Clean On Off Keying Synthesis

Max-Felix Müller

2020
September

Contents

List of Figures

1 Motivation

After the replay attack on the remote controlled realis a signal was synthesised to reduce noise being transmitted. By generating the output signal from a sine wave the spectrum was cleaner, but there still were some harmonics from the rectangular on off modulation signal. Instead of that, the project just used the original signal but only transmitted it, when the original signal was on. That way only the noise on top of the signal was being transmitted.

To clean the output in the time and frequency domain a more sophisticated method of signal generation has to be used.

2 Starting point

At the end of the replay attack project, this was the resulting flowgraph using signal synthesis.

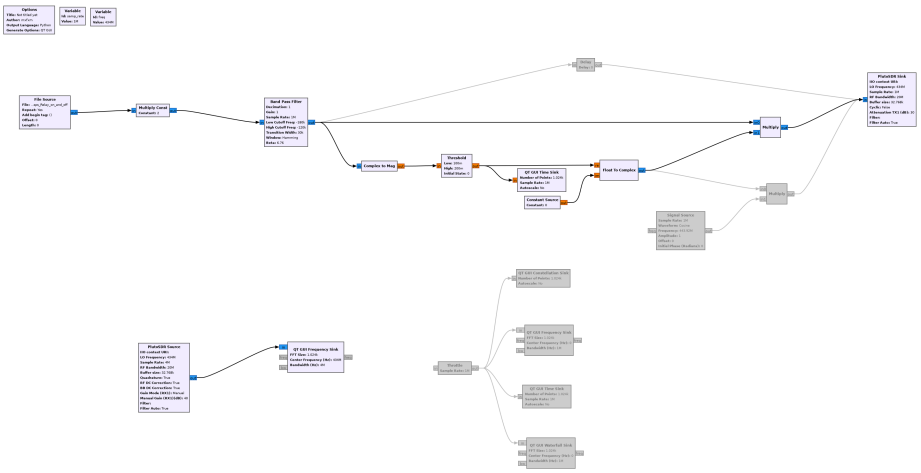

Figure 1: The result of the previous project, titled replay attack on a remote controlled relais

After amplification the flowgraph first filters the captured signal with a band-pass filter to minimize out of band noise in that signal. The resulting signal is converted from complex numbers to a magnitude which is done by adding the squares of the real and the imaginary part and taking the square root of that.

$$Mag = \sqrt{Re^2 + Im^2}$$

Using a threshold block it can be detected whether the carrier frequency is currently turned on or off. The output of the threshold block is either a one or a zero. Depending on the state of that, the original signal is transmitted or not (by multiplying it with the result). When the signal is not transmitted, there is no noise. The noise in the frequency band of the remote is transmitted when the signal is on though.

3 Creating the flowgraph

Using the described flowgraph as a starting point, some blocks were added to remove the noise also during transmission.

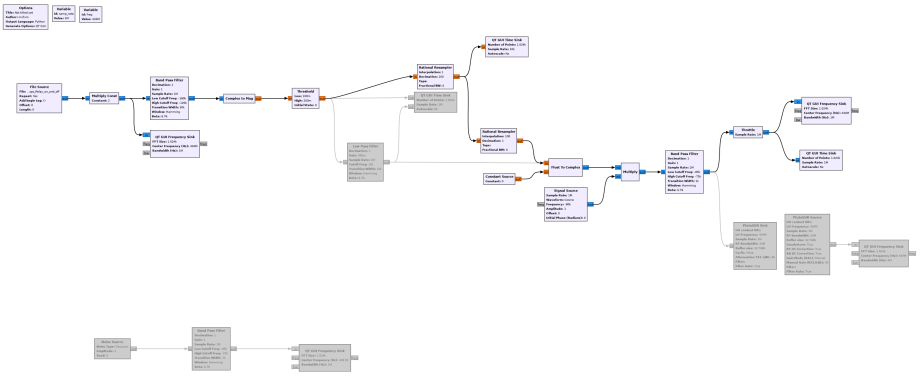

Figure 2: The full flowgraph for a clean on off keyed signal

All major parts of the flowgraph are described here...

