General Interests:

Secure Proximity / Distance Measurement

GPS Spoofing and Spoofing Detection

Usable Authentication (2FA)

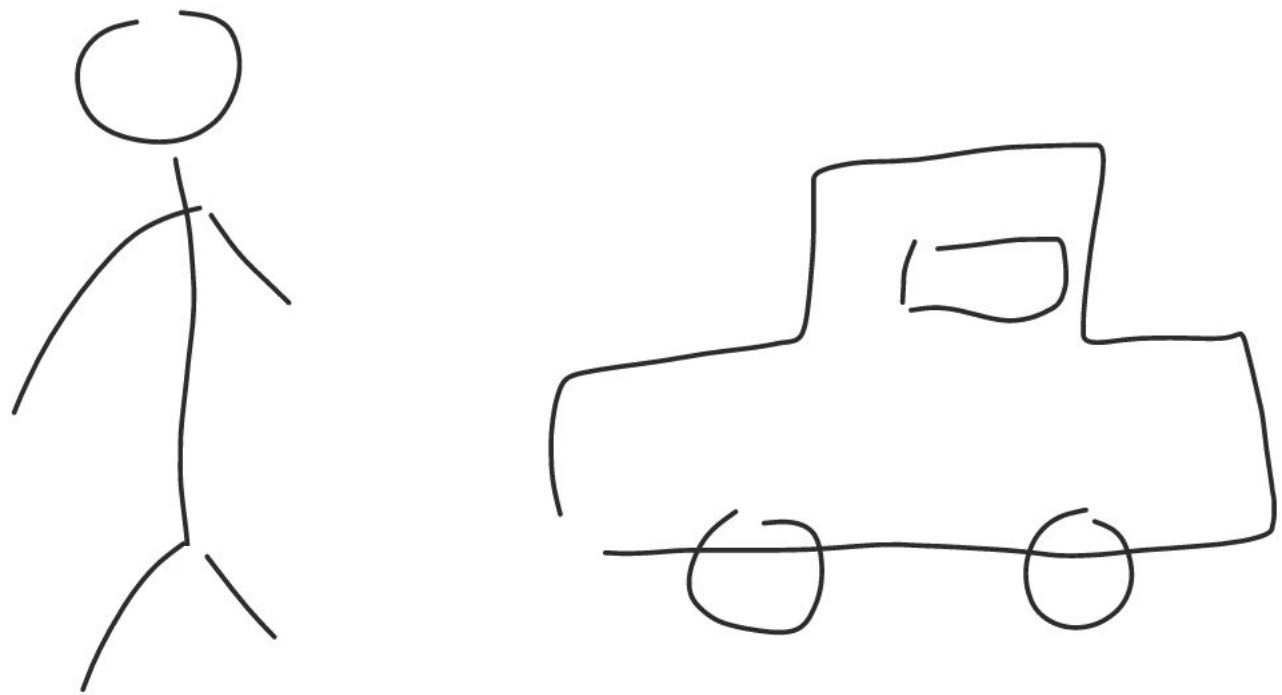
Security of Blockchains / Cryptocurrencies

