TVRO 发烧园地　第十一期／2005 年

THE SKY OF TVRO FAN　(总第一一七期)

1996 年 3 月创刊　　2005 年 11 月 28 日　　本期共八页

卫视资讯

1．清华同方推出机顶盒：www.tsinghuadtv.com

2．厦门市第一个卫星电视频道海峡卫视，2005 年 10 月 1 日正式更名为厦门卫视。

3．法国电信自称进行了是世界上第一个实况高清电视广播，采用先进的 MPEG-4 压缩技术，经由 ADSL2＋网络进行广播。

4．东风华高新科技集团有限公司有线数字电视系统用户终端接收机（透明）DVB-CFH 型通过广电总局入网。（电话：0758-2823328）

杭州三星东信网络技术有限公司有线数字电视系统用户终端接收机（透明）SMT-1600C 型通过广电总局入网。（电话：0571-86726588-8037）

浙江 001 集团有限公司卫星数字电视接收机 CRD-2000 型通过广电总局入网。（电话：0570-7110858）

福建天诚电子科技开发有限公司卫星数字电视接收机 NHF-D918 型通过广电总局入网。（电话：0591-83859203）

宁波万吉电子科技有限公司卫星数字电视接收机 WJ2000 型通过广电总局入网。（电话：0574-63471838）

四川九州电子科技股份有限公司卫星数字电视接收机 DVC-2028 型通过广电总局入网。（电话：0816-2469417）

郑州通信设备有限公司卫星数字电视接收机 OL-2008 型通过广电总局入网。（电话：0371-68621166）

德州科海电子有限公司 KU 频段卫星电视地球接收站室外单元 KHKU1125-B 型通过广电总局入网。（电话：028-83288140）

5．2005/11 期《电视技术》刊登董震的文章《构建数字电视服务营销竞争优势》一文不确。

6．广州建龙电器有限公司专业的机顶盒设计，制造商：www.tiartop.com，TEL：020-36999206

7．大华数字科技有限公司也推出机顶盒：www.dahuadigital.com，电话：0571-28939686

8．康佳集团股份有限公司数字网络事业部也推出各种机顶盒。电话：0755-26608866-6090/6851/6852

9．湖南广播影视集团组建“快乐购物有限公司”（快乐购物公司）在 2005 年 10 月底完成注册，相关的购物频道预计在 2006 年 1 月中旬开播。

10．日前开通“高尔夫，英语辅导，真人秀，欧洲足球”四个数字付费频道，并已获国家广电总局批准为全国性数字电视频道。

11．董震认为：高清是重振电视业务高端市场，再次拉开与其他网络业务差距的利器，高清付费电视是以高品质节目创造高效益的全新的数字付费电视业务，电信行业在此无力涉足。并且，虽然垄断已经被打断，有线网络与电视台依然是：“唇亡齿寒”的关系。付费电视节目的推广应该是以节目为龙头，以市场为主导，以技术为支撑，以资本为纽带，提供全面业务竞争服务正不可避免的

到来，只有“团队才能成就梦想”。

12．飞利浦投资有限公司消费电子产品部马婷女士讲：飞利浦机顶盒产品将进军中国。

13．Irdeto 在 IPTV 方面，目前已与华为，中兴，同洲，裕兴数码合作。

14．上海东方有线付总经理罗小布讲，2005 年 11 月 14 日央视“高清影视”频道已经落户上海，由于上海地区 640MHZ 的频宽已经占满，而高清节目需要 800MHZ 的频宽，现在正在进行网络改造，计划明年 3 月份开通高清频道。

高清离我们还有多远？

——松下 TZ-CCH1000A 高清有线电视机顶盒

央视高清频道自今年 8 月 23 日起在亚 4 卫星 C 波段开始试播以来，杭州成为第一个落地城市。在杭州使用的高清有线电视机顶盒是由山东松下电子信息有限公司生产的 TZ-CCH1000A 型（注：在前面板注明的型号为：TZ-CCH1000，而后面板和说明书注明的型号为 TZ-CCH1000A，本人也不知为何）数字有线电视顶盒。最近我们拿到一台，有机会近距离了解该型号的机器。

