## HackRF One in transmit mode

The HackRF device is not very well specified, so I decided to do some measurements to see how it performs and what kind of output levels can be expected.

First a bit about how it works. The simplified block diagram in the transmit mode is as follows:

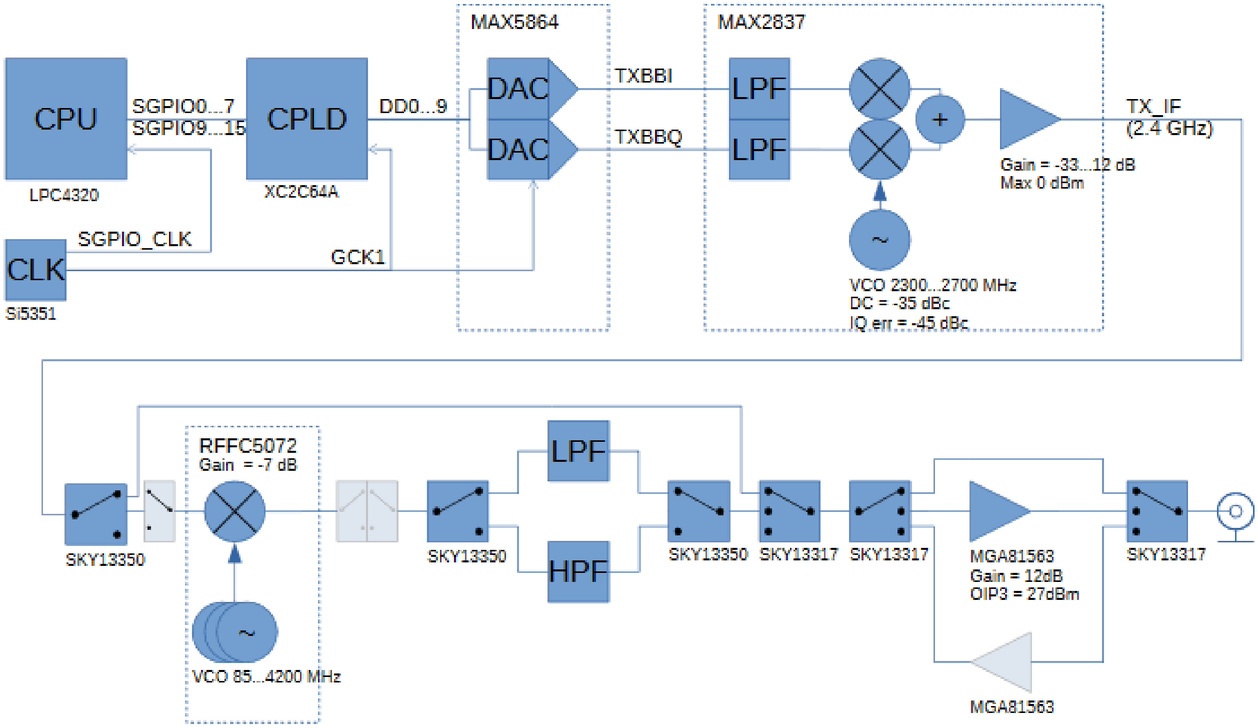


Figure 1. HackRF block diagram in TX mode. Numbers are specifications from datasheets.

## Data path control

At frequencies 2.15...2.75 GHz the RFFC5072 mixer is bypassed. The TX_IF signal is fed directly to the output. The center frequency is controlled by default by the MAX2837 integrated VCO. When the mixer is bypassed, output level should be about 10 dB higher than at other frequencies.

At frequencies below 2.15 GHz the mixer is used for downconverting TX_IF to the final center frequency. TX_IF is fixed at about 2.4 GHz. Low pass filter is selected to filter out unwanted image frequencies.

At frequencies above 2.75 GHz the mixer is used for upnconverting TX_IF to the final center frequency. TX_IF is fixed at about 2.4 GHz. High pass filter is selected to filter out unwanted image frequencies.

Output amplifier can be selected in all the modes, providing additional gain. The device can also feed antenna power, which means feeding 3.3 V DC to the output connector.

## Measurements

The setup for the measurement was a single 50 ohm cable directly from HackRF antenna port to spectrum analyzer (Rohde&Schwartz FSL). Resolution bandwidth was 10 MHz.

