موسسه رستگارفن

شماره ثبت: ۳۶۸۲۱

عنوان سند :

بررسی عملکرد و مشخصات ماژول *HackRF One*

چکیده

در این گزارش به بررسی عملکرد و مشخصات ماژول *HackRF One* پرداخته شده است. این ماژول یک گیرنده فرستنده *half_duplex* می‌باشد که در بازه فرکانسی ۱ مگاهرتز تا ۶ گیگاهرتز کار می‌کند. در این گزارش مشخصات بارز این ماژول از منابع گردآوری شده و گزارش شده است.

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

۱-مقدمه

HackRFOne یک ماژول برای پروژه‌ها و اندازه‌گیری‌های مربوط به *RF* در بازه فرکانسی *MHz* ۱ تا *GHz* ۶ با برنامه‌های منبع باز[۱] برای *SDR*ها می‌باشد. این ماژول می‌تواند از طریق پورت *USB* به کامپیوتر متصل شود یا برای عملکرد به صورت مستقل (*standalone*) برنامه‌ریزی گردد.

سیستم بازه فرکانسی وسیعی از ۱ تا ۶۰۰۰ مگاهرتز را پوشش داده و همچنین باندهای رادیویی مجوز دار و غیر مجوز دار زیادی را تحت پوشش دارد. سخت افزار بیشترین نرخ نمونه *MS/s* ۲۰ را دارد که حتی برای اندازه‌گیری سیگنال‌های پهن باند مانند *WFM*، *DECT*، *WiFi* و غیره کافی می‌باشد. *ADC* رزولوشن ۸ بیت داشته و رنج دینامیکی *dB* ۴۸ ارائه می‌دهد. داده *IQ* دیجیتالی شده توسط یک *Xilinx CPLD* و یک پردازنده *ARM Cortex* مجتمع شده پردازش می‌شود. به علت طراحی و انتخاب قطعات، ماژول تنها عملکرد یک طرفه را پشتیبانی می‌کند.

شکل (۱-۱): ماژول HackRF One.

کل مدار به صورت کم مصرف طراحی شده و تغذیه ماژول از طریق پورت *USB* انجام می‌پذیرد. بورد ماژول یک سوکت *Micro-B USB* دارد. برای همزمان سازی چندین برد *HackRFOne*، کانکتورهایی برای ورودی و خروجی

---

[۱] *Open source*

کلاک در نظر گرفته شده است. این سیگنال‌ها می‌توانند برای استفاده بردهای متعدد به صورت موازی، به طور مثال برای اندازه‌گیری روی سیستم‌های *MIMO* یا سیستم‌های تمام داپلکس، به کار روند.

PCB به صورت ۴ لایه بوده و تمام المان‌ها *SMD* می‌باشند.

ماژول *HackRF One* دارای قابلیت‌های زیر می‌باشد:

- فرکانس کاری از *MHz* ۱ تا *GHz* ۶
- گیرنده فرستنده *half-duplex*
- تا ۲۰ میلیون نمونه در ثانیه
- نمونه‌های ربعی ۸ بیتی (۸ بیت *I* و ۸ بیت *Q*)
- سازگار با *GNU Radio*، *SDR#* و ...
- گین دریافت و ارسال و فیلتر باند پایه قابل پیکره‌بندی به صورت نرم‌افزاری
- توان پورت آنتن قابل کنترل به صورت نرم‌افزاری (*mA* ۵۰ در *V* ۳/۳)
- کانکتور آنتن *SMA* مادگی
- ورودی و خروجی کلاک *SMA* مادگی برای همزمانی
- کلیدهای مناسب برای برنامه‌ریزی
- هیدرهای پین داخلی برای توسعه
- *USB 2.0* سرعت بالا
- تغذیه از طریق *USB*
- سخت افزار *open source*
- نرخ‌های داده پشتیبانی شده: *Msps* ۲ تا *Msps* ۲۰ (ربعی)

HackRF One یک کلید *RESET* و یک کلید *DFU* برای آسانی در برنامه‌نویسی دارد.

