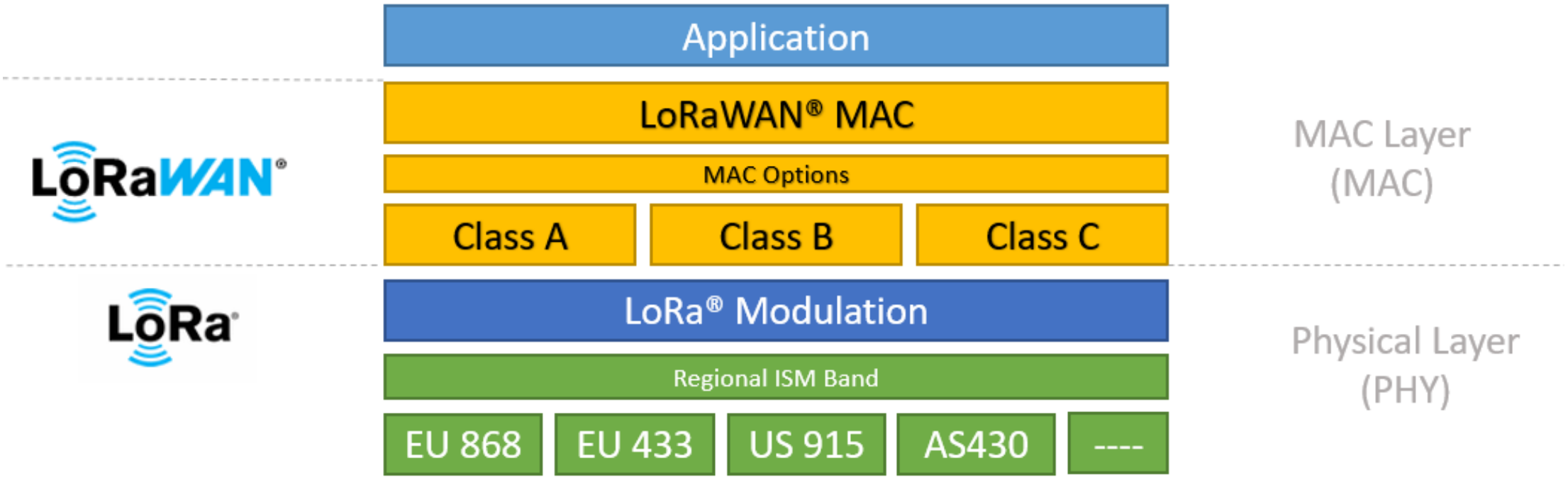
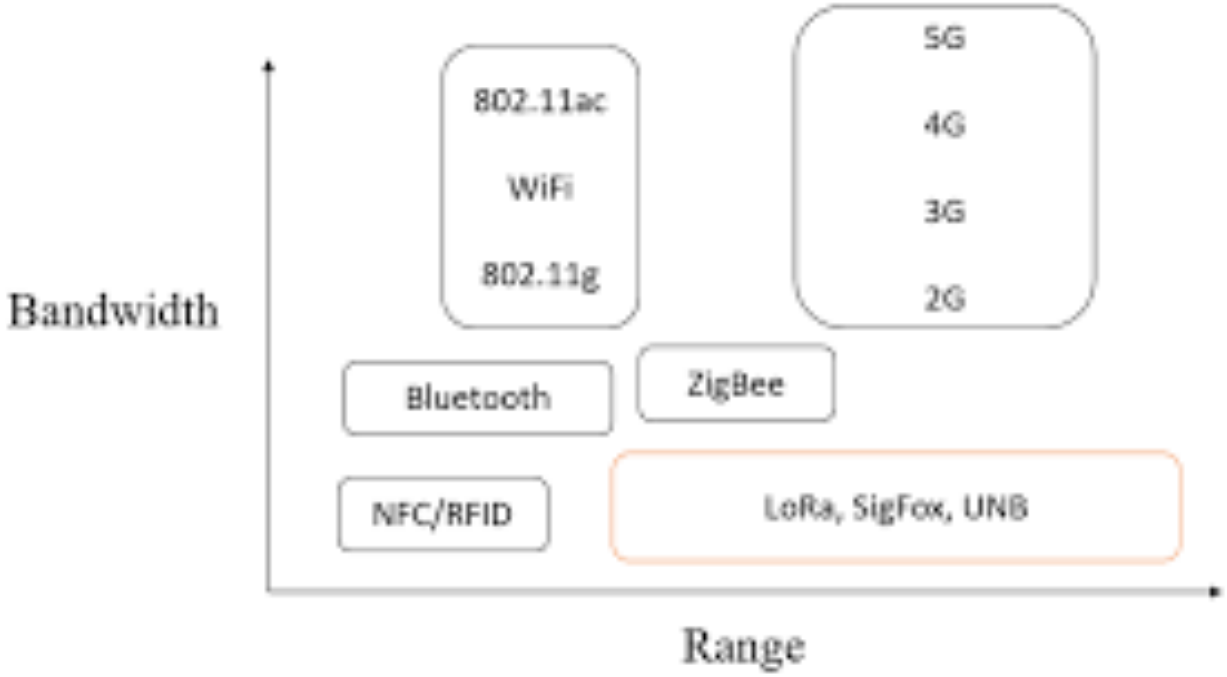
IoT Internet of Things

Hartmut Seitter

Today I would like to cover LoRa and LoRaWAN from a technical point of view
What is the difference between LoRa and LoraWAN

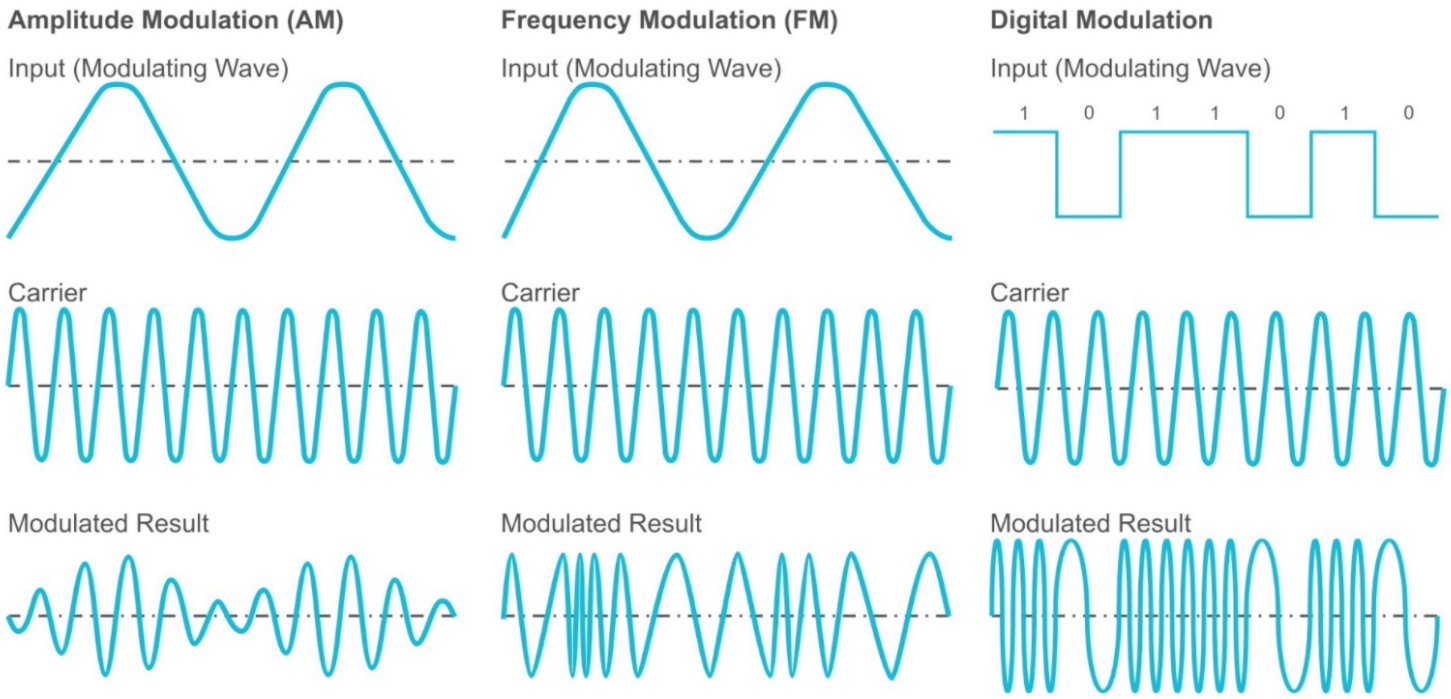


LoRa is complementary to existing IoT communication technologies

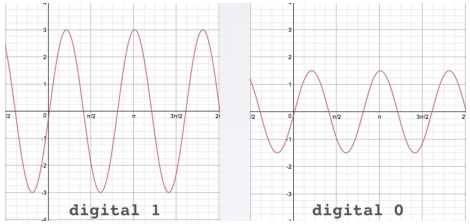


https://www.researchgate.net/figure/Bandwidth-vs-Range-of-wireless-technology-4_fig1_329657897