The HackRF was controlled from command line using the following command line as the base for frequency looping and gain settings:

```
hackrf_transfer -c 127 -x 35 -a 0 -f 6000000
```

These settings drive a maximum DC signal from the DAC (-c 127), set the  MAX2837 gain to 35 dB (-x 35), and bypasses the output amplifier (-a 0).

## Frequency response

Frequency response was measured by increasing the output frequency in 10 MHz steps and setting the spectrum analyzer trace to max hold mode. Three gain settings were plotted in different colors: green(-x25 -a0), black(-x35 -a0) and blue (-x25 -a1):

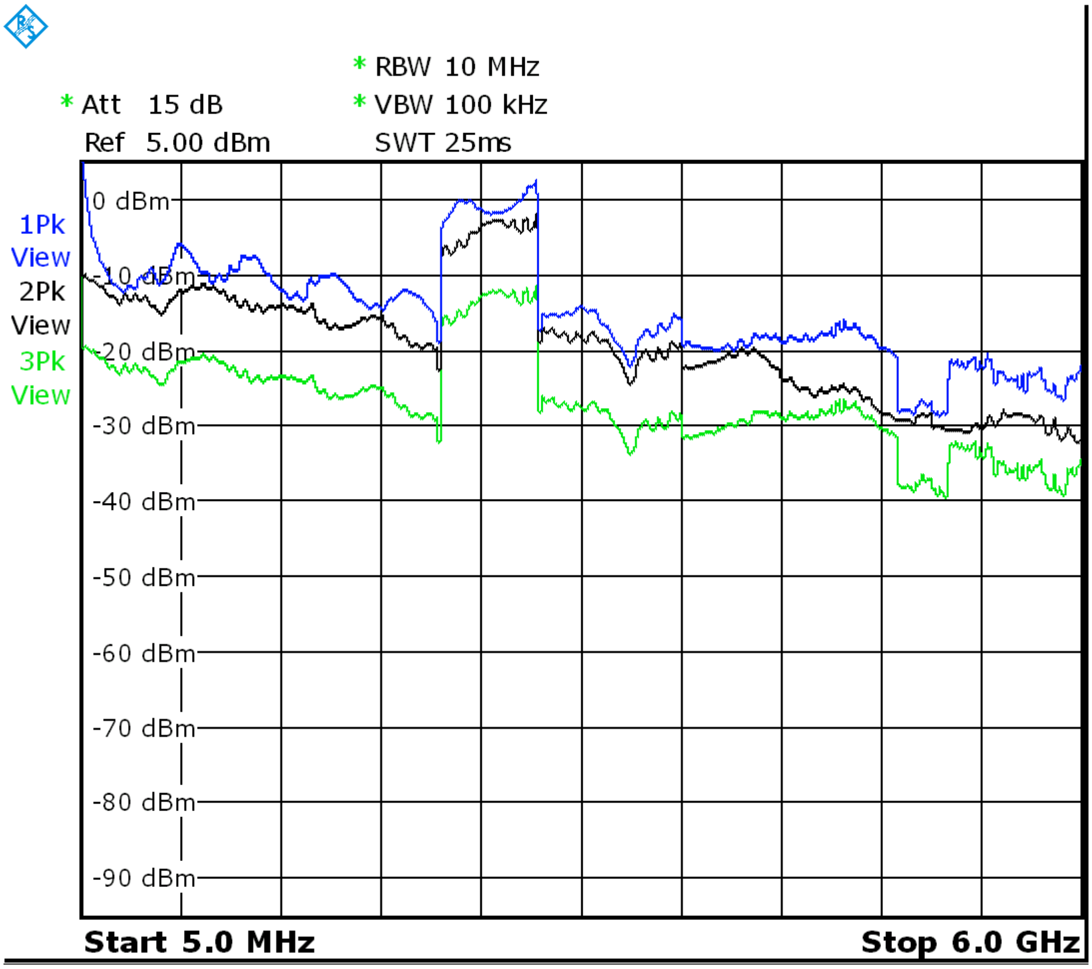


Figure 2. Output amplitude versus frequency at various gain settings.