توان ارسال بیشینه مطلق *HackRF One* با فرکانس کاری تغییر می‌یابد:

- *MHz* ۱۰ تا *MHz* ۲۱۵۰: *dBm* ۵ تا *dBm* ۱۵ با کاهش فرکانس افزایش می‌یابد
- *MHz* ۲۱۵۰ تا *MHz* ۲۷۵۰: *dBm* ۱۳ تا *dBm* ۱۵
- *MHz* ۲۷۵۰ تا *MHz* ۴۰۰۰: *dBm* ۰ تا *dBm* ۵ با کاهش فرکانس افزایش می‌یابد
- *MHz* ۴۰۰۰ تا *MHz* ۶۰۰۰: *dBm* ۱۰- تا *dBm* ۰ عموماً با کاهش فرکانس افزایش می‌یابد

در بیشتر بازه‌های فرکانسی تا *GHz* ۴، توان *TX* بیشینه بین ۰ و *dBm* ۱۰ است. بازه فرکانسی با بهترین عملکرد *MHz* ۲۱۵۰ تا *MHz* ۲۷۵۰ می‌باشد.

در حالت کلی، توان خروجی برای کار کردن در فاصله نزدیک یا برای تحریک یک تقویت‌کننده خارجی کافی می‌باشد. اگر یک تقویت‌کننده خارجی متصل کنید، بایستی یک فیلتر میانگذر خارجی نیز برای فرکانس کاری مورد نظر اضافه نمایید.

بیشترین توان دریافت *HackRF One*، *dBm* ۵- می‌باشد. بالاتر از *dBm* ۵- می‌تواند خسارت دائمی به قطعه وارد آورد. پس بهتر خواهد بود که یک تضعیف‌کننده خارجی استفاده نمایید.

هم اکنون برد *HackRF One* با نرم‌افزارهای *'SDR-Radio'*، *'GNU Radio'* و *'SDR#'* کار می‌کند. به علت منبع باز بودن و مجوز مجانی پروژه، پروژه نرم‌افزاری دیگر در هر زمان می‌تواند اضافه شود.

۱-۱- تفاوت‌ها بین Jawbreaker و HackRF One

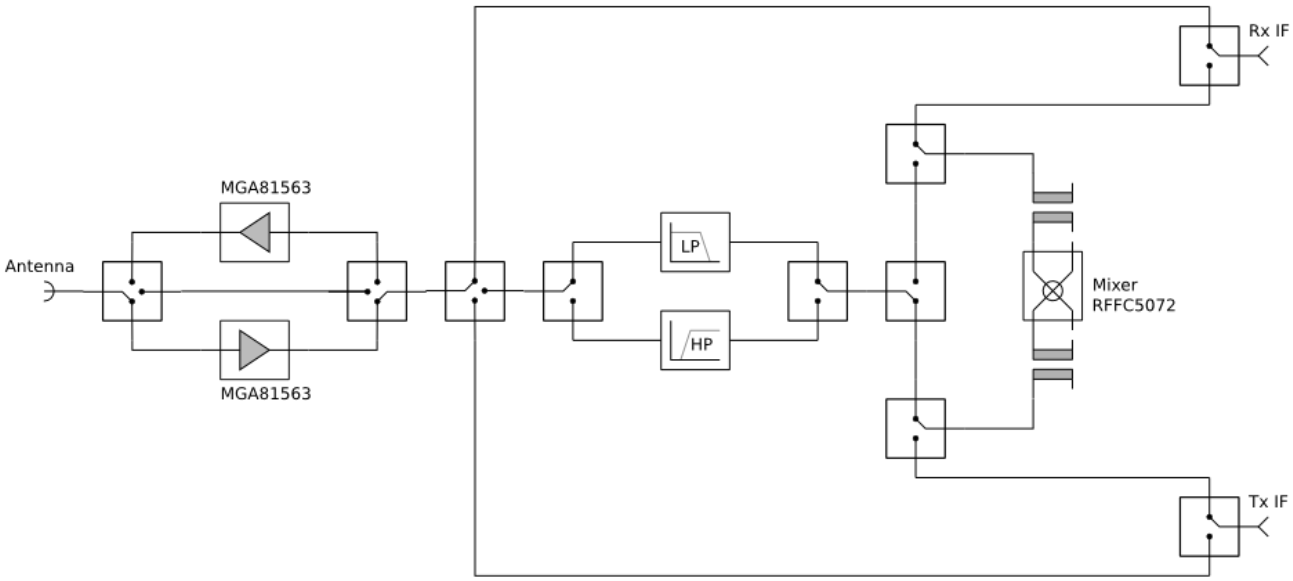
Jawbreaker پلتفرم بتا قبل از *HackRF One* بود. *HackRF One* تغییرات و بهبودی‌های زیر را دارد:

- پورت آنتن: هیچ تغییری برای استفاده از پورت آنتن *SMA* روی *HackRF One* نیاز نیست.
- آنتن *PCB*: حذف شده است.
- اندازه: *HackRF One* کوچکتر می‌باشد (با اندازه *PCB* ۱۲۰ *mm* در ۷۵ *mm*)
- محفظه: نسخه تجاری *HackRF One* از *Great Scott Gadgets* با محفظه پلاستیک تزریق شده عرضه شده است.
- کلیدها: *HackRF One* یک کلید *RESET* و یک کلید *DFU* برای برنامه‌نویسی آسان دارد.
- ورودی و خروجی کلاک: نصب شده و کاربردی بدون تغییر.
- کانکتور *USB*: *HackRF One* یک پورت *USB* جدید و *USB layout* بهبود یافته دارد.
- تخته مدار: پین‌های زیادی برای گسترش موجود هستند، و سرآمدهای پین روی *HackRF One* نصب شده‌اند.
- کلاک بلادرنگ: یک *RTC* روی *HackRF One* نصب شده است.
- *LPC4320*: *Jawbreaker* یک *LPC4330* داشت.

- توان پورت آنتن: *HackRF One* می‌تواند تا *۵۰ mA* در *۳/۳ V DC* روی پورت آنتن اعمال نماید.
- بازه فرکانسی بهبود یافته: عملکرد *HackRF One RF* بهتر از *Jawbreaker* می‌باشد، بخصوص در انتهای بالایی و پایینی بازه فرکانسی کاری. *HackRF One* می‌تواند در *۱MHz* یا حتی پایین‌تر کار کند.

۲-۱- مدار HackRF One

به بلوک دیاگرام ارائه شده در ***Error! Reference source not found.*** توجه فرمایید. مسیر سیگنال در برد *HackRF One* انعطاف‌پذیری بالایی دارد. سوئیچ‌های *RF* در تمام نقاط اتصال مهم، انتخاب المان‌های متعدد را، براساس برنامه ریزی کاربر ممکن می‌کنند.



شکل (۲-۱): بلوک دیاگرام سرجلویی HackRF One.

بعد از آنتن دو تا تقویت کننده *MGA81563* قرار دارند، که یکی برای مسیر ارسال و دیگری برای مسیر دریافت به کار می‌رود. تقویت کننده‌ها می‌توانند توسط سوئیچ‌های *RF* (*SKY13317*) در مسیر یا خارج از مسیر سیگنال قرار بگیرند.

بعد از تقویت کننده یک فیلتر پایین‌گذر و یک فیلتر بالا گذر قرار گرفته‌اند، که می‌توانند برای محدود کردن سیگنال در مسیر ورودی یا خروجی استفاده شوند. بعد از فیلتر سیگنال به میکسر *RFFC 5072* می‌رسد. این میکسر می‌تواند تا *GHz* ۶ استفاده شود. سیگنال بسته به برنامه‌ریزی کاربر می‌تواند به بالا یا به پایین میکس شود، و سرانجام به مدار باندپایه اعمال می‌گردد. میکسر و فیلترها می‌توانند توسط سوئیچ‌های *RF* بای‌پس شوند، که در اینصورت سیگنال‌های *IF* مستقیماً به تقویت کننده‌ها یا مستقیماً به آنتن سوئیچ می‌شوند.

قطعه *Maxim MAX2837* به عنوان چیپ باندپایه مورد استفاده قرار گرفته است، که بازه فرکانسی ۲/۳ تا *GHz* ۲/۷ را پوشش می‌دهد.چیپ از فیلترهای یکپارچه استفاده می‌کند که سیگنال بسیار خطی و عدد نویز بسیار پایین می‌دهد. سپس داده *IQ* به چیپ *ADC/DAC* به نام *Maxim MAX5864* داده می‌شود. هر دو مبدل *ADC* و *DAC* رزولوشن ۸ بیت دارند و بیشترین نرخ نمونه‌برداری *MS/s* ۲۰ توسط این مبدل‌ها پشتیبانی می‌شود. نهایتاً سیگنال-های دیجیتال به یک *Xilinx XC2C CPLD* می‌رسند. کل سیستم و تمام رابط‌ها توسط یک پردازنده *Cortex* دو هسته‌ای *ARM* قدرتمند (*NXP LPC4320*) کنترل می‌شوند. همچنین برد حافظه فلش *MB* ۱ را پشتیبانی می-کند.

