

YIDONG ZHONGDUAN YUANLI YU SHIJIAN



21 世纪高职高专规划教材
高等职业教育规划教材编委会专家审定

移动终端原理与实践

主 编 蔡卫红
副主编 孔凡凤 欧红玉



北京邮电大学出版社
www.buptpress.com



世纪高职高专规划教材

高等职业教育规划教材编委会专家审定

移动终端原理与实践

主 编 蔡卫红
副主编 孔凡凤 欧红玉



北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书是采用理、实结合模式编写的新型课程教材,全书采用项目教学的方法,全面介绍了移动终端原理与维修基本技术,结构层次由浅入深,循序渐进。项目教学内容以数字移动终端为载体,将数字移动终端维修技术分为8个项目,分别介绍了移动终端电路原理、维修工具的使用、移动终端测试维修方法。全书图文并茂,通俗易懂,每个项目都设有项目学习内容引导以及项目习题,方便课程教师与学生的学习与交流。

本教材为高职高专使用教材,可作为电子信息类、通信类等相关专业移动终端维修课程的教学用书,适合高职高专院校开展理、实结合一体化课程教学使用;也可作为移动终端维修培训教材;同时适合从事移动终端生产、移动终端维修中级技术人员、业余爱好者阅读。

图书在版编目(CIP)数据

移动终端原理与实践 / 蔡卫红主编. --北京:北京邮电大学出版社, 2013. 8

ISBN 978-7-5635-3526-2

I. ①移… II. ①蔡… III. ①移动终端—高等职业教育—教材 IV. ①TN87

中国版本图书馆 CIP 数据核字(2013)第 122083 号

书 名: 移动终端原理与实践

主 编: 蔡卫红

责任编辑: 彭 楠 马晓仟

出版发行: 北京邮电大学出版社

社 址: 北京市海淀区西土城路 10 号(邮编: 100876)

发 行 部: 电话: 010-62282185 传真: 010-62283578

E-mail: publish@bupt.edu.cn

经 销: 各地新华书店

印 刷: 北京鑫丰华彩印有限公司

开 本: 787 mm×1 092 mm 1/16

印 张: 15.75

字 数: 392 千字

版 次: 2013 年 8 月第 1 版 2013 年 8 月第 1 次印刷

ISBN 978-7-5635-3526-2

定 价: 32.00 元

· 如有印装质量问题,请与北京邮电大学出版社发行部联系 ·

前 言

为培养移动通信技术相关专业在移动终端维修方面高素质、高技能型人才,真正提高学生实践能力,编者在总结多年理论与实践教学的基础上,编写了《移动终端原理与实践》教材。

本书为基于工作过程的新型教材,采用项目-任务式的结构,全面介绍了移动终端原理与维修方法。全书分为8个项目:项目一为移动终端认知;项目二为移动终端基本电路了解;项目三为移动终端收/发射频电路结构认知;项目四为项目实践——移动终端拆卸与元器件识别;项目五为移动终端主要电路案例分析;项目六为项目实践——移动终端维修工具使用及元器件焊接;项目七为项目实践——GSM移动终端电路识图;项目八为项目实践——移动终端信号测试与故障检修。内容涉及移动终端的发展、基本电路原理、射频电路结构分类、拆卸方法、元器件识别、主要电路原理、维修工具使用、元器件焊接、电路识图、信号测试方法和基本故障维修等。

本书在编写的过程中,坚持“以就业为导向,以能力为本位”的基本思想,基于岗位技能,采用理论、实践一体化教学的编写思路,较好地体现了“理论够用,能力为本,面向应用性技能型人才培养”的职业教育特色。

本书由湖南邮电职业技术学院的蔡卫红老师主编,孔凡凤老师、欧红玉老师任副主编。其中项目一、项目四、项目五、项目六、项目七、项目八由蔡卫红老师编写,项目二由孔凡凤老师编写,项目三由欧红玉老师编写。

由于编者水平有限,书中难免有不妥或错误之处,恳请读者批评指正。

编 者

目 录

项目一 移动终端认知	1
任务1 移动终端发展及终端设备	1
任务2 手机卡与存储器	8
任务3 GSM 移动终端信号处理	12
项目习题1	14
项目二 移动终端基本电路了解	15
任务1 基本单元电路	15
任务2 逻辑/音频电路与 I/O 接口	24
项目习题2	27
项目三 移动终端收/发射频电路结构认知	28
任务1 移动终端接收机/发射机电路结构分类	28
任务2 GSM 移动终端射频电路结构分类	31
任务3 CDMA 移动终端射频电路结构分类	37
任务4 WCDMA/TD-SCDMA 移动终端射频电路结构分类	42
项目习题3	47
项目四 项目实践——移动终端拆卸与元器件识别	48
任务1 常见移动终端拆卸实践	48
任务2 移动终端主要元器件识别	56
项目习题4	67
项目五 移动终端主要电路案例分析	68
任务1 移动终端电源电路/充电电路原理案例分析	69
任务2 移动终端接收和频率合成电路原理案例分析	75
任务3 移动终端发射电路原理案例分析	88
任务4 移动终端显示电路/卡电路原理案例分析	94
任务5 移动终端其他电路原理案例分析	97
项目习题5	103