3.1 Input bandpass filter

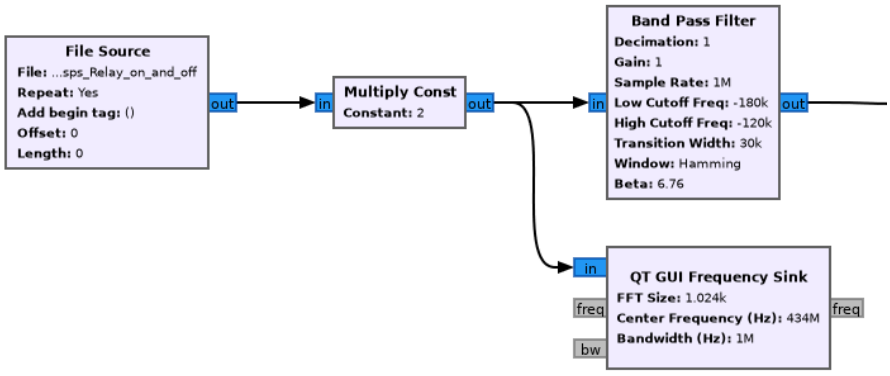

Figure 3: The input bandpass filter in the flowgraph

This is the same as in the origianl project. The bandpass filter at the input is used to reduce the noise that is out of the frequency band of the remote control. That way the following singal analysis works more reliably.

The bandpass filter uses complex tabs to be able to work on only one half of the spectrum. In this case, the band was detected by looking at the spectrum of the original signal and finding the peak during transmission. Gain and decimation were kept as one to have the blocks funcionally separated.

3.2 On or off?

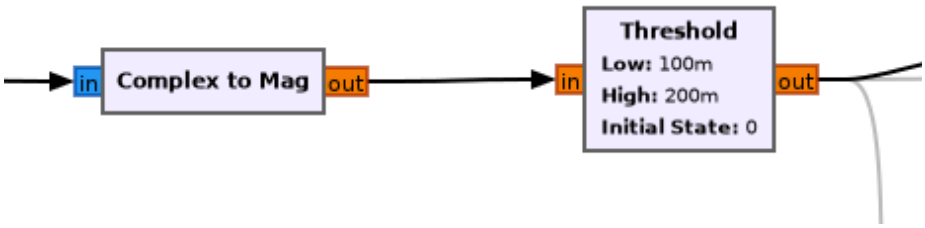

Figure 4: Using a threshold block, the current state of the signal can be extracted

Also just as before, the signal is converted to a magnitude. The threshold block is used to find whether the signal is currently on or off. This is the analysis part.