Trusted Computing

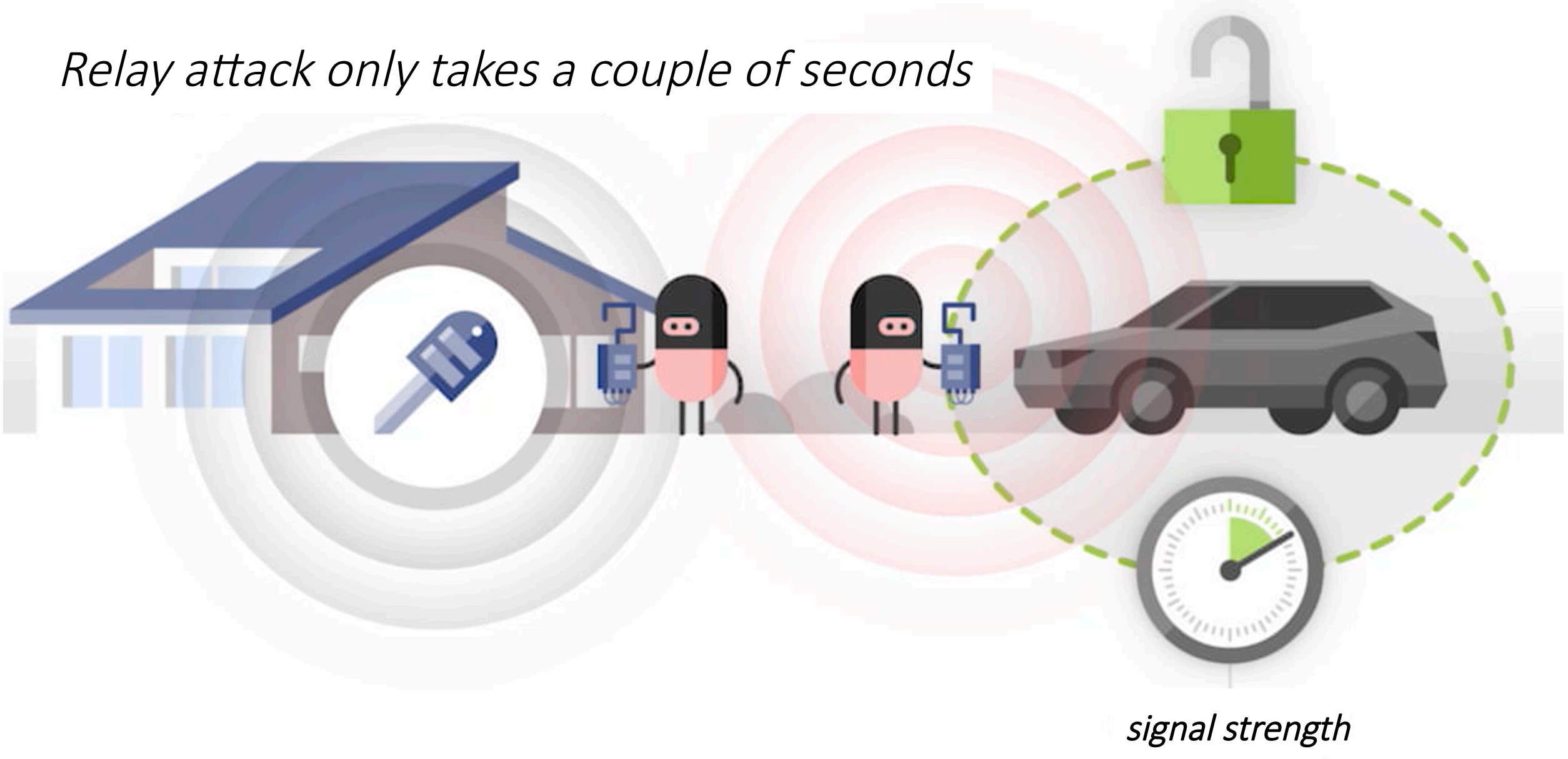
Secure Proximity / Distance Measurement

Srdjan Čapkun

ETH zürich

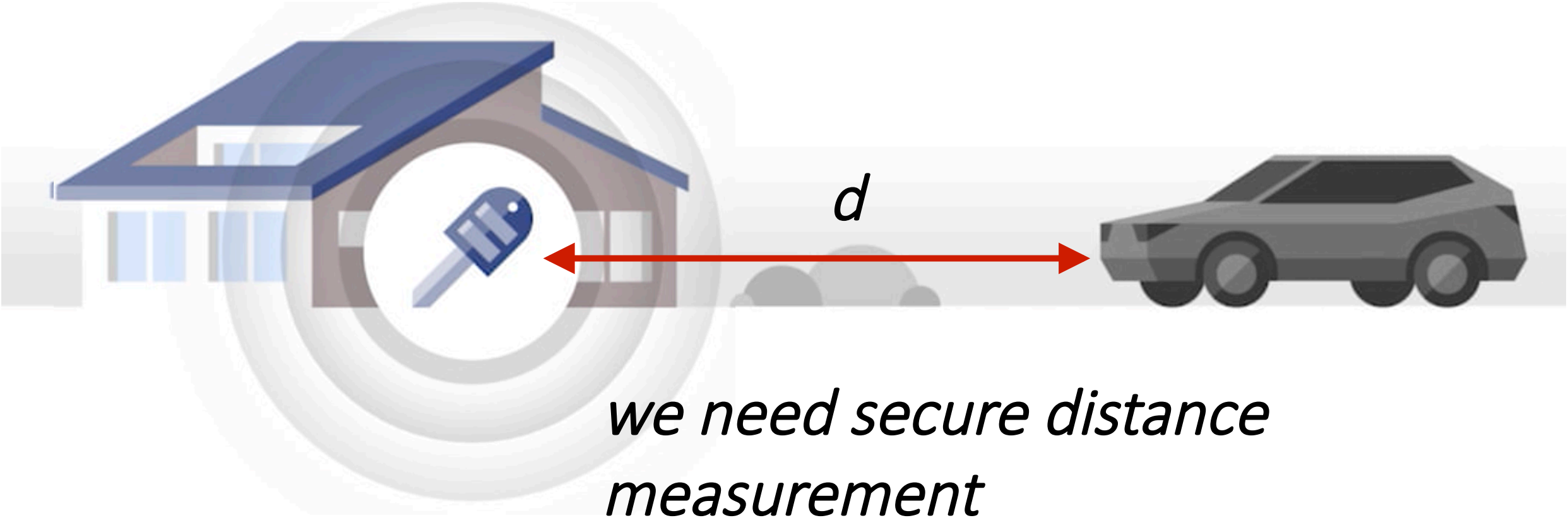


Relay attack only takes a couple of seconds

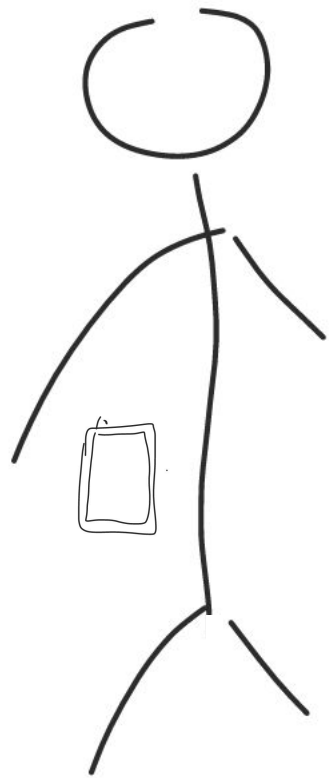


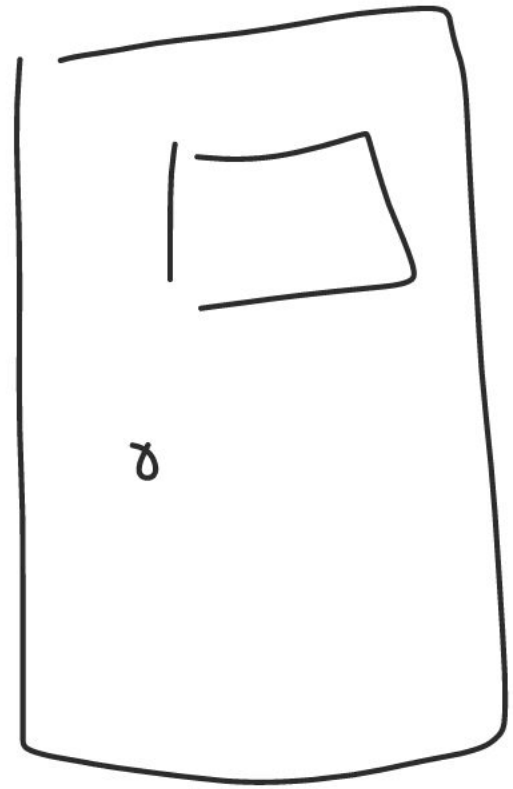
signal strength

