HackRF One 使用手册

一、前言

- 二、硬件介绍
 - 1. IC 介绍
 - 2. 无线链路介绍
 - 3. PCB 介绍
- 三、WINDOWS 下安装 HackRF One 驱动与 SDR#
- 四、SDR#使用介绍
 - 1. 收听 FM 广播
 - 2. 监听对讲机
 - 3. 监听家用无线遥控
 - 4. 监听家用无线遥控
 - 5. 观察 GSM 信号
 - 6. 观察 WIFI 信号
 - 7. 安装 LEVELMETER 插件
- 五、UBUNTU 下编译安装 HACKRF 源码
- 六、UBUNTU 下安装及使用 GNURADIO 进行 FM 发射
- 七、HackRF One 固件更新
- 八、HackRF One CPLD 更新
- 九、问题与注意事项

二、硬件介绍

HackRF One 是一个完全开源的软件无线电硬件,频率从 10MHZ 到 6GHZ 范围,采样带 宽最大 20MHZ,8BIT 采样,USB 2.0 通讯。



下图介绍 HackRF One 硬件构造:

1. IC 介绍

RF ANT 无线收发天线接口。

RF AMP 开启拥有固定 14DB 增益,在不同的频率下实际增益会有差别。

On Board ANT 是板载天线。

Mixer 负责 10MHZ 到 2100MHZ 和 2700MHZ 到 6000MHZ 混至 AFE 中频。

AFE 是 2100MHZ 到 2700MHZ 宽带前端。

AD/DA 模数/数模转换。

CPLD 可编程逻辑 IC, 数字信号处理。

MCU 微处理器,负责与上位机通讯。

CLOCK 可编程时钟发生器,负责为 Mixer, AFE, CPLD, MCU 提供时钟,输入输出参考时钟。 FLASH 存储 MCU 程序。

POWER 提供 3.3V,1.8V 电源。

2. 无线链路介绍

频率为 2100MHZ 到 2700MHZ: 黄色标线为无线信号接收链路。 深红色线为无线信号发射链路。 无论发射还是接收都不通过 Mixer 处理。

频率为 10MHZ 到 2100MHZ 和 2700MHZ 到 6000MHZ: 短白色线为公共链路。 长白线为接收公共链路。 桔黄线为发射公共链路。 粉红线为 2700MHZ 以上过滤器链路。

黑色线为 2100MHZ 以下过滤器链路。

信号经过 Mixer 处理,接收为输入频率混合至中频,发射为中频混合至输出频率。

其余信号链路为公共部分。

3. PCB 介绍

HackRF One 为四层 PCB,第一层和第四层为信号,第二层和第三层为电源和地。 六个空为 3MM 接地螺丝孔。 裸露小焊点为测试点。 三、WINDOWS 下安装 HackRF One 驱动与 SDR#

WINDOWS 下的驱动为 libusb, libusb 有 32 位和 64 位版本,为了方便安装通常使用 zadig 来安装。

SDR#绑定了 zadig 只需下载 SDR#即可获得相应系统下的 zadig, SDR#官方地址 (<u>http://www.sdrsharp.com/</u>)。

下载后执行 install.bat 自动下载生成 sdrsharp 目录,在此目录下有 zadig.exe,与此同时 SDR#软件也同时下载完毕,此软件为绿色免安装软件,无须执行其它步骤 SDRSharp.exe 为 SDR#主程序。

将 HackRF One 插上计算机 USB,在任务管理器中看到如下图:

▷ □ 内存技术设备
🔺 📭 其他设备
hackRF One
▷ 🔚 人体学输入设备
▷ <u>□</u> 软件设备
🕨 🖬 声音、视频和游戏控制器

打开 zadig 做如下图片演示的选择:

HackRF	One		/	✓ 🗌 Edit
Driver	(NONE)	WinUSB (v6.1.7600.16385)	•	More Information WinUSB (libusbx)
USB ID	1D50 6089	Install Driver]	libusb-win32 libusbK

安装成功后在设备管理器显示如下图,说明驱动安装成功:



四、SDR#使用介绍

1. 收听 FM 广播

打开 SDR#后将设置调整到下图所示。



箭头指向从上到下分别表示:

音量大小,频率 HZ,设备源,,FM 调制,调制带宽 180K, Correct IQ 为频率中心噪声。

下图箭头指示为启动停止,配置按钮。

HackRF Controller 为配置面板,DEVICE 下为设备名称,这个只有 Jawbreaker 选项,和 作者说的一样 JUST a String, Sample Rate 为采样速率,LNA Gain 与 VGA Gain 分别是 AFE 增 益控制,AMP 为 RX AMP 启用/停止,PPM 为频率误差补偿。

PPM 在 HackRF 中若有测试具体值出可做适当修正以求得到较高的频率基准,原始的 HACKRF One 清单元件做出的硬件通常在 5 到 10 之间,特别修正后的 PPM 可以做到 5 左右, 频率越高对 PPM 要求越高,否则频率偏差较大。

urce	HackRF Controller				
	Device 🖌	HackRF			
dio	Jawbreaker	/ ×			
0.17	Sample Rate 🛛 🖌				
O AM	10 MSPS	~			
O DSB	LNA Gain				
t 📃		62			
Black	VGA Gain				
th					
180000 :	✔ Amp				
loh	Frequency correction (ppm)	0.0 🜲			
E0 -		C1			