项目六 项目实践——移动终端维修工具使用及元器件焊接	104
任务 1 移动终端主要维修工具使用	104
任务 2 移动终端元器件焊接	112
项目习题 6	118
项目七 项目实践——GSM 移动终端电路识图	119
任务 1 GSM 移动终端电路识图实践基础	119
任务 2 移动终端射频电路识图实践	126
任务 3 移动终端音频处理/逻辑控制电路识图实践	130
项目习题 7	141
项目八 项目实践——移动终端信号测试与故障检修	142
任务 1 移动终端常见供电电压/信号波形/信号频率测试	142
任务 2 诺基亚 3210 手机电路分析与测试实践	153
任务 3 移动终端故障分析与处理	219
任务 4 诺基亚 3210 手机主要故障分析与检修技巧	222
任务 5 诺基亚 3210 手机故障维修实例	236
项目习题 8	245
参考文献	246

项目一 移动终端认知

项目目的

1. 了解手机的发展历程和各代手机的优缺点；
2. 掌握 GSM 手机终端电路组成和主要技术参数及应用；
3. 掌握 CDMA 手机主要技术参数及应用；
4. 了解 SIM 和 UIM 卡管脚排列、功能和卡中数据、密码情况及应用；
5. 掌握移动终端中存储器的分类、作用及应用；
6. 掌握 GSM 手机信号处理和开机过程。

项目工具

1. 1G、2G、3G 移动终端；
2. GSM 手机 SIM 卡和 CDMA 手机 UIM 卡；
3. 移动终端图纸。

项目重点

1. GSM 手机和 CDMA 手机主要技术参数；
2. SIM 卡和 UIM 卡管脚排列、功能和卡中数据、密码情况；
3. GSM 手机存储器的分类和应用；
4. GSM 手机电路组成。

任务 1 移动终端发展及终端设备

[任务导入]

移动通信是指通信双方，至少有一方是在移动中进行的传输与交换，固定点与移动体(车辆、船舶、飞机)之间、移动体之间的通信，都属于移动通信的范畴。

手机是移动电话的简称，又称为手提电话、手提、大哥大，是便携的、可以在较大范围内移动的电话终端。手机是移动通信技术发展的产物。随着经济的发展和时间的推移，手机已经成为人们日常生活必不可少的工具，具有非常广阔的发展前景。

目前在全球范围内使用最广的手机是 GSM 手机。第 1 代模拟手机已经淹没在移动通信技术发展的潮流中,3G 手机开始走上了普及的道路。在中国大陆及中国台湾地区以 GSM 最为普遍,这些都是所谓的第 2 代手机(2G)。2G 手机都是数字制式的,除了可以进行语音通信外,还可以收发短信(短消息、SMS)、彩信(多媒体短信、MMS)、无线应用协议(WAP)、通用分组无线业务(GPRS)等。部分手机除了典型的电话功能外,还包含了 PDA、游戏机、MP3、照相、录音、摄像、GPS 等更多的功能。

1. 手机发展进程

(1) 模拟手机

第 1 代手机(1G)是指模拟的移动电话,也就是 20 世纪八九十年代在中国香港、美国等影视作品中出现的大哥大。最先研制出大哥大的是美国摩托罗拉公司的 Cooper 博士。由于当时的电池容量限制和模拟调制技术需要硕大的天线和集成电路的发展状况等制约,这种手机外表四方,只能成为可移动但算不上便携。很多人称呼这种手机为“砖头”或是“黑金刚”等。

这种手机有多种制式,如 NMT、AMPS、TACS,但是基本上使用频分复用方式,只能进行语音通信,收讯效果不稳定,且保密性不足,无线带宽利用不充分。此种手机类似于简单的无线电双工电台,通话锁定在一定频率,所以使用可调频电台就可以窃听通话。

(2) GSM/CDMA 手机

第 2 代手机也是最常见的手机。通常这些手机使用 PHS、GSM 或 CDMA 这些十分成熟的标准,具有稳定的通话质量和合适的待机时间。为了适应数据通信的需求,在第 2 代手机中,一些中间标准也得到支持,例如支持彩信业务的 GPRS 和上网业务的 WAP 服务,以及各式各样的 Java 程序等。

1993 年,我国开始建设“全球通(GSM)”数字移动电话网。经过十多年的发展,2G 网络已经遍布全国每个角落。

2001 年年底,中国联通开通了 CDMA 网络——“联通新时空”(现已转让给中国电信),它属于码分多址(CDMA)方式,其核心技术以 IS-95 作为标准,是增强型 IS-95。CDMA 和 GPRS 实际上各有优缺点,难分高低。