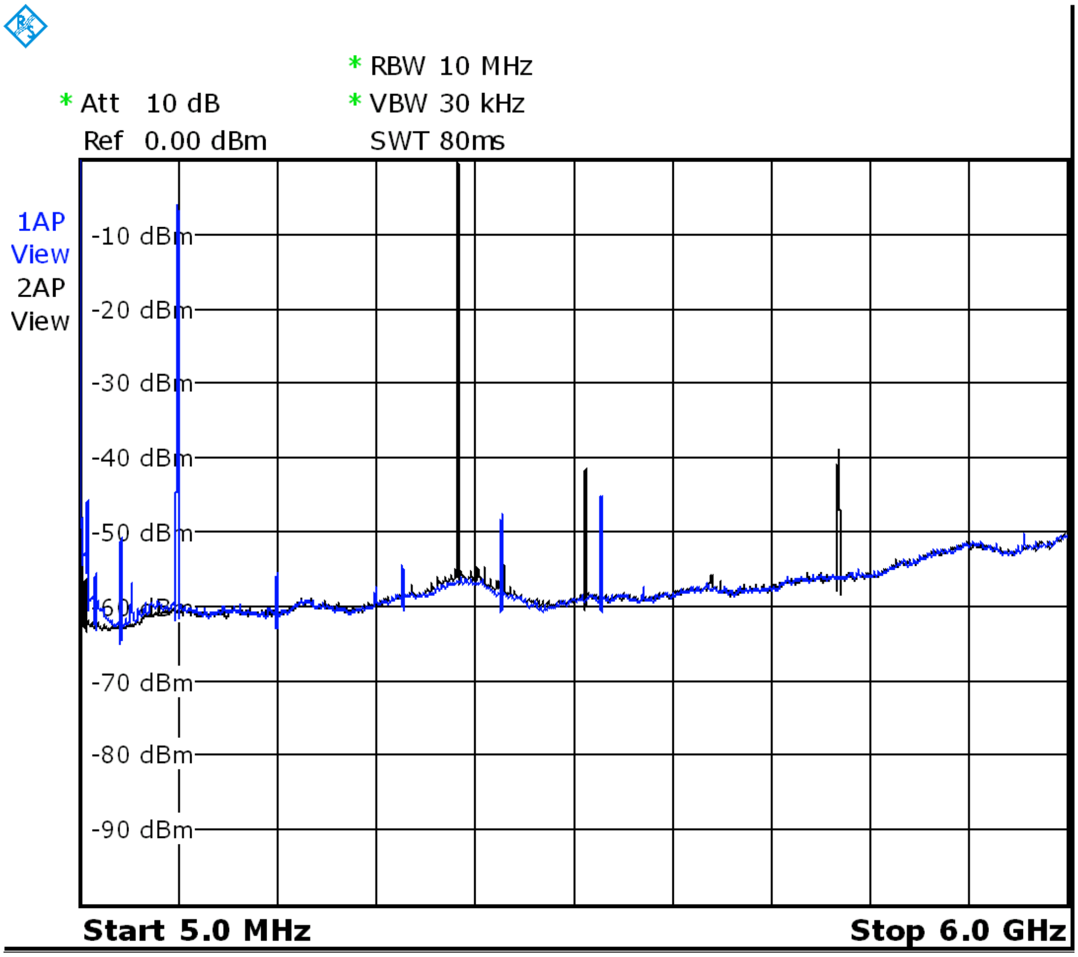
The response is nowhere near flat, so the actual transmit power depends heavily on frequency. The mixer bypass range is clearly visible, providing about 15 dB of more output power than at nearby frequencies. Outside the bypass region, the response drops roughly linearly 20 dB from 0 to 6 GHz.

There is considerable amount of ripple in the response (about 5 dB), and the shape differs depending if the output amplifier is active or not. The period of the ripple is about 500 MHz, so it doesn't point to the measurement cable, but to something internal to the device instead.

The effect of the measurement cable termination mismatch could be the small ripple of about 100 MHz and 2 dB, and the cable attenuation should be about 1 or 2 dB at 6 GHz.

**Spurious emissions versus output frequency**

The output level of the unwanted spurious signals was measured with -x25 -a1 settings.



* Att 10 dB
Ref 0.00 dBm
* RBW 10 MHz
* VBW 30 kHz
SWT 80ms

Start 5.0 MHz
Stop 6.0 GHz

Figure 3. Spurious emissions at output frequencies 600 MHz (blue) and 2300 MHz (black).

At 600 MHz, harmonic distortion peaks appear at 1200 MHz and 1800 MHz, and both are at about 50 dB below the transmitted signal. These will increase significantly when the output level is increased.

A more significant spur is at 2564 MHz, which results from the TX_IF signal leaking to the output. There is also a spur at 3164 MHz, which is the LO frequency leaking. Both of these are a result of inadequate low pass filtering, but they can be defeated by using an external transmit filter.