3.3 Resampling

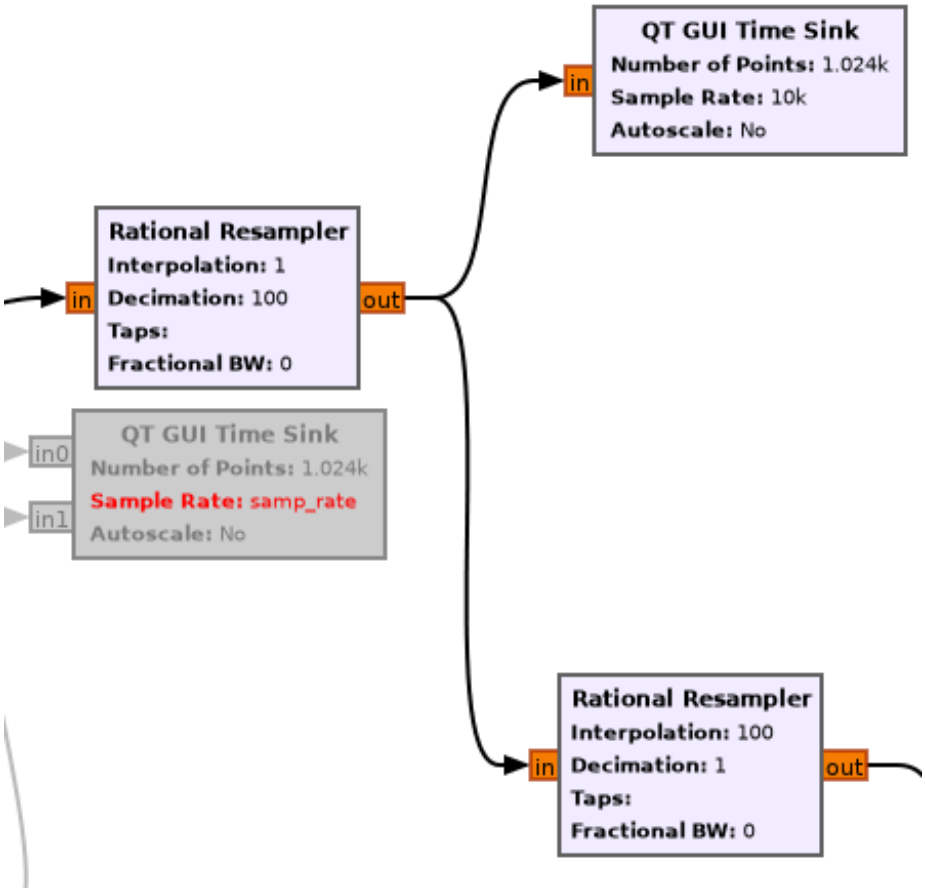

Figure 5: Downsampling the signal to reduce filesize. Instead of saving, the signal is directly resampled back up to continue the oparation in this case

After analysing, the signal is resampled with a decimation of 100. This reduces the sampling rate from 1 Msps down to only 10 ksps.

$$1Msps/100 = 1ksps$$

After this point, only the information is transported. If this were to be saved as a file again, filesize would be reduced by a signifficant amount. The information of the carrier wave is no longer in the signal. This also removes the sharp edges that were originally included in the output signal of the threshold block, because the highest frequency in a 10 ksps signal can only be 5 kHz.

Instead of saving it, the signal is directly resampled once more. By interpolating with 100 the information signal is back to 1 Msps sample rate.

$$100 * 1ksps = 1Msps$$

The signal is then converted back to a complex signal by adding an imaginary part of 0.

3.4 Signal source

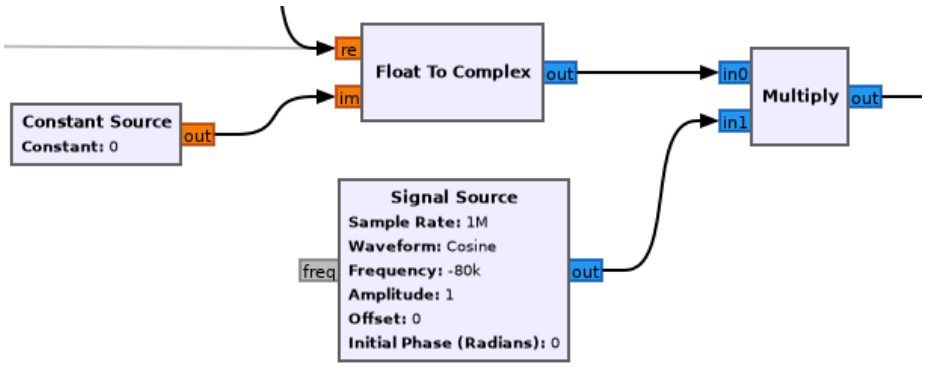

Figure 6: The signal source is used to generate the new carrier frequency. It is a negative frequency since the SDR will later modulate it with its set center frequency

A signal source is used to create the new carrier frequency. The waveform (sine or cosine) does not matter in this application. The frequency that the signal source is outputting is negative. By setting the right center frequency on the SDR, the modulation will work out in a way, that the original frequency is produced exactly.