通常在 FM 频率 LNA 设置在白天设置为 16,晚上设置为 8 即可正常工作,VGA 设置为 10, AMP 勾选。

设置完成后点击 CLOSE 或直接关闭即可。

点击启动按钮显示如下图





当选择好波峰后便能听到 FM 广播了。

2. 监听对讲机

如下图所示



选择 NFM,将 Correct IQ 勾选去除,以免听到不断的微波背景噪声,在波形窗口中偶 尔出现的波峰即是对讲机发出的信号。

3. 监听家用无线遥控

家用无线遥控通常是 315MHZ 和 433.92MHZ,将频率直接移动到这个中心频率即可, 其他方法同 FM。

4. 观察 GSM 信号

GSM 信号有两个频率 870MHZ, 950MHZ。



000.950.000.000



上图演示了两个频率下的 GSM BUSH 情况采样均为 10MSPS。

5. 观察 WIFI 信号



上图箭头指示了 WIFI 信号在通讯时的水波情况, 2.458GHZ 为 10 频道情况, 具体频率根据 附近的 WIFI 信号调整。

下表给出了 2.4G 频率:	長以供参考。				
信道	中心频率	信道	中心频率		
1	2412MHz	8	$2447 \mathrm{MHz}$		
2	2417MHz	9	2452MHz		
3	2422MHz	10	$2457 \mathrm{MHz}$		

2427MHz

2432MHz

2437MHz

あまい 供会せ

6. 安装 LEVELMETER 插件

将下载的 LevelMeter 文件复制到 sdrsharp 目录,用记事本打开 Plugins.xml 文件在 sharpPlugins 根下添加下面的代码重新启动即可。

11

12

13

<add

4

5

6

key="LevelMeter"

中心频率 2447MHz

2462MHz

2467MHz

2472 MHz

value="SDRSharp.LevelMeter.LevelMeterPlugin,SDRSharp.LevelMeter" /> 启动后在左侧窗口下多出 LevelMeter 项,如下图所示

Frequency Manager *
▼ LevelMeter *
Peak Power VF0 S1 -100 -110 -120 -130 -140 -140 dB
Mode Feak Power VFO V Smoothing show popup window
Peak Power VFO [dB] Avg Power BW [dB] Peak Power BW [dB]





五、UBUNTU 下编译安装 HACKRF 源码

在 UBUNTU 下使用 GIT 同步源码,同步地址 https://github.com/mossmann/hackrf.git 执行命令行: git clone <u>https://github.com/mossmann/hackrf.git</u> cd hackrf cd host mkdir build cd build cmake ../ make sudo make install 至此 HackRF 安裝完成。

执行

hackrf_info 如下图说明 hackrf 正确识别。

🕲 😑 🗊 ubuntu@ubuntu: ~

ubuntu@ubuntu:~\$ hackrf_info Found HackRF board. Board ID Number: 2 (HackRF One) Firmware Version: git-69c4997 Part ID Number: 0x0066434b 0x0066434b Serial Number: 0x0000000 0x0000000 0x238863c8 0x3271374b ubuntu@ubuntu:~\$ 六、UBUNTU下安装及使用 GNURADIO 进行 FM 发射 GNURADIO 安装相对比较复杂,具体安装步骤可以看官网流程。 或下载 GNURADIO LIVECD 将 ISO 直接坐到 U 盘中即可。 启动 gnuradio-companion,执行命令或者点击下图箭头指向图标即可。



拷贝 wbfm_tx_hackrf.grc 和 WAV 音频文件到 Documents 文件夹并加载,如下图



双击 WAV File Source 如下图

	800	Propertie	es: Wav File Source		
Options	General	Advanced	Documentation		
ID: wbfm_tx_hackrf Generate Options: No GUI		ID	blocks_wavfile_source_0		
Run Options: Prompt for Exit	File		/home/ubuntu/Documents/lethergo.wav		
	R	lepeat	Yes ‡		
	NC	hannels	2		
Wav File Source File:ger - Let Her Go.wav Repeat: Yes WBFM Transmit			ß		
Audio Rate: 32k Quadrature Rate: 320k Tau: 300u Max Deviation: 75k					
			Cancel OK		

选择加载好 WAV 文件后执行 F5,F6 或者点击 build generate, execute。 修改发射频率,双击 SINK 如下图,将 Frequency 修改掉即可。

Ge	neral	Advanced	Documentation		- H	Baramatar		
		ID	osmosdr_sink_0			ID: ppm		
	Inp	ut Type	Complex float32 🛟		М	Value: 0		
	Device	Arguments				Type: Float Short ID: p		
	Num	Channels -	1	•				
Sample Rate (sps) Ch0: Frequency (Hz) Ch0: Freq. Corr. (ppm)			8e6			l Interpolator t: 1 out		
			đ	Ch0: R	F Gain (dB)	14		
	Ch0: IF	F Gain (dB)	16					
1	Ch0: Bl	B Gain (dB)	47					
	Ch0:	Antenna				osmocom Sink		
<u>c</u>	h0: Bar	ndwidth (Hz)	250e3		-0	Sample Rate (sps): 8M Ch0: Frequency (Hz): 105M Ch0: Freq. Corr. (ppm): 0 Ch0: RF Gain (dB): 46 Ch0: IF Gain (dB): 46 Ch0: 8B Gain (dB): 14 Ch0: Bandwidth (Hz): 250k		

七、HackRF One 固件更新

源码编译在源码 WIKI 上已经写得很清楚。 执行下面的代码及可更新 hackrf_spiflash -w hackrf_usb_rom_to_ram.bin 更新完毕后,重新插拔 USB 线即可。

- 八、HackRF One CPLD 更新 必须在 UBUNTU 下进行,WINDOWS 下没有成功做。
- 九、问题与注意事项

1.SDR#点击停止后无法再次启动

HACKRF 会占用较多 USB 资源,在使用 HACKRF 时将其它 USB 设备先拔出,例如 USB 蓝牙鼠标,键盘。

2.使用时 RX,USB 灯突然熄灭 USB 线松动,线接触不良