该型号机器最大的特点是设计有 HDMI 数字音、视频输出接口，当然如要欣赏 HDMI 所带给我们的绚丽画质和震撼音效，我们需要一台带有 HDMI 接口的、与“720P”（1280*720 像素）或者是“1080i”（1920*1080 像素）标准相兼容的高清电视机。我们测试用的电视机是夏华 37 寸液晶高清电视机，它具有 HDMI 接口。

有人会问什么是 HDMI？？使用它有什么好处？

HDMI（高清晰度多媒体接口）是首个也是业界唯一支持的不压缩全数字音、视频接口，HDMI 支持单线缆上的标准、增强或高清晰度视频和多声道数字音频。

HDMI 新近成为连接 HD 设备、显示设备和元件的数字标准，并通过单线缆传输原始高清晰度数字视频和数字音频。HDMI 和 DVI 都以 Silicon Image 的高速数字 TMDS®技术，HDMI 完全兼容以 DVI（数字视频接口）为基础的设备。此外，HDMI 是首个也是唯一的消费类电子设备数字接口，可提供：

- 不压缩的高清晰度视频
- 压缩或不压缩的多声道音频
- 智能格式和命令数据

大家如要了解更多 HDMI 相关信息可以访问它的官方网站：http://cn.hdmi.org/（还是中文的）

做为一台高清有线电视机顶盒，它是可以完全能够接收并处理标清电视节目（DVB 标准），它的调试和使用与一台普通机顶盒也没多大的区别。松下 TZ-CCH1000A 高清有线电视机顶盒的外观尺寸为 30×21×67 厘米，属于目前国际上较流行的中等尺寸机器。

该机的前面板被设计成上、下两部分。上部分为镜面设计，在中间可以显示当前频道位置或当前时间（待机状态下）的 LED 显示屏上隐藏在镜面后面。面板上的五个按钮与下部另五个按钮遥相呼应，可以实现该机的操作并且可直接设置接收机菜单。松下 TZ-CCH1000A 使用永新同方加密方案，卡槽位于前面板右侧的隐藏仓门后。

松下 TZ-CCH1000A 高清有线电视机顶盒的后面板配备了高品质的视频和音频输出端子。基本输出端是两组标准的 AV 输出端子、一组 S 端子和一个音频光纤输出，当然还有一组色差端子和更先进的 HDMI 端口。新软件可以通过 RS232 接口写入接收机。

如前所述，高清有线电视机顶盒与普通有线电视机顶盒没有任何区别，菜单设计和操作相当简单和方便。主菜单只有四个选项：节目指南、电子邮件、智能卡管理和系统设置。

节目指南：类似我们常讲的 EPG。在“节目指南”中可以选择节目、查看节目信息或进行节目预订，节目预订最多可以通过预定 20 套节目。

电子邮件：有线电视运营商发给客户的邮件，在“电子邮件”中可以显示。

智能卡管理：“智能卡管理”是对智能卡进一步管理菜单。

系统设置：系统设置可以确认和更改本机的设置，也可搜索节目和对节目进行编辑。

该菜单包括频道设置、输出设置、机顶盒信息、软件更新和其他设置。

一、频道设置：包括了自动节目搜索、频道参数设定、频道管理和节目信息四个分选项。

自动节目搜索有点象我们卫星接收机中的网络搜索功能，可以自动根据一组节目参数接收到与之相关的所有节目；当然在频道参数设定中可以设定自动频道搜索中使用的频率、符号率和调制方式的；在接收到所有节目后，可以在频道管理项中进行频道删除、重排和进行喜爱节目的编排；节目信息是当前节目信号强度显示。

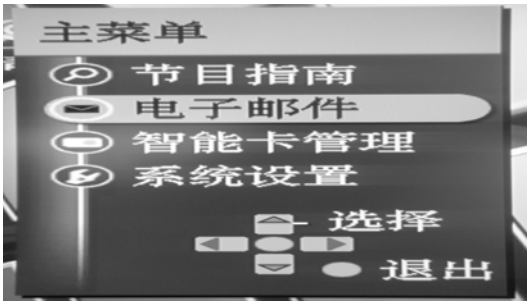
二、输出设置：包括了屏幕模式、HDMI 优先模式、模拟视频输出、数字视频输出、数字音频输出和 HDMI 信息六个分选项。

