

## Abgabe PHYSEC 1

### Spionage!

a)

Zuerst muss inspectrum installiert werden. Als nächstes wird inspectrum gestartet und die mitgegebene file namens SecretSignal.raw geöffnet. Anschließend wird das Programm mit der rechten Maustaste angeklickt: Add derived plot -> Add sample plot. Eine horizontale „Spannweite“ öffnet sich. Es muss entsprechend mit der Maus angepasst werden. Es ist bekannt, dass Amplitude-Shift Keying, abgekürzt ASK als digitale Modulationsart verwendet wurde. Entsprechend werden Nullen und Einsen zugewiesen, siehe Abbildung 3. Darüber hinaus ist bekannt, dass die Nachricht mit der Präambel 0x55 anfängt, welche nicht teil der eigentlichen Nachricht ist. Danach wird in Bytes aufgeteilt und mit ASCII kodiert.

b)

Die Nachricht besteht aus dem wiederholten String „Money4Physec“. Abfolge: 0x55, 0x4D, 0x6F, 0x6E, 0x65, 0x79, 0x34, 0x50, 0x68, 0x79, 0x73, 0x65, 0x63, 0x55, 0x4D und so weiter...

Hex	Value	Hex	Value	Hex	Value	Hex	Value	Hex	Value	Hex	Value	Hex	Value	Hex	Value
00	NUL	10	DLE	20	SP	30	0	40	@	50	P	60	`	70	p
01	SOH	11	DC1	21	!	31	1	41	A	51	Q	61	a	71	q
02	STX	12	DC2	22	"	32	2	42	B	52	R	62	b	72	r
03	ETX	13	DC3	23	#	33	3	43	C	53	S	63	c	73	s
04	EOT	14	DC4	24	\$	34	4	44	D	54	T	64	d	74	t
05	ENQ	15	NAK	25	%	35	5	45	E	55	U	65	e	75	u
06	ACK	16	SYN	26	&	36	6	46	F	56	V	66	f	76	v
07	BEL	17	ETB	27	'	37	7	47	G	57	W	67	g	77	w
08	BS	18	CAN	28	(	38	8	48	H	58	X	68	h	78	x
09	HT	19	EM	29	)	39	9	49	I	59	Y	69	i	79	y
0A	LF	1A	SUB	2A	*	3A	:	4A	J	5A	Z	6A	j	7A	z
0B	VT	1B	ESC	2B	+	3B	;	4B	K	5B	[	6B	k	7B	{
0C	FF	1C	FS	2C	,	3C	<	4C	L	5C	\	6C	l	7C	
0D	CR	1D	GS	2D	-	3D	=	4D	M	5D	]	6D	m	7D	}
0E	SO	1E	RS	2E	.	3E	>	4E	N	5E	^	6E	n	7E	~
0F	SI	1F	US	2F	/	3F	?	4F	O	5F	_	6F	o	7F	DEL

Abbildung 1: Quelle: Hier klicken

Diese Tabelle weist jedem Byte die entsprechende ASCII Kodierung zu:




	Hex 	ASCII.Wert 
1	55	U
2	4D	M
3	6F	o
4	6E	n
5	65	e
6	79	y
7	34	4
8	50	p
9	68	h
10	79	y
11	73	s
12	65	e
13	63	c

Abbildung 2: Tabelle 2

Diese zwei Screenshots zeigen wie der Anfang vom Signal mithilfe von inspectrum analysiert aussieht. Farbige Kodierung sowie Umrandungen wurden hinterher selbst hinzugefügt.