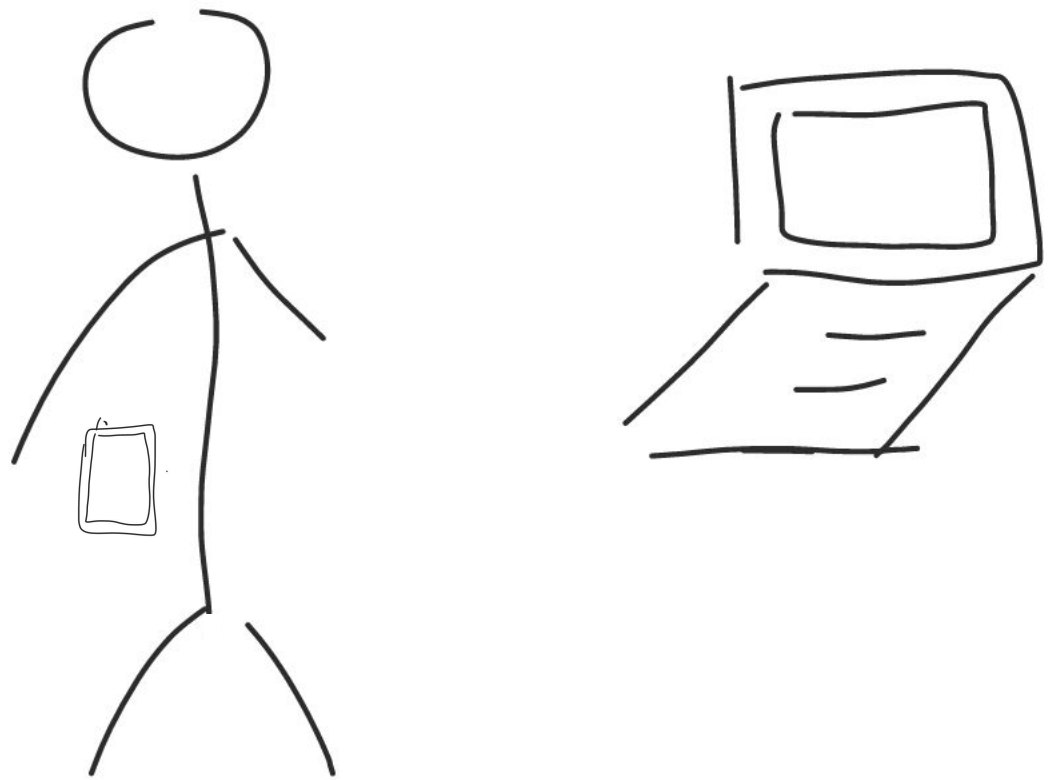

09-25-2017 Mon 01:01:41
WEST MIDLANDS POLICE
Camera 01

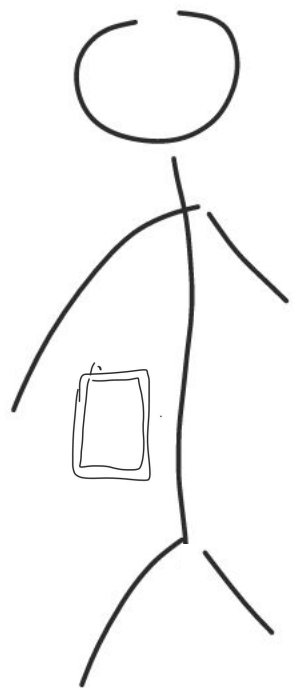


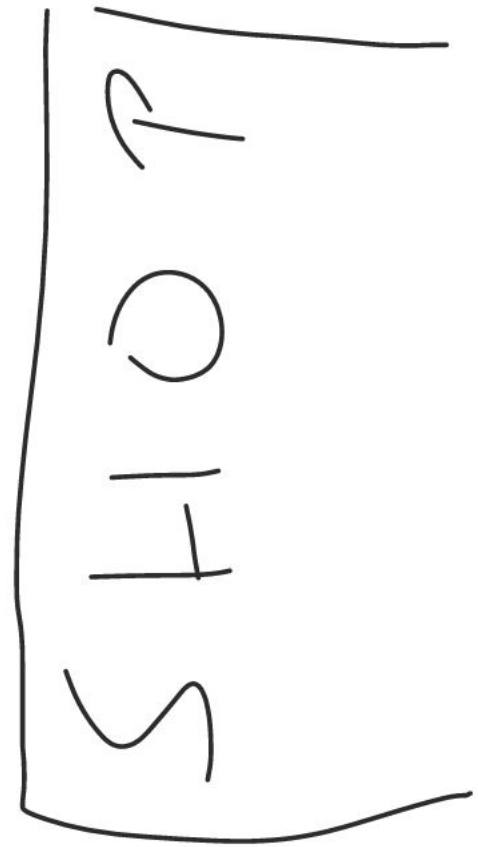
we need secure distance measurement

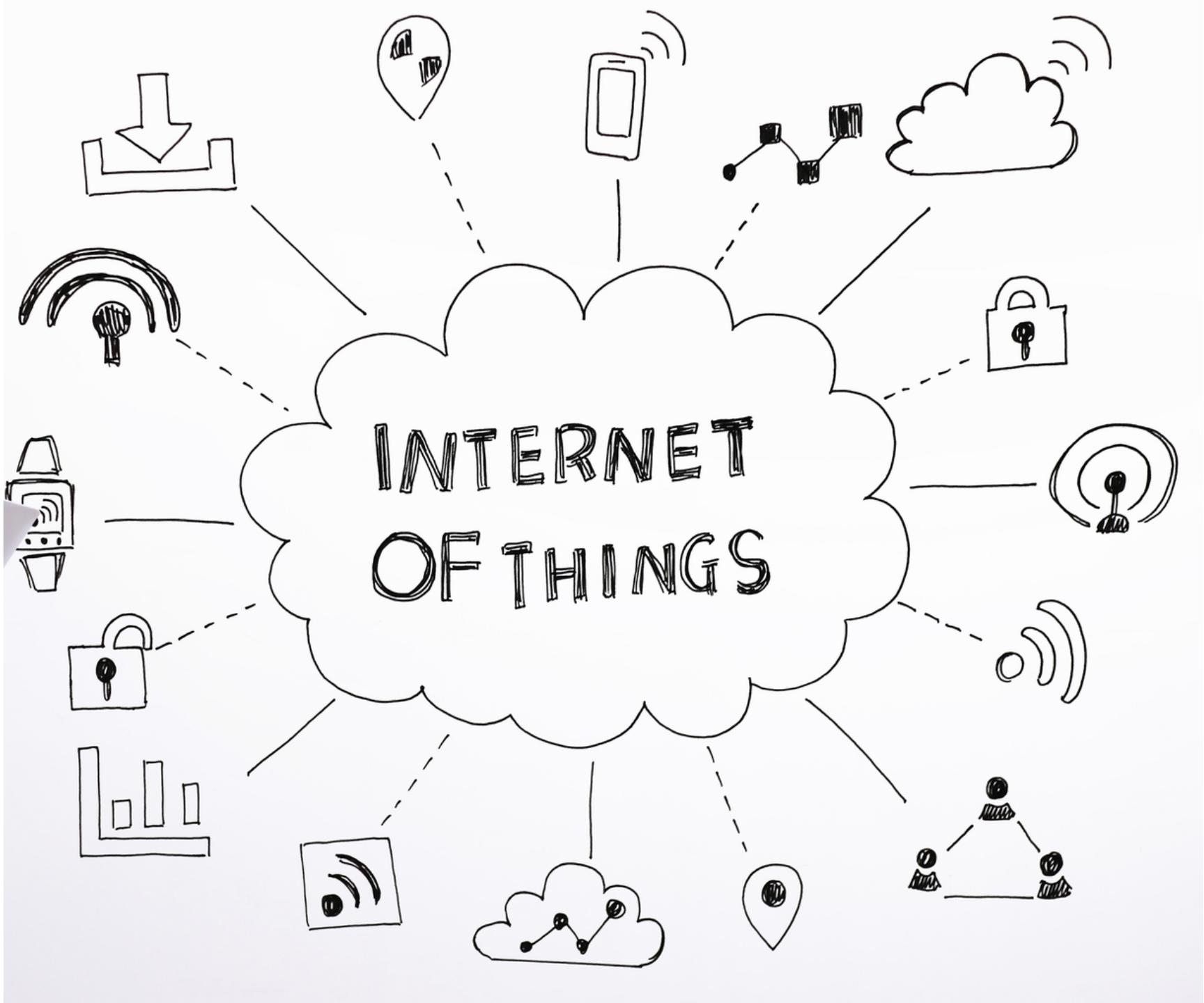



γ






SHOT


INTERNET
OF THINGS

need to know where other objects/ people are