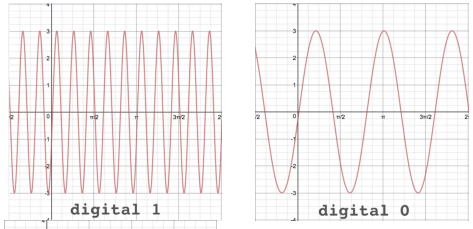
Radio waves transmit data on air – we use different modulation types to use a carrier to transmit data



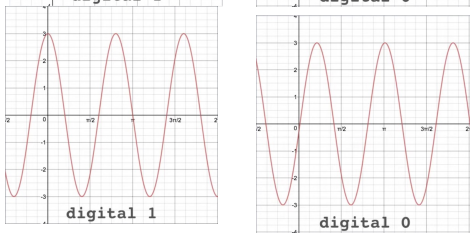
Modulation types samples to send and receive a digital 0 and digital 1



AM Modulation – Only the amplitude changes.
very susceptible to noise and interference

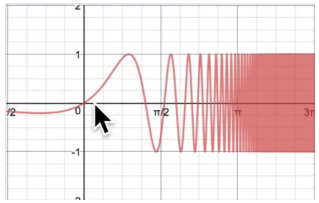


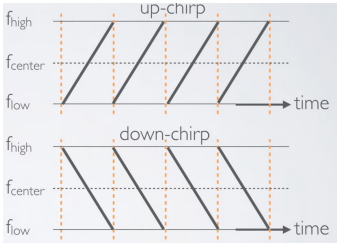
FSK Modulation – Only the frequency changes.
More robust against nois and interference



PSK Modulation – Only the phase of the signal changes.
More robust against noise and interference

Many other modulation types exist

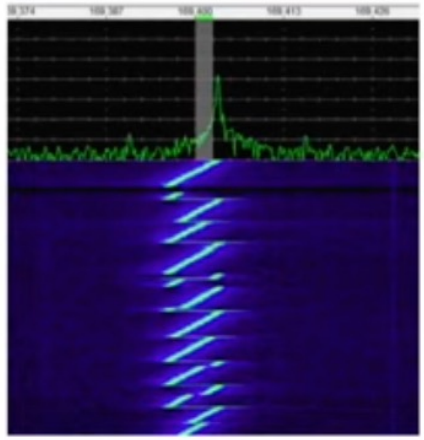




Chirp Spread Spectrum (CSS) modulation
The frequency is increased (up chirp) or decreased (down chirp) in time

Radio modulation and LoRa

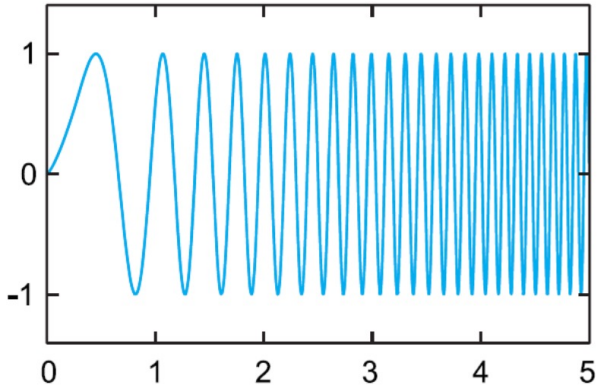
- **LoRa uses a chirp spread spectrum modulation**
  - **This means there is a bandwidth in which the symbols are modulated**
  - **There is a center frequence and around it the symbols are modulated with a high bandwidths (typically 125kHz)**
  - **The spread wave form makes it robust against interference**



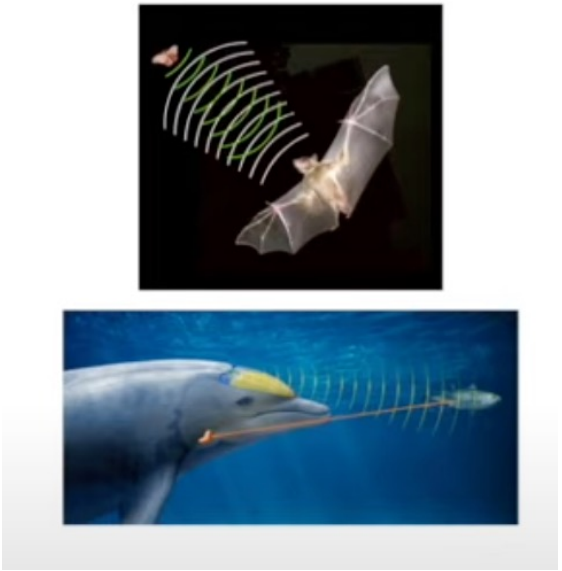
LoRa spectrogram

LoRa Modulation

In LoRa modulation, the spreading of the signal's spectrum is achieved by generating a chirp signal that continuously varies in frequency,

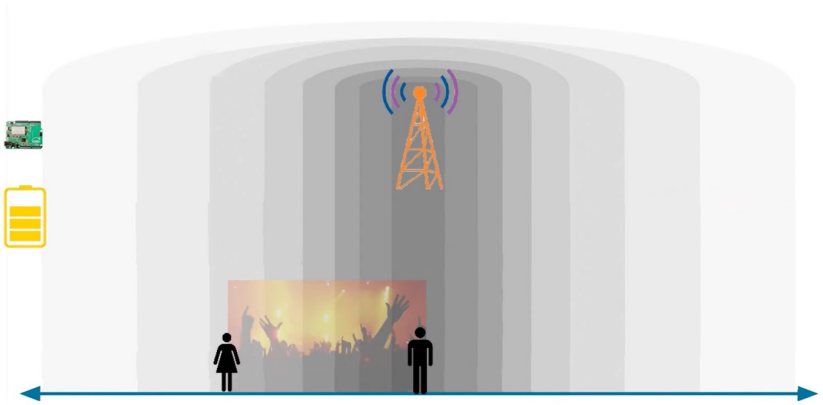


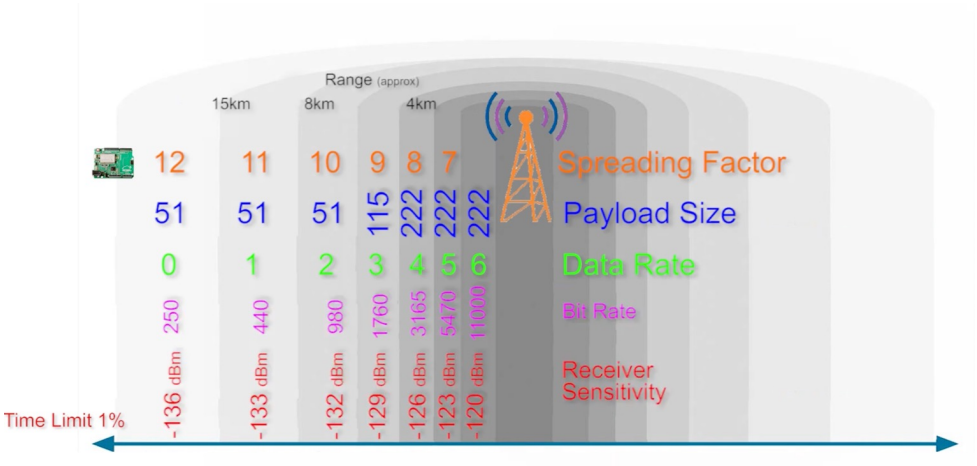
By increasing the chip rate, we increase the frequency components of the total signal spectrum. In other words, the energy of the total signal is now spread over a wider range of frequencies.



LoRa is not the only one who uses chirp modulation ☺

A





When the sender and receiver location increased the received signal becomes at a certain distance unusable

The sending power can be increased (think on battery energy

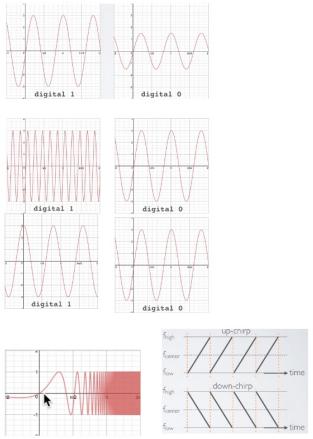
Analogy to human communication
Noise is added to the speech signal
I can speak louder and/or I can speak more slowly and more clearly so that the speech (signal) can be reach wider distance