At 2300 MHz output frequency (mixer bypass range), there is a significant 2nd harmonic at 4600 MHz. The 3100 MHz spur is a mystery, maybe the software leaves LO in the mixer running even when the mixer is bypassed?

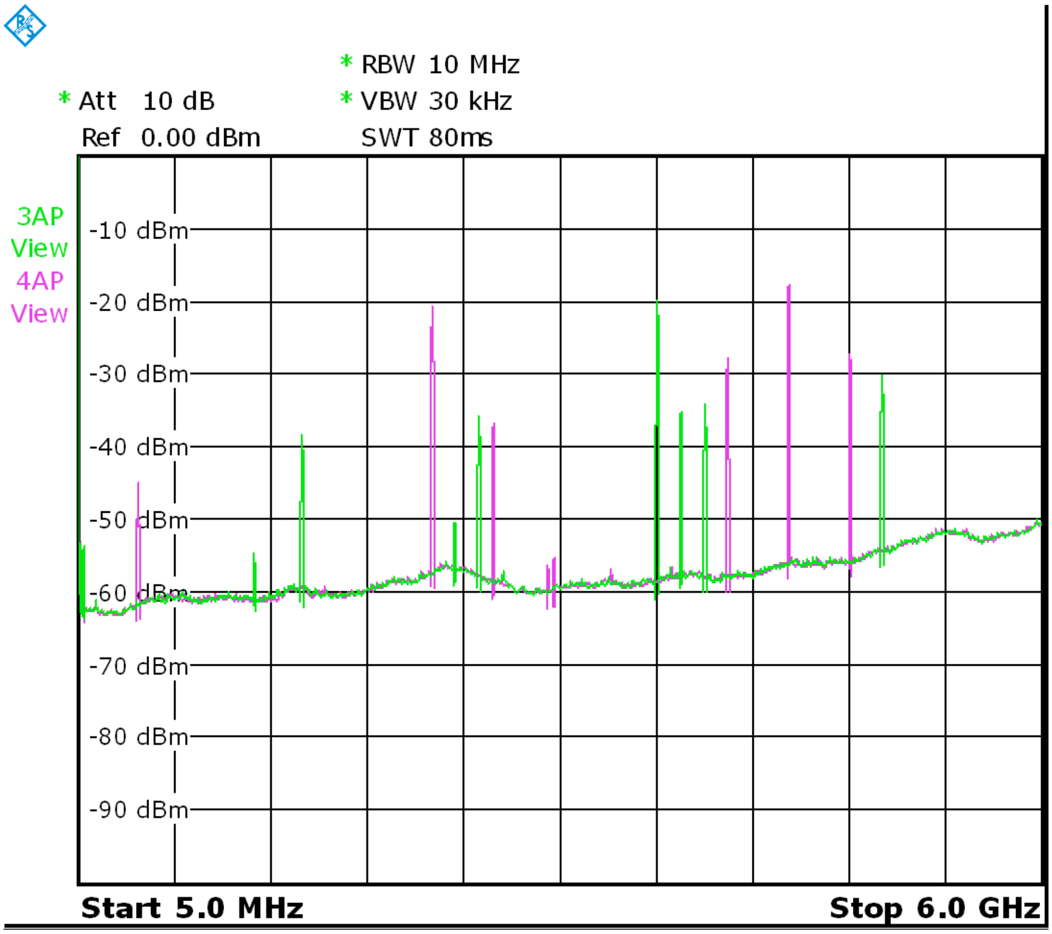


Figure 4. Spurious emissions at output frequencies 3600 MHz (green) and 4800 MHz (magenta).

At frequencies above 2.75 GHz there are a huge number of spurs.

The 3600 MHz is only 10...15 dB higher than the spurs. TX_IF is at 2350 MHz and LO at 1250 MHz here, and both are relatively low spurs. The most significant spurs originate from the harmonics of the LO frequency. The upside harmonics are in order: 3*LO, 5*LO – TX_IF and 4*LO. The two highest spurs in the lower side are at 2*LO and 3*LO – TX_IF.

At 4800 MHZ the situation is even worse. 2*LO is 10 dB above the desired frequency.

The design looks flawed as a general any-frequency transmitter at these frequencies. The spurs below 2.4 GHz indicate that the highpass filtering is not adequate, but the spurs appearing near the desired frequency cannot be filtered even with any kind of external wideband filter.

The firmware seems to take care, though, that the spurs never appear very near the output frequency, so a narrow, tuned bandpass filter may be used.

