Planning a Student Contest: Fostering Self-guided Learning of Signal Processing in Communications Engineering

Workshop GeCON 2023

IEEE Student Branch Karlsruhe

Charlotte Muth, Marcus Müller, David Winter, Andrej Rode, Sebastian Koslowski, Felix Wunsch, Laurent Schmalen

August 1, 2023

Overview

1. Challenge Description
2. Hands-On Part
   - Demo 1 – Morse
   - Demo 2 – AFSK, FM & Envelope Modulation
   - Demo 3 – Music File
   - Demo 4 – OFDM
3. Q&A

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

IEEE Student Branch Karlsruhe: Introduction

General:

- Founding in 1988
- approx. 100 members

Board:

- Counselor: Prof. Jürgen Becker (ITIV)
- Chair: Charlotte Muth (CEL)
- Vice Chair: Andrej Rode (CEL)
- Treasurer: Marcus Müller (CEL)

Infos

Homepage: `www.ieee-ka.de`
Contact: info@ieee-ka.de

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Technical Presentations

Networking

- After-work-beer every two months
- Hang out with your (favorite) PhD students

Signal Intelligence Challenge

Student Paper Contest

- Write a paper about your research
- Win a trip to a Flagship IEEE conference

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Signal Intelligence Challenge: Overview

- Detect, demodulate, decode and decipher RF signals
  - Signals emitted at low power in unlicensed band
  - One signal often contains multiple messages, or hints to other signals
- Groups of 2 – 4 students
- 3 weeks duration
- Competitive point system
- But **ungraded**, no credits
- Prizes (high-value)
  - Software-Defined Radio Devices (winners, ca 1000 €)
  - Computer Hardware (runner-ups, ca 100 €)
  - Restaurant/brewery vouchers (participants, ca 25€)

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Signal Intelligence Challenge: Participants

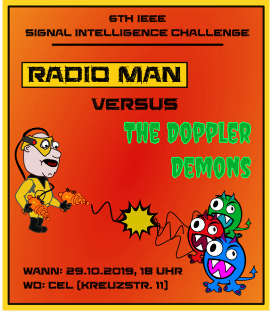
- Mostly advertised towards electrical engineering students
  - . . . but also mechatronics students, physics & computer science students
  - Winning teams often mixed
- Earliest intended audience: ca 5th semester (EEs @ KIT: *Communications Engineering I*)
  - Meaningless for non-EE students
- Some teams take part for several years, no limit

ISIC '22 finale. Left to right: Participants (12×), Organizers (2×)

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Signal Intelligence Challenge: Themes

- Surrounding story, worldbuilding
- Sets topics for Challenges
- Flags from context



2019: Superheroes

2018: Hung over on a space station

2017: Espionage

2016: Bank heist

2015: Peeking behind the veil

2022: Helping the lost & confused

Signal Intelligence Challenge: Timeline

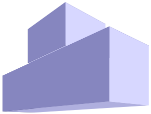
Challenge

Advertise

Nov 1
Kick-off

Nov 12
New Challenges

Nov 23
Deadline



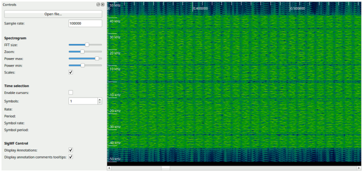
Nov 24
Ceremony

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Signal Intelligence Challenge: Tools

Hardware: USRPs, RTL-SDR dongles, . . .
Software:

- GNU Radio
- Matlab
- Python
- Specialized tools (Gqrx, inspectrum, Audacity, webtools like `dcode.fr`, . . .)
- . . .



/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Automated Feedback for Solutions

Matrix (maubot) to hand in solutions

general prompts	
!help	display general prompts
!register	register new team
!addmember	add member to team
@SR#<solution>#isic	hand in flags
!stats	display current points
!problem	notify orga of problem

Automatic notification if solutions did not match the actual solutions but were close.

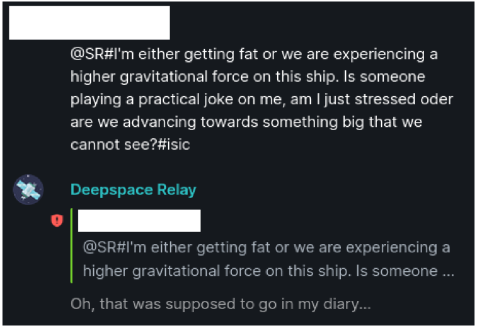
Features:

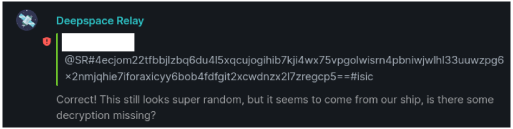
- Automated handing in and tracking of points
- Limited notification of close but not correct solutions
- Unique replies for correct solutions

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Automated Feedback for Solutions

- Nomenclature:
  - Individual signal: **Challenge**
  - Secret message to be found: **Flag**
- correct flag gives 100 points
- Bonus for handing in first, second, . . . is 5/4/3/2/1 points
- No penalty for wrong solutions, but hand-in is limited to 1 per minute





/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Signal Intelligence Challenge: Goals

- Primarily: Fun!
  - For students, and
  - for organizers
- Bring students closer to commmunications engineering
- Establishes student branch as hub
- Build inter-faculty bridges
- Teach
  - Hands-on digital signal processing
  - Practical aspects of digital reception
  - Tools of the trade (GNURadio, USRPs, Python, ...)
  - Independently approaching engineering problems ...
  - ... in a group of peers