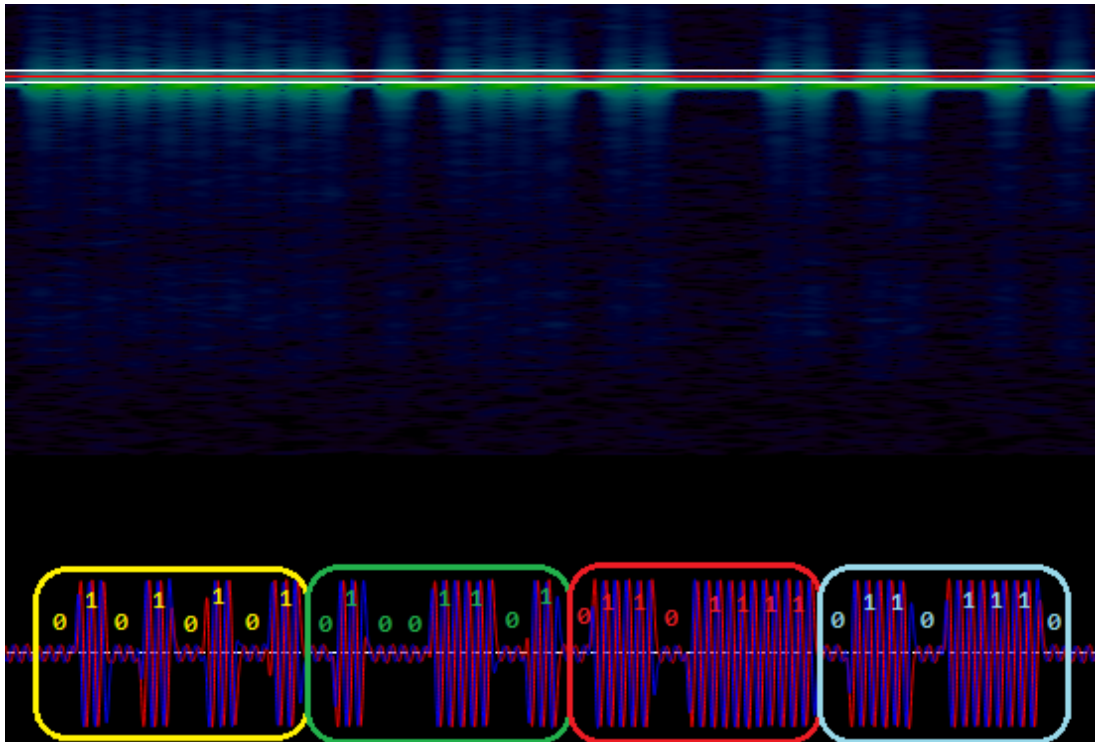


Abbildung 3: Bits und Bytes

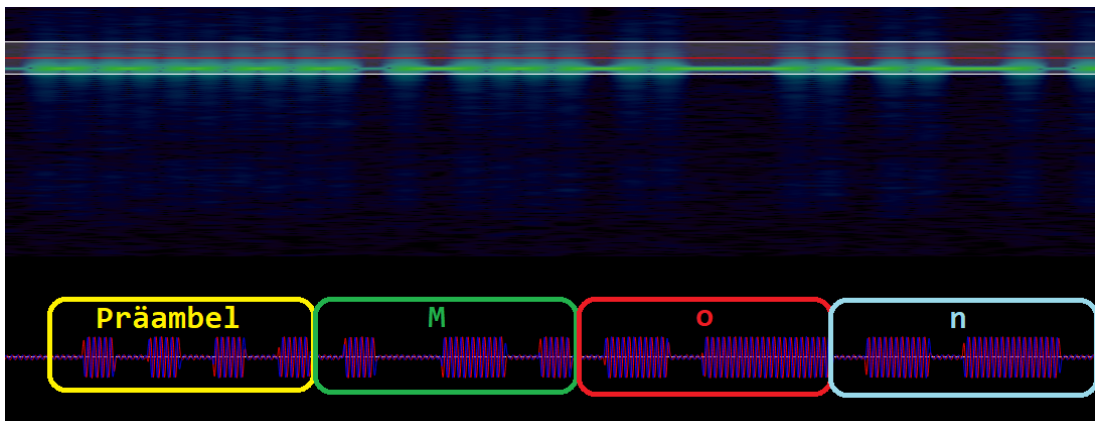


Abbildung 4: Bytes ASCII kodiert

Man erkennt, dass sich die Nachricht wiederholt.

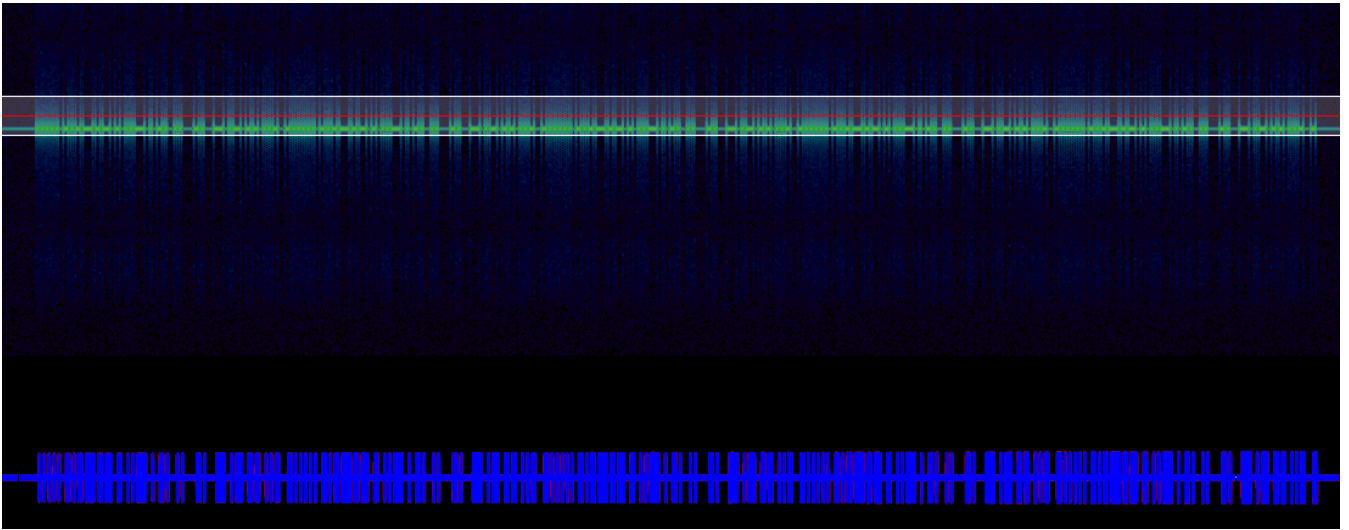
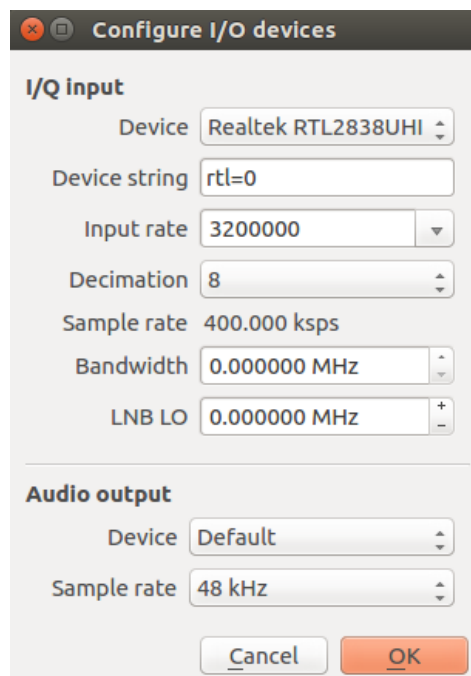