3.5 Output bandpass filter

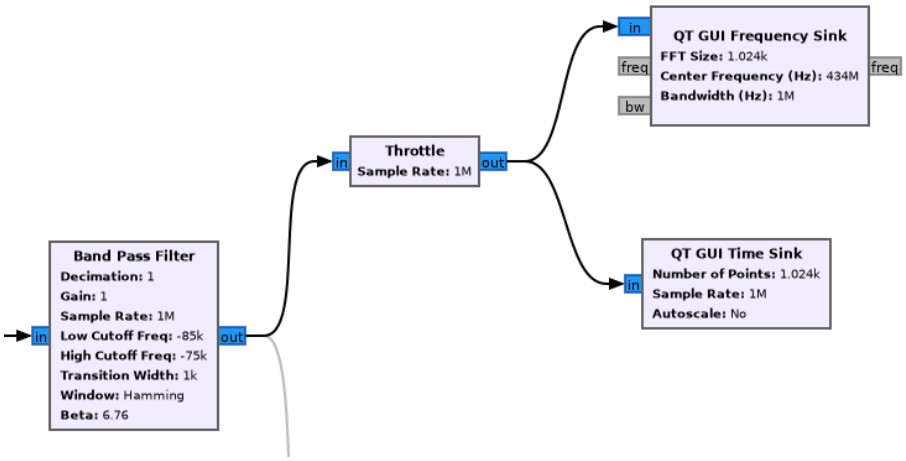

Figure 7: A second bandpass is used at the output to reduce edge sharpness of the on off keyed signal even further than by just resampling

The output signal is filtered using a very narrow bandpass filter. The transition width of 1 kHz is very sharp, the band is also rather narrow. This is done to acchieve a very clean signal in the frequency domain. The multiplication with the output of the threshold block also produces a clean time domain signal.

For testing purposes the output is throtteld and viewed in a time and a frequency sink.

4 Results

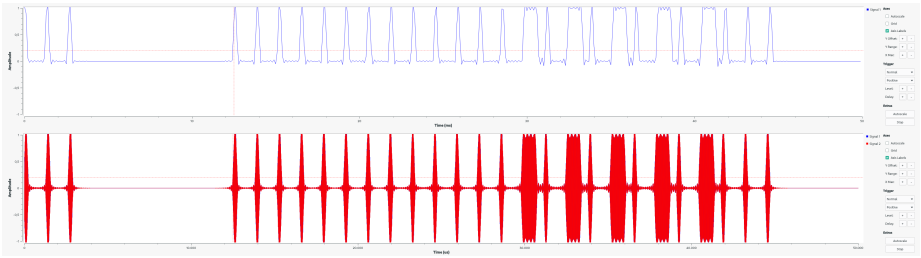

Figure 8: The resulting signal as viewed in the time domain. There is also the downsampled signal visible

To compare the signals, the intput and output signal are viewed in the frequency domain.

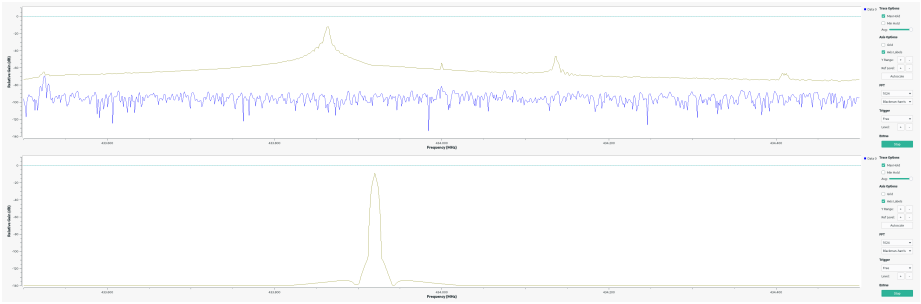

Figure 9: This is the frequency domain view of the input signal. The noise is quite high and the signal has a broad peak. There is noise in and out of the transmission band. The frequency domain of the synthesized signal is cleaner. The filtering produces a very clean spectrum with only one single, narrow peak at the frequency where the transmission is supposed to be

For both images, the peak hold was turned on. In the original signal, the noise is clearly visible while the synthesized signal shows no noise at all. Also the width of the transmitted signal is narrower now. The frequency is off from the original remotes frequency, but it is exactly where the text on the remote says it should be.

5 Lessons learned

Downsampling has the same effect as a lowpass filter, since in a signal with lower sampling rate no high frequency signals can be included. Downsampling can be used to reduce sample rate and therefor file size of stored signals. However the sample rate can not drop below the "information rate".

To produce a clean spectrum, the time domain signal will suffer. There is a lot of filtering necessary, which will introduce some ripple in the time domain.

The frequency printed on the remote control is not necessarily where it transmits in reality.