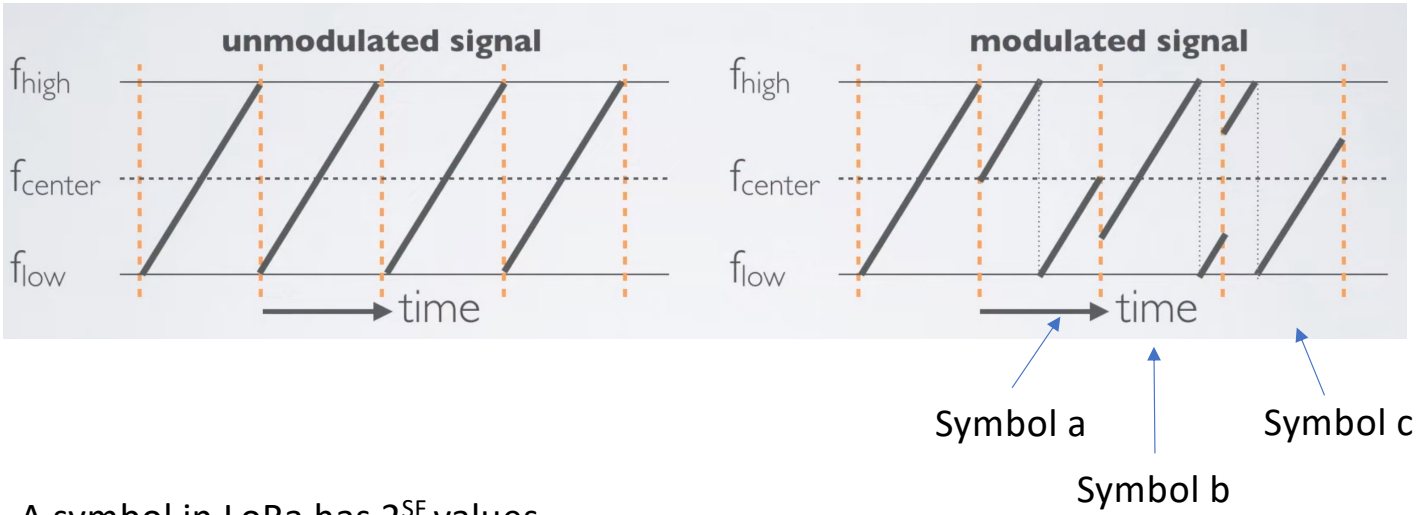
On the electronic part

LoRa uses the spreading factor (communicate more slowly and clearly) to reach wider distance between sender and receiver

Which will have effects on the payload to be transmitted
The data and bit rate

LoRa Modulation - Spreading Factor, Chirp and Chips

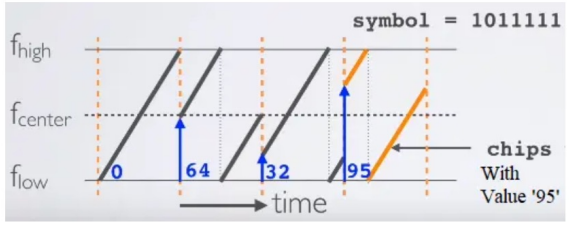




A symbol in LoRa has 2^{SF} values.

SF of 7 has 127 values
SF of 12 has 4096 values

e.g. Using SF 7 the value of 95 dec.
Is represented by this chip



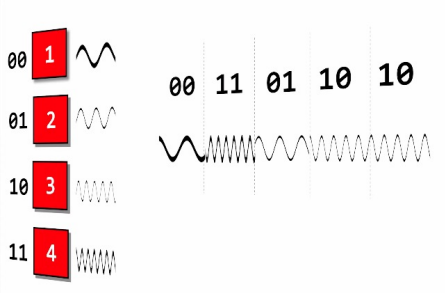
LoRa is a more or less a “frequency shift chirp modulation”

- **LoRa uses S = 0,1,2,…. 2^{SF} -1 Symbols and SF is the Spreading Factor (7….12)**
  - **With a SF of 7 we can send 128 Symbols**

$$c(nT_s + kT) = \frac{1}{\sqrt{2^{SF}}} e^{j2\pi\left((s(nT_s))+k) \mod 2^{SF}\right)\frac{k}{2^{SF}}}$$

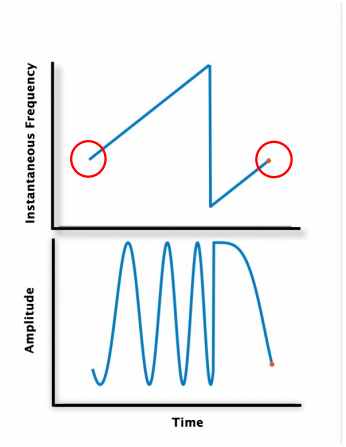
That’s the formular the chip wave form.
For each symbol we get another wave form

FSK – very easy and straight forward



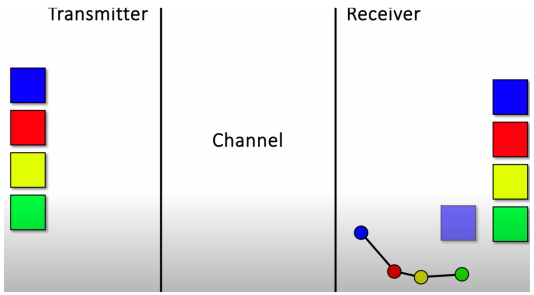
Example: Symbol 33 on SF of 7

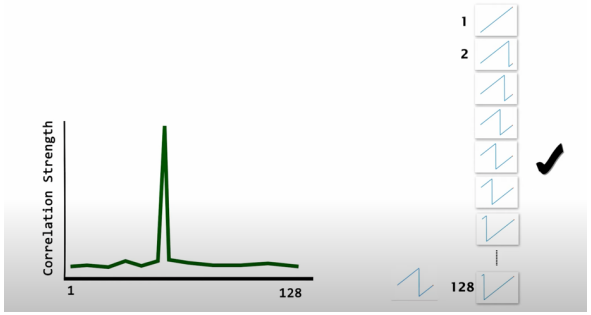
Interesting – the end frequency is the same as the starting frequency



LoRa sends different symbols (values) in a chirp – how to demodulate it?

Correlation might be a possibility





example

The sender sends symbols in these for colors
The receiver uses correlation to identify the colors

Using SF 7 there are 128 possible symbols and the Receiver is doing a similarity check to get the symbols

Sounds simple but in reality there are some hurtles
e.g. synchronisation, correlation calculation is 'expensive'

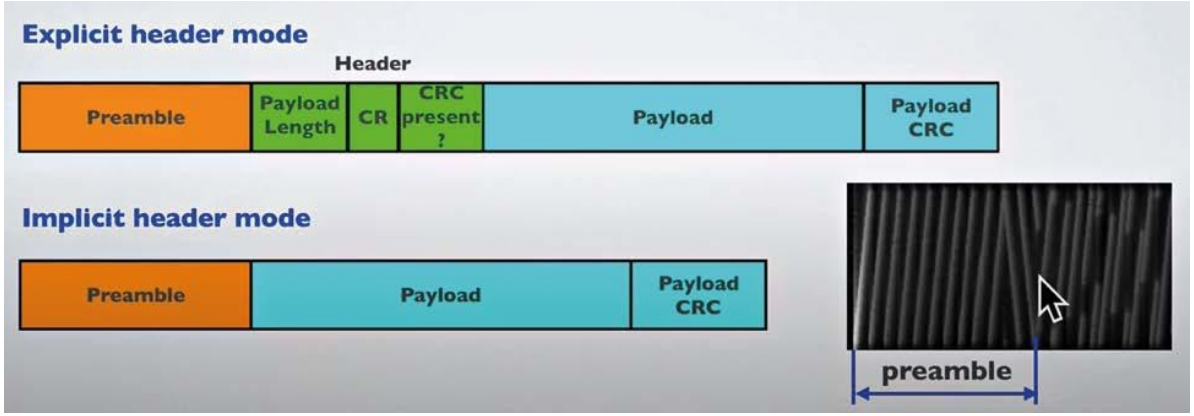
Dechirping and FFT is used to make it simpler and less 'expensive'
up and down chirps are used which simplify the mathematical formular and makes it simpler to recover the symbol received

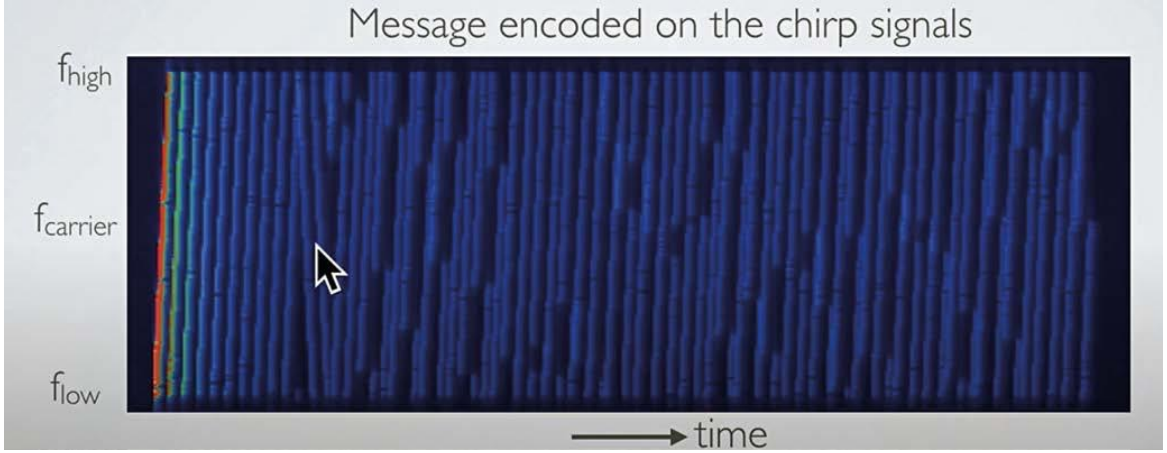
When the received symbol is multiplied with a downchirp ref. signal we get a pure frequency signal which can be passed to FFT

LoRa Sender and Receiver Message synchronisation

For decoding the symbols correctly it's important that sender and receiver are in synch, so that the receiver knows when a chirp starts and ends.