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

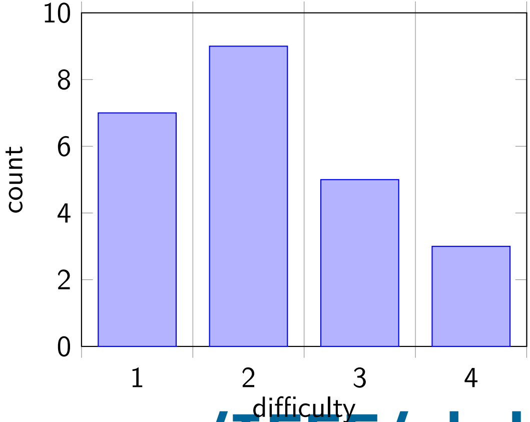
Signal Intelligence Challenge: Goals

- Primarily: Fun!
  - For students, and
  - for organizers
- Bring students closer to commmunications engineering
- Establishes student branch as hub
- Build inter-faculty bridges
- **Teach**
  - Hands-on digital signal processing
  - Practical aspects of digital reception
  - Tools of the trade (GNURadio, USRPs, Python,. . .)
  - Independently approaching engineering problems . . .
  - . . . in a group of peers

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Structure

1. Recognize the structure of the signal & choose appropriate tools(e.g. standard FM radio receiver) to find solution
2. Analyze the signal to recognize structure & apply minor signal processing
3. Apply some communication engineering knowledge & signal processing
4. Be a communication engineer & find unconventional signal representations



/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Participation

Team	1.1	1.2	2.1	2.2	2.3	2.4	3.1	4.1	4.2	5.1	5.2	6.1	6.2	6.3	7.1	7.2	8.1	8.2	9.1	10.1	10.2	10.3	11.1	11.2	total
T1	103	104	104	105	104		105								101										726
T2	105	103	103		103		103			104		103	104		104	104	103	103		103	103		103	104	1655
T3																									0
T4	102	102	101		101		102						103		103							104			818
T5	104	105	105	104	105	105	104	105	105	105	105	105	105	105	105	105	105	105	105	105	105	105	104	105	2516
T6	101		102		102		101	104				104	102		102	103	104	104		104	104	103	105		1545

Challenge difficulty: 1, 2, 3, 4

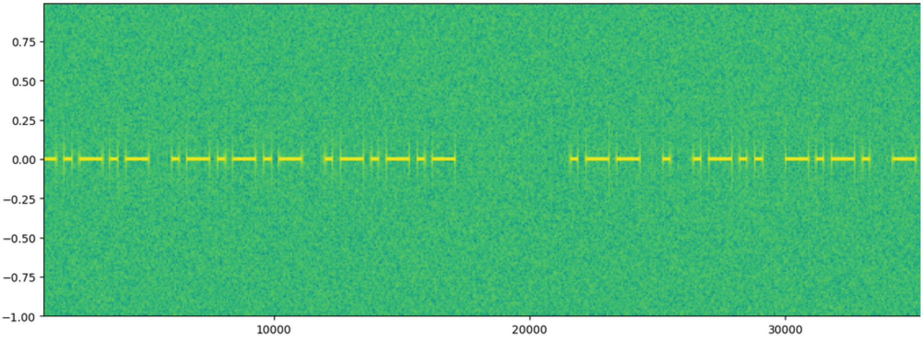
/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Hands-On Part

- Find the shared data sets and notebooks on zenodo
- We show in this part solving the challenges in jupyter notebooks, but during the challenge students work with whichever tools they want. There are lots of great tools helping decryption, standard modulation methods, . . .
- We will demonstrate the idea behind the challenge, developing a solution (with your aid) with way less trial and error then most students will need

