统级隔离和箱级隔离等技术使红信号和黑信号完全隔离开来。然后再对隔离后的红信号采取特殊的严格措施，以使其达到限值的要求，而对于黑信号仅达到电磁兼容的要求即可。所以红黑设计是 TEMPEST 设计的核心。

1997年英国学者 Markus G. Kuhn 和 Ross J.

Anderson 在实验室内完成了以 Soft-TEMPEST 技术为理论基础的攻击与防护型 TEMPEST 计算机。使用软件控制计算机红信号的发射，同时加入专用的攻击程序，当有人企图截获时进行自卫还击。预计未来十年这种计算机将逐渐占据优势。

近几年来，我国在防信息泄漏计算机基础理论的研究、低泄漏计算机的研制、电磁兼容材料的开发等方面取得了不少成果。但是，我国在 TEMPEST 技术研究方面起步较晚，尚有许多艰苦的工作要做。可以相信，在不久的将来，我们一定能够研制出高性能的防信息泄漏计算机，进入世界先进行列。