Abbildung 5: Gesamte Nachricht

## Funkfernbedienungen

Für diese Aufgabe wurde das Programm *gqrx* mit folgenden Einstellungen verwendet:



FFT Settings

FFT size  RBW: 3.1 Hz

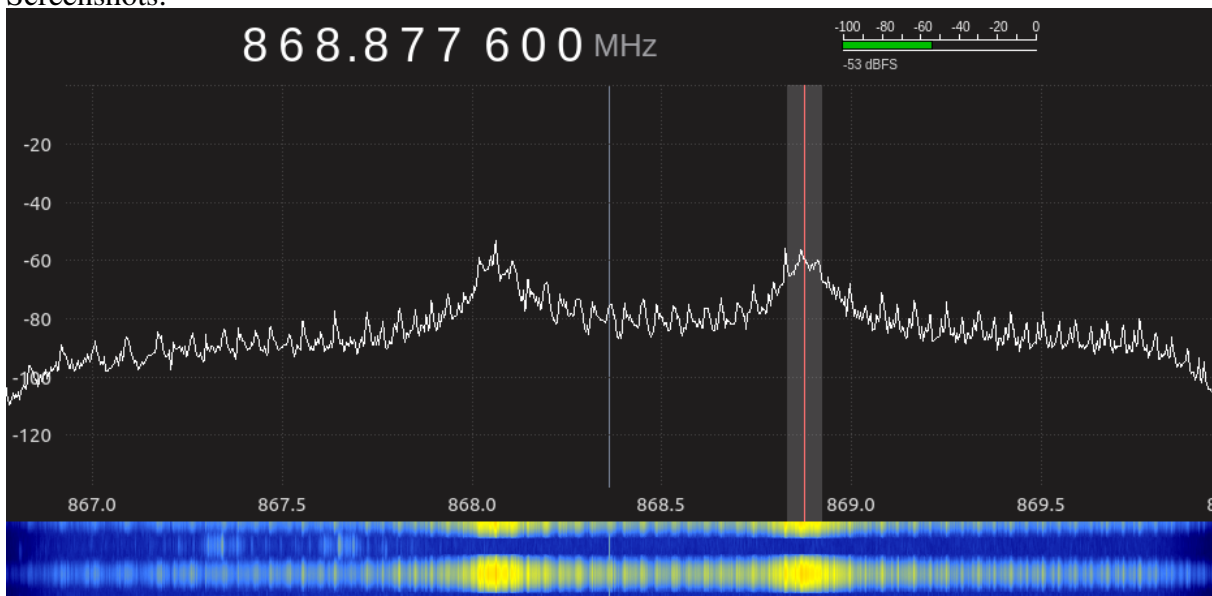
Rate  Overlap: 883%

Time span  Res: - s

Abbildung 6: FFT Size

## Signal 1

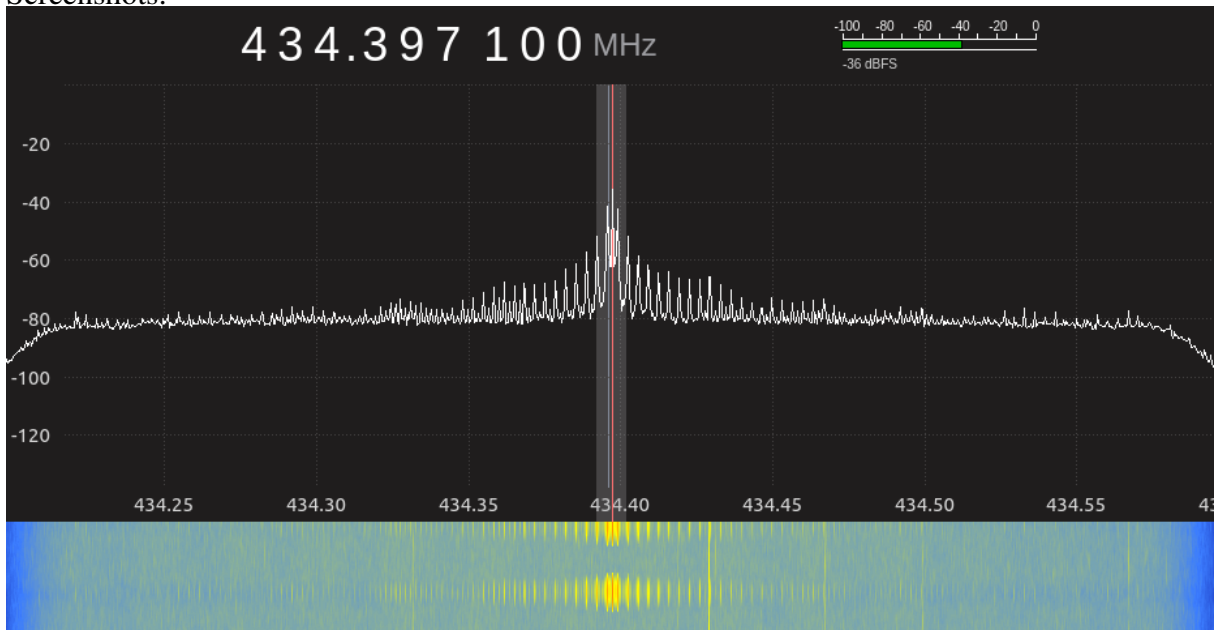
- Modell: BMW 1er
- Mittenfrequenz: 868.877 MHz. Es gab jedoch weitere Frequenzberge.
- Screenshots:





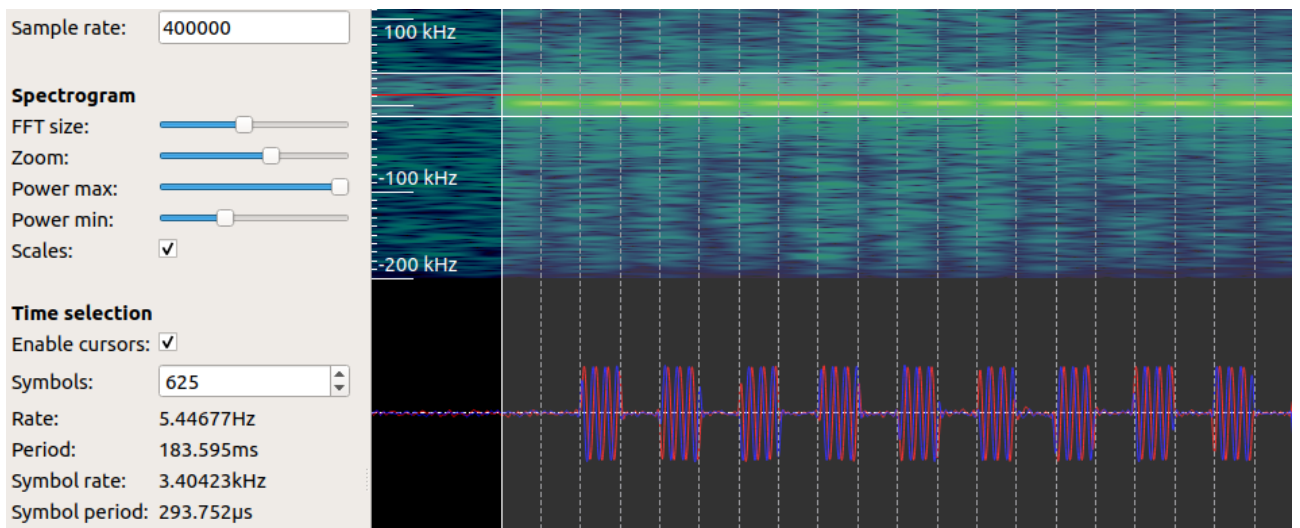
- Mittenfrequenz: 434.397 MHz

- Screenshots:



Das Sendemuster hebt sich deutlich von dem des BMW ab

- Symbolrate: ca. 625 Symbole pro Signal - ca. 3.40kHz bei Sample rate von 400 000ksps
- Modulation: ASK

