A Experimental Study on Modulation Technology based on Electromagnetic Compromising Emanation

Jun Shi [1], Baoxu Liu [2]

[1)] Technology Center, Beijing State Secrecy Bureau, Beijing, China (shijun@bjbmj.gov.cn)
[2)] Computering Center, Institute of High Energy Physics, Beijing, China (liubx@ihep.ac.cn)

***Abstract*—This article firstly introduced the direct transmission manner and the modulation manner based on electromagnetic information leakage and modulation principle, then made a comparison between them. The concept and the theoretical model of modulation technology based on electromagnetic compromising emanation are proposed, and its information leakage mechanism is systemically studied, then it is testified in a certain office automation device. The experiment results show that the phenomenon of electromagnetic compromising emanation is commonly existent, and the model set up for the study on electromagnetic information leakage from information technology equipment is validated. Correctly understand the workings of electromagnetic compromising emanation will be helpful for the Improvement of identify capability for the captured information, and it is also hoped to play a motivating role on electromagnetic compromising emanation attacking and defending.**

***Keywords*—Electromagnetic Compromising Emanation, Modulation Technology, Information Compromising Mechanism**

电磁泄漏发射调制技术的实验研究

石军 [1]　刘宝旭 [2]

[1)] 北京市国家保密局技术中心，北京 100743，中国
[2)] 中国科学院高能物理研究所计算中心，北京 100049，中国

摘　要 根据信息设备工作时存在电磁泄漏发射及调制技术原理，给出了信息设备电磁泄漏发射存在的两种方式并进行了比较说明。据此，提出了电磁泄漏发射调制的概念及其原理模型并对泄漏机理进行了定性分析，对某型办公自动化信息设备进行了实验方法验证。实验结果表明：被测信息设备电磁泄漏发射调制是存在的，所建电磁泄漏发射调制泄漏机理模型是正确的。正确认识电磁泄漏发射调制有利于提高所捕获信息的可识别复现能力，希望本文研究结果能对信息设备电磁泄漏发射调制的攻击与防御技术起到积极的重大推动作用。

关键词 电磁泄漏发射，调制技术，泄漏机理

1. 引言

电子信息系统中的各类计算（机）主机、显示屏、键盘、电源线、信号线等设备工作时，均能向周围空间辐射一定能量的电磁波，可能造成数据信息被窃取或偷窃。从工作原理上来看，信息设备工作时产生的电磁泄漏，有以下两种情况：一种情况是显示器或可识别信息（显示）设备等辐射出的（视频）电磁波，其频率较低，这类电磁泄漏信息远距离捕获较难，对所截获信息的解读比较简单；另一种情况是从信息设备的内部单元（如运算控制部件等）和外部设备等泄漏的信号，其频率一般较高，这类电磁泄漏信号被截获的几率大大增强，但最终获取可识别信息比较复杂。

在无线(移动)通信系统中，调制技术是非线性电子线路系统中的一项重要应用，它可将正常信道内的信息变换到别的信道中去，不但形成干扰，而且极易失密[1]，因此，电磁泄漏发射调制是信息安全领域一个不容忽视的重大问题。

2. 电磁泄漏发射调制技术理论基础

2.1 电磁泄漏发射调制技术原理

电磁泄漏发射调制技术指的是信息设备的电磁泄漏发射调制信号与一定功率强度的（类似）载波信号发生相互作用而产生多次发射的技术，其实质可以认为是一种广义的频谱变换过程，即电磁泄漏发射调制信号的频谱出现在载频的两侧，此频谱特性可以作为电磁泄漏发射调制类型的判据。

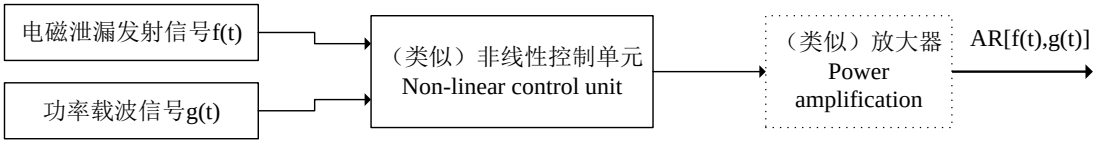

图 1　电磁泄漏发射调制技术原理框图

一般情况下，由于电磁泄漏发射信号相对于正常信道信号能量较小，因此，电磁泄漏发射调制起作用的前提是要经过放大电路进行功率增强，如图 1 中的虚线框放大器，A 是增益系数。图 1 中，（类似）非线性单元指的是功能类似的各类非线性电路单元，其输入输出之间的关系可以用幂级数来表示，略去三次方以上高阶较小项，可表示为