三、机顶盒信息：显示机器的型号、版本等信号。

四、软件更新：手动更新最新的软件版本，如果将其他设置选项中的软件更新项设置为自动后，一旦进入待机状态，就会自动确认来自有线电视台的新软件版本信号，并进行版本更新。

五、其他设置：包括了菜单语言、屏幕保护和软件更新三个分选项。

作为一台高清有线电视机顶盒，除了给用户一个操作简便、直观地菜单设计，也要提供给用户尽可能高的图像输出品质和输出端口，要不然 HDTV 就没有意义了！　　深圳 娄军



摘自：《2005 国际有线电视技术研讨会论文集》

数字电视条件系统的破解与反破解技术

吕品　天柏宽带网络科技有限公司　董事长

【摘要】

本文结合国内外数字电视条件接收技术的发展和应用实践,探讨 CA 技术的安全性及反破解对策。本文针对宽带互联网迅速发展，CA 技术将面临的新挑战，着重指出当前国内使用的部分条件接收技术存在的一个严重缺陷，希望能起到亡羊补牢的警示作用。

广播电视的条件接收系统是以单向实时广播模式运作的信息保安系统，目的是确保只有合法授权的用户才能有条件地享受被保护的信息(内容)服务。

从 CA 技术推出那天起，破解者们就开始加以攻击，而 CA 技术的开发者们也不断地从黑客击中中发现自身的弱点加以完善。回顾历史，CA 的破解及反破解大致经历了以下几个阶段：

1、基于算法的破解

数字电视起步初期，一些条件接收开发者仍然沿用模拟加密的思路，采用一些比较简单的算法对广播信号中的某些参数加密从而达到有条件接收的目的。一个经典的做法是利用改变 PID 配合可寻址授权来实现 CA，主要用在卫星广播上，但很快就被人用逐一试探 PID 的方法破解了。近年也有国内企业用类似的方法做简单的低成本 CA，但由于 DVB 广播参数上能加密的数据有限，只要配合码流分析仪，一般都可以被破解。这种方法除了用于临时的、低值的服务外，已基本没有前途。

从算法入手是破解 CA 的最直接方法。由于解密部分是在 IC 卡内实现的，如果 CA 厂家选的 IC 卡功能比较弱，又没有完整卡上操作系统(COS)支持的话，是很难实现高安全度的复杂算法的。随着计算技术和密码学理论的发展，许多原以为非常难破的加密算法纷纷告破。到目前为止，大部分密钥长度小于 100bit 的单一算法都有很大机会被破，就连曾被公认为破解难度极大的 128bitRSA 算法也被一群高中生用几十台 PC 联网破解了。要对付算法破解，主要有两种措施，一是加长密钥，根据香农定理，信息的容量与其长度成指数关系，密文的信息量越大，破解的难度就越大；二是采用多重算法，根据密码学原理，加密系统有四个要素，即：密文= 算法(明文，密钥)。在大部分的加密应用中，明文和密钥是被保护的对象，四个要素中有一半是未知的，安全性是比较高的。但在数字广播的实际应用中，明文与密文是可截取的，而一个可靠的加密系统采用的算法应该是可以公开的，所以采用单一算法的 CA 系统，只有一个未知要素，比较容易被解析或穷举方法破解，但如果采用多重算法的话，情况就完全不同了，因为：密文= 算法 2 (算法 1 (明文，密钥 1)，密钥 2)，所以整个系统中有六个要素，其中三个是未知的，这就大大增强了安全性，使解析法的破解几乎没有可能，如果再配合长密钥和时间因子的话，穷举法也非常难破。但要做到这点，必须选择功能强大的 IC 卡。许多新一代的智能卡已内置了 DES 和 1024-bitRSA 等公认的高强度加密算法。以硬件协处理的方式大大加快了 IC 卡的信息处理能力，这已成为国际上提高 CA 安全性的重要手段。