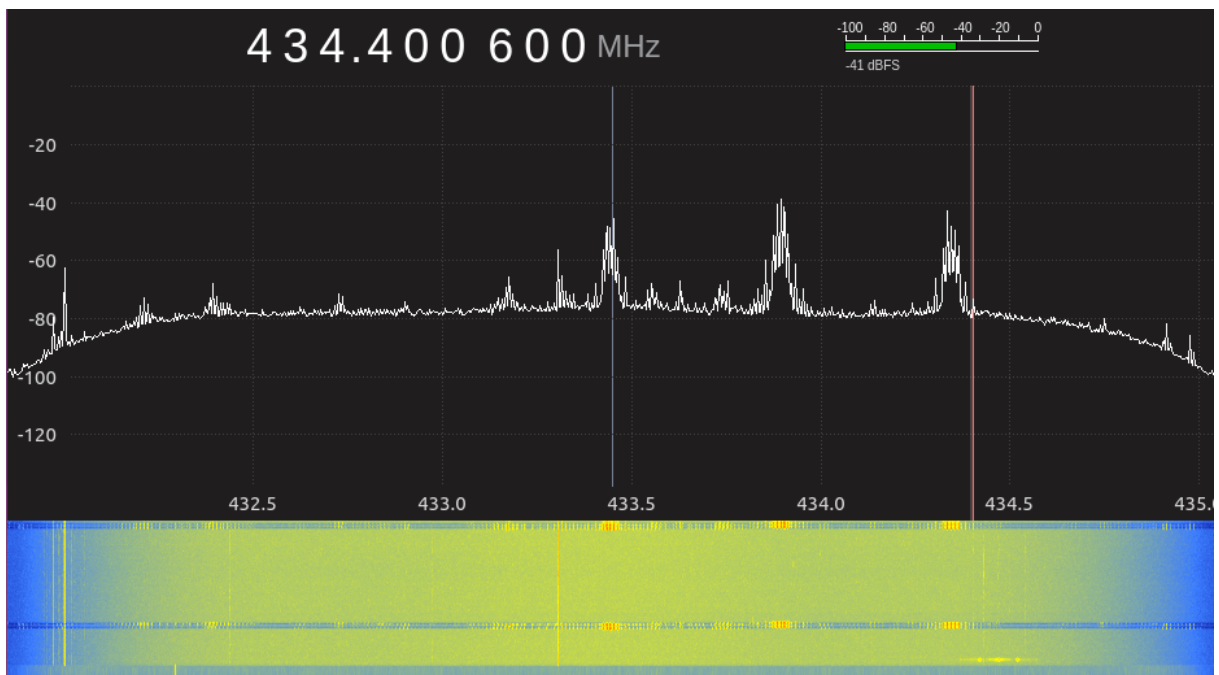
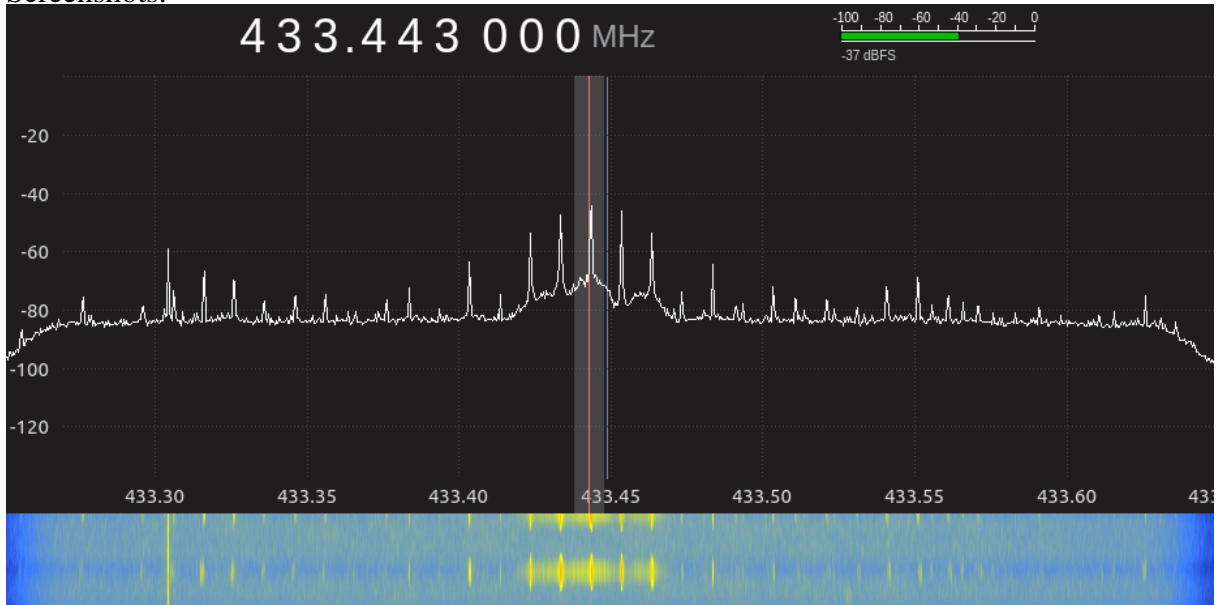


- Untersuchung:
  - ersten 430 Symbole 1, 0 alternierend - Präambel
  - letzten 204 Symbole fuer Oeffnung/Schliessung verantwortlich
  - beide Signale unterscheiden sich nicht