作为第 2 代向第 3 代的过渡,有时又将中国移动的 GPRS、中国电信的 CDMA 称为 2.5G(2 代半)。

(3) 3G 手机

随着经济的发展和时间的推移,用于第 3 代移动通信系统(3G)的手机已经走上历史舞台。3G 是 3rd Generation 的缩写,指第 3 代移动通信技术。第 3 代手机最初的目标之一是开发一种可以全球通用的无线通信系统,但最终的结果是出现了多种不同的制式,主要有 WCDMA、CDMA2000 和 TD-SCDMA。这些新的制式都基于 CDMA(码分多址)技术,在带宽利用和数据通信方面都有进一步发展。

相对第 1 代模拟制式手机和第 2 代 GSM、CDMA 等数字手机,一般地讲,第 3 代手机是指将无线通信与国际互联网等多媒体通信结合的新一代移动通信系统。它能够处理图像、音乐、视频流等多种媒体形式,提供包括网页浏览、电话会议、电子商务等多种信息服务。为了提供这种服务,无线网络必须能够支持不同的数据传输速度,也就是说在室内、室外和行车的环境中能够分别支持至少 2 Mbit/s、384 kbit/s 以及 144 kbit/s 的传输速度。

表 1-1 为 3 代移动通信的主要特点。

表 1-1 3 代移动通信比较

第 1 代	第 2 代	第 3 代
模拟(蜂窝)	数字(双频)	多频
仅限话音通信	话音和数据通信	当前通信业务和一些新业务
主要用于户外覆盖	户内/户外覆盖	无缝全球漫游
固定电话网的补充	与固定电话网相互补充	结合数据网、因特网等,作为信息通信技术的重要方式
以企业用户为中心	企事业单位和消费者	通信用户
主要接入技术:FDMA	主要接入技术:TDMA	主要接入技术:CDMA
主要标准:TACS、AMPS 等	主要标准:GSM 等	重要标准:WCDMA、CDMA2000、TD-SCDMA 等

(4) 4G 手机

4G 手机距离我们将不再遥远。工信部 2010 年 12 月批复同意具有我国自主知识产权的准 4G 网络(TD-LTE)的规模试验总体方案,上海、杭州、南京、广州、深圳、厦门 6 个城市成为首批试点城市。

4G 移动系统网络结构可分为 3 层:物理网络层、中间环境层、应用网络层。物理网络层提供接入和路由选择功能,它们由无线和核心网的结合格式完成。中间环境层的功能包括 QoS 映射、地址变换和完全性管理等。物理网络层与中间环境层及其应用环境之间的接口是开放的,它使发展和提供新的应用及服务变得更为容易,提供无缝高数据率的无线服务,并运行于多个频带。这一服务能自适应多个无线标准及多模终端,跨越多个运营者和服务,提供大范围服务。第 4 代移动通信系统的关键技术包括信道传输技术;抗干扰性强的高速接入技术;调制和信息传输技术;高性能、小型化和低成本的自适应阵列智能天线;大容量、低成本的无线接口和光接口;系统管理资源;软件无线电、网络结构协议等。第 4 代移动通信系统主要是以正交频分复用(OFDM)为技术核心。OFDM 技术的特点是网络结构高度可扩展,具有良好的抗噪声性能和抗多信道干扰能力,可以提供比目前无线数据技术质量更高(速率高、时延小)的服务和更好的性能价格比,能为 4G 无线网提供更好的方案。例如,无线区域环路(WLL)、数字音讯广播(DAB)等都将采用 OFDM 技术。4G 移动通信对加速增长的广带无线连接的要求提供技术上的回应,对跨越公众的和专用的、室内和室外的多种无线系统和网络保证提供无缝的服务。通过对最适合的可用网络提供用户所需求的最佳服务,能应付基于因特网通信所期望的增长,增添新的频段,使频谱资源大扩展,提供不同类型的通信接口。运用路由技术为主的网络架构,以傅里叶变换来发展硬件架构实现第 4 代网络架构,移动通信将向数据化、高速化、宽带化、频段更高化方向发展,移动数据、移动 IP 将成为未来移动网的主流业务。

2. 手机发展大记事

- 1956 年,爱立信公司和瑞典一家公司合作制造了世界上第一部可移动式通信电话;
- 1973 年 4 月,世界上第一部移动电话(摩托罗拉 3200)由美国著名的摩托罗拉公司的工程技术人员马丁·库帕发明,这种电话重约 1.13 千克,靠电池运转,总共可通话 10 分钟。此电话的发明标志着世界进入移动通信的新时代;