2、基于 IC 卡的破解

在通常的加密技术应用中，解密机是破译者争夺的关键设备，许多间谍故事都是围绕着它展开的，但在 CA 系统中，作为解密机的 IC 卡却是破解者唾手可得的。与电信行业不同，数字广播是单向系统。一旦 IC 卡被破，非法使用者是无法追踪的，所以数字电视黑客们都把 IC 卡作为重点攻击对象。IC 卡的破解主要有两种方法：对功能比较简单的 IC 卡，有人采用完全复制的方法，特别是那些采用通用程序制造，不经厂家个性化授权(如在半导体厂出厂前预置专用的客户密码识别号等)的 IC 卡最容易被破解，早期的 CA 厂家几乎都受过这样的攻击，但随 IC 卡技术的发展，完全拷贝复制的情况已少见，代之而起的是仿制卡。由于一些 CA 厂家采用了功能不强的 IC 卡，在卡内不能完成

全部的 EMM，ECM 解密工作，要借助机顶盒内的 CPU 做部分解密操作，有的甚至只在 IC 卡中存密钥，解密都在盒内做，安全性相当差。对这种 IC 卡，破译者一般有两种做法，一是先找出密钥库，放人自制卡中替代，考虑到运营商会经常更改密钥，黑客们还会提供在线服务，以电子邮件等方法及时发布密钥更改升级。二是找出 IC 卡的授权操作指令加以修改或屏蔽，让 EMM 无法对 IC 卡发生作用，所以很多伪卡就是用过期真卡把有效期延长而成的，而且伪卡往往对所有节目都开放，不能自选节目组合，因为破译者并没有也无需解出卡的全部程序加以控制。对于 IC 卡的破解主要靠选择性能好的卡来防范。功能强大的 IC 卡可以在卡内完成所有的 CA 解密操作，对外是一个完全的黑盒子，配合加密 flash 存储技术，用电荷记录密钥，即便采用版图判读的 IC 卡反向工程也无法读到有关信息。由于 IC 卡破译者需要对卡做各种连读的读写，以图找出规律，新一代的智能卡设置了反黑客功能，能用模糊逻辑区别正常信号与试探信号，一旦发觉被攻击能自动进入自锁，只有原厂才能开锁重新启用，从而大大增强了破译难度。

3、系统的破译

系统级的破译是 CA 黑客的最高境界，也是当前危害最大的盗版方式。主要有两种做法：一是从系统前端拿到 CA 系统的程序进行反汇编，找出加密的全部算法和密钥，这对于那些还在采用 windows 环境和对称密钥的系统是非常大的威胁。几年前，在欧洲某电视台就有工程师趁系统维护的机会拷贝了 CA 程序，交给黑客破解的实例。现在黑客们可能会更多地利用网络释放病毒来破译。要防止此类攻击，除了加强前端管理外，最好的方法是将 CA 前端的加密机做成专门硬件模块或用 IC 卡直接加密，使黑客即便盗走了前端系统也难以攻击。

第二种是当前兴起的 CA 共享方式。根据 DVB CA 的定义，IC 卡与机顶盒之间(无论大卡还是小卡都有同样的问题)有一个信息通道，输进卡的是 ECM、EMM，输出卡的是控制字。目前市场上有许多 CA 厂家对这个通道并未加留意，直接用来传输数据，有的虽然作了加密处理，但其算法在所有的盒子和卡之间都是相同的，从而形成一个致命的漏洞。黑客们构造了如下的 CA 共享系统（如图 1、2)。

盗版者按节目数首先购买几台正版机和 IC 卡，然后大量制造盗版机，盗版机与正版机软硬件完全相同，只是用一张以太网卡加一个 7816 的 IC 卡接口电路代替原有的 IC 卡模块，称之为 CA 共享卡。在使用过程中，盗版者先用 IC 卡转接器代替 IC 卡插入正版机，再在转接器上插入正版 IC 卡，仿真器带 PC 接口可以把正版机在看节目时的机卡之间的通信全部引到 CA 共享服务器上，通过 IP 宽带网向盗版用户发布，盗版机上的 CA 共享卡可模仿 IC 卡的作用将相应节目的正版机卡对话送到盗版机中。由于安全通道没有个性化加密，所有机卡对话在看相同节目时都是相同的。盗版机只要收到正版 IC 卡发出的信号(无论是否加密)即可解出控制字正常收看节目了，情况就如同大批盗版机在共享一台正版机的授权一样。故这种盗版机又被称为无卡共享机。这只是一种随着宽带 IP 网普及而兴起的新型解密方法，由于 CA 只要求每 10 秒左右换一次加扰控制字，故宽带网络足以支持解密。由于这种方法用户只要买一台盗版机即可在家上网获得实时授权，隐蔽性强，危害极大。要对付这种盗版方法的关键就是在机卡之间建立起一条每台机顶盒每次开始看节目都不同的安全通道，即采用所谓的“一机一卡，一次一密”。天柏公司在其所有的 CA 系统上都采用了这种技术，并注册了国内外专利。但现有的许多 CA 系统要抵抗这种攻击则需要对其 CA 内核及 IC 卡进行彻底修改。