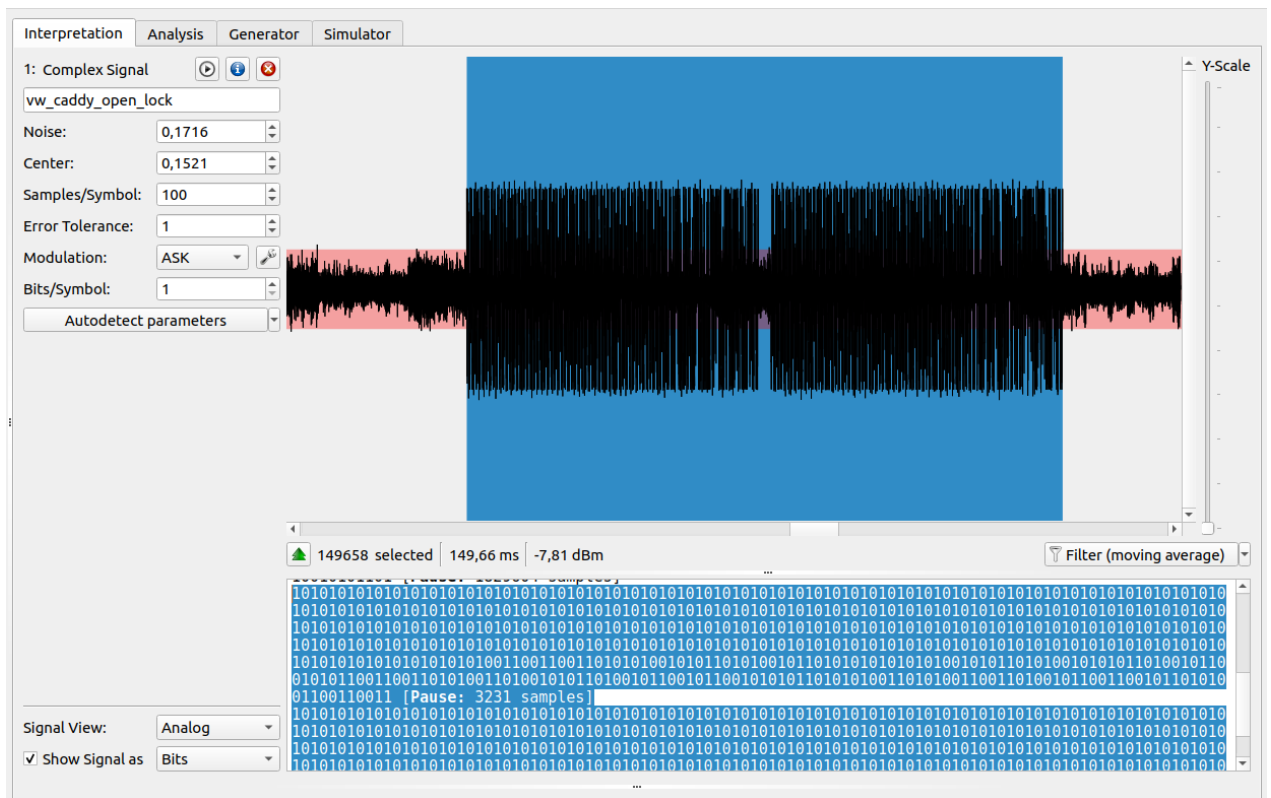


## Signal 3

- Modell: Mercedes CLA
- Mittenfrequenz: 433.443 MHz
- Screenshots:







Bei  $Decimation = 0$  kann man erkennen, dass die Fernbedienung auf mehreren Frequenzen sendet

- Symbolrate: ca. 406 Symbole pro Signal - ca. 5.88kHz bei Sample rate von 400 000kps
- Modulation: Laut URH autodetect ASK

## Theorie Link Budget

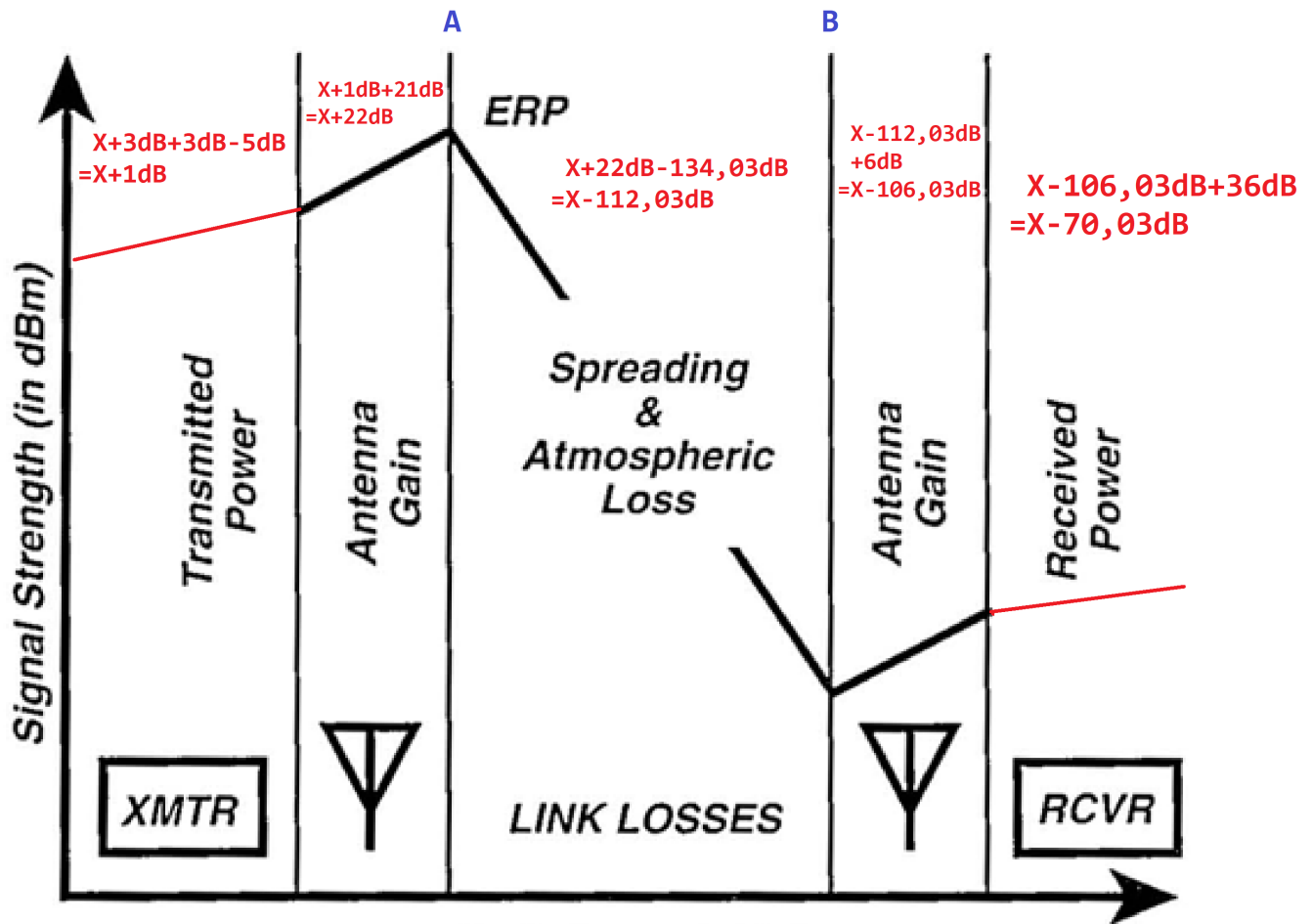


Abbildung 7: Grafik 2  
Quelle Skizze (Ohne farbige Notizen)

a)

Maßeinheiten werden der besseren Übersicht halber ausgelassen in den Rechenwegen, aber nicht in den Endergebnissen selbst bei den Teilaufgaben a), b) sowie c)!