- 1989 年,世界上第一款翻盖式手机摩托罗拉 MicroTac 950 诞生,这款手机开创了时尚化的崭新天地,最终为今天各种各样的纤薄手机的发展奠定了基础;
- 1995 年,爱立信 GH337 成为第一款进入国内的 GSM 手机;
- 1995 年,爱立信公司推出的爱立信 GH398 成为第一款可编铃声手机;
- 1997 年,汉诺佳 CH9771 成为第一款内置天线手机;
- 1998 年,诺基亚 6110 成为第一款内置游戏手机;
- 1999 年,第一款中文手机摩托罗拉 CD928+ 诞生;
- 1999 年,摩托罗拉 328C 成为第一款翻盖设计手机;
- 1999 年,爱立信推出了 R250s PRO 三防手机;
- 2000 年,诺基亚 7110 成为国内最早支持 WAP 的手机;
- 2000 年,三星 SCH-M188 成为第一部 MP3 手机;
- 2000 年,西门子 6688 成为第一部支持扩展卡音乐手机;
- 2000 年,爱立信 R380sc 成为第一部塞班(Symbian)智能手机;
- 2000 年,夏普和日本沃达丰合作推出的 J-SH04 首部拥有摄像头的手机;
- 2001 年,三星公司推出了世界上第一部双屏手机三星 A288;
- 2001 年,第一款彩屏手机西门子 S1088 诞生;
- 2002 年,摩托罗拉推出的 V70 手机采用了 360° 旋转设计,这样的设计可以说是彻底颠覆了传统的手机打开方式,开创了旋转的新时代,后来 LG KG928,索尼爱立信 W550i、S700,夏普 V903SH,诺基亚 7373、N93 等均采用了各种不同的旋转外型设计;
- 2002 年,摩托罗拉 V8060 是中国第 1 代机卡分离式 CDMA 手机;
- 2003 年,索尼爱立信 P802 成为第一部 UIQ 智能手机;
- 2003 年,诺基亚 6650 成为国内第一款 WCDMA 手机;
- 2004 年,摩托罗拉 Razr v3 将超薄设计提高到了一个新的水平,带来了超薄设计的潮流;
- 2006 年,LG 推出了首部采用红外触摸感应按键手机——LG Chocolate KG90;
- 2007 年,LG 推出第一款金属外壳超薄滑盖手机——LG Shine,带动了目前手机设计领域的金属风潮;
- 2007 年,苹果 iPhone 成为跨时代的手机设计革命;
- 2008 年,三星 SCH-B600 成为第一部千万像素拍照手机;
- 2008 年,HTC G1 成为第一部安卓(Android)智能手机;
- 2008 年,诺基亚 5800 成为最具人气的触屏手机;
- 2008 年,海信 TM86 成为第一款获得验证的 TD 手机;
- 2009 年,三星公司生产的 S7550 手机成为全球第一款太阳能手机;
- 2010 年,LG 公司生产的 LG990 手机成为全球第一款双核手机;
- 2010 年,HTC EVO 4G 成为全经一款支持 4G 网络的手机;
- 2012 年,LG 公司生产的 LG Optimus 4X HD 成为全球的第一款四核手机。

3. 移动终端设备

(1) GSM 手机

手机与 SIM 卡共同构成 GSM 移动通信系统的终端设备,也是移动通信系统的重要组

成部分。虽然手机品牌、型号众多,但从电路结构上都可简单地分为射频部分、逻辑音频部分、接口部分和电源部分。

手机的基本组成框图如图 1-1 所示。

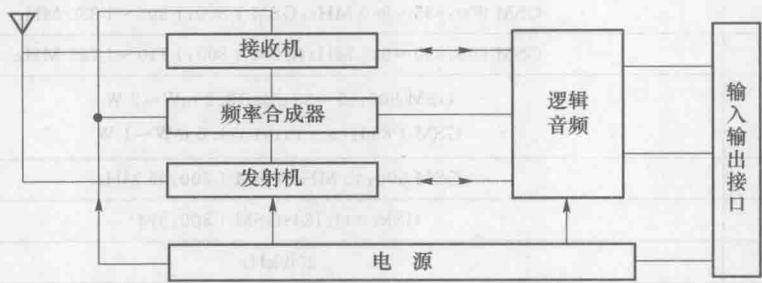


图 1-1 GSM 手机组成框图

1) 射频部分

射频部分由天线、接收电路、发送电路、调制解调器和振荡器等高频系统组成。其中发送部分是由射频功率放大器和带通滤波器组成,接收部分由高频滤波、高频放大、下变频、中频滤波放大器组成。振荡器完成收信机高频信号的产生,具体由频率合成器控制的压控振荡器实现。