need to know where we are

need to know where other objects/ people are

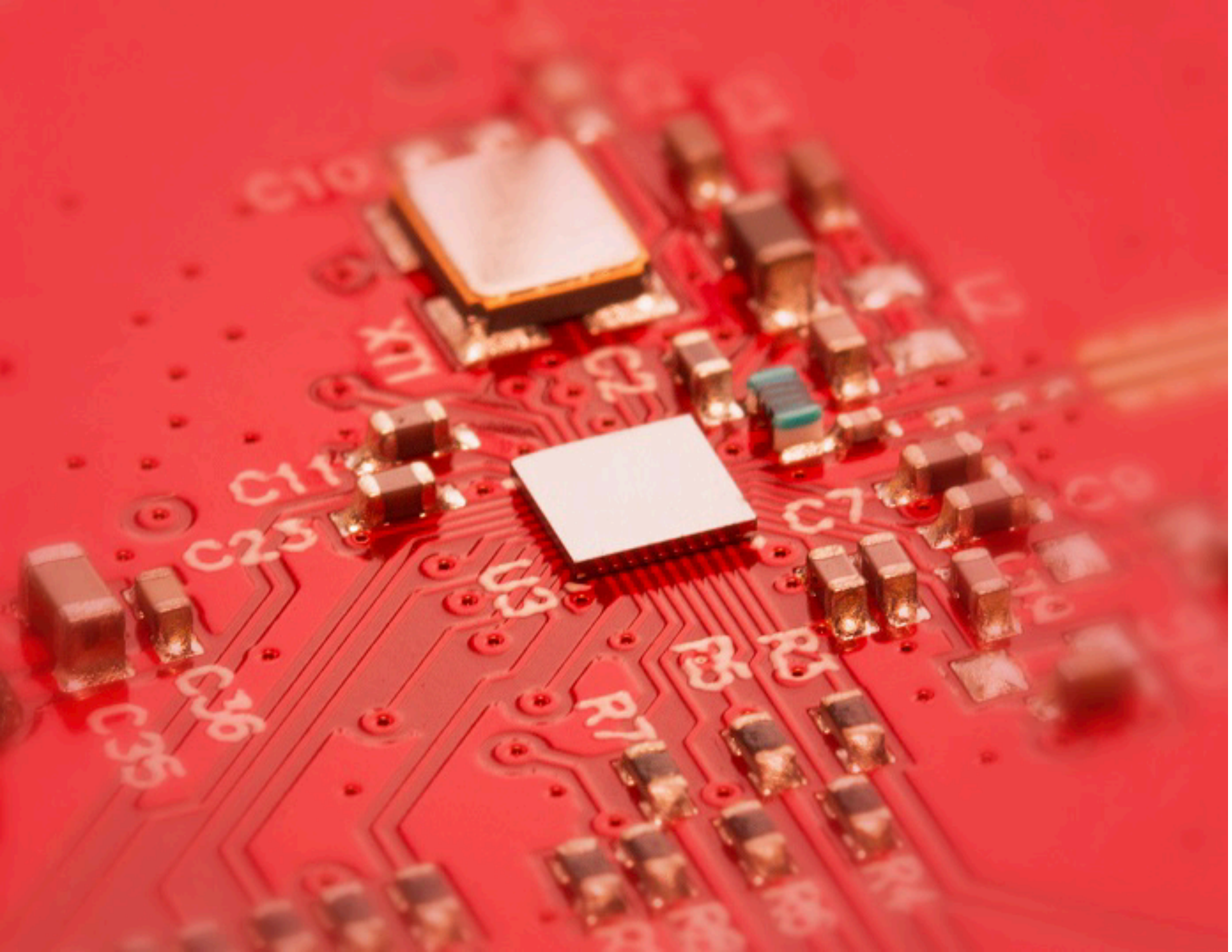
need to know where we are

securely

until now no fully secure distance measurement or positioning systems

until now no fully secure distance measurement or positioning system

[so we decided to build one at ETH]