HackRF One سه تا کنترل گین آنالوگ متفاوت روی *RX* و دو تا روی *TX* دارد. سه تا کنترل گین *RX*، در طبقات *RF* (*"amp"*، ۰ تا *dB* ۱۴)، *IF* (*"lna"*، ۰ تا *dB* ۴۰ با گام‌های *dB* ۸) و باند پایه (*"vga"*، ۰ تا *dB* ۶۲ با گام‌های *dB* ۲) هستند. دو تا کنترل گین *TX* در طبقات *RF* (۰ یا *dB* ۱۴) و *IF* (۰ تا *dB* ۴۷ در گام‌های *dB* ۱) هستند.

HackRF One دو تا تقویت کننده *RF* نزدیک به پورت آنتن دارد، یکی برای ارسال و یکی برای دریافت. این تقویت کننده‌ها تنها دو حالت تنظیم دارند: خاموش یا روشن. در حالت خاموش تقویت‌کننده‌ها کاملاً بای‌پس می-شوند. در حالت روشن به طور اسمی *dB* ۱۴ گین دارند، اما مقدار واقعی گین با فرکانس تغییر می‌کند. عموماً در فرکانس‌های بالاتر گین کمتری انتظار داشته باشید. برای کنترل دقیق‌تر گین از کنترل گین‌های *IF* و باندپایه استفاده کنید.

۳-۱- کلاک

سیگنال‌های کلاک *HackRF* توسط *Si5351* تولید می‌شوند. طرح کلاک به صورت زیر می‌باشد:

- فرکانس کریستال: *MHz* ۲۵ (۲۵ یا ۲۷*MHz* را پشتیبانی می‌کند)
- فرکانس کلاک ورودی اختیاری: *MHz* ۱۰ توصیه شده (۱۰ تا *MHz* ۴۰، یا بالاتر را با تقسیم پشتیبانی می‌کند)
- فرکانس *VCO*: ۸۰۰*MHz* (۶۰۰ تا *MHz* ۹۰۰ را پشتیبانی می‌کند)
- کلاک *MAX2837*: *MHz* ۴۰
- کلاک‌های *MAX5864* ارجح: ۸، ۱۰، ۱۲,۵، ۱۶، *MHz* ۲۰
- کلاکی در دو برابر نرخ *MAX5864* به *CPLD* و *SGPIO* داده می‌شود.
- کلاک *LPC43xx*: *MHz* ۱۲ (از کریستال مجزا بنابراین *USB DFU* مبتنی بر *ROM* کار خواهد کرد)

۱-۴- LEDهای HackRF One

هنگامی که *HackRF One* از طریق *USB* به کامپیوتری متصل شود، ۴ عدد *LED* بایستی روشن شوند: *3V3*، *1V8*، *RF* و *USB*. *LED*های *3V3*، *1V8* و *RF* بیانگر این هستند که تغذیه‌های داخلی بدرستی عمل می‌کنند. *LED* مربوط به *USB* نشان می‌دهد که *HackRF One* از طریق کابل *USB* با کامپیوتر در ارتباط است.

*LED*های ارسال و دریافت نشان می‌دهند که در حال حاضر عملیات ارسال یا دریافت در حال انجام می‌باشند.

۱-۵- رابط کلاک خارجی

HackRF One یک سیگنال کلاک *MHz* ۱۰ روی *CLKOUT* تولید می‌کند. سیگنال یک موج مربعی *MHz* ۱۰ از *V* ۰ تا *V* ۳ برای یک بار امپدانس بالا می‌باشد.

پورت *CLKIN* روی *HackRF One* یک ورودی امپدانس بالا است که یک موج مربعی *V*۰ تا *V* ۳ در *MHz* ۱۰ می‌پذیرد. سیگنال بالاتر از *V* ۳/۳ و پایین‌تر از *V* ۰ روی این ورودی اعمال نکنید. سیگنال کلاک در فرکانس غیر از *MHz* ۱۰ متصل نکنید (مگر اینکه سیستم عامل را برای پشتیبانی آن تغییر دهید). در ضمن می‌توان پورت *CLKOUT* یک *HackRF One* را به پورت *CLKIN* یک *HackRF One* دیگر متصل نمود.