Finally a sample of spurs when transmitting in the FM radio range at 100 MHz. Distortion is relatively low, but there is a choice between low frequency noise or a relatively high 2nd harmonic depending on whether the amplifier is used or not.

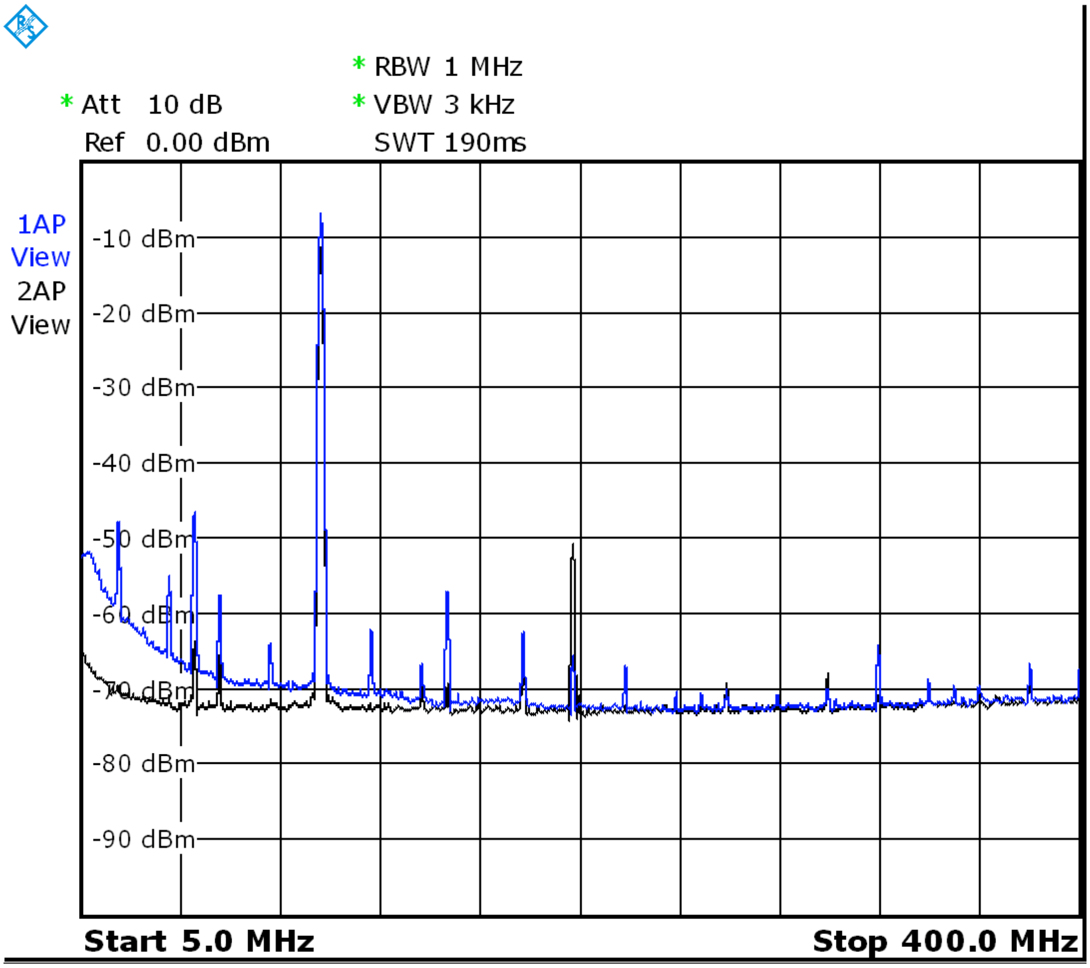


Figure 5. Spurious emissions at 100 MHz at two gain settings in colors blue (-x 25 -a 1) and black (-x 35 -a0).

## Output level versus harmonic distortion

Harmonic distortion was measured using Rohde & Schwartz FSEB 30 Spectrum analyzer.

The results show that the output amplifier gives about 6 dB of more output power at 600 MHz at comparable distortion levels. The distortion will however be more in the 2nd harmonic term as opposed to 3rd harmonic without the amplifier.