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

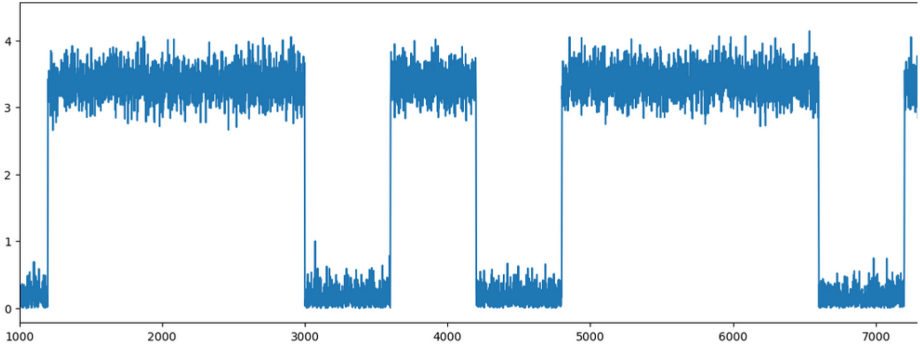
Demo 1: Morse Code



Easy way: play signal over audio, use morse decoding app

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

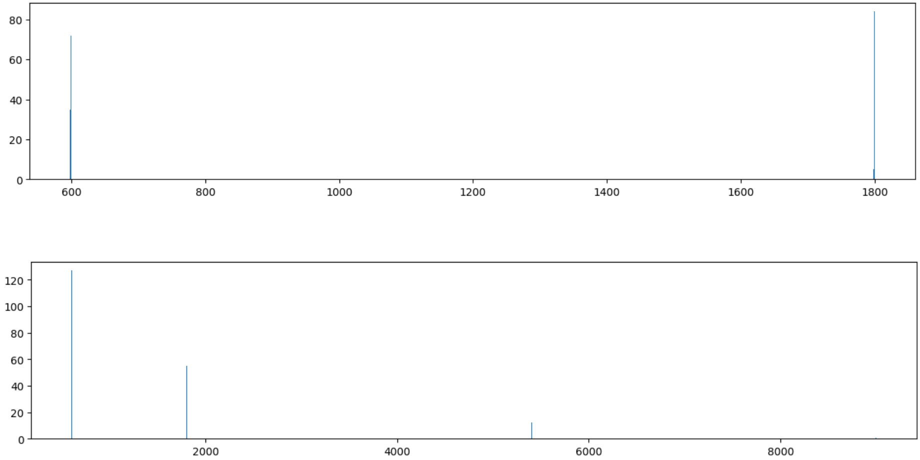
Harder way: demodulate



/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 1: Morse Code

Harder way: measure symbol lengths and pause lengths



Demo 1: Morse Code

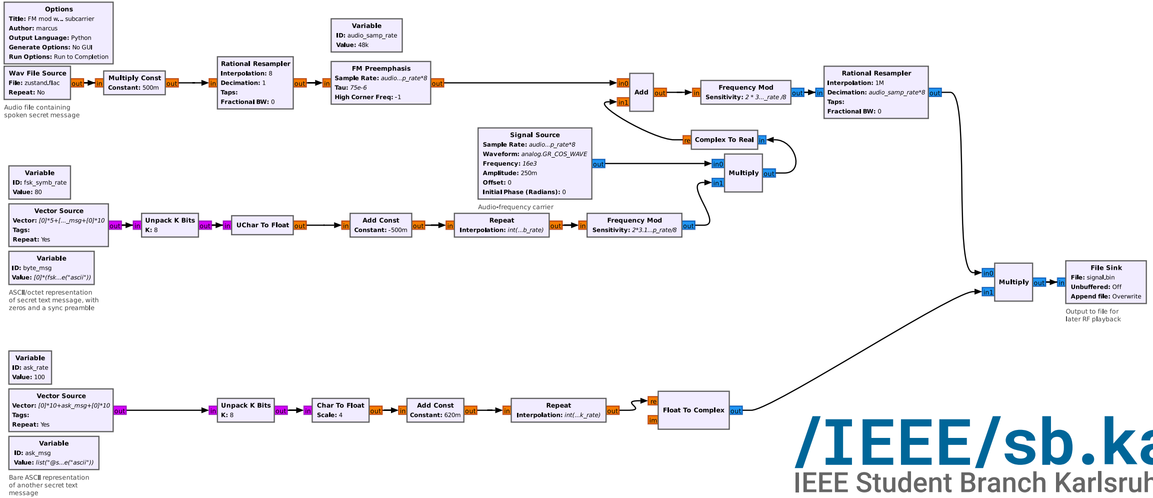
```
def translate_morse(dec):
    ret = []

    for k,v in dec:
        if k:
            if v > 1000:
                ret.append("-")
            else:
                ret.append(".")
        else:
            if 2000 > v > 1000:
                ret.append(" ")
            elif v > 2000:
                ret.append("   ")

    return "".join(ret)
```

```
morse.decrypt(translate_morse(dec))
```

```
'... WELCOME TO GECON AND THANK YOU FOR BEING HERE. THANKS FOR INSPIRING EDUCATORS.'
```

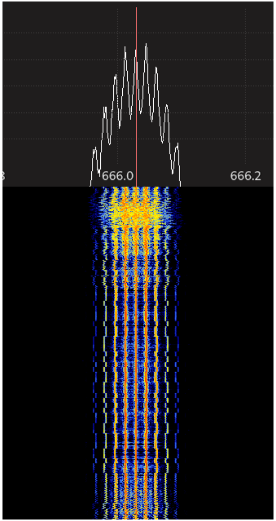
b.ka
IEEE Student Branch Karlsruhe

Unknown to the participants!



/IEEE/sb.ka
IEEE Student Branch Karlsruhe

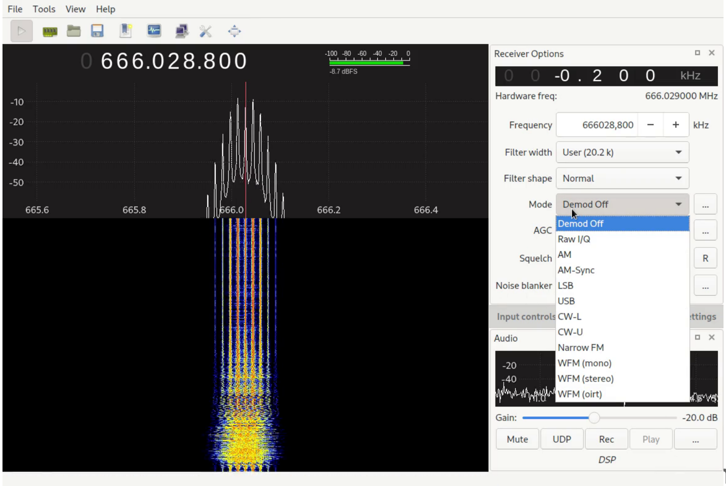
Demo 2: AFSK, FM & Envelope Modulation – Spectrum



- Experienced insight: FM-like characteristics, strange sidelobes
- Normal approach: Try FM, this looks analog and isn't AM

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Using Gqrx to modulate:

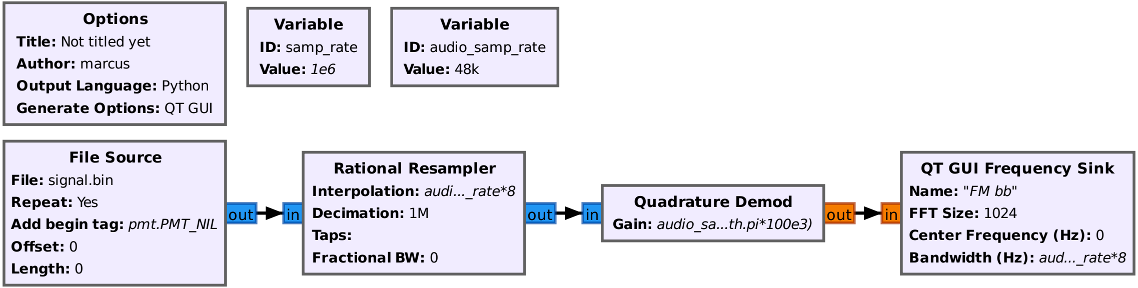


E/sb.ka
it Branch Karlsruhe

Demo 2: AFSK, FM & Envelope Modulation – Remaining Signal

- FM demodulation yields a flag
- But sidelobes and quality raise suspicion

→ Look at signal after FM demodulation



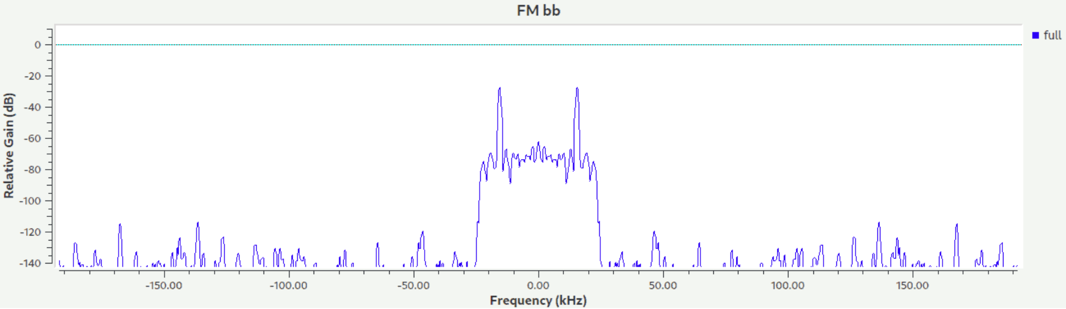
High-SNR FM demodulator built in GNU Radio Companion

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 2: AFSK, FM & Envelope Modulation – Remaining Signal

- FM demodulation yields a flag
- But sidelobes and quality raise suspicion

→ Look at signal after FM demodulation

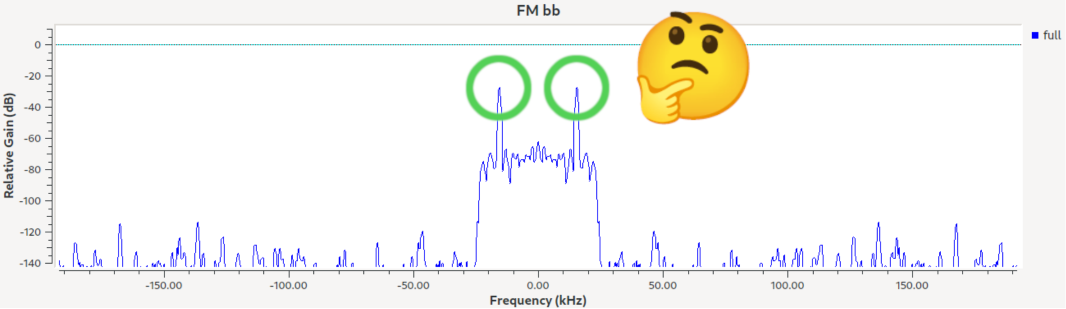


Spectrum after FM demodulation

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

- FM demodulation yields a flag
- But sidelobes and quality raise suspicion

→ Look at signal after FM demodulation

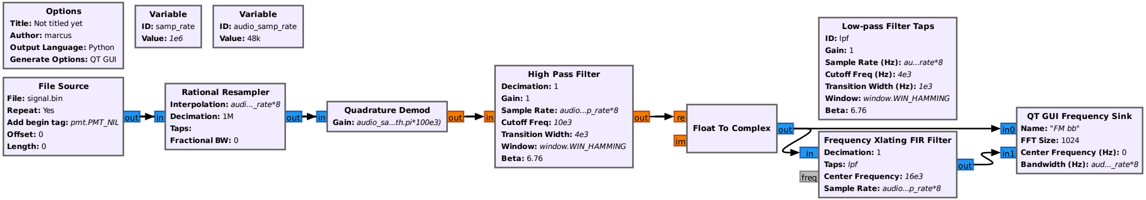


Spectrum after FM demodulation

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 2: AFSK, FM & Envelope Modulation – Remaining Signal

- Spikes in audio baseband spectrum seem to shift
- Zoom in and activate *Max Hold*

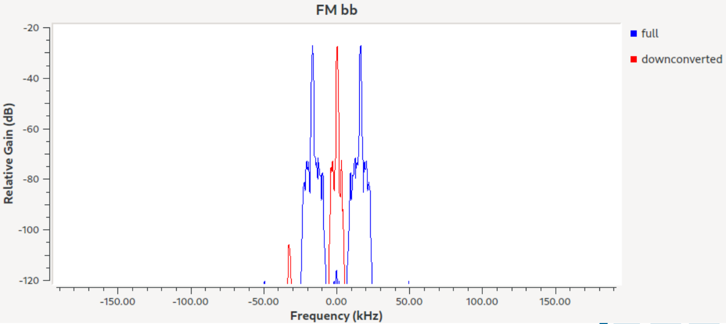


FM demodulator with high-pass filter and approximate mixing to complex baseband

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 2: AFSK, FM & Envelope Modulation – Remaining Signal