HackRF One از *CLKIN* به جای کریستال داخلی استفاده می‌کند. هنگامی که سیگنال کلاک روی *CLKIN* دریافت شود، سوئیچ کردن از/ به *CLKIN* تنها موقعی رخ می‌دهد که عملیات ارسال یا دریافت شروع شود.

۱-۶- استفاده از کلیدهای HackRF One

کلید *RESET* میکروکنترلر را ریست می‌کند. این یک راه اندازی مجدد است که باید باعث بازخوانی (*re-enumeration*) *USB* گردد.

کلید *DFU* یک *USB DFU bootloader* واقع در *ROM* میکروکنترلر را فعال می‌کند. این *bootloader* راه‌اندازی *HackRF One* را با سیستم عامل آسیب دیده ممکن می‌کند زیرا *ROM* نمی‌تواند رونویسی شود.

برای فعال کردن مود *DFU*: کلید *DFU* را فشار داده و نگه دارید. درحالیکه کلید *DFU* را نگه داشته‌اید، *HackRF One* را با فشار دادن و رها کردن کلید *RESET* یا با روشن کردن *HackRF One* ریست نمایید. کلید *DFU* را رها کنید.

کلید *DFU* تنها *bootloader* را در طی ریست فعال می‌سازد. یعنی اینکه می‌تواند برای عملیات دیگر توسط سیستم عامل استفاده شود.

۱-۷- تخته مدار HackRF One

تخت مدار *HackRF One*[۱] از هیدرهای *P9*، *P20*، *P22* و *P28* تشکیل می‌شود. این چهار هیدر روی *HackRF One* تجاری از *Great Scott Gadgets* نصب شده‌اند.

- *P9* باندپایه

یک رابط آنالوگ مستقیم به *ADC* دوتایی و *DAC* دوتایی سرعت بالا.

---

[۱] *Expansion Interface*

جدول (۲-۱): رابط *P9*

Function	*Pin*	*Function*	*Pin*
GND	*9*	*GND*	*1*
TXBBI-	*10*	*GND*	*2*
TXBBQ+	*11*	*GND*	*3*
TXBBI+	*12*	*RXBBQ-*	*4*
TXBBQ-	*13*	*RXBBI-*	*5*
GND	*14*	*RXBBQ+*	*6*
GND	*15*	*RXBBI+*	*7*
GND	*16*	*GND*	*8*

- *P20 GPIO*

دسترسی به *GPIO*، *ADC*، *RTC* و توان را فراهم می‌کند.

جدول (۳-۱): رابط *P20 GPIO*

Function	*Pin*	*Function*	*Pin*
GPIO3_15	*12*	*VBAT*	*1*
GND	*13*	*RTC_ALARM*	*2*
ADC0_6	*14*	*VCC*	*3*
GND	*15*	*WAKEUP*	*4*
ADC0_2	*16*	*GPIO3_8*	*5*
VBUSCTRL	*17*	*GPIO3_0*	*6*
ADC0_5	*18*	*GPIO3_10*	*7*
GND	*19*	*GPIO3_11*	*8*
ADC0_0	*20*	*GPIO3_12*	*9*
VBUS	*21*	*GPIO3_13*	*10*
VIN	*22*	*GPIO3_14*	*11*

- *P22 I2S*

I2S، *SPI*، *I2C*، *UART*، *GPIO* و کلاک‌ها.

جدول (۴-۱): رابط *P22 I2S*

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

- *P28 SD*

SDIO، *GPIO*، کلاک‌ها و *CPLD*.

جدول (۵-۱): رابط *P28 SD*

Function	*Pin*	*Function*	*Pin*
GND	*12*	*VCC*	*1*
GCK2	*13*	*GND*	*2*
GCK1	*14*	*SD_CD*	*3*
BIAUX14	*15*	*SD_DAT3*	*4*
B1AUX13	*16*	*SD_DAT2*	*5*
CPLD_TCK	*17*	*SD_DAT1*	*6*
BANK2F3M2	*18*	*SD_DAT0*	*7*
CPLD_TDI	*19*	*SD_VOLT0*	*8*
BANK2F3M6	*20*	*SD_CMD*	*9*
BANK2F3M12	*21*	*SD_POW*	*10*
BANK2F3M4	*22*	*SD_CLK*	*11*