2) 逻辑音频部分

发送通道的处理包括语音编码、信道编码、加密、TDMA 帧形成。其中信道编码包括分组编码、卷积编码和交织。接收通道的处理包括均衡、信道分离、解密、信道解码和语音解码。逻辑控制部分对手机进行控制和管理,包括定时控制、数字系统控制、天线系统控制以及人机接口控制等。

3) 接口部分

接口模块包括模拟语音接口、数字接口及人机接口 3 部分。模拟语音接口包括模/数(A/D)转换、数/模(D/A)转换、话筒和耳机;数字接口主要是数字终端适配器;人机接口主要有显示器和键盘。

4) 电源

电源部分为射频部分和逻辑部分供电,同时又受到逻辑部分的控制。

手机的硬件电路由专用集成电路组成。专用集成电路包括收信电路、发信电路、锁相环电路、调制解调器、均衡器、信道编解码器、控制器、识别卡和数字接口、语音处理专用集成电路等部分。手机的控制器由微处理器构成,包括中央处理器(CPU)、可擦写可编程只读存储器(EPROM)和电可擦写可编程只读存储器(EEPROM)等部分。

另外,软件也是手机的重要组成部分。手机的整个工作过程由 CPU 控制,CPU 由其内部的软件程序控制,而软件程序来源于 GSM 规范。

GSM 双频手机的技术指标如表 1-2 所示。

表 1-2 GSM 双频手机的技术指标

参数	数值
频率	GSM 900、GSM 1 800
接收频率范围	GSM 900:935~960 MHz;GSM 1 800:1 805~1 880 MHz
发射频率范围	GSM 900:890~915 MHz;GSM 1 800:1 710~1 785 MHz
输出功率	GSM 900:(5~33 dBm)3.2 mW~2 W GSM 1 800:(0~30 dBm)1.0 mW~1 W
双工间隔	GSM 900:45 MHz;GSM 1 800:95 MHz
信道数	GSM 900:124;GSM 1 800:374
信道间隔	200 kHz
功率级别数	GSM 900:15;GSM 1 800:16
接收灵敏度	GSM 900:-102 dBm;GSM 1 800:-100 dBm
频率误差	$<1\times10^{-7}$
平均相位误差	$<5.0^{\circ}$
峰值相位误差	$<20.0^{\circ}$

(2) CDMA 手机

当前大部分厂商生产的 CDMA 手机都是 CDMA2000 1x 模式,且使用美国高通公司开发出来的 CDMA 移动台芯片应用组(主要有 MSM3100、MSM3300、MSM5100、MSM5105 等几个系列)。不同 CDMA 手机具体的卡接口技术不同,在整机电路设计中所应用的硬件也有区别,有机卡分离与机卡一体两种类型。

1) CDMA 手机技术指标

CDMA 手机一般的技术指标如表 1-3 所示。

表 1-3 CDMA 手机的技术指标

指标项	技术参数
接收频率范围	869.820~893.190 MHz
本振频率范围	966.88±12.5 MHz
接收中频	85.38 MHz
发射频率范围	824.820~848.190 MHz
发射中频频率	130.38 MHz
输出功率	0.32 W
抗干扰性能	单音:900 kHz 时为-30 dBm 双音:900 kHz 与 1700 MHz 时为-43 dBm
发射频率偏差	±300 Hz 或更低
伪波发射	900 kHz 低于-42 dBc/30 kHz 1.98 MHz 低于-54 dBc/30 kHz
最小发射能量控制	-50 dBm 以下
接/发频率间隔	45 MHz
频道带宽	20 CH

续表

指标项	技术参数
频率空间	1.25 MHz
系统主时钟	19.2/19.68/19.8 MHz
工作电压	DC 3.2~4.2 V
频率稳定性	± 0.5 PPM

中国电信现行 CDMA 网的上行频率为 825~835 MHz,下行频率为 870~880 MHz。

2) CDMA 手机比 GSM 手机的优越之处

① 接通率高。上网的人都有经验,在同时上网的人数少的时候上网,网塞少、容易接通。打手机也是同样的道理,对于相同的带宽,CDMA 系统是 GSM 系统容量的 4~5 倍,网塞大大下降,接通率自然提高。

② 手机电池的使用寿命延长。CDMA 采用功率控制和可变速率声码器,平均功耗较低,手机电池使用寿命延长。

③ “绿色手机”。普通的手机(GSM 和模拟手机)功率一般能控制在 600 mW 以下,而 CDMA 手机的问世,给人们带来了“绿色”环保手机的曙光,因为与 GSM 手机相比,CDMA 手机的发射功率可以减小很多。CDMA 手机发射功率最高只有 200 mW,普通通话功率更小,其辐射作用可以忽略不计,对健康没有不良影响。基站和手机发射功率的降低,将大大延长手机的通话时间,这意味着电池的寿命延长了,对环境起到了保护作用,故称之为“绿色手机”。