This is done by the preamble
Sender sends 8 up-chirps flowed by 2 down-chirps
And then the first symbol follows





Data Rate, Chip Rate, Symbol Rate and duration

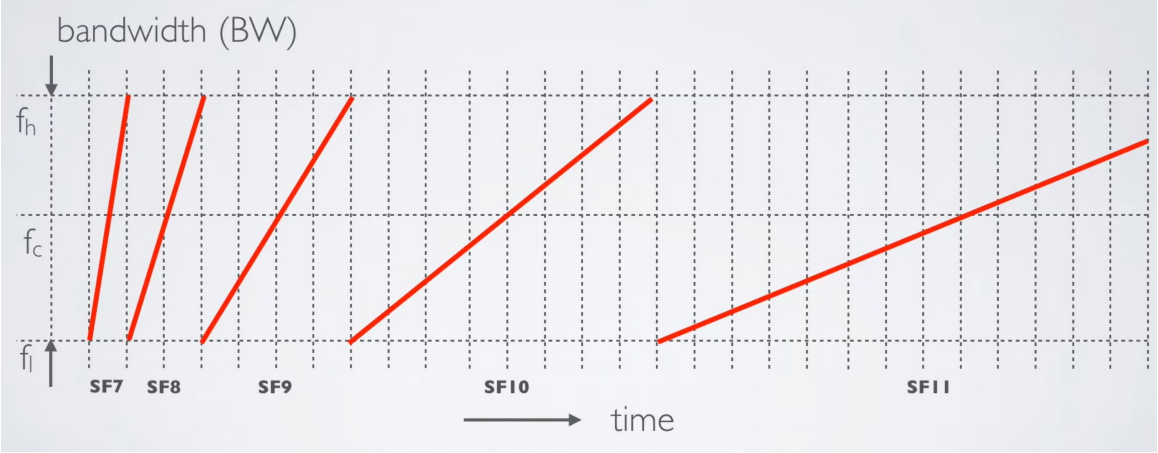
- **Bandwidth and Chip rate is the same**
  - **In LoRa we have different Bandwidth e.g. 125kHz, 250kHz, 500kHz**
  - **This means on 125kHz we can send 125000 chips/sec**

- **Symbol Rate = Rs = Symbols per Second**
  - **Rs = Bandwidth / 2^{SF}**
  - **Rs = 125000 / 2^7 = 977 symbols/sec**
  - **Rs = 125000 / 2^{12} = 30 symbols/sec**

- **Symbol duration**
  - **Ts = 2^{SF}/BW**
  - **Ts = 2^7/125000 = 1.024ms**
  - **Ts = 2^{12}/125000 = 32.7ms**

$$\mathrm{SNR} = \frac{P_{\mathrm{signal}}}{P_{\mathrm{noise}}},$$

Be aware:
There are other characteristics which influence the symbol rate such as error correction values etc.



SNR – Signal Noise Ratio

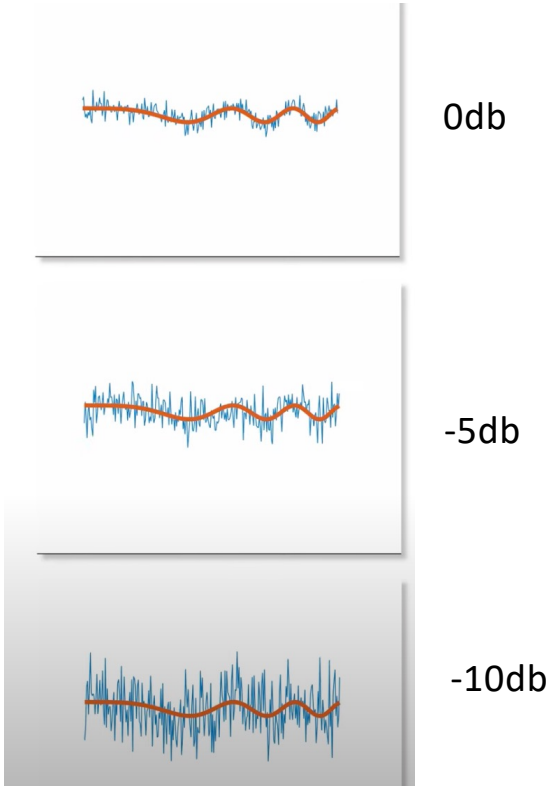
- **The SNR is defined as the ratio between the signal power to the noise power**

$$\mathrm{SNR} = \frac{P_{\mathrm{signal}}}{P_{\mathrm{noise}}},$$

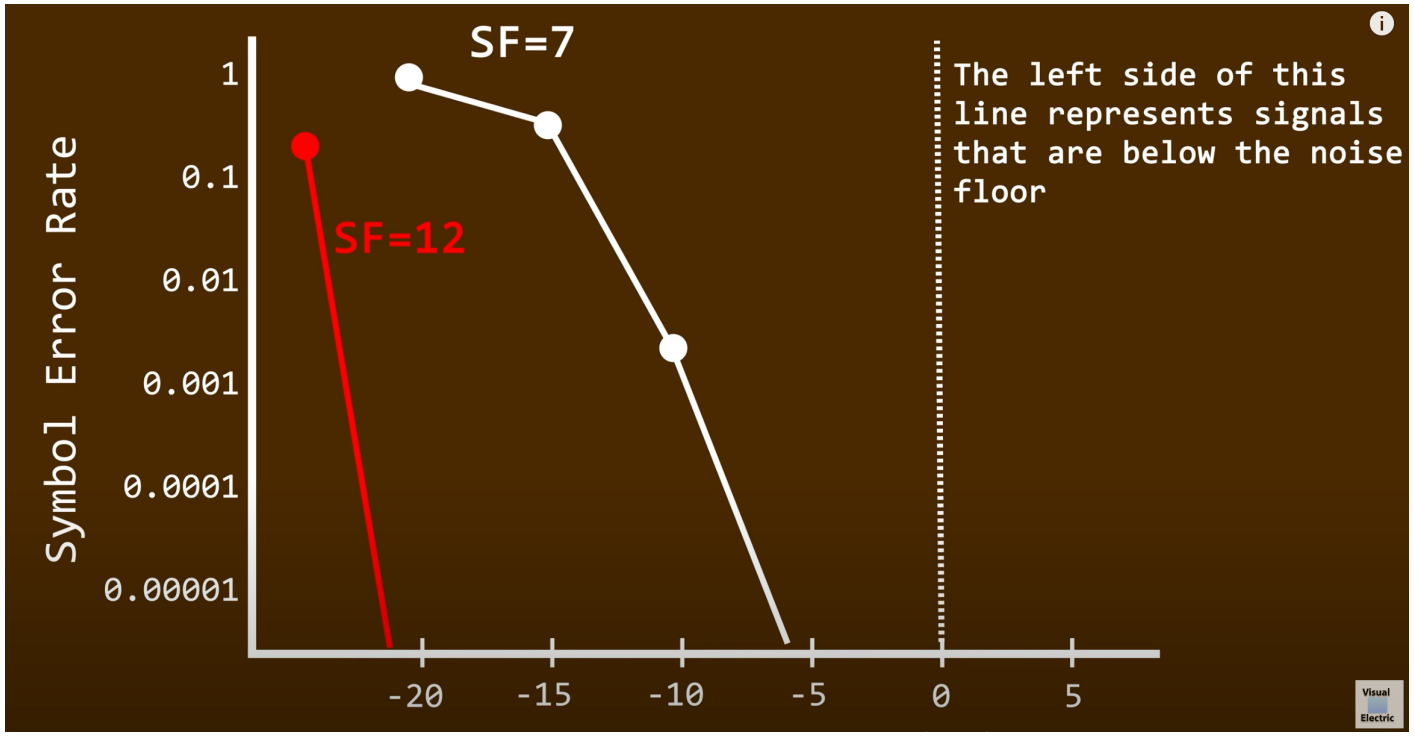
SNR limits over the SF

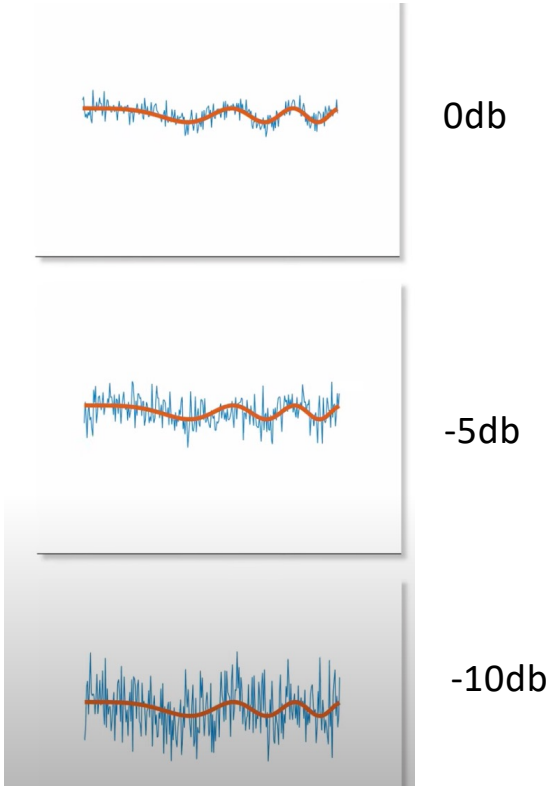
Spreading Factor	chips/symbol	SNR limit (dB) [2]
7	128	-7.5
8	256	-10
9	512	-12.5
10	1024	-15
11	2048	-17.5
12	4096	-20

