mossmann / **hackrf**

HackRF One

Dominic Spill edited this page on Sep 12, 2017 · 16 revisions

HackRF One is the current hardware platform for the HackRF project. It is a Software Defined Radio peripheral capable of transmission or reception of radio signals from 1 MHz to 6 GHz. Designed to enable test and development of modern and next generation radio technologies, HackRF One is an open source hardware platform that can be used as a USB peripheral or programmed for stand-alone operation.

Features

- half-duplex transceiver
- operating freq: 1 MHz to 6 GHz
- supported sample rates: 2 Msps to 20 Msps (quadrature)
- resolution: 8 bits
- interface: High Speed USB (with USB Micro-B connector)
- power supply: USB bus power
- software-controlled antenna port power (max 50 mA at 3.3 V)
- SMA female antenna connector (50 ohms)
- SMA female clock input and output for synchronization
- convenient buttons for programming
- pin headers for expansion
- portable
- open source

Differences between Jawbreaker and HackRF One

Jawbreaker was the beta platform that preceded HackRF One. HackRF One incorporates the following changes and enhancements:

- Antenna port: No modification is necessary to use the SMA antenna port on HackRF One.
- PCB antenna: Removed.
- Size: HackRF One is smaller at 120 mm x 75 mm (PCB size).
- Enclosure: The commercial version of HackRF One from Great Scott Gadgets ships with an injection molded plastic enclosure. HackRF One is also designed to fit other enclosure options.
- Buttons: HackRF One has a RESET button and a DFU button for easy programming.
- Clock input and output: Installed and functional without modification.
- USB connector: HackRF One features a new USB connector and improved USB layout.
- Expansion interface: More pins are available for expansion, and pin headers are installed on HackRF One.

Clone this wiki locally

https://github.com/mossmann

⬇ Clone in Desktop

- Real-Time Clock: An RTC is installed on HackRF One.
- LPC4320 microcontroller: Jawbreaker had an LPC4330.
- RF shield footprint: An optional shield may be installed over HackRF One's RF section.
- Antenna port power: HackRF One can supply up to 50 mA at 3.3 V DC on the antenna port for compatibility with powered antennas and other low power amplifiers.
- Enhanced frequency range: The RF performance of HackRF One is better than Jawbreaker, particularly at the high and low ends of the operating frequency range. HackRF One can operate at 1 MHz or even lower.

Enclosure Options

The commercial version of HackRF One from Great Scott Gadgets ships with an injection molded plastic enclosure, but it is designed to fit two optional enclosures:

- Hammond 1455J1201: HackRF One fits this extruded aluminum enclosure and other similar models from Hammond Manufacturing. In order to use the enclosure's end plates, you will have to drill them. An end plate template can be found in the HackRF One KiCad layout.

- Acrylic sandwich: You can also use a laser cut acrylic enclosure with HackRF One. This is a good option for access to the expansion headers. A design can be found in the HackRF One hardware directory. Use any laser cutting service or purchase from a reseller.

Using HackRF One's Buttons

The RESET button resets the microcontroller. This is a reboot that should result in a USB re-enumeration.

The DFU button invokes a USB DFU bootloader located in the microcontroller's ROM. This bootloader makes it possible to unbrick a HackRF One with damaged firmware because the ROM cannot be overwritten.

To invoke DFU mode: Press and hold the DFU button. While holding the DFU button, reset the HackRF One either by pressing and releasing the RESET button or by powering on the HackRF One. Release the DFU button.

The DFU button only invokes the bootloader during reset. This means that it can be used for other functions by custom firmware.

SMA, not RP-SMA

Some connectors that appear to be SMA are actually RP-SMA. If you connect an RP-SMA antenna to HackRF One, it will seem to connect snugly but won't function at all because neither the male nor female side has a center pin. RP-SMA connectors are most common on 2.4 GHz antennas and are popular on Wi-Fi equipment. Adapters are available.

Transmit Power

HackRF One's absolute maximum TX power varies by operating frequency:

- 10 MHz to 2150 MHz: 5 dBm to 15 dBm, generally increasing as frequency decreases
- 2150 MHz to 2750 MHz: 13 dBm to 15 dBm
- 2750 MHz to 4000 MHz: 0 dBm to 5 dBm, increasing as frequency decreases
- 4000 MHz to 6000 MHz: -10 dBm to 0 dBm, generally increasing as frequency decreases

Through most of the frequency range up to 4 GHz, the maximum TX power is between 0 and 10 dBm. The frequency range with best performance is 2150 MHz to 2750 MHz.