$R = a_0 + a_1 x(t) + a_2 x(t)^2 + a_3 x(t)^3$　式中：a_1、a_2、a_3 的值与非线性器件的结构及其工作状态有关。

不失一般性，设 $f(t) = v_f \cos w_f t$，$g(t) = v_g \cos w_g t$，$x(t) = f(t) + g(t)$

则

$$
\begin{aligned}
R &= a_0 + a_1[f(t)+g(t)] + a_2[f(t)+g(t)]^2 + a_3[f(t)+g(t)]^3 \\
&= a_0 + \frac{1}{2}a_2(v_f^2+v_g^2) + (a_1 v_f + \frac{3}{4}a_3 v_f^3 + \frac{3}{2}a_3 v_f v_g^2)\cos w_f t + (a_1 v_g + \frac{3}{4}a_3 v_g^3 + \frac{3}{2}a_3 v_g v_f^2)\cos w_g t \\
&\quad + a_2 v_f v_g[\cos(w_f + w_g)t + \cos(w_f - w_g)t) + \frac{3}{4}a_3 v_f^2 v_g[\cos(2w_f + w_g)t + \cos(2w_f - w_g)t] \\
&\quad + \frac{3}{4}a_3 v_f v_g^2[\cos(2w_g t + w_f)t + \cos(2w_g - w_f)t] + \frac{1}{2}a_2 v_f^2 \cos 2w_f t + \frac{1}{2}a_2 v_g^2 \cos(2w_g t) \\
&\quad + \frac{1}{4}a_3 v_f^3 \cos 3w_f t + \frac{1}{4}a_3 v_g^3 \cos 3w_g t
\end{aligned}
$$

由上分析可知，非线性单元输出产生了众多互调信号（如二阶互调、三阶一型互调）与谐波信号（如二次谐波、三次谐波），若这些信号落入感兴趣的接收机频带内，则会产生有用信息泄漏，造成失密。

2.2 电磁泄漏发射调制信号泄漏机理

图 2 中：S_{C_Modem}为基带调制信号；$S_{C_passband}$为频带通信信号；S_{C_PA}为带通放大信号；S_{C1}为输入调制器的合成信号；S_{C2}、S_{C3}和S_{C4}分别为带通滤波器、放大器及天线的输入合成信号。另外，图 2 中调制器框图是指各类调制器、各类非线性控制器件及寄生调制电路等的总称，放大器是各类信号功率放大器件、运算放大器及光电倍增管等的总称，天线框图是各类发射接收天线、各类通信线（缆）及各类电源线等的总称。

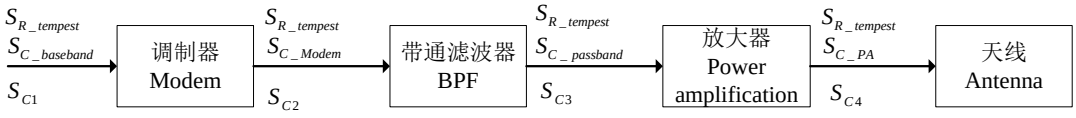

图 2　电磁泄漏发射调制信号泄漏机理框图

由 $S_{C1}=E\left(S_{R\_tempest},S_{C\_baseband}\right)$

$$S_{C2}=E\left(S_{R\_tempest},S_{C\_Modem}\right)=E\left[S_{R\_tempest},\mathrm{R1}\left(S_{C1}\right)\right]$$

$$S_{C3}=E\left(S_{R\_tempest},S_{C\_passband}\right)=E\left[S_{R\_tempest},\mathrm{R2}\left(S_{C2}\right)\right]$$

$$S_{C4}=E\left(S_{R\_tempest},S_{C\_PA}\right)=E\left[S_{R\_tempest},\mathrm{R3}\left(S_{C3}\right)\right]$$