Rauschsignal ist um den Faktor 10 höher als das Nutzsignal



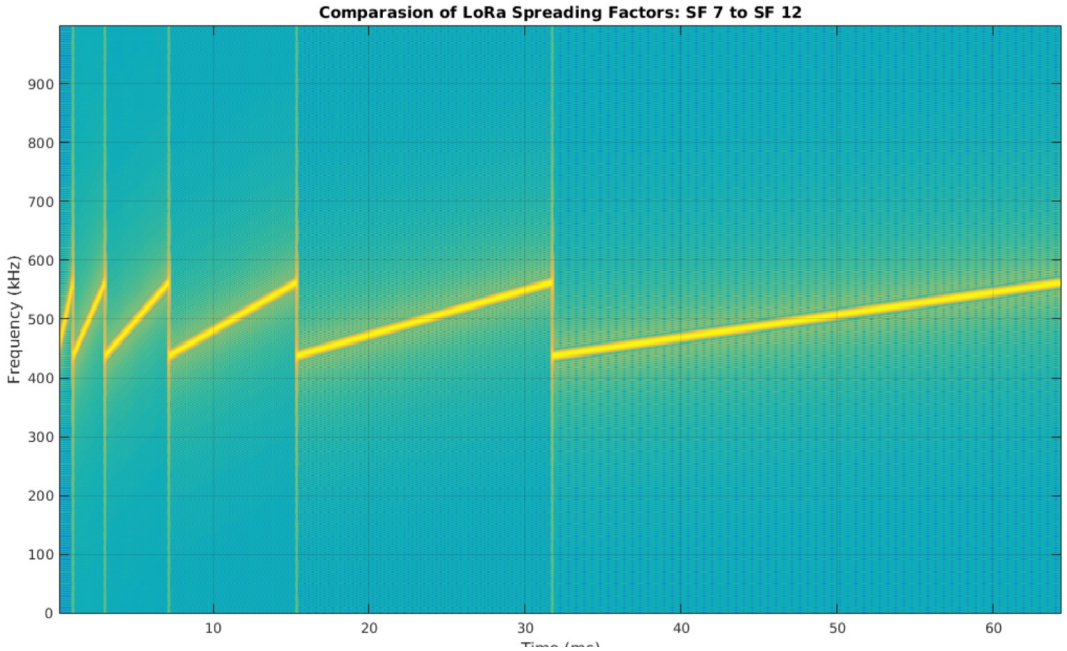
Signal to noise ratio in db





LoRa – Spreading Factor SF

- A spreading factor is an important aspect for the LoRa modulation.
- **It represents the rate on which the signal changes frequency.**
  - The spreading factor is expressed as a number ranging from 7–12, representing the speed of a frequency change in a chirp.
  - Higher numbers mean that the chirp lasts longer meaning that sweep across the bandwidth lasts longer.



LoRa Modulation

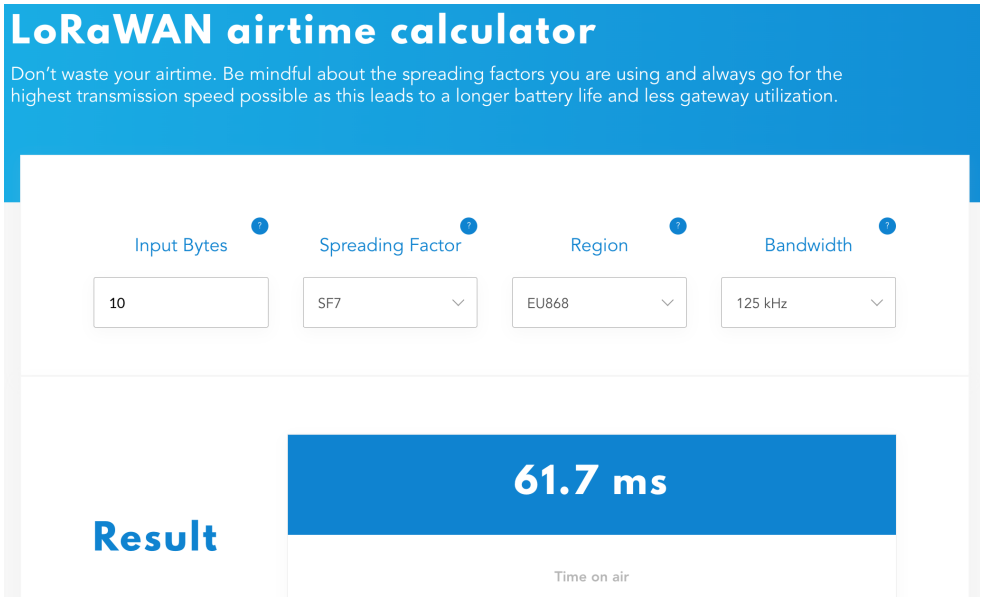
- In LoRa terms, the amount of spreading code applied to the original data signal is called the *spreading factor* (SF). LoRa modulation has a total of six spreading factors (SF7 to SF12).

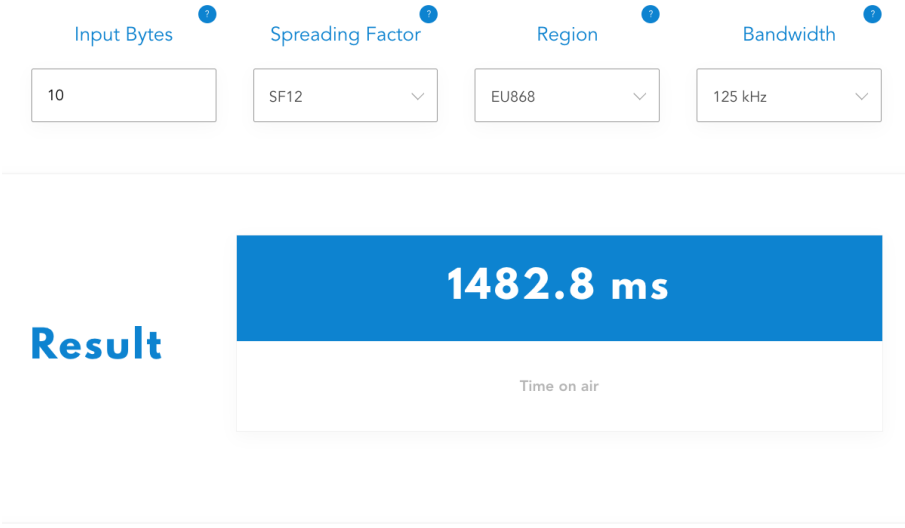
Spreading Factor (For UL at 125 KHz)	Bit Rate	Range (Depends on Terrain)	Time on Air for an 11-byte payload
SF10	980 bps	8 km	371 ms
SF9	1760 bps	6 km	185 ms
SF8	3125 bps	4 km	103 ms
SF7	5470 bps	2 km	61 ms

Lower SF
↓
Shorter range
↓
Less time on air
↓
Lower energy consumption
↓
Higher data rate

Data Rate (DR)	Spreading Factor (SF)	Channel Frequency	Uplink or Downlink	Bitrate (Bits/Sec)	Maximum User Payload Size (Bytes)
0	SF10	125 kHz	Uplink	980	11
1	SF9	125 kHz	Uplink	1,760	53
2	SF8	125 kHz	Uplink	3,125	125
3	SF7	125 kHz	Uplink	5,470	242
4	SF8	500 kHz	Uplink	12,500	242
5 – 7					
8	SF12	500 kHz	Downlink	980	53
9	SF11	500 kHz	Downlink	1,760	129
10	SF10	500 kHz	Downlink	3,125	242
11	SF9	500 kHz	Downlink	5,470	242
12	SF8	500 kHz	Downlink	12,500	242
13	SF8	500 kHz	Downlink	21,900	242

Don’t waste any airtime!