new radio IC

low power

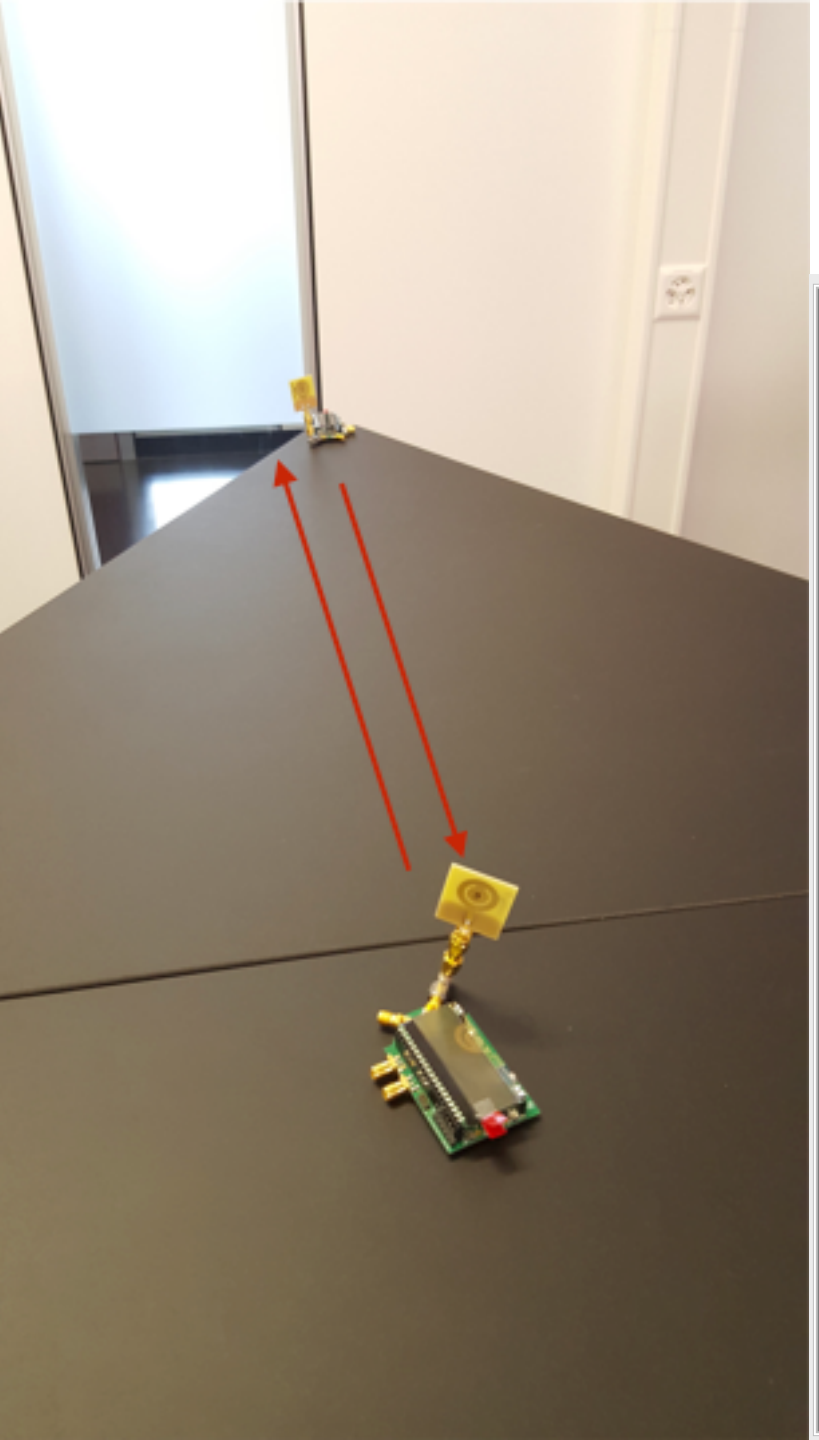
provably secure

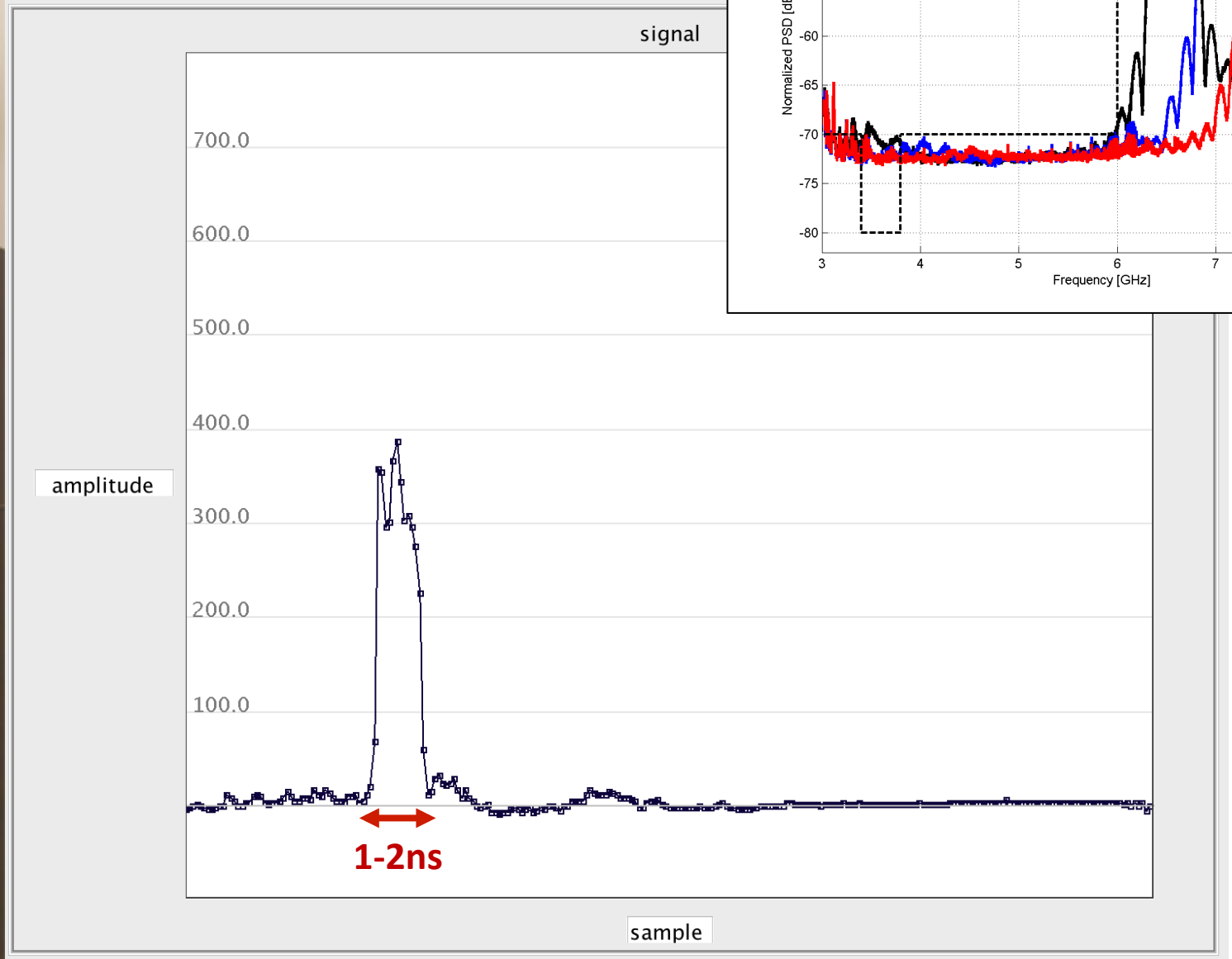
precise

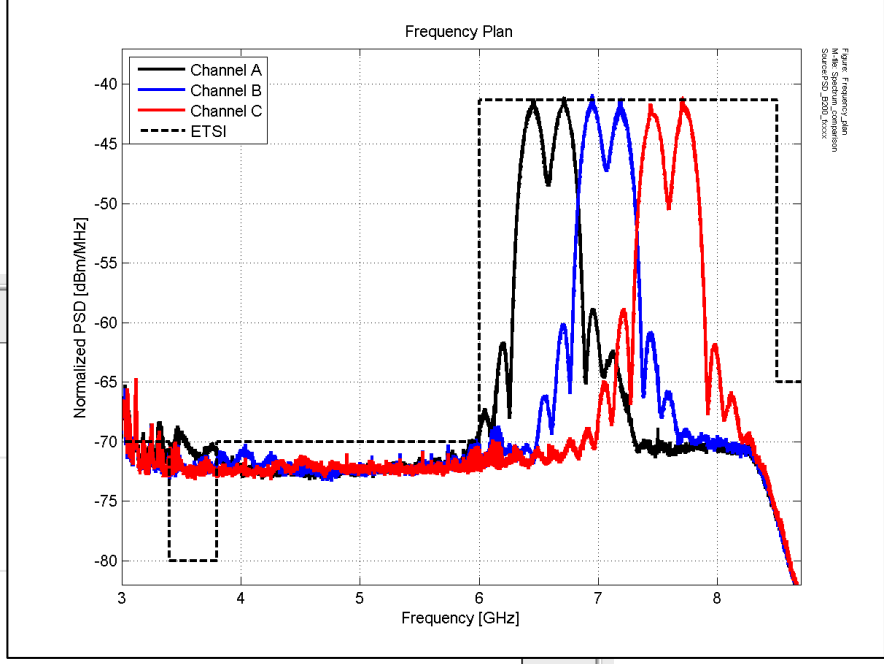
fast

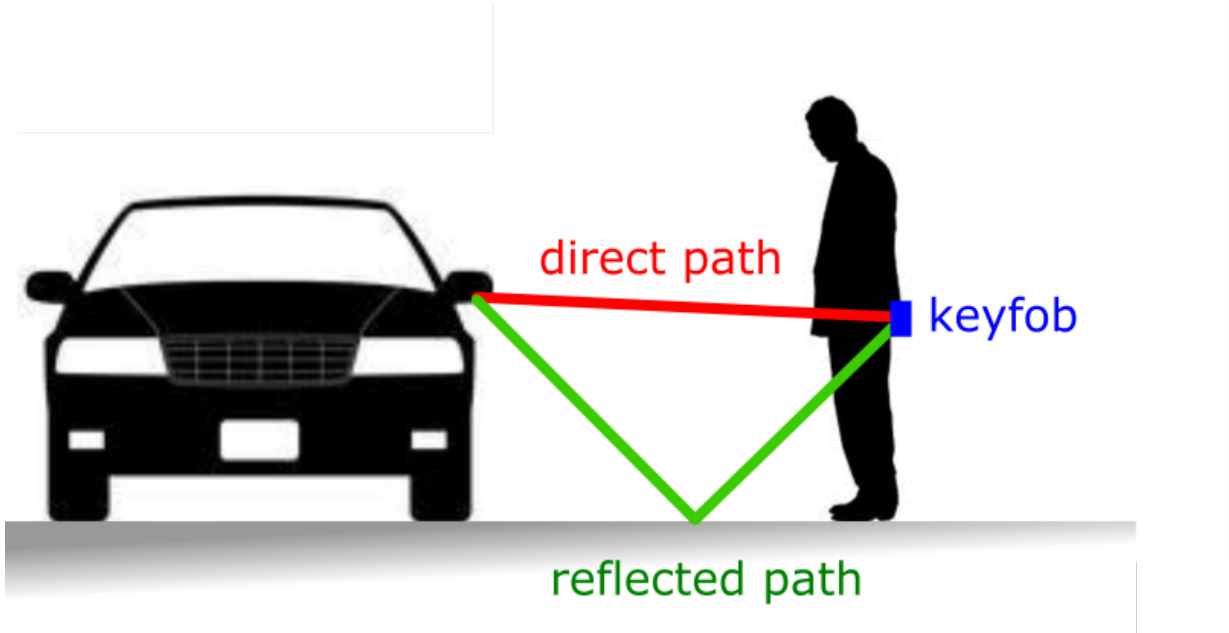
3db ETH zürich

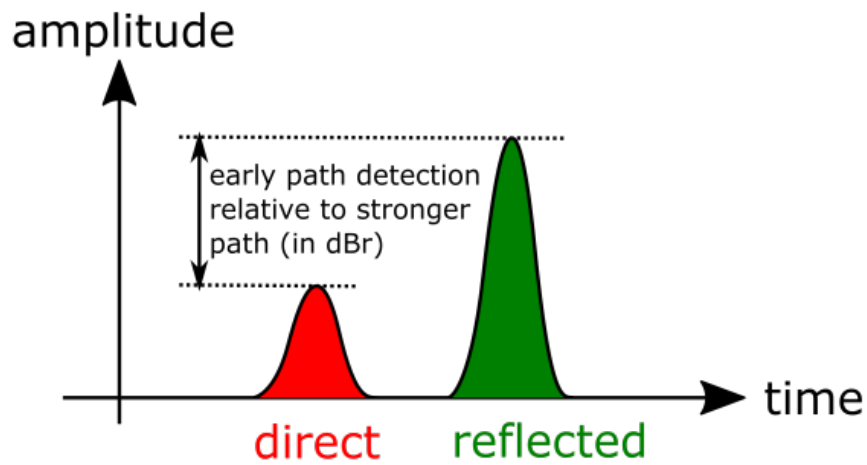

RangingApplication
continous verifier
UWB CONTROLLER
distance
distance[m]
0.14
Reconnect
update
run
hold
distance [m]
7.0
6.0
5.0
4.0
3.0
2.0
1.0
sample
display
distance
signal
show raw value
off
on
delay [ms]
0
250
500
750
1000
3db
distance[m]
0.14




signal
amplitude
700.0
600.0
500.0
400.0
300.0
200.0
100.0
1-2ns
sample


Frequency Plan
Channel A
Channel B
Channel C
ETSI
Normalized PSD [dBm/MHz]
-40
-45
-50
-55
-60
-65
-70
-75
-80
3
4
5
6
7
8
Frequency [GHz]