式中：E（）代表一种代数运算算子，R1、R2 和 R3 分别表示各非线性器件的转移特性。

由上所述，分析 S_{C1} 表达式中各成分可知：由于 $S_{R\_tempest}$ 的能量远小于 $S_{C\_baseband}$，因此 S_{C1} 中电磁泄漏发射调制信号的成份较小，二次信号泄漏距离有限。分析 S_{C2}、S_{C3} 表达式中与 $S_{R\_tempest}$ 有关的成分可知：主要是组合频率成份 $\pm mf_R \pm nf_c$，m 和 n 均为正整数或零，f_R 为广义频带信号 $S_{R\_tempest}$ 的载波频率，f_c 为通信频带载波频率。因此，S_{C2}、S_{C3} 中含有的电磁泄漏发射调制信号比 S_{C1} 中要多且更容易发生泄漏。S_{C4} 除了包含 S_{C3} 中的各组合频率成份外，由于这些成份均需经过放大器进行功率增强，且天线的发射效率比电路的无意辐射要高，因此，S_{C4} 造成的 $S_{R\_tempest}$ 二次泄漏发射距离将比其余 S_{C1}、S_{C2}、S_{C3} 的更远，危害更严重。

此模型是信息设备电磁泄漏发射调制的等效原理框图，实际信息设备只要符合以上功能特征，均能产生电磁泄漏发射调制，如办公自动化设备（具有传真、扫描、打印、复印功能的一体机，无线话筒，对讲机，各类移动通信终端等）与/或电子信息系统设备（计算机设备，密码设备及其它辅助设备等）就能产生电磁泄漏发射调制。

3. 实验分析

对某一品牌型号的办公自动化信息设备测试如下，测试方法参考文献[2]。

不处理信息时的信号频谱和正常工作处理信息时信号发生调制后的发射频谱图如图 3 所示。

图 3 中，处理信息时泄漏信号发生调制后的发射频谱曲线图的主体在上方，不处理信息时的被测设备通电噪声信号频谱曲线图的主体在下方，由图 3 可知，泄漏信号与载波信号产生调制，从而实现了对泄漏信号的频谱搬移。出现图 3 现象的原因：一是接收机扫描时间与被测设备完成一次正常工作的时间不匹配；二是被测设备正常工作时，其电磁泄漏发射是阵发式的，具有瞬时性，这与周期性的视频信号电磁泄漏发射明显不同。接收机实际测试结果、测向结果及被测信息设备工作原理分析结果、实际测试信号类型近似传输带宽分析均表明：该载频上调制的是真实泄漏信息。

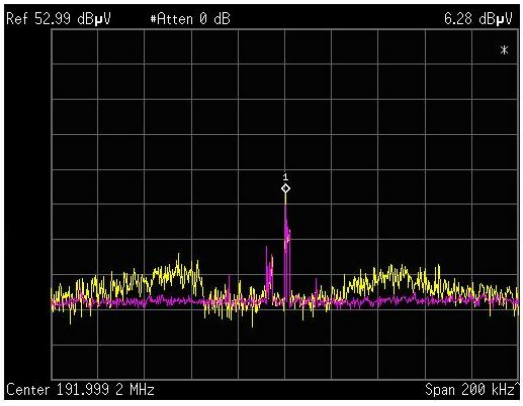

图 3　电磁泄漏发射调制技术原理框图

4. 结论

根据以上电磁泄漏发射调制泄漏机理模型分析和实验测试验证，可知：该类被测设备存在可引起信息安全隐患的电磁泄漏发射调制现象，所建信息泄漏机理模型具有通用性，这和被测信息设备工作原理分析结果相对应。

捕获信息只是窃取信息的手段，如何对所捕获的信息进行可识别复现才是目的，正确区分信息设备电磁泄漏方式，有助于更好地解决信息复现技术与保密防御技术的发展，是开发此类信息对抗设备所必须具备的基本技术要求。目前，国家系列保密标准还没有电磁泄漏发射调制等相关内容，还不能与信息化条件下的高新技术发展水平相适应，从性价比的角度来看，还不能有效地应对电磁泄漏发射“旁道攻击”方式，希望本文研究结果能对信息设备电磁泄漏的攻击与防御技术起到积极的重大推动作用。

参考文献(References)

[1] Da-li Zhu, De-gang Sun,Fang Jiang, et al, “Research on Information Compromising Emanation of Cross Modulation Derived from Mobile Stations,” *Computer Engineering & Science*, vol. 27,no. 7, pp. 86-8, September 2005.

[2] Jun. Shi, “A New Test Approach to Electromagnetic Information Leakage,” *Netinfo Security*, no. 9, pp. 121-123, September 2011.