④ 话音质量高。CDMA 采用了先进的数字语音编码技术,并使用多个接收机同时接收不同方向的信号。

⑤ 不易掉话。基站是手机通话的保障,当用户移动到基站覆盖范围的边缘时,基站就应该自动“切换”来保障通信的继续,否则就会掉话。CDMA 系统切换时的基站服务是“单独覆盖—双覆盖—单独覆盖”,而且是自动切换到相邻较为空闲的基站上,也就是说,在确认手机已移动到另一基站单独覆盖地区时,才与原先的基站断开,这种“软切换”大大减少了掉话的可能性。

⑥ 保密性能更好。通话不会被窃听,要窃听通话,必须要找到码址。但 CDMA 码址是个伪随机码,而且共有 4.4 万亿种可能的排列。因此,要破解密码或窃听通话内容非常困难。

(3) 国际移动设备识别码(IMEI 码)

在移动电话机背面标签上有一些代码,这些代码有其特殊的含义。首先是 15 位数字组成的国际移动设备识别码(IMEI 码),每部移动电话机出厂时设置的该号码都是全世界唯一的,作为移动电话机本身的识别码,不仅标在机背的标签上,还以电子方式存储于移动电话机中,具体地说,是在移动电话机电路板中的电可擦除存储器中。IMEI 码各部分含义如下。

第 1~6 位数字(TAC)——型号批准号,由欧洲型号批准中心分配;

第 7~8 位数字(FAC)——厂家装配号码,表示生产厂家或最后装配所在地,由厂家进行编码;

第 9~14 位数字(SNR)——序号码,这个独立序号唯一地识别每个 TAC 和 FAC 中的每个移动设备;

第 15 位数字(SP)——备用,一般为 0。

在移动电话机开机的状态下,甚至不需要插卡,从键盘上输入“* #06 #”,就会在屏幕上显示移动电话机中存储的 IMEI 码。

任务 2 手机卡与存储器

[任务导入]

手机与手机卡共同构成移动通信终端设备。GSM 手机的手机卡叫 SIM 卡,机卡分离式 CDMA 手机的手机卡叫 UIM 卡,SIM 或 UIM 都是“用户识别模块”的意思。

无线传输比固定传输更易被窃听,如果不提供特别的保护措施,很容易被窃听或被假冒一个注册用户。系统通过引入 SIM 卡或 UIM 卡,使手机在入网或通话时通过鉴权来防止未授权用户的接入,这样保护了网络运营者不被假冒用户免费通信的利益;通过对传输加密,可以防止在无线信道上被窃听,从而保护了用户的隐私。无线电通信从不保密的禁区解放出来。

手机卡上存储了所有属于本用户的信息和各种数据,每一张卡对应一个移动用户电话号码。机卡分离后,使手机不固定地“属于”一个用户,实现“手机号码随卡不随机”的功能。

只有在处理异常的紧急呼叫(如拨打 112)时可以不插入卡。维修者也可以在无卡的情况下,通过拨打“112”来判断移动电话机发射是否正常。

移动电话可以说是一个可通话的计算机系统,运行的程序需要存储器,处理数据需要存储器,存储数据也需要存储器。没有存储器,系统就无法工作。

手机中的存储器组一般包括两种不同类型的存储器:数据存储器 and 程序存储器。数据存储器即 SRAM——静态随机存储器,又称暂存器;手机中的程序存储器大多由两部分组成,包括 EEPROM——电可擦写可编程只读存储器(俗称码片)和 FLASH——闪速只读存储器(俗称字库或版本)。

1. SIM 卡

(1) SIM 卡的内容

SIM 卡是一张符合通信网络规范的“智能”卡,它内部包含了与用户有关的、被存储在用户这一方的信息。SIM 卡内部保存的数据可以归纳为以下 4 种类型。

1) 由 SIM 卡生产商存入的系统原始数据,如生产厂商代码、生产串号、SIM 卡资源配置数据等基本参数。

2) 由 GSM 网络运营商写入的 SIM 卡所属网络与用户有关的、被存储在用户这一方的网络参数和用户数据等,包括:

① 鉴权和用户密钥 Ki;

② 国际移动用户号(IMSI);

- ③ A3——IMSI 认证算法;
- ④ A5——加密序列生成算法;
- ⑤ A8——密钥(Kc)生成前,用户密钥生成算法。

3) 由用户自己存入的数据。如缩位拨号信息、电话号码簿、移动电话机通信状态设置等。

4) 用户在使用 SIM 卡过程中自动存入及更新的网络接续和用户信息。如临时移动台识别码(TMSI)、位置区域识别码(LAI)、密钥(Kc)等。上面第 1 类属永久数据,第 2 类数据只有 GSM 网络运营商才能查阅和更新。