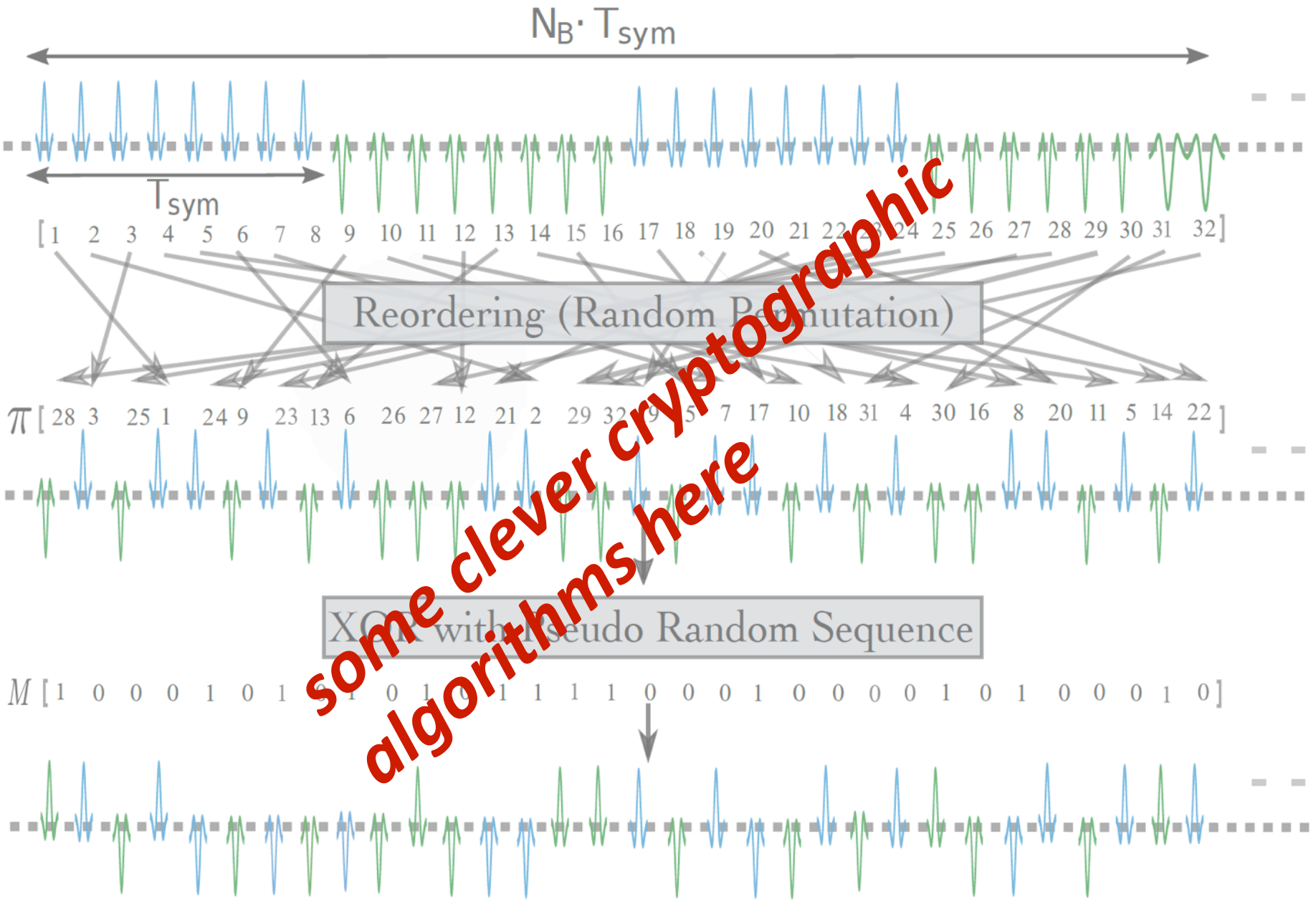




weaker signal
but
true distance

stronger signal
but
longer distance

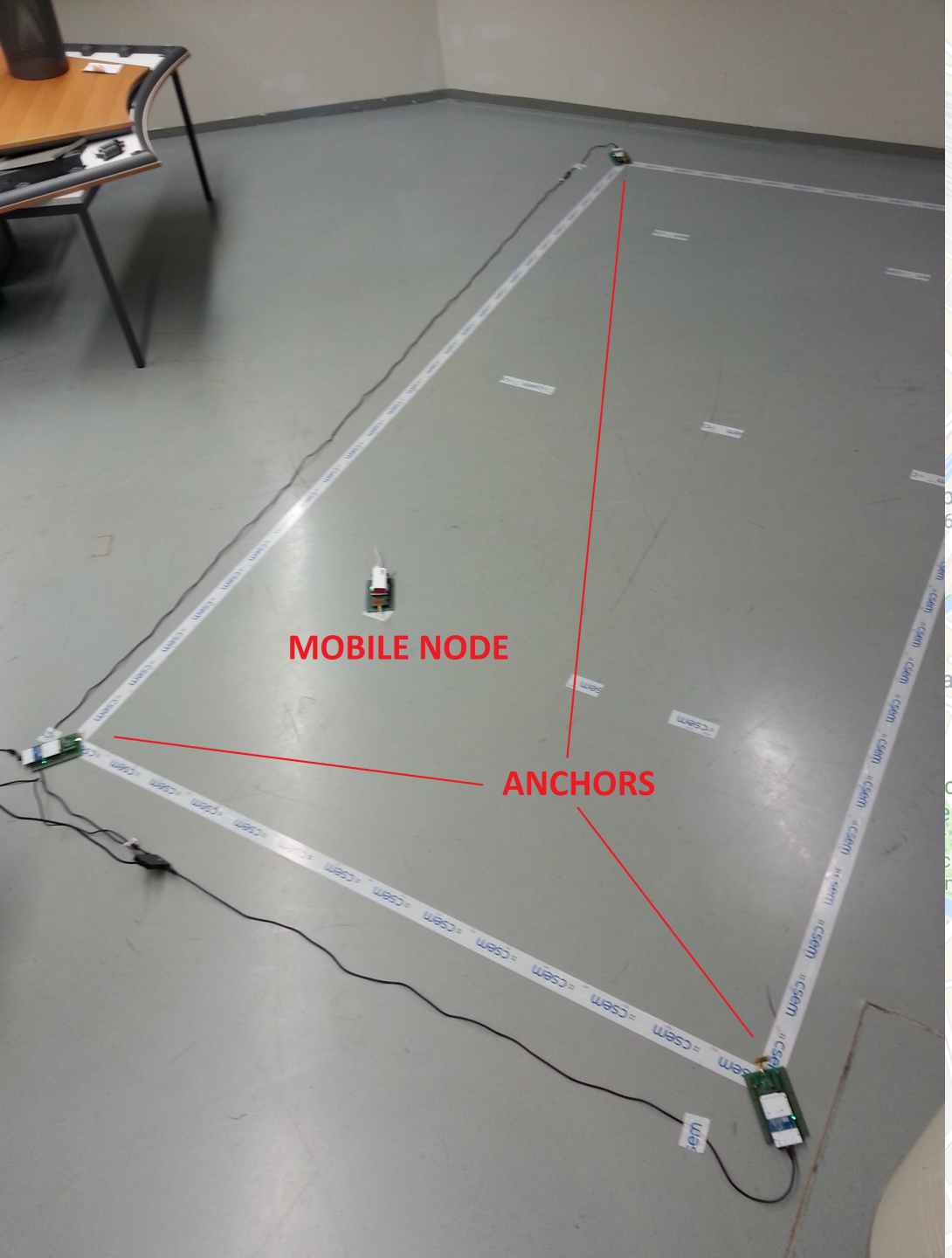
early_path_scenario.svg

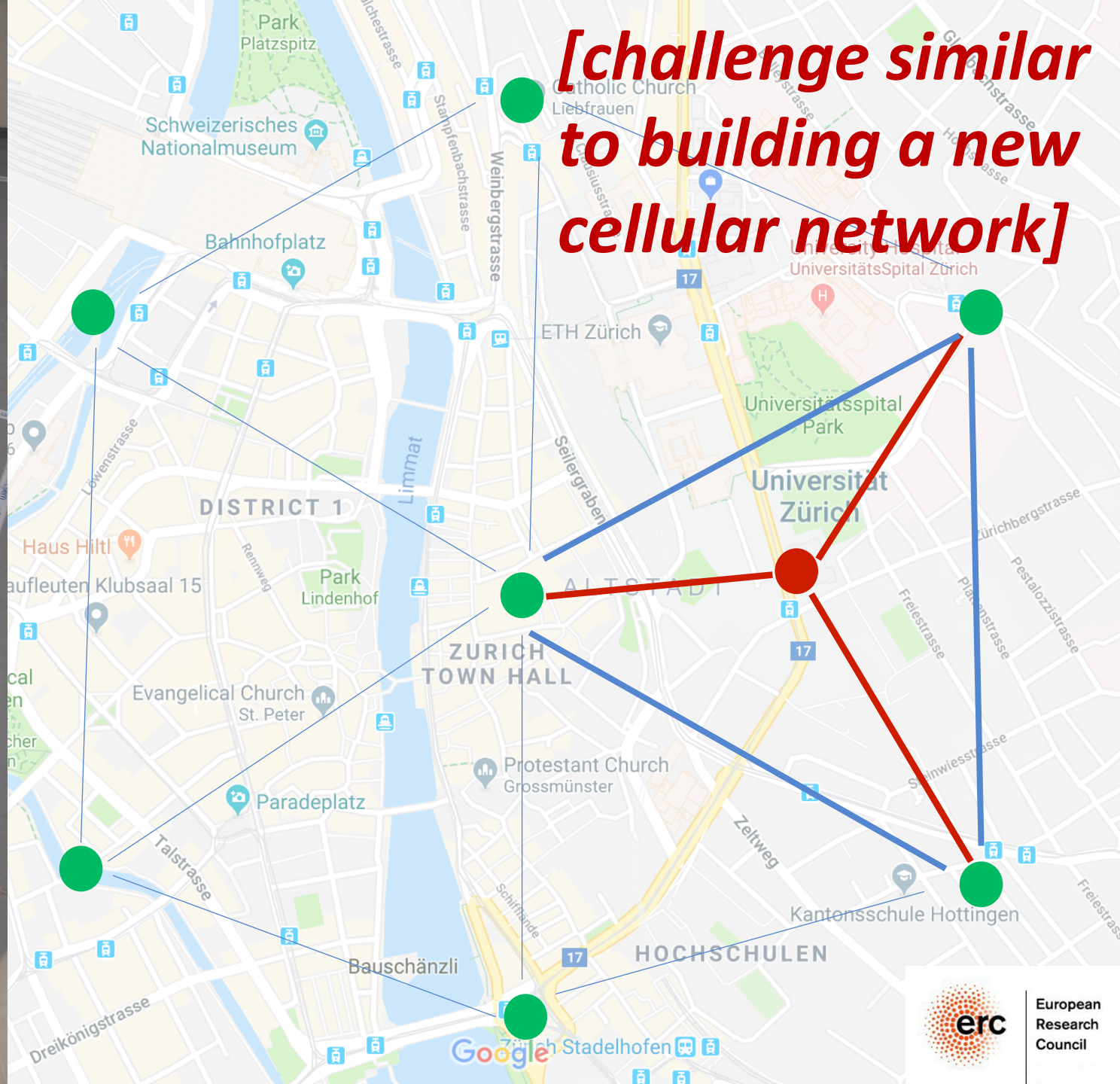


some clever cryptographic algorithms here

special secure modulation

long range





European Research Council

Long Term Goal:
widely deployed secure positioning infrastructure

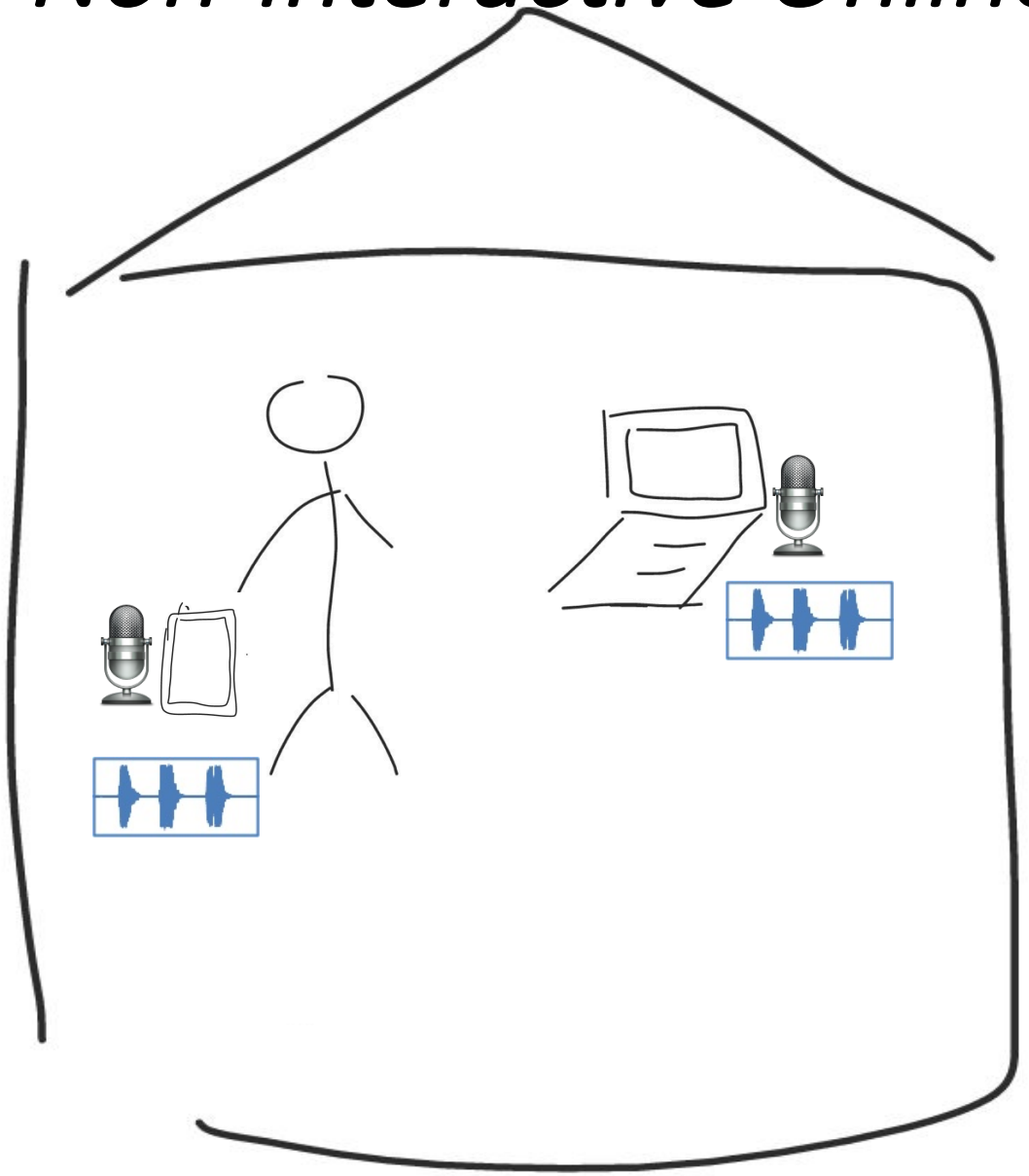
Standardization:

802.15.4z (UWB)

- *Interact with relevant partners*
- *Increase adoption*

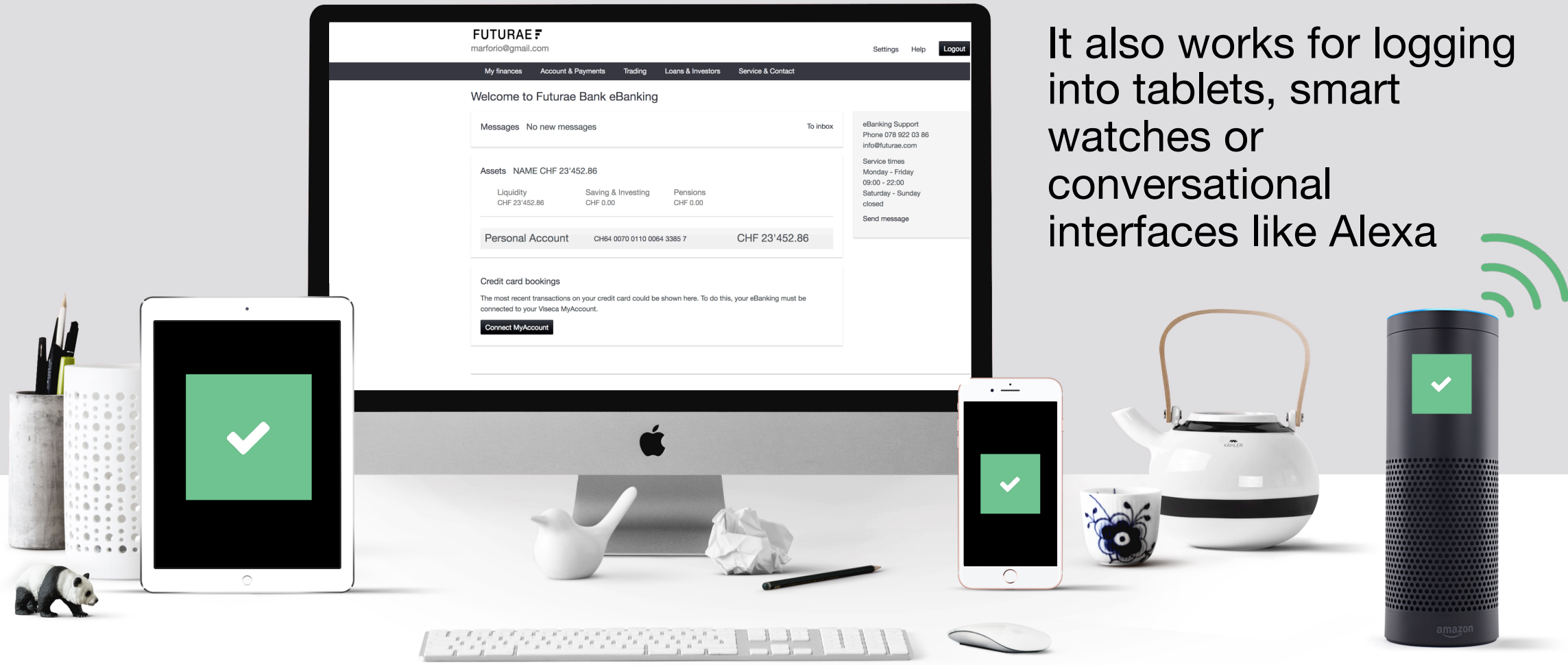
But RF is not the only sensing modality

SoundProof: Non-Interactive Online Authentication



ETH zürich FUTURAE

SoundProof: Non-Interactive Online Authentication



It also works for logging into tablets, smart watches or conversational interfaces like Alexa

ETH zürich FUTURAE

Funding:

- *ERC (1.5-2.5 M$ / 5y / single PI)*
- *Swiss NCCR: 100M / 10 y / many PIs*
- *Industry (ZISC, 25+ M$ / 10y)*

- *Commercialization*

it is time to "de-virtualize"

we need to "get physical" again to …

it is time to “de-virtualize”

we need to “get physical” again to …

… secure existing systems

… enable deployment of new systems

ETH zürich

ZISC Zurich Information Security & Privacy Center

https://www.zisc.ethz.ch

capkuns@inf.ethz.ch