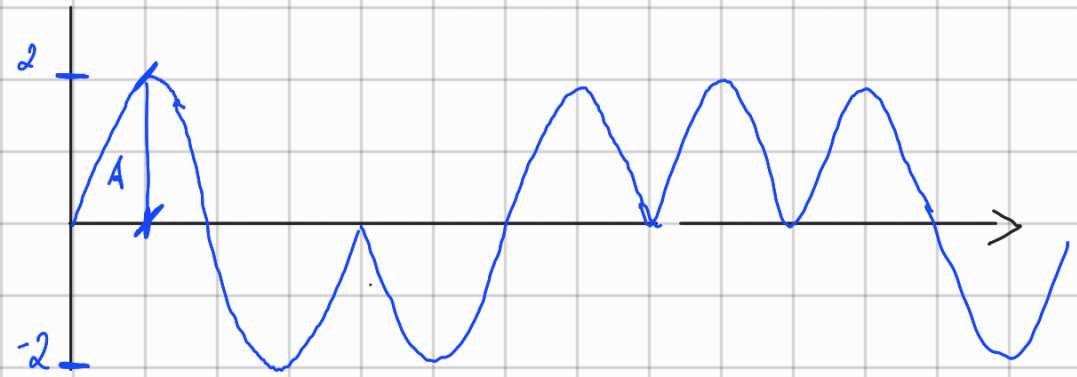
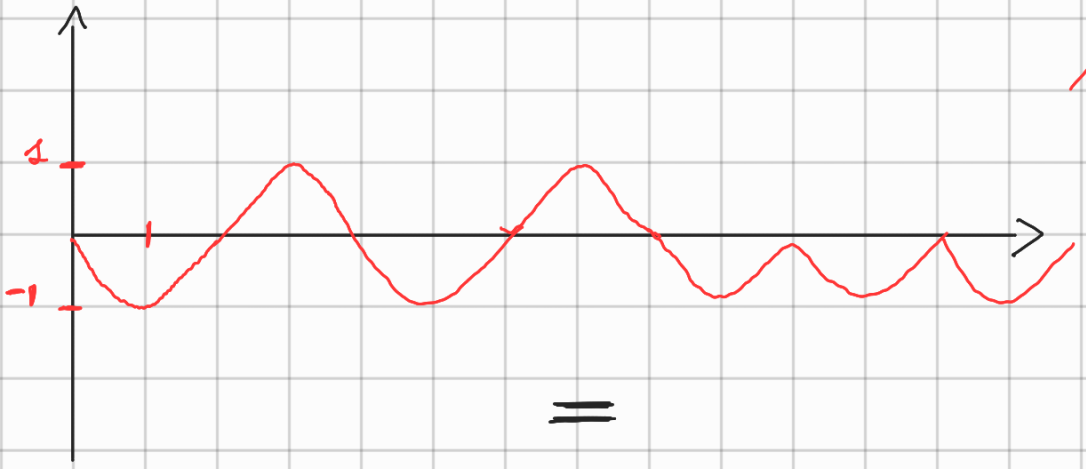