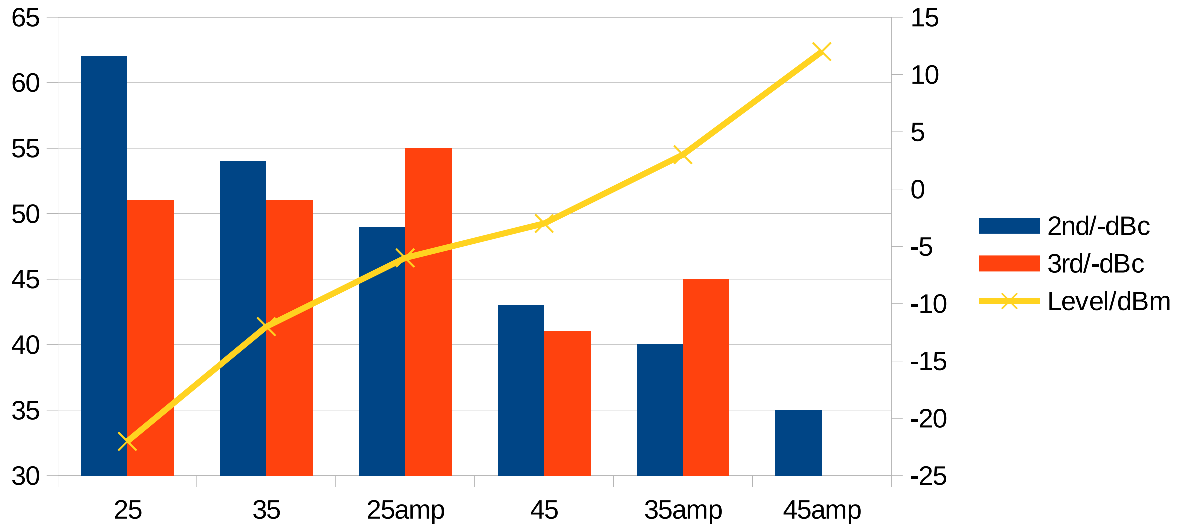


Figure 6. Harmonics at 600 MHz output frequency.

At 2300 MHz the behavior is not as consistent as at 600 MHz. Distortion levels exceeding -40 dBc are hardly achieved.

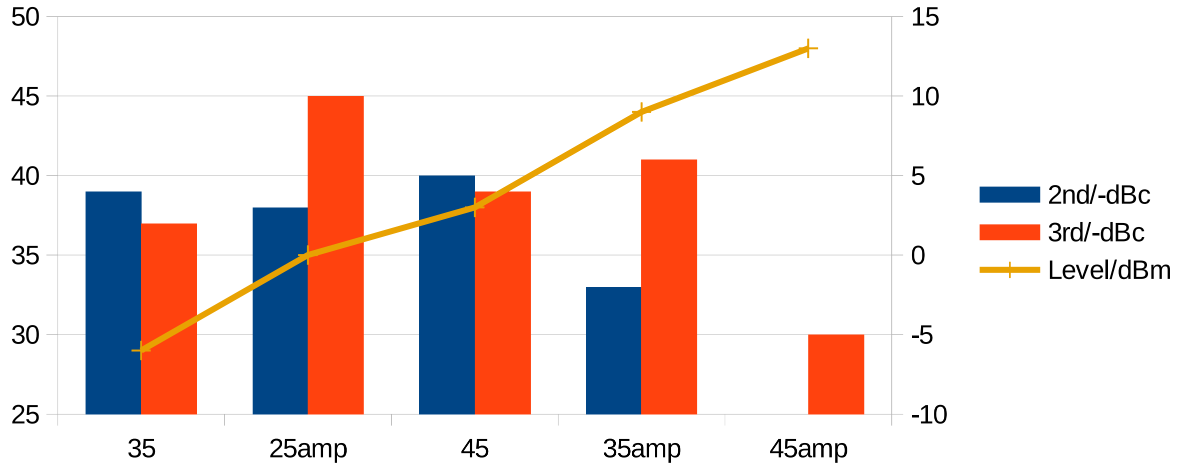


Figure 7. Harmonics at 2300 MHz output frequency.

### Carrier leakage

Carrier leakage (or in other words baseband DC offset) is an important parameter in an I/Q-modulated transmitter, but it cannot be measured using the hackrf_transfer tool’s “-c” setting. It requires a modulated baseband signal, so it was not measured here. MAX2837 datasheet specifies it as -35 dBc, which usually requires compensating.

### Conclusion

The HackRF One is not a general purpose radio transmitter due to its wideband spurious emissions, especially at frequencies over 2.7 GHz. It can still be used for many kinds of projects and hacking indoors.