Mode	Bitrate (bits/sec)	Max payload size (bytes)
SF7/125kHz	5470	222
SF8/125kHz	3125	222
SF9/125kHz	1760	115
SF10/125kHz	980	51
SF11/125kHz	440	51
SF12/125kHz	250	51
SF7/250kHz	11000	222

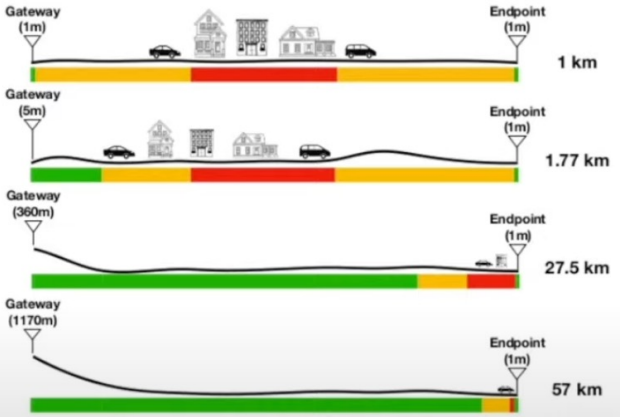
https://www.thethingsnetwork.org/airtime-calculator

LoRa Range – theoretical and empirical maximum – and range considerations

- The theoretical maximum in free space **~ 850 km**
- The world record set by **The Things Network Community** during **The Things Virtual Conference 2020** using a helium balloon: **832 km**

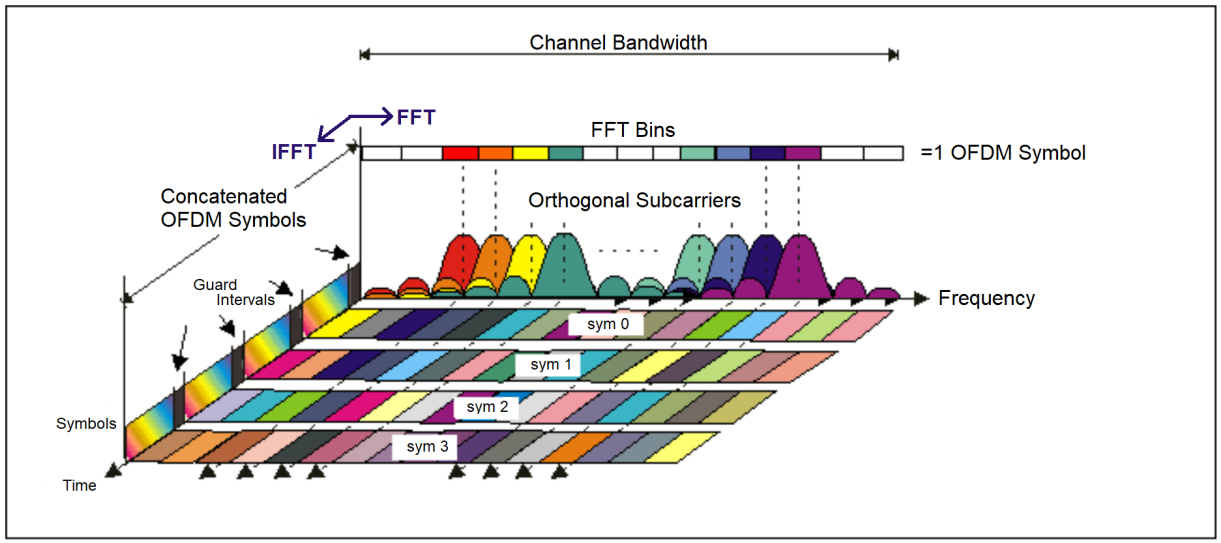
Image sources: "LoRa World Record broken: 832km/517mi using 25mW" article by The Things Network (www.thethingsnetwork.org), "The Things Network sets new LoRaWAN transmission record" by Gareth Halfacree (abopen.com)

- Range depends on whether there is a line of sight, and whether the gateway is located indoor or outdoor
  - indoor **~ 500 m**
  - outdoor, on top of a house roof **~ 2 km**
  - outdoor, on top of a high-altitude building **> 10 km**
- Gateway elevation example



5G uses OFDM modulation (more complex than LoRa but higher data rates)

- Orthogonal Frequency Division Multiplexing (OFDM) is an efficient modulation format used in modern wireless communication systems including 5G. OFDM combines the benefits of Quadrature Amplitude Modulation (QAM) and Frequency Division Multiplexing (FDM) to produce a high-data-rate communication system.



Frequency-Time Representative of an OFDM signal

Modulation schemes for 5G IoT

•**Quadrature Amplitude Modulation (QAM)**: This is the foundational modulation technique for both 4G and 5G, which encodes data by changing both the amplitude and phase of the carrier signal.

•**Low-order QAM variants**: For 5G IoT, protocols like LTE-M use lower-order QAM variants (QPSK, 16-QAM, 64-QAM) instead of higher-order ones used for high-speed mobile data.

Bidirectional communication

- Simple demodulation process → end-devices can perform it too!
- LoRa devices and gateways → "modulator-demodulator" modules
  - uplinks
  - downlinks

Image source: "All about LoRa and LoRaWAN" (www.sghoslya.com)

One difference of LoRa Gateways is the fact that they can support multiple channel on the same time

An end device can do one at a time

Device classes

Class A

implemented by all end devices

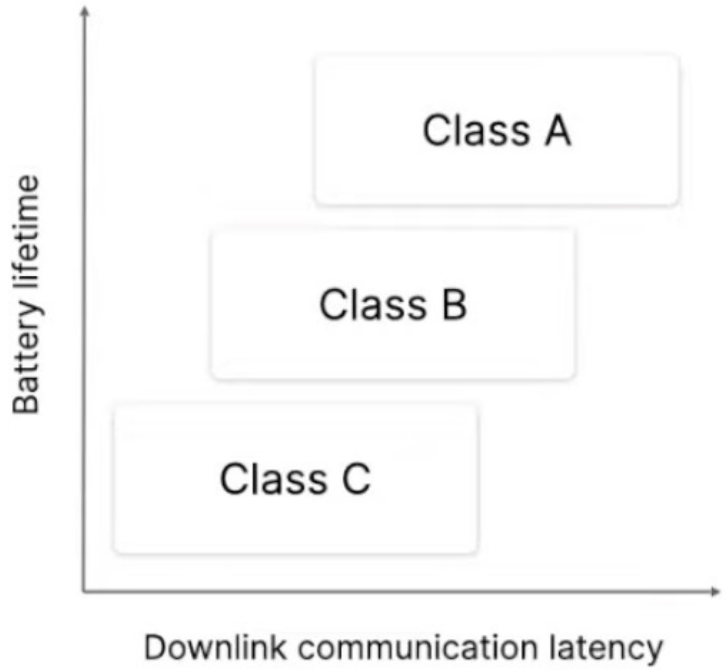
end device initiates transmission

Class B

transmission initiated by the end device or on fixed interval by network

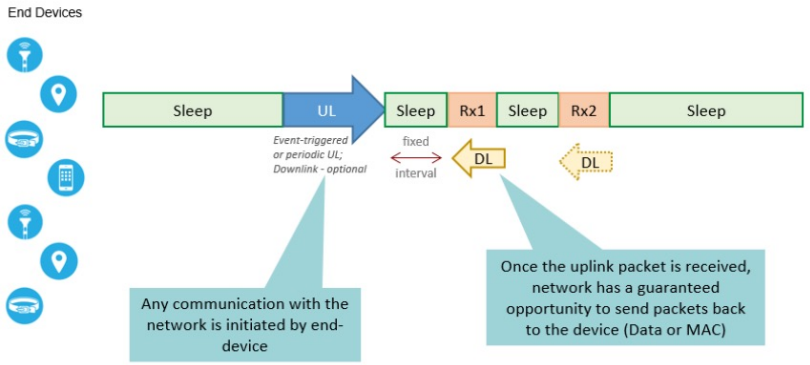
Class C

transmission initiated by the network at any time

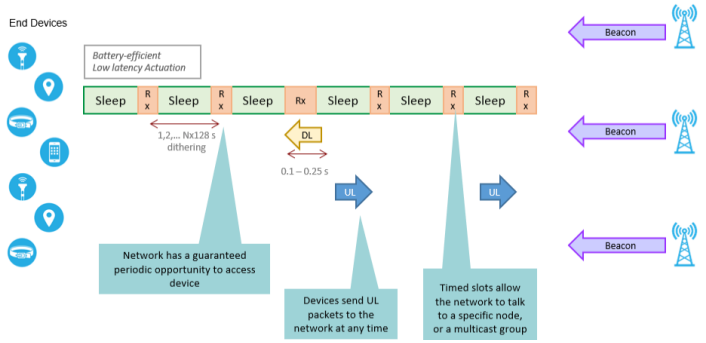


Device classes

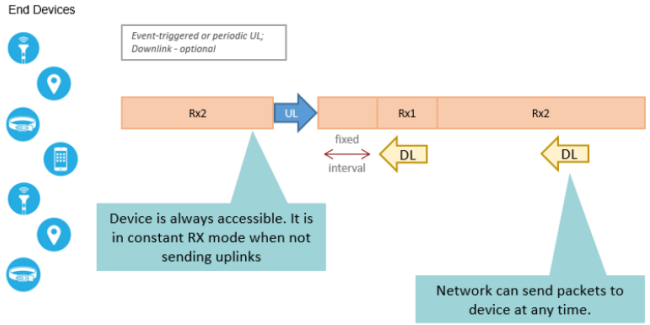
Class A device
Implemented by all devices
End device initiate transmission



Class B device
Transmission initiated by the end device or on fixed time interval by network



Class C device
Transmission initiated by the end device and the network any time
(they are always on!)