Orientiert man sich an der Formel aus dem mitgegebenen Dokument *zsmfssg\_U1.pdf*, dann berechnet sich der Verlust in dB wie folgt:

$20 * \log_{10}(r * f * \frac{4\pi}{c})$ , wobei  $r$  die Distanz in Metern, 120000,  $f$  die Frequenz in Hz, hier  $10^9$  und  $c$  die Lichtgeschwindigkeit in m/s, also 299792458.

Wir setzen ein:

$$20 * \log_{10}(120000 * 10^9 * \frac{4\pi}{299792458}) \approx 134.03.$$

**i) Matrikelnummer mit 22 am Ende**

Rechnung für die Matrikelnummer die mit 22 endet:

$$\begin{aligned} X - 134,03 &= 22 \\ \equiv 156,03 &= X. \end{aligned}$$

Daraus folgt, dass X etwa 156,03 dBm stark sein sollte.

**ii) Matrikelnummer mit 30 am Ende**

Rechnung für die Matrikelnummer die mit 22 endet:

$$\begin{aligned} X - 134,03 &= 30 \\ \equiv 164,03 &= X. \end{aligned}$$

Daraus folgt, dass X etwa 164,03 dBm stark sein sollte.

**b)**

„Nehmen Sie an, dass das Signal mit 100 dBm gesendet wird. Der Empfänger soll nach allen Verlusten/Verstärkungen ein 60 dB Signal erhalten. Wie muss die Frequenz geändert werden, damit dieses Ziel erreicht wird?“

Wie in Abilldung 7 auf Seite 10 deutlich wird "gewinnt" das Signal von Punkt B bis hin zur fertigen Verarbeitungen 42 dBm. Das heißt, nachdem das Signal bei B ankommt, kommen noch 6 dBi Gewinn durch die Antenne hinzu und 42 dB durch den Verstärker. Sei 100 dBm die Stärke des ausgestrahlten Signals bei Punkt A. Gesucht ist f.

Es soll gelten:

$$100 - 20 * \log_{10}(120000 * f * \frac{4\pi}{299792458}) + 6 + 36 = 60$$

$$\equiv -20 * \log_{10}(120000 * f * \frac{4\pi}{299792458}) = -82$$

$$\equiv \log_{10}(120000 * f * \frac{4\pi}{299792458}) = 4,1$$

$$\equiv \frac{\ln\left(\frac{480000\pi * f}{299792458}\right)}{\ln(10)} = 4,1$$

$$\equiv \ln\left(\frac{480000\pi * f}{299792458}\right) = 4,1 * \ln(10)$$

$$\equiv \ln\left(\frac{480000\pi * f}{299792458}\right) = 4,1 * \ln(10) = \ln(10^{4,1})$$

$$\equiv \frac{480000\pi * f}{299792458} = 10^{4,1}$$

$$\equiv f = \frac{10^{4,1} * 299792458}{480000\pi}$$

$$\equiv f = \frac{10^{4,1} * 149896229}{240000\pi} \approx 2502819,86$$

Check:

$$100 \text{ dBM} - 20 * \log_{10}\left(120000 * \frac{10^{4,1} * 149896229}{240000\pi} * \frac{4\pi}{299792458}\right) \text{ dBM} + 6 \text{ dBM} + 36 \text{ dBM} = 60 \text{ dBM}$$

Check erfolgreich. Das heißt, es muss mit der Frequenz von etwa 2502819,86 Hz, beziehungsweise 2,5 MHz gesendet werden.

**c)**

„Das Signal wird nun wieder mit einer Frequenz von 1 GHz gesendet. Wie muss sich die Entfernung von Sender/Empfänger ändern, sodass der Empfänger nach allen Verlusten/Verstärkungen ein Signal mit Leistungspegel 60 dB erhält? Nehmen Sie dafür erneut an, dass das Signal mit 100 dB gesendet wurde.“

Gesucht ist r. Es soll gelten:

$$100 - 20 * \log_{10}\left(r * 10^9 * \frac{4\pi}{299792458}\right) + 6 + 36 = 60$$

$$\equiv \log_{10}\left(r * 10^9 * \frac{4\pi}{299792458}\right) = 4,1$$

$$\begin{aligned}
& \equiv \frac{\ln\left(\frac{2 * 10^9 \pi * r}{149896229}\right)}{\ln(10)} = 4,1 \\
& \equiv \ln\left(\frac{2 * 10^9 \pi * r}{149896229}\right) = 4,1 * \ln(10) \\
& \equiv \ln\left(\frac{2 * 10^9 \pi * r}{149896229}\right) = \ln(10^{4,1}) \\
& \equiv \frac{2 * 10^9 \pi * r}{149896229} = 10^{4,1} \\
& \equiv r = 10^{4,1} * \frac{149896229}{2 * 10^9 \pi} \\
& = \frac{149896229}{2 * 10^{4,9} \pi} \approx 300,34
\end{aligned}$$

Check:

$$100 \text{ dB} - 20 * \log_{10}\left(\frac{149896229}{2 * 10^{4,9} \pi} * 10^9 * \frac{4\pi}{299792458}\right) \text{ dB} + 6 \text{ dB} + 36 \text{ dB} = 60 \text{ dB}$$

Check erfolgreich. Das heißt, die Distanz muss etwa 300,34 m betragen.