- Spikes in audio baseband spectrum seem to shift
- Zoom in and activate *Max Hold*



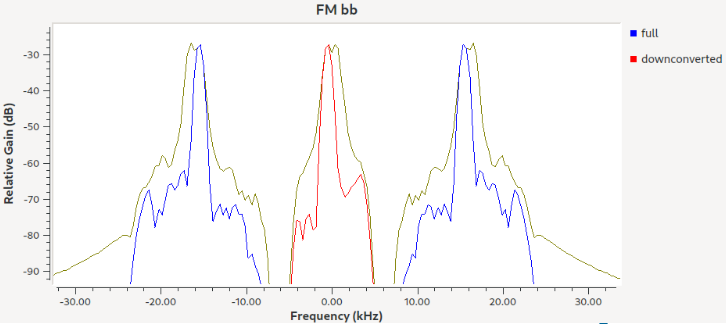
Spectrum after demodulator

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 2: AFSK, FM & Envelope Modulation – Remaining Signal

- Spikes in audio baseband spectrum seem to shift
- Zoom in and activate *Max Hold*

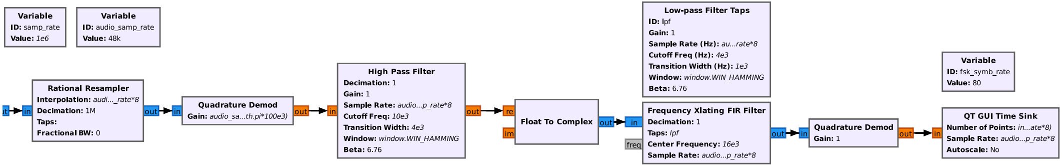
$\rightarrow$ Looks a lot like 2-FSK



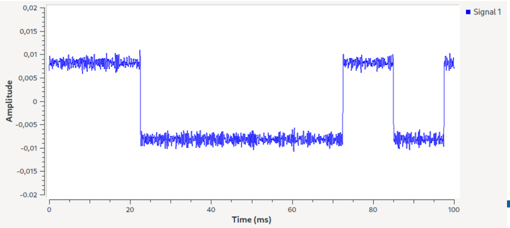
Zoomed-in spectrum after FM demodulation

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 2: AFSK, FM & Envelope Modulation – Demodulating 2-FSK



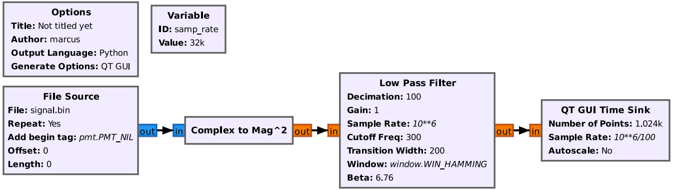
Demodulating the FSK-modulated signal inside the FM signal



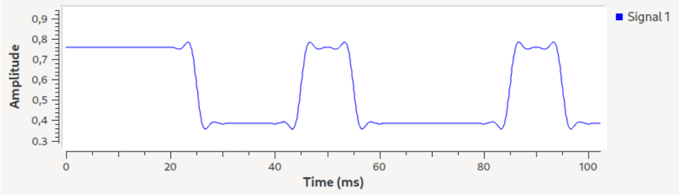
After the FSK demodulator

IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 2: AFSK, FM & Envelope Modulation – Envelope Modulation



Demodulating the envelope-modulated (ASK) signal



After the envelope detector

Demo 3: Music File

Modulated music file[1]

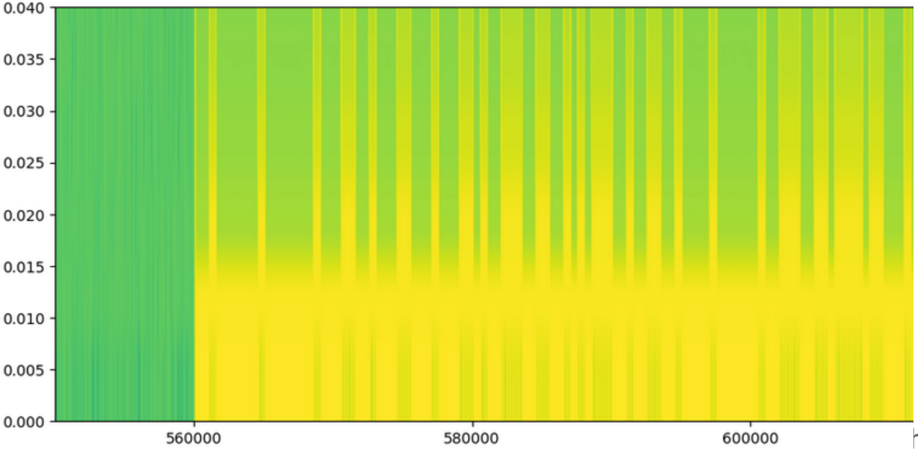
- On-off keying with solution: *@SR#Signal interference cancellation is very important in things like NOMA, which seem to be quite exiting for humans.#isic*
- Signal interference cancellation: Remove a dominant signal in order to decode real signal (in our case: dominant signal is music)
- Music file also has left and right channel, so maybe combine these?