https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/

Limitation on LoRaWAN

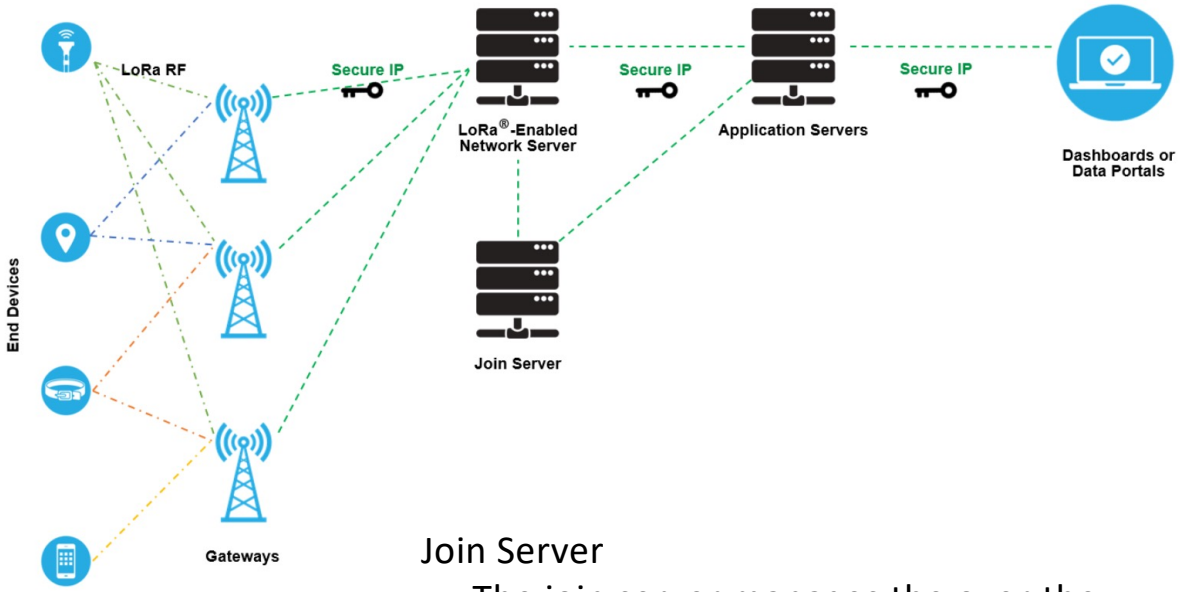
- **Limited payload – 51 bytes to 241 bytes depending on the data rate**
- **Low data rates – max 5,5kbps on 125kHz bandwidth**

- **Don’t send any text or json messages – use a simple encoder and decoder to send binary values**

- **Async. communication – more uplink than downlink capacity**

Let's cover the security aspect of IoT on the LoRaWAN security concept

LoRaWAN Network Elements



Join Server
- The join server manages the over-the-air activation process for end devices to be added to the network.

End Device
- Sensor or actuator which is wireless connect to a LoRaWAN network through gateways using LoRa modulation

Gateways
- Receives RF modulated msgs and forwards these data to network server

Network server
- Device address checking
- Frame authentication and frame counter mgnt
- ……

Application Servers
- Application servers are responsible for securely handling, managing and interpreting sensor application data.

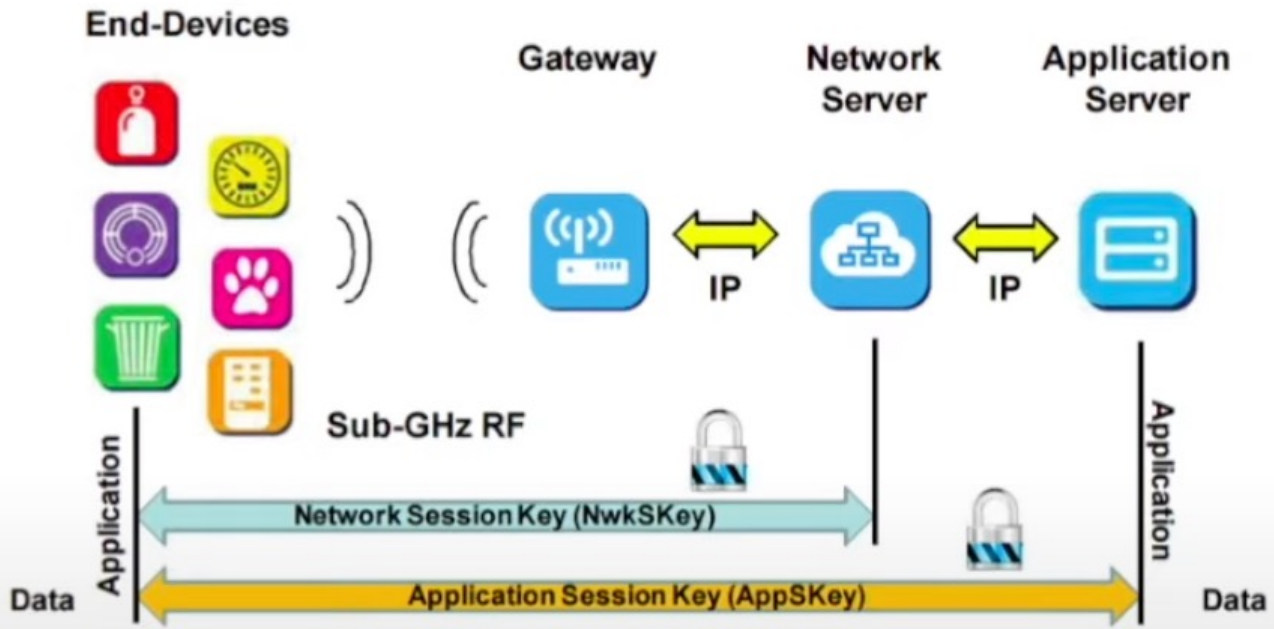
Normally there are three pillars of security

- **Authenticity**
  - **We know with which device we are communicating -> it is authenticated**
- **Integrity**
  - **The data which is exchanged is not tampered with**
- **Confidentiality**
  - **The data self is encrypted and the network cannot see what the data is, only the application layer**

LoRaWAN two layer security

Two-layer security with AES encryption algorithm:

- 128-bit NwkSKey
- 128-bit AppSKey



The Network session key is for the integrity and authenticity
The Application session key is for the confidentiality

IoT security – example LoRaWAN security concept

- **LoRaWAN session**
  - **We have a Network session – end device and Network server**
    - **device address,**
    - **Network session key,**
    - **Frame counters,**
    - **MAC state (which channel, data rates, etc)**
  - **We have an Application session – maintained by the end device and the application server**
    - **Application session key**
    - **Frame counters**

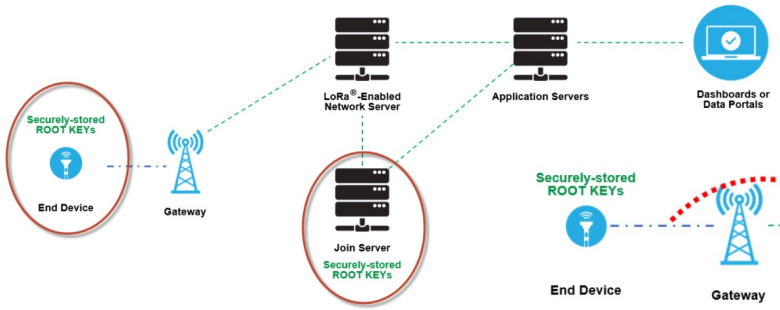
  During a LoRaWAN session the session keys don’t change, frame counters are increased and never reused

IoT security – example LoRaWAN security concept

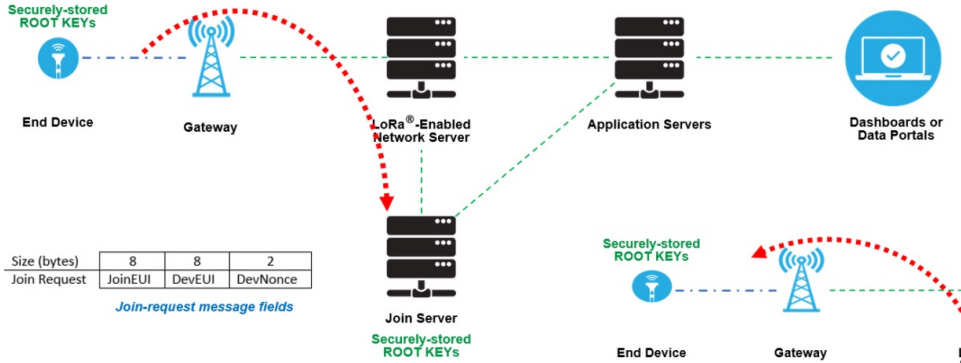
https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/

The Join Procedure

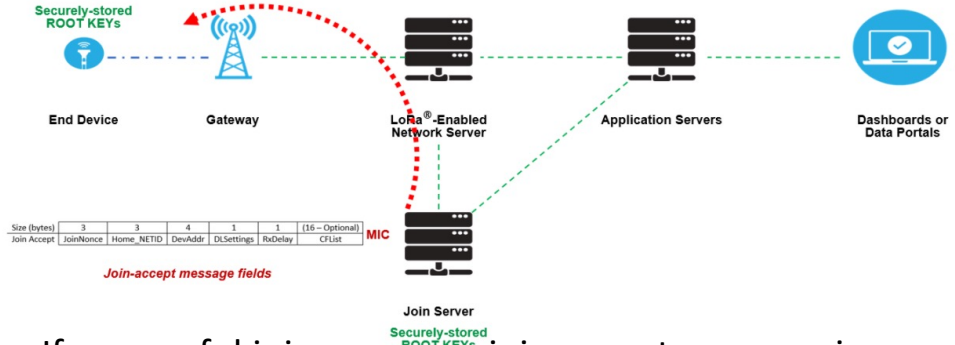
We will begin with the security keys, as illustrated in Figure 15. Individual root keys are securely stored on the end devices, and matching keys are securely stored on the join server.