4、结束语

“道高一尺，魔高一丈”，由于利益的驱动，不论采用何种技术，CA 系统都存在被破的可能，本人始终相信“世上没有不可破的 CA，只有不值得破的 CA”，问题是如何在 CA 设计时就做好准备，迎接挑战。写这篇文章前，我有过很长时间的犹豫，担心被同行们认为是商业目的的炒作。

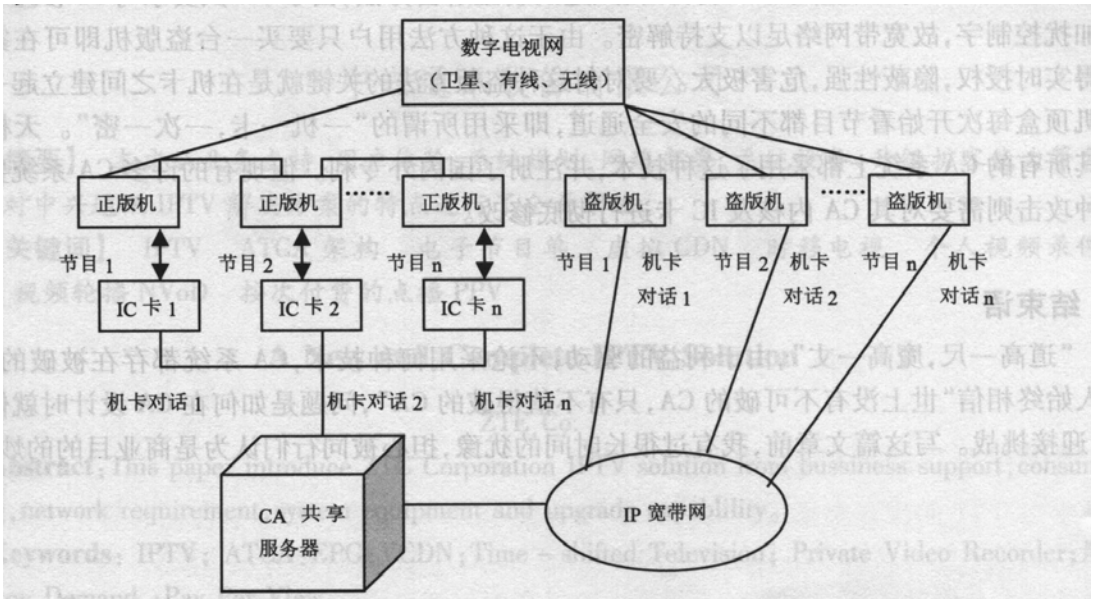


图 1　CA 共享盗版系统

图 2　CA 破解工具

122° E　C 波段最新节目指南

亚洲 4 号/Asiasat-4（122 ° E）：一、3940、V、27500，免费：①欧洲足球，②早期教育，③东方物流，④彩民在线，⑤老年福，⑥英语辅导，⑦视觉生活；二、4020、V、27500，爱迪德 II(Irdeto2)：①CCTV 电视指南（免费），②CCTV 风云足球，③CCTV 高尔夫、网球，④CCTV 风云剧场，⑤CCTV 风云音乐，⑥CCTV 第一剧场，⑦CCTV 世界地理，⑧CCTV 家庭影院，⑨CCTV 怀旧经典，⑩CCTV 央视精品；三、4060、V、27500，永新同方：CCTV 高清影视；四、4100、V、27500，免费：①靓妆，②天元围棋，③吉祥购物，④留学世界，⑤汽摩频道，⑥GTV 游戏竞技，⑦孕育指南，⑧青年学苑，⑨梨园频道。