Overall, the output power is enough to perform over-the-air experiments at close range or to drive an external amplifier. If you connect an external amplifier, you should also use an external bandpass filter for your operating frequency.

Before you transmit, know your laws. HackRF One has not been tested for compliance with regulations governing transmission of radio signals. You are responsible for using your HackRF One legally.

Receive Power

The maximum RX power of HackRF One is -5 dBm. Exceeding -5 dBm can result in permanent damage!

In theory, HackRF One can safely accept up to 10 dBm with the front-end RX amplifier disabled. However, a simple software or user error could enable the amplifier, resulting in permanent damage. It is better to use an external attenuator than to risk damage.

External Clock Interface (CLKIN and CLKOUT)

HackRF One produces a 10 MHz clock signal on CLKOUT. The signal is a 10 MHz square wave from 0 V to 3 V intended for a high impedance load.

The CLKIN port on HackRF One is a high impedance input that expects a 0 V to 3 V square wave at 10 MHz. Do not exceed 3.3 V or drop below 0 V on this input. Do not connect a clock signal at a frequency other than 10 MHz (unless you modify the firmware to support this). You may directly connect the CLKOUT port of one HackRF One to the CLKIN port of another HackRF One.

HackRF One uses CLKIN instead of the internal crystal when a clock signal is detected on CLKIN. The switch to or from CLKIN only happens when a transmit or receive operation begins.

To verify that a signal has been detected on CLKIN, use `hackrf_debug --si5351c -n 0 -r` . The expected output with a clock detected is `[ 0] -> 0x01` . The expected output with no clock detected is `[ 0] -> 0x51` .

Hardware Documentation

Schematic diagram, assembly diagram,and bill of materials can be found at https://github.com/mossmann/hackrf/tree/master/doc/hardware

Expansion Interface

The HackRF One expansion interface consists of headers P9, P20, P22, and P28. These four headers are installed on the commercial HackRF One from Great Scott Gadgets.

P9 Baseband

A direct analog interface to the high speed dual ADC and dual DAC.

Pin	Function
1	GND
2	GND
3	GND
4	RXBBQ-
5	RXBBI-

Pin	Function
6	RXBBQ+
7	RXBBI+
8	GND
9	GND
10	TXBBI-
11	TXBBQ+
12	TXBBI+
13	TXBBQ-
14	GND
15	GND
16	GND

P20 GPIO

Providing access to GPIO, ADC, RTC, and power.

Pin	Function
1	VBAT
2	RTC_ALARM
3	VCC
4	WAKEUP
5	GPIO3_8
6	GPIO3_0
7	GPIO3_10
8	GPIO3_11
9	GPIO3_12
10	GPIO3_13
11	GPIO3_14
12	GPIO3_15
13	GND
14	ADC0_6
15	GND
16	ADC0_2
17	VBUSCTRL
18	ADC0_5
19	GND
20	ADC0_0

Pin	Function
21	VBUS
22	VIN

P22 I2S

I2S, SPI, I2C, UART, GPIO, and clocks.

Pin	Function
1	CLKOUT
2	CLKIN
3	RESET
4	GND
5	I2C1_SCL
6	I2C1_SDA
7	SPIFI_MISO
8	SPIFI_SCK
9	SPIFI_MOSI
10	GND
11	VCC
12	I2S0_RX_SCK
13	I2S_RX_SDA
14	I2S0_RX_MCLK
15	I2S0_RX_WS
16	I2S0_TX_SCK
17	I2S0_TX_MCLK
18	GND
19	U0_RXD
20	U0_TXD
21	P2_9
22	P2_13
23	P2_8
24	SDA
25	CLK6
26	SCL

P28 SD

SDIO, GPIO, clocks, and CPLD.

Pin	Function
1	VCC
2	GND
3	SD_CD
4	SD_DAT3
5	SD_DAT2
6	SD_DAT1
7	SD_DAT0
8	SD_VOLT0
9	SD_CMD
10	SD_POW
11	SD_CLK
12	GND
13	GCK2
14	GCK1
15	B1AUX14
16	B1AUX13
17	CPLD_TCK
18	BANK2F3M2
19	CPLD_TDI
20	BANK2F3M6
21	BANK2F3M12
22	BANK2F3M4

Additional unpopulated headers and test points are available for test and development, but they may be incompatible with some enclosure or expansion options.

Refer to the schematics and component documentation for more information.