The root keys are securely stored on the end device and the join server

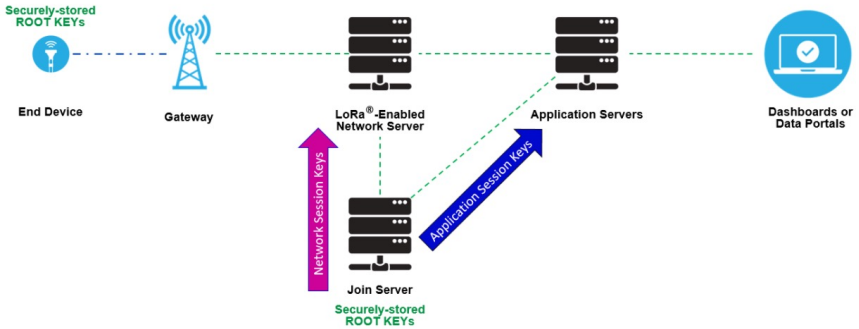


End device sends a join request msg with the JoinEUI and DevEUI fields

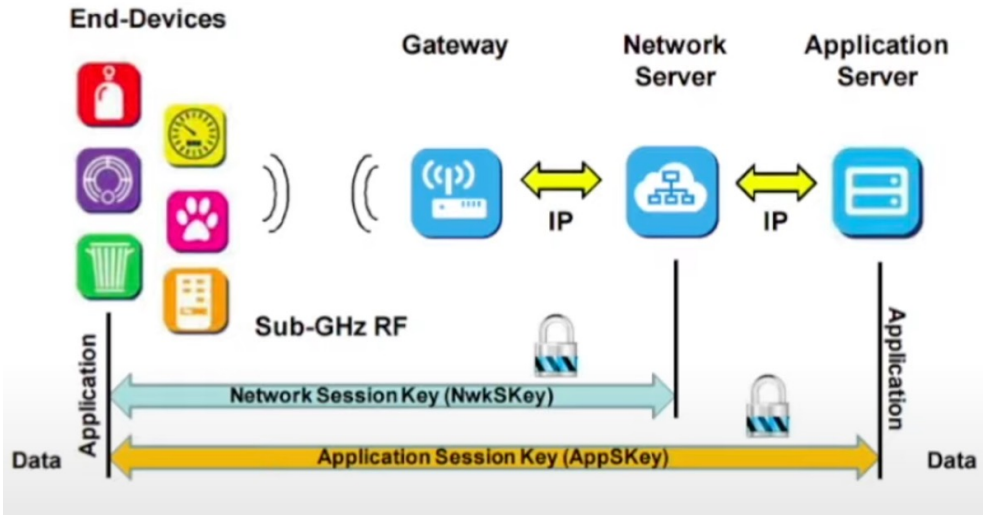


If successful join reques, a join accept message is sent to the device

IoT security – example LoRaWAN security concept



The end device and join server derives the session key based on the keys exchanged and the join server share these keys with the network server and application server



The control traffic between the end device and network server is secured by the network session key and the traffic between the end device and the application server is secured by the application session key

LoRaWAN keys

Table 4: LoRaWAN Specification 1.1.x Unique ID and Security EUI Requirements

EUI	Size in Bytes	Protected (secure) Memory	Required to restore Session Context
JoinEUI	8		
DevEUI	8		
DevAddr	4		
NetID	3	YES*	
AppKey	16	YES*	
NwkKey	16	YES*	
NwkSEncKey	16	YES*	YES
NwkSIntKey	16	YES*	YES
SNwkSIntKey	16	YES*	YES
FNwkSIntKey	16	YES*	YES
AppSKey	16	YES*	YES
FCntUP	4	YES*	YES
AFCntDown	4	YES*	YES
NFCntDown	4	YES*	YES
JoinNonce	3	YES*	
DevNonce	2	YES*	
Total:	**~150 bytes**		

*Should be stored in a way that prevents extraction and re-use by malicious actors.

IoT security – example LoRaWAN security concept

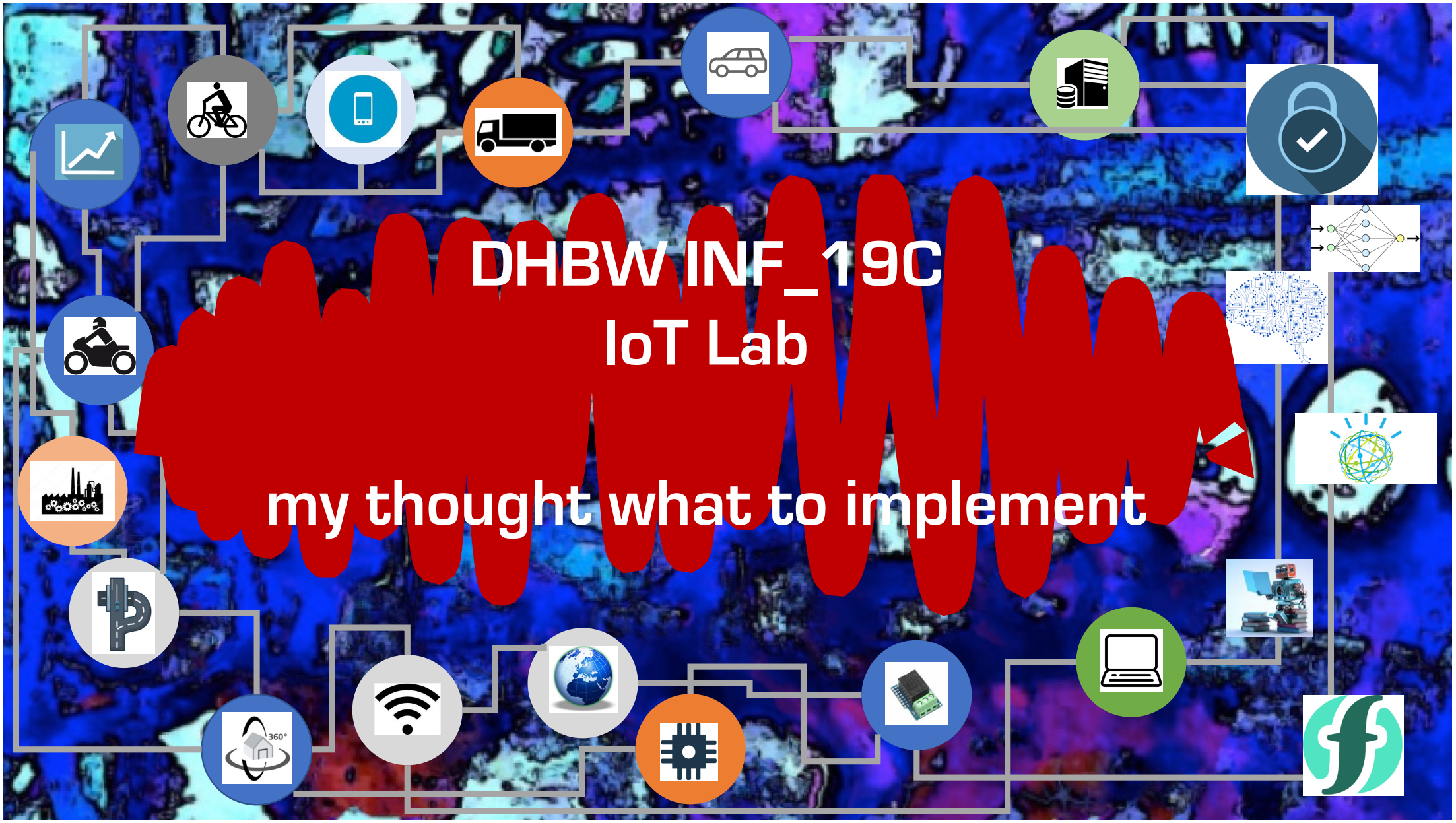
- **There are other security features available, however we will not discuss it here**

One last statement on IoT security LoRaWAN security today.

When you are building such solutions and you have to secure it, you have to think about how to manage all these keys in a secure way.

In our multigeiger project (nuclear radiation measurement) with ESP32 and LoRaWAN, the user have to enter the keys manually on the ESP32 and the will be stored in a secure environment in the end device.

Handle keys with care!!!


DHBW INF_19C
IoT Lab
my thought what to implement

Block diagram IoT Lab

Accelerator sensor

Gyroscope sensor

Moisture sensor

Ultrasonic sensor

Temperature sensor

Micro-controller

LoRaWAN

Connectivity Hub LoraWan e.-g. TTN

WiFi

WiFi

BLE

Connectivity Hub e.g. smartphone

WiFi

LTE

IoT server

Analytics on sensor data

MQTT will also be used