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

[1] KIT hymne piano version: https://www.youtube.com/watch?v=tsJiiBMUroY

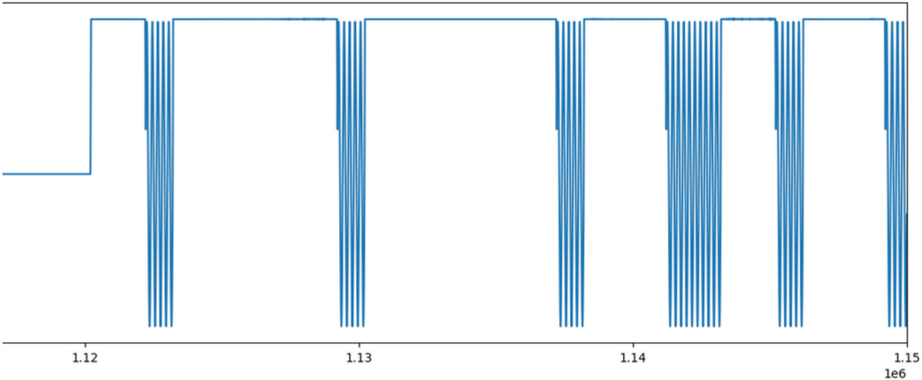
Demo 3: Music File

After subtracting right and left audio channel, signal strength is reduced and additional signal visible:



Demo 3: Music File

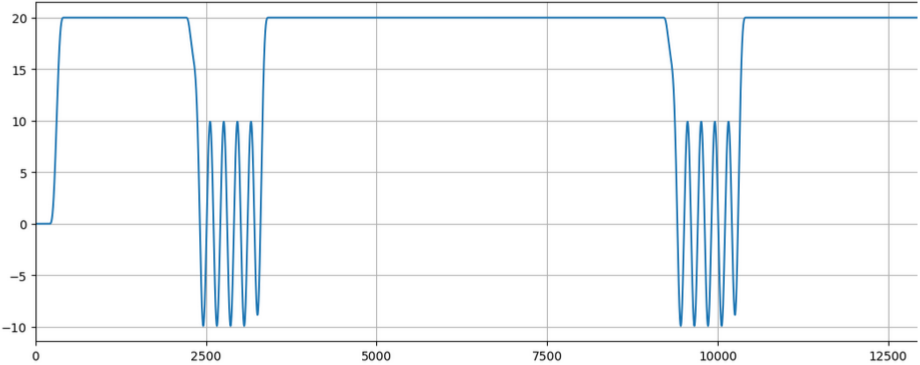
Correlating with frequency $f = 0.02 \cdot f_s$:



/IEEE/sb.ka
IEEE Student Branch Karlsruhe

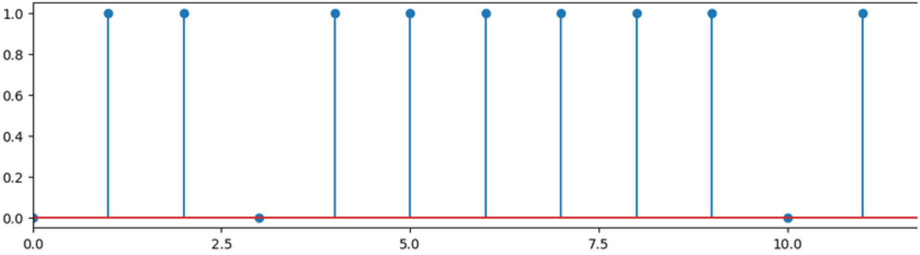
Demo 3: Music File

Low pass filtering to get a good decision threshold:



/IEEE/sb.ka
IEEE Student Branch Karlsruhe

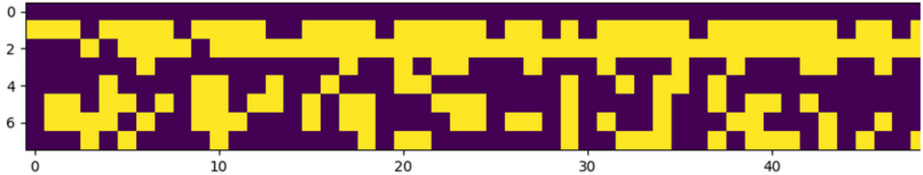
Sampling every $N = 1000$ sample:



/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 3: Music File

Arrange bit in blocks of 8 bit for ASCII mapping, also shift bit to fit ASCII structure:



Result: *@FF#Nerd Nobd, fhvg yitvf br o riaox mrgeats ar acf. Jhgf pngeeq gamrhtiau nlhs...#usvq*
$\rightarrow$ decryption needed

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 3: Music File

Try Viginere encryption, since no specific key is given (a bunch of online tools can brute force this when trying small key lengths)

```
'@SR#Signal interference cancellation is very important in things like NOMA, which seem to be quite exiting for humans.#isic'
```

```
n="isic"
t="usvq"

up = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
low = "abcdefghijklmnopqrstuvwxyz"

offset = [int(-ord(n[i])+ord(t[i])) for i in range(4)]
off=[]
for o in offset:
    off.append(low[o])
off
```

```
['m', 'a', 'n', 'o']
```

Let's try *NOMA* since it also shows up in the other challenge.