摘自：《广播与电视技术》2005/11 期

西欧公司纷纷开办高清电视

高清电视正在全球加速发展．美国和日本处于领先地位。欧洲也不甘心落后。自 2004 年以来，西欧一些公司像赛跑似地竞相宣布开办高清电视．到目前为止．已有 10 多家公司宣布开办高清电视，或者在试验高清电视。许多公司都把在德国举办的 2006 年足球世界杯视为是开办高清电视的良好时机。准备开办高清电视的西欧公司如表所列。

国家	公司	公司类别	基本情况
英国	BSkyB	卫星电视运营商	计划 2006 年开播 HDTV
	NTL	有线电视运营商	在实验高清电视
	Telewest	有线电视运营商	要在 BSkyB 之前开播 HDTV
	BBC	公共广播机构	计划 2006 年第二季度开播
德国	Premiere	卫星电视运营商	2005 年 11 月开播 HDTV
	Kabel Deutschland	有线电视运营商	准备开办 HDTV
	ProSiehenSat1 produktion	节目制作公司	2004 年 10 月以高清和标清同时广播《热带大草原》这个高清节目
法国	TPS	卫星电视运营商	2005 年开办 HDTV
	Canal+Group	卫星电视运营商	2005 年 10 月开播商业 HDTV
	France Telecom	电信运营商	2005 年实验实况 HDTV 广播
荷兰	EssenKabelKom	有线电视运营商	2006 年第一季度开播 HDTV
北欧	SBS Broadcasting		2005 年 9 月开播一个 HDTV 电影频道

德国宝马（原佳力）CATV 仪器

www.universalam.com

PRK3CP、PRK3CDG、PRK4CP

便携式多制式高级卫星/电视频谱场强仪

◆测量精度：SUB、TV 和 SAT±1.5dB
◆测量范围：20/30-130dBμV
◆测量频率：5-862MHz/900-2150MHz
◆内置香港/内地频道，另可存储 99 个频道
◆内置丽音解碼，TFT 彩色液晶显示器
◆可用专用软件对仪器进行遥控和升级，为以后更新测量功能预留空间
◆*内置 MPEG-2 译码,可显示数字电视图像
◆*内置 QPSK、QAM、COFDM 比特误码率和调制误码率测量，可显示 QAM 星座图
◆*支持智能卡接口，适用有条件接收系统，可收加密电视
◆*带有传输流输入输出接口，可提供码流数据供码流分析用

PRK3CP/PRK3CDG/PRK4CP 是宝马电子 PRK 系列场强仪和频谱分析仪家族最新成员，精度和可靠性可满足 TV/FM/SAT/CATV/DVB 系统频谱和场强的高精度测量，适用于模拟和数字电视信号,符合欧洲标准。

PRK 系列仪器设计采用微机智能控制系统，业界最新流行的屏显菜单选择功能（OSD），具备自动分类衰减、自动校准补偿功能,能进行场强电平、V/A、C/N、数字频道功率等测量，可内置 QPSK、QAM、COFDM 和 MPEG-2 解碼，测量 BER 和 MER,并可显示 QAM 星座图。PRK 系列强大的数字信号测试功能，适应当前的数字化潮流。

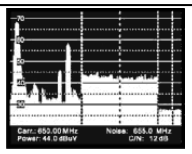
PRK 系列频谱分析功能强大，带有频率合成扫描，可选分辨率带宽、扫描时间和频率范围。伴音载波随所选制式在 4-9MHz 之间自动选择，并可测试 NICAM（丽音）伴音。

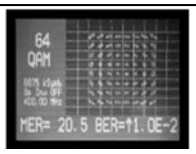
PRK 系列仪器设计先进，软件功能强大，是进行模拟/数字电视信号测量和分析的首选！

备注：带*标记为选配功能，请注意不同型号间的功能差别。

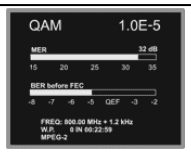
参考图例

视频/音频测量


频谱模式的载波/噪声比测量



QAM星座图



QAM调制信号的误码率测量