图 1-2 为 SIM 卡外形。个人识别码(PIN)是 SIM 卡内部的一个存储单元,PIN 密码锁定的是 SIM 卡。若将 PIN 密码设置开启,则该卡无论放入任何移动电话机,每次开机均要求输入 PIN 密码,密码正确后才可进入 GSM 网络。若错误地输入 PIN 码 3 次,将会导致“锁卡”的现象,此时只要在移动电话机键盘上按一串阿拉伯数字(PUK 码),就可以解锁。但是用户一般不知道 PUK 码。特别提醒:如果尝试输入 10 次仍未解锁,就会“烧卡”,必须再去购买新号了。设置 PIN 码可防止 SIM 卡未经授权而使用。



图 1-2 SIM 卡外形

如果 SIM 卡在一部移动电话机上可以用,而在另一部移动电话机上不能用,有可能是因为在移动电话机中已经设置了“用户限制”功能,这时可通过用户控制码(SPCK)取消该移动电话机的限制功能。例如,三星 600、摩托罗拉 T2688 等机型,移动电话机的“保密菜单”可进行 SIM 卡限定设置,即设置后的移动电话机只能使用限定的 SIM 卡。设置后的移动电话机换用其他 SIM 卡时会被要求输入密码,密码输入正确方可进入网络。如果忘记密码,则只能用软件故障维修仪重写移动电话机码片进行解锁。而设置后的 SIM 卡能在其他移动电话机中正常使用,不会提问密码。即“用户限制”功能用密码锁定的是移动电话机。

在我国,有一些移动电话机生产商或经销商,把移动电话机与“中国移动”或“中国联通”的 SIM 卡做了捆绑销售(价格相对较便宜),那么,移动电话机在使用时就只能使用“中国移动”或“中国联通”的 SIM 卡,这不是故障,而是使用了“网络限制”功能,即“锁网”。这时可通过 16 位网络控制码(NCK)来解除锁定,但需通过 GSM 网络运营商才能解决。

上述“PIN 码”、“用户限制”密码和“网络限制”密码均为不同的概念,同时与“话机锁”密码也不同。设置“话机锁”密码可防止移动电话机未经授权而使用。许多款移动电话机出厂时的话机锁密码为“1234”,也有的是全“0”等。

(2) SIM 卡的构造

SIM 卡是带有微处理器的芯片,包括 5 个模块:微处理器、程序存储器、工作存储器、数

据存储器和串行通信单元,每个模块对应一个功能。至少有 5 个端口:电源、时钟、数据、复位、接地端。图 1-3 为 SIM 卡触点端口功能,图 1-4 为移动电话机中 SIM 卡座。

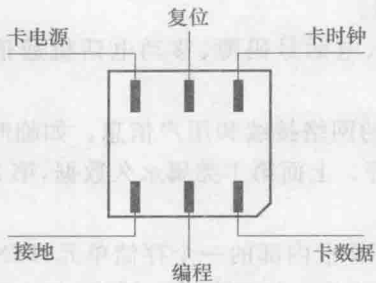


图 1-3 SIM 卡触点功能

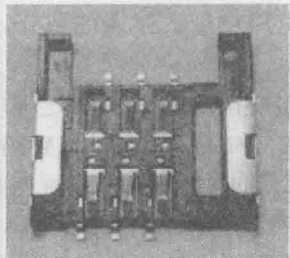


图 1-4 SIM 卡座

SIM 卡座在移动电话机中提供移动电话机与 SIM 卡通信的接口。它通过卡座上的弹簧片与 SIM 卡接触,所以如果弹簧片变形,会导致 SIM 卡故障,例如显示“检查卡”、“插入卡”等。早期生产的移动电话机设有卡开关,卡开关是判断卡是否插入的检测点,如摩托罗拉 328 移动电话机,由于卡开关的机械动作多,容易造成卡开关损坏。现在新型的移动电话机已经将此去除,而是通过数据的收集来识别卡是否插入,减少卡开关不到位或损坏造成的问题。

卡电路中的电源 SIM VCC、SIM GND 是卡电路工作的必要条件。卡电源用万用表就可以检测到。SIM 卡插入移动电话机后,电源端口提供电源给 SIM 卡内的单片机。检测 SIM 卡存在与否的信号只在开机瞬时产生,当开机检测不到 SIM 卡存在时,将提示“Insert Card”(插入卡);如果检测 SIM 卡已存在,但机卡之间的通信不能实现,会显示“Check Card”(检查卡);当 SIM 卡对开机检测信号没有响应时,移动电话机也会提示“Insert Card”(插入卡)。SIM 卡的供电分为 5 V(1998 年前发行)、5 V 与 3 V 兼容、3 V、1.8 V 等,当然这些卡必须与相应的移动电话机配合使用,即移动电话机产生的 SIM 卡供电电压与该 SIM 卡所需的电压要匹配。