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

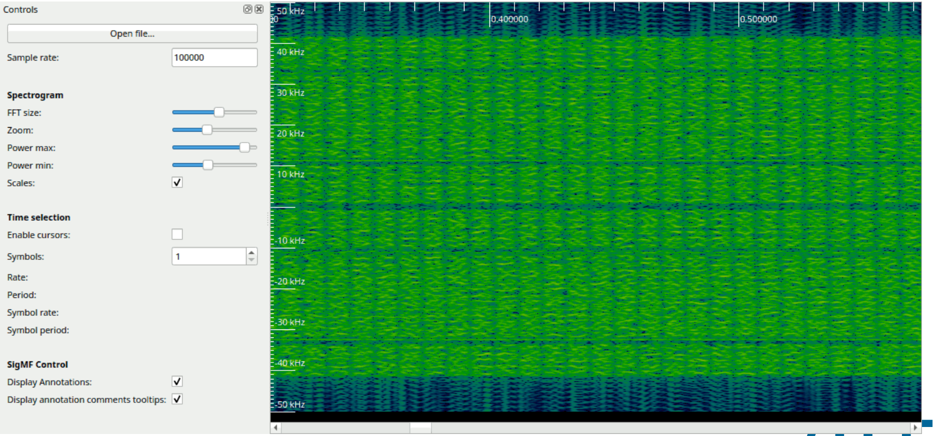
Demo 3: Music File

```python
# key="noma"
shifts = [26-low.find(d) for d in key]

i = 0
for c in message:
    if c in up:
        print(up[(up.index(c) + shifts[i%4]) % 26], end="")
        i = i + 1
    elif c in low:
        print(low[(low.index(c) + shifts[i%4]) % 26], end="")
        i = i + 1
    else:
        print(c, end='')
print()
```

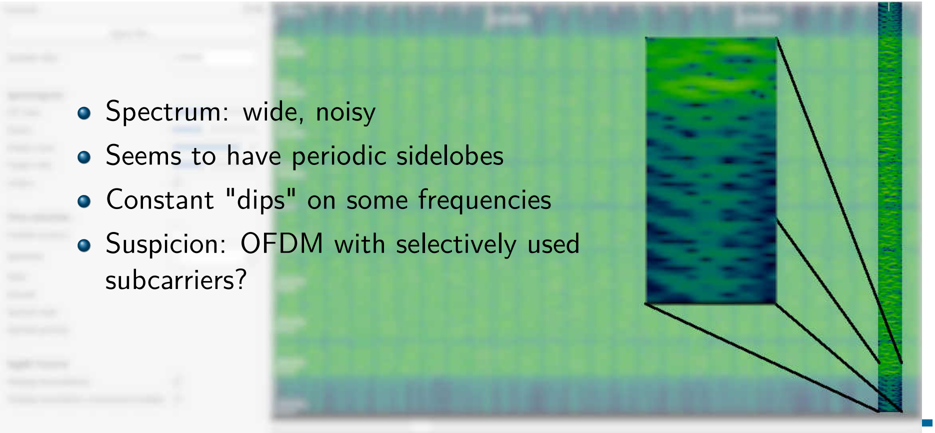
```
@SR#Beep Boop, this might be a final message or not. Just passed something blue...#isic
```

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 4: OFDM – Spectrum



/IEEE/sb.ka
IEEE Student Branch Karlsruhe



- Spectrum: wide, noisy
- Seems to have periodic sidelobes
- Constant "dips" on some frequencies
- Suspicion: OFDM with selectively used subcarriers?

IEEE Student Branch Karlsruhe

Demo 4: OFDM – Strategy

Requisites for decoding OFDM signals

- Find OFDM parameters (Subcarrier spacing & count, cyclic prefix length)
- Identify occupied subcarriers
- Find per-subcarrier constellation

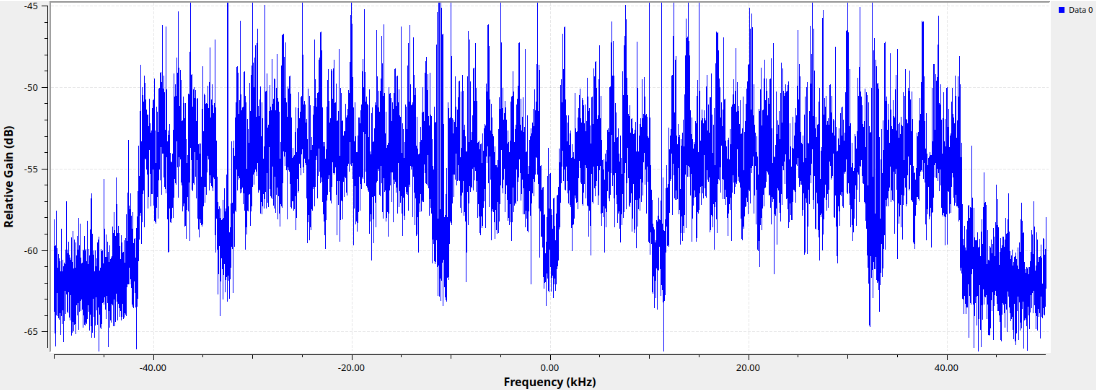
Parameter estimators for OFDM[2] exist in literature