$[A=2 \rightarrow Bit=1]$
$[A=-2 \rightarrow Bit=0]$

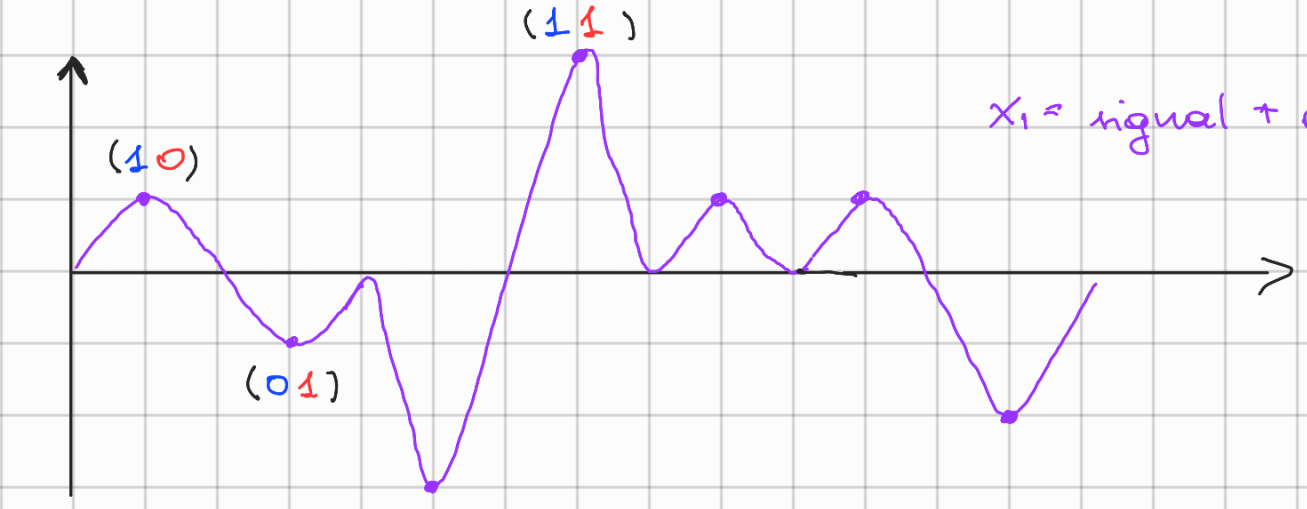
Signal: 1001110

+



Authentication: 0101000

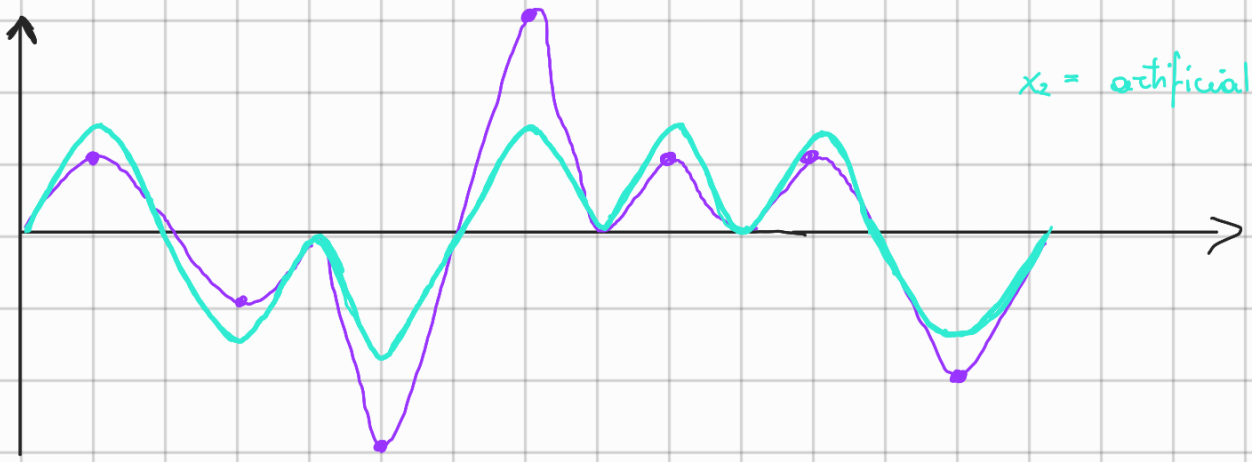
=



X_1 = signal + authentication

→ In this way also an attacker sniffing the transmission can decode between the signal and the authentication

Let's add some artificial noise to bring the signal within a certain range so that the attacker cannot decode the signal.