对于卡电路中的 SIM I/O、SIM CLK、SIM RST,全部是由 CPU 的控制来实现的。虽然手机与网络之间的数据传输随时随地进行着,但确定哪个时刻数据传输往往很难。有一点可以肯定,当移动电话机开机时刻与网络进行鉴权时必有数据沟通,这时尽管时间很短,但测量时一定有数据,所以我们在判定卡电路故障时,这个时间段上监测为最佳。正常开机的移动电话机,在 SIM 卡座上用示波器可以测量到 SIM I/O、SIM CLK、SIM RST 信号,它们一般是一个 3 V 左右的脉冲。若测不到,说明 SIM 卡座供电开关管周边电阻电容元件脱焊、SIM 卡座脱焊,也有可能是卡座接触不良,SIM 卡表面脏或使用废卡。使用 SIM 卡时要小心,不要用手去触摸上面的触点,以防止静电损坏,更不能折叠。如果 SIM 卡脏了,可用酒精棉球轻擦。

SIM 卡的存储容量有 3K、8K、16K、32K、64K、128K 等。STK 卡是 SIM 卡的一种,它能为移动电话机提供增值服务,如移动电话机银行等。

每当移动用户重新开机时,GSM 系统要自动鉴别 SIM 卡的合法性,GSM 网络的身份鉴权中心对 SIM 卡进行鉴权,即与移动电话机对一下“口令”,只有在系统认可之后,才为该移动用户提供服务,系统分配给用户一个临时号码(TMSI),在待机、通话中使用的仅为这

个临时号码,这就增加了保密度。

目前,网络运营商在用户入网时没有对移动电话机的国际移动设备识别码(IMEI)实行鉴别,如果实行鉴别,带机入网的用户数量可能会下降,不利于吸引更多的用户使用 GSM 移动电话机。

2. UIM 卡

机卡分离式 CDMA 手机,“入网”时需要配置 UIM 卡(机卡一体式手机无须配置)。UIM 卡功能、外型与 SIM 卡相似,同样有电源、时钟、数据、复位、接地端,只是各个触点的具体位置排列与 SIM 卡略有差异。相应地,CDMA 手机中必须有一个 UIM 卡电路,以给 UIM 卡提供电源、时钟、数据、复位等。

3. 手机中的存储器

(1) 数据存储器

数据存储器(RAM)的作用主要是存储一些手机运行过程中须暂时保留的信息,如暂时存储各种功能程序运行的中间结果,作为运行程序时的数据缓存区。手机中常用的存储器是静态存储器(SRAM),又称随机存储器,其对数据(如输入的电话号码、短信息、各种密码等)或指令(如驱动振铃器振铃、开始录音、启动游戏等指令)的存取速度快,存储精度高,但其中所存信息一旦断电,就会丢失。数据存储器正常工作时须与微处理器配合默契,即在由控制线传输的指令的控制下,通过数据传输线与微处理器交换信息。数据存储器提供了整个手机工作的空间,其作用相当于计算机中 RAM 内部存储器。

(2) 程序存储器

部分手机的程序存储器由两部分组成,一个是快擦写存储器(FlashROM),俗称字库或版本;另一个是电擦除可编程只读存储器(EEPROM),俗称码片。手机的程序存储器存储着手机工作所必须的各种软件及重要数据,是整机的灵魂所在。

在手机程序存储器中,FlashROM 作为只读存储器(ROM)来使用,主要是存储工作主程序,即以代码的形式装载话机的基本程序和各種功能程序。话机的基本程序管理着整机工作,如各项菜单功能之间的有序连接与过渡的管理程序、各子菜单返回其上一级菜单的管理程序、根据开机信号线的触发信号启动开机程序的管理等,各功能程序如电话号码的存储与读出、铃声的设置与更改、短信息的编辑与发送、时钟的设置、录音与播放、游戏等菜单功能的程序。快擦写存储器是一种非易失性存储器,当关掉电路的电源后,所存储的信息不会丢失。它的存储器单元是电可擦除的,即快擦写存储器既可电擦除,又可用新的数据再编程。快擦写存储器在手机中一般用于相对稳定的、正常使用手机时不用更改程序的存储,这与它们有限的擦除、重写能力有关。若 FlashROM 发生故障,整个手机将陷入瘫痪。

码片(EEPROM)的主要特点是能进行在线修改存储器内的数据或程序,并能在断电的情况下保持修改结果。根据数据传输方式分类,码片可以分为两大类:一类为并行数据传送的码片,另一类为串行数据传送的码片。

现各种类型的手机所采用的码片很多,但其作用几乎是一样的,在手机中主要存放系统参数和一些可修改的数据,如手机拨出的电话号码、菜单的设置、手机解锁码、PIN 码、手机的机身码(IMEI)等以及一些检测程序,如电池检测程序、显示电压检测程序等。码片出现问题时,手机的某些功能将失效或出错,如菜单错乱、背景灯失控等。此时有如下现象:显示