- Unrealistic for participants to know
- One-off job → manual identification

[2] `gr-inspector` by former student Sebastian Müller

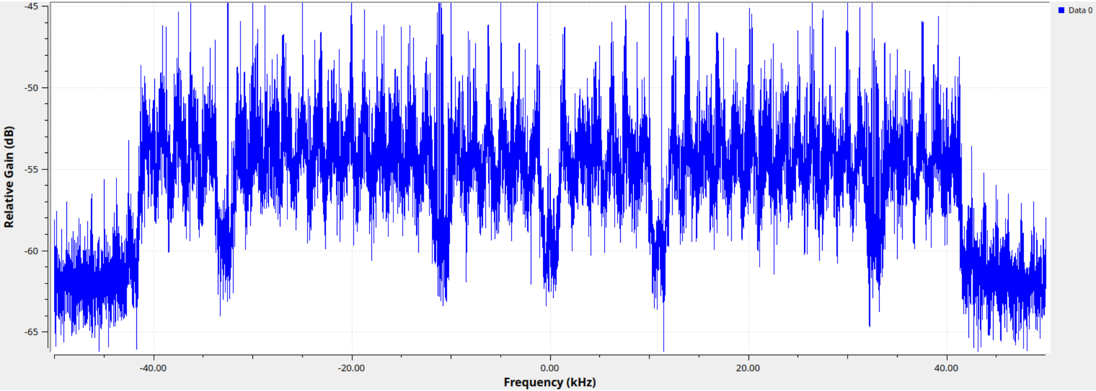
/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 4: OFDM – Subcarrier Count



/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 4: OFDM – Subcarrier Count



52 used subcarriers by manual count, ca. 1.54 kHz spacing
Best guess: 100 kHz bandwidth, $N_{\mathrm{FFT}} = 64$

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Assuming Communications Engineering II is known:
If $N_{\mathsf{FFT}} = 64$, then the sample-wise product of the signal with a 64-delayed version of itself has CP-length plateaus

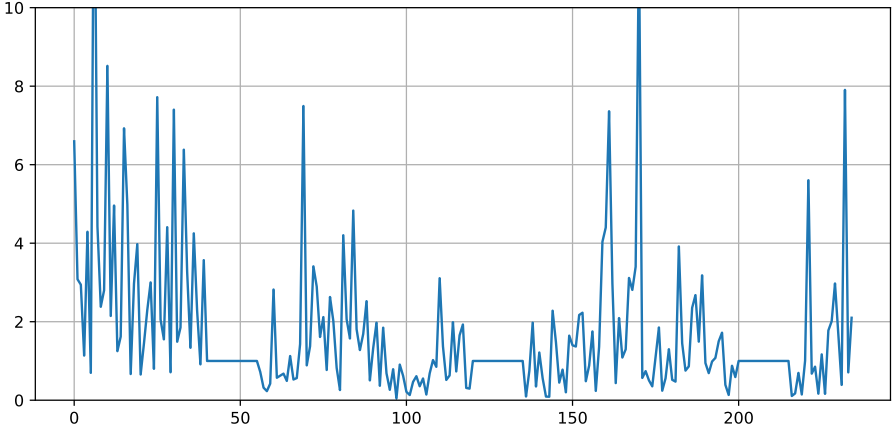
```
"""
Calculate a fixed-lag correlation
"""
flcorr =  [
    np.sum(in_sig[pos:pos+1] *
    in_sig[pos+N:pos+N+1].conj()) /
    np.sum(abs(in_sig[pos: pos+1]**2))
    for pos in range(length-N-1)
]
```

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 4: OFDM – Cyclic Prefix

Assuming Communications Engineering II is known:

If $N_{\mathsf{FFT}} = 64$, then the sample-wise product of the signal with a 64-delayed version of itself has CP-length plateaus



E/sb.ka
ent Branch Karlsruhe

Demo 4: OFDM – Demodulation

- It's OFDM – look out for Schmidl&Cox symbols
- Demodulate with DFT using $N = 64$, $L_{\mathrm{CP}} = 16$
- Visualize constellation points

...lots of experimentation, **or** open the GNU Radio OFDM example (which happens to be identically parameterized)

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 4: OFDM – Data Interpretation

Inspection showed: QPSK, with some strange identical BPSK-only symbols (ignore these, or use GNU Radio OFDM RX)

```
00000000: ffd8 ffe0 0010 4a46 4946 0001 0101 0048  ......JFIF.....H
00000010: 0048 0000 ffe1 205a 4578 6966 0000 4949  .H.... ZExif..II
00000020: 2a00 0800 0000 0700 1201 0300 0100 0000  *...............
00000030: 0100 0000 1a01 0500 0100 0000 6200 0000  ............b...
00000040: 1b01 0500 0100 0000 6a00 0000 2801 0300  ........j...(...
```

IEEE Student Branch Karlsruhe

Demo 4: OFDM – Data Interpretation

Inspection showed: QPSK, with some strange identical BPSK-only symbols (ignore these, or use GNU Radio OFDM RX)

```
00000000: ffd8 ffe0 0010 4a46 4946 0001 0101 0048  ......JFIF.....H
00000010: 0048 0000 ffe1 205a 4578 6966 0000 4949  .H.... ZExif..II
00000020: 2a00 0800 0000 0700 1201 0300 0100 0000  *...............
00000030: 0100 0000 1a01 0500 0100 0000 6200 0000  ............b...
00000040: 1b01 0500 0100 0000 6a00 0000 2801 0300  ........j...(...
```

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Demo 4: OFDM – Data Interpretation

Inspection showed: QPSK, with some strange identical BPSK-only symbols (ignore these, or use GNU Radio OFDM RX)

Result: *@SR#If telescopes use mirrors, we'll never see space vampires coming.#isic*

/IEEE/sb.ka
IEEE Student Branch Karlsruhe

Thank you kindly for your attention!

Are there any questions?

/IEEE/sb.ka
IEEE Student Branch Karlsruhe