We tell the receiver the noise we added ⇒ removing the noise can
↳ need to protect this information decode the signal

① How do we add this noise?
↳ according to the CSI = Channel State Information
↳ predefined but in such a way that if the signal is received from a different channel ⇒ action of channel moves x_2 to x_3 in such a way that by removing the additive noise Alice obtains $x_4 \neq x_1$
⇒ Alice must not succeed in authentication verification

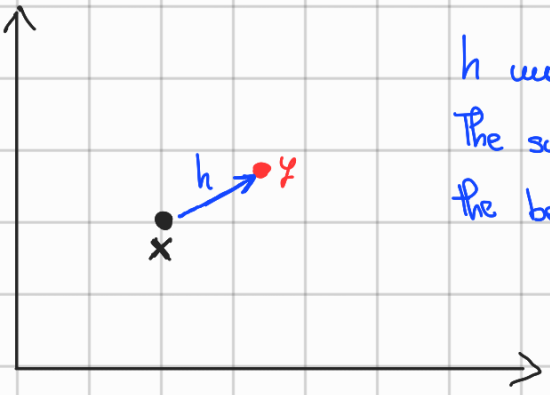
CHANNEL STATE INFORMATION

$y = h \cdot x + w$

x = transmitted signal
h = channel gain → action of wireless channel over transmitted signal
w = receiver noise → due to receiver instrumentation

h is usually due to:
- channel fading (distance and obstacles)
- signals interference (others signals but same frequency)
- multipath (interference with reflected signals)

→ to estimate the value of h we transmit pilot signals and define the mapping to the actual received signal → this defines the channel.
We use several pilot signals to average the channel.
If we use multiple subchannels for transmission (e.g., multiple frequencies) then need to CSI for each of them → use the matrix notation: $\bar{y} = H \cdot \bar{x} + \bar{w}$



h moves x into a different point.
The smaller the action of the channel.
the better the channel is

Usually $C_{BE} \neq C_{AB}$,
but as "d" decreases, the two channels will be similar still being highly correlated

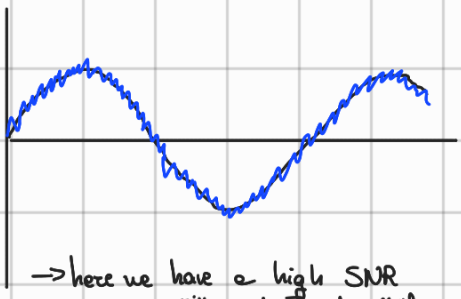
w cannot be removed (in most cases) and adds some uncertainty in the received signal.
However what is important is the Signal-to-Noise Ratio (SNR):

$$SNR = P_x / P_w$$

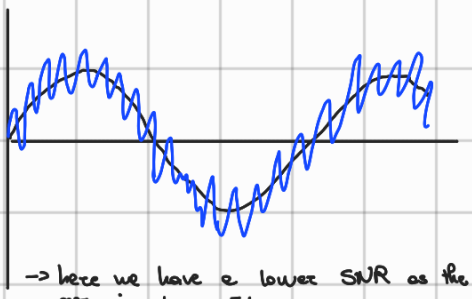
and indicates how better is the signal compared to the noise.

The idea is the following: - signal

- noise



-> here we have a high SNR
=> we can still understand well the shape of the signal



-> here we have a lower SNR as the noise affects more our signal reception.

-> Usually noise is considered being distributed according to a Gaussian distribution
=> Additive White Gaussian Noise (AWGN)

We want that the noise we add (whatever logic we might use) is such that if A receives the message from E, the channel C_{AE} introduces a noise in the signal that by removing the additive noise (the one we add), then A won't be able to successfully authenticate the message.

$x = x_1 + x_2$ | x_1 = data , x_2 = authentication

$x' = x + n$ | n = additive noise

Assuming that is able to perfectly retrieve x' from $y_E = h(C_{BE}) \cdot x' + w_E$

we want this: $y_A = h(C_{AB}) \cdot x' + w_A \Rightarrow y_A - n = x'' = x_1'' + x_2'' \mid x_2'' \neq x_2$