**d)**

„In der Vorlesung haben Sie zwei Approximierungen gelernt, wie man Dezibel Werte ohne Logarithmus berechnen kann.

$$\begin{aligned}
3 \text{ dB} & \mapsto 2 : 1 \\
10 \text{ dB} & \mapsto 10 : 1
\end{aligned}$$

Berechnen Sie die approximierten Absolutbeträge von 113 dB jeweils mit einer der beiden Approximationen und vergleichen Sie diese mit dem korrekten Wert. Sind die Approximationen gut? Begründen Sie Ihre Antwort. Können Sie mit einer Kombination aus beiden Approximationen einen besseren Wert erreichen?“

Bekannt ist aus *zsmfssg\_U1.pdf*:

$$10 * \log_{10}(Faktor) = dB$$

Benutzt man <http://www.sengpielaudio.com/Rechner-FaktorVerhaeltnisPegelDezibel.htm> ergibt sich der richtige Faktor mit 199526231496.8883 was sich übrigens mit  $10^{11.3}$  berechnen lässt.

### **Methode 1**

$$113 = 37 * 3 + 2 \rightarrow 2^{37}$$

Der Rest ist somit 2.

Kontrolle:

$$10 * \log_{10}(2^{37}) = 111.38 \text{ dB}$$

Je kleiner der Differenzbetrag mit dem richtigen Faktor, desto besser:

$$10^{11.3} - 2^{37} \approx 62087278025$$

### **Methode 2**

$$113 = 11 * 10 + 3 \rightarrow 10^{11}$$

Der Rest ist somit 3.

Kontrolle:

$$10 * \log_{10}(10^{11}) = 110 \text{ dB}$$

Je kleiner der Differenzbetrag mit dem richtigen Faktor, desto besser:

$$10^{11.3} - 10^{11} \approx 99526231497$$

### **Kombination aus beiden Approximationen**

$$113 = 11 * 10 + 1 * 3 \rightarrow 10^{11} * 2^1 = 2 * 10^{11}$$

Der Rest ist somit 0.

Kontrolle:

$$10 * \log_{10}(2 * 10^{11}) \approx 113.01 \text{ dB}$$

Je kleiner der Differenzbetrag mit dem richtigen Faktor, desto besser:

$$| 10^{11.3} - 2 * 10^{11} | \approx 473768503$$

Wie in Abildung 8 auf Seite 15 klar wird, ist hier die Kombination am besten, gefolgt von Methodik 1. Methodik 2 ist in diesem Fall am schlechtesten. Wenn man als Kriterium nimmt, dass Methodiken 1 und 2 auf den richtigen ganzen dB Wert kommen, dann sind es keine guten Approximationen. Wenn relativ genaue Werte benötigt werden, eignen sich diese nicht, aber sie können hilfreich sein um grob abzuschätzen. Wie gesagt ist die Kombination am besten, wo auch der Rest mit 0 am kleinsten war. Methodik 1 hatte den zweit kleinsten Rest mit 2, gefolgt von Methodik 2 mit Rest 3, was mathematisch gesehen kein Zufall war.

	dB	Differenzbeträge
Methodik 1	111.38	62087278025
Methodik 2	110.00	99526231497
Kombination	113.01	473768503

Abbildung 8: Vergleich

## Reading assignment

a)

Im Paper heisst es „In order to combat jamming attacks, existing wireless systems typically consider the employment of spread spectrum techniques, including DSSS [55], [56] and FHSS solutions [57]. To be specific, DSSS employs a PN sequence to spread the spectrum of the original signal to a wide frequency bandwidth“.

Das heisst, dass sogenannte Frequenzspreizung benutzt werden. DSSS benutzt dafür pseudo noise um das original Signal auf eine weite Frequenzbandbreite zu spreizen. Somit wird der Aufwand für einen Angreifer deutlich erhöht.

b)

Im Paper wird erwähnt „For instance, in Fig. 5, we feature two types of industrial standards for WMAN, namely WiMAX and LTE“.

WiMAX und LTE werden somit erwähnt. Das anfängliche WiMAX, IEEE 802.16, hatte laut den Autoren eine maximale Übertragungsrate von 40 Mb/s. Später, so steht es im Paper, bekam es ein Upgrade, und wurde zu IEEE 802.16m mit den Übertragungsraten von bis zu 1 Gb/s bei stationärem Empfang und 100 Mb/s bei mobilem Empfang. Im Buch „Mobile WiMAX: A Systems Approach to Understanding IEEE 802.16m Radio Access Technology“ (Amazon Link) vom Stanford Dozenten Sassan Ahmadi, steht auf Seite 539, dass IEEE 802.16m vom Format 0 eine maximale Abdeckung von 18 km habe. IEEE 802.16m vom Format 1 komme sogar auf 100km.

LTE erreicht laut dieser Quelle (hier klicken) bis zu 2998,6 Mb/s im Brutto Downlink und bis zu 1497,8 Mb/s im Brutto Uplink als Release 10 der sogenannten 3GPP-Norm. Diese Quelle (hier klicken) behauptet eine „LTE-Basisstation, die mit 800 MHz sendet, besitzt einen Funkzellenradius von bis zu 10 km“.