Wireless Physical Layer Security

Chapter 0: Welcome, Orga & Intro

Christian Zenger, Johannes Kortz, Jonathan Mazyrko

The WPLS Team – Welcome




- Christof Paar, Christian Zenger, Johannes Kortz, Jonathan Mazyrko
  - Chair for Secure Mobile Networking, PHYSEC GmbH

- Research Interests
  - Future Wireless Systems
  - Intelligent Reflective Surfaces
  - Radio-Frequency Machine Learning Systems
- Contact
  - Moodle Course
  - Passwort: wpls2023

Content & Schedule

WPLS Content Overview

The course covers

A. Fundamentals and theory in the lecture part
B. Practical experience and opportunity to ask questions in the lab part
C. Self-guided exploration of the topic area in the home exercise part

Organization of this course

- Lab course language is German (slides are in English)
- Attendance at the lecture and lab parts is **strongly recommended**
  - Contact us in case of any problems & we will find a solution!
- Assignments shall be handled **in groups of 3 students**
- Each group is responsible for its hardware!
- You can work either at your own computer or laptop

Organization of this course

- Home exercises & programming tasks will be graded
- One submission per group (but name your group partner)
- **You pass, if:**
  - **sum of all exercises > 70%**
  - **no exercise < 50%**
- The course will cover five (six for master students) mandatory exercises and at the end a chance to compensate a failed assignment.

Hardware Tools and Testbeds

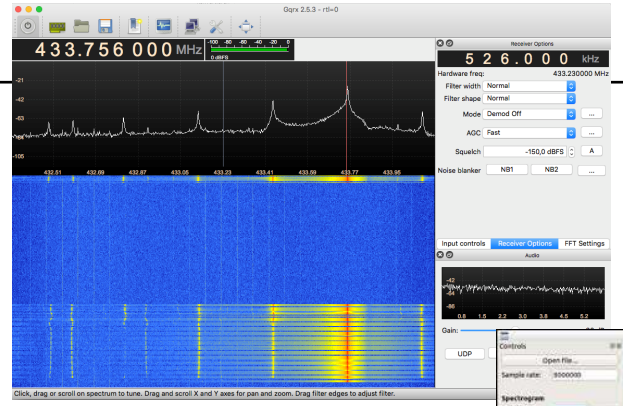
1. RTL-SDR + Antenna
2. HackRF One SDR
3. Bootable USB drive with software (can be replaced by a VM)
4. 3 Raspberry Pis
5. Wi-Fi sticks
6. ZigBee sticks
7. BLE sticks
8. USB adapters
9. Powerbank

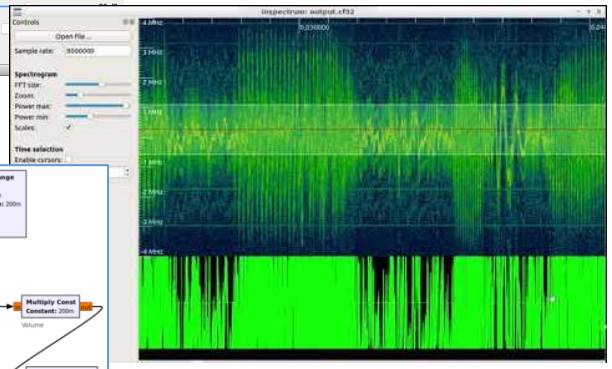
Hardware testbeds

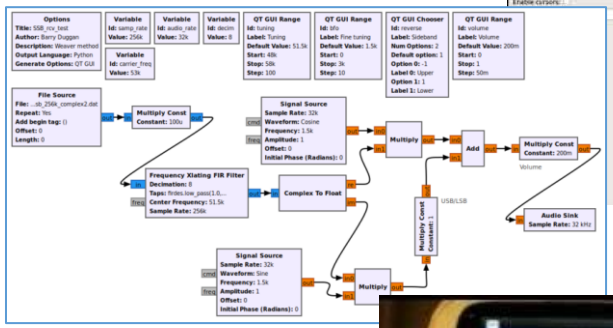
Usefull software

- gqrx (Linux)
  - Open source software defined radio receiver (SDR)
  - supports RTL-SDR & HackRF One
- inspectrum / baudline
  - Spectrum analyzer
- GNU Radio Companion
  - Tool for creating signal flow graphs and generating flow-graph source code
  - Supports RTL-SDR & HackRF One
- SDR Touch (license needed)
  - Mobile application for Android to use SDR with smartphone

Preinstalled on USB drive







Distribution of the hardware testbeds

- Find yourselves in groups of 2-3
  - Use Moodle to team up!
- Book a time slot in Moodle to receive your kit on campus
- Arrive on time to avoid large gathering of students
- To reduce infection risk, bring your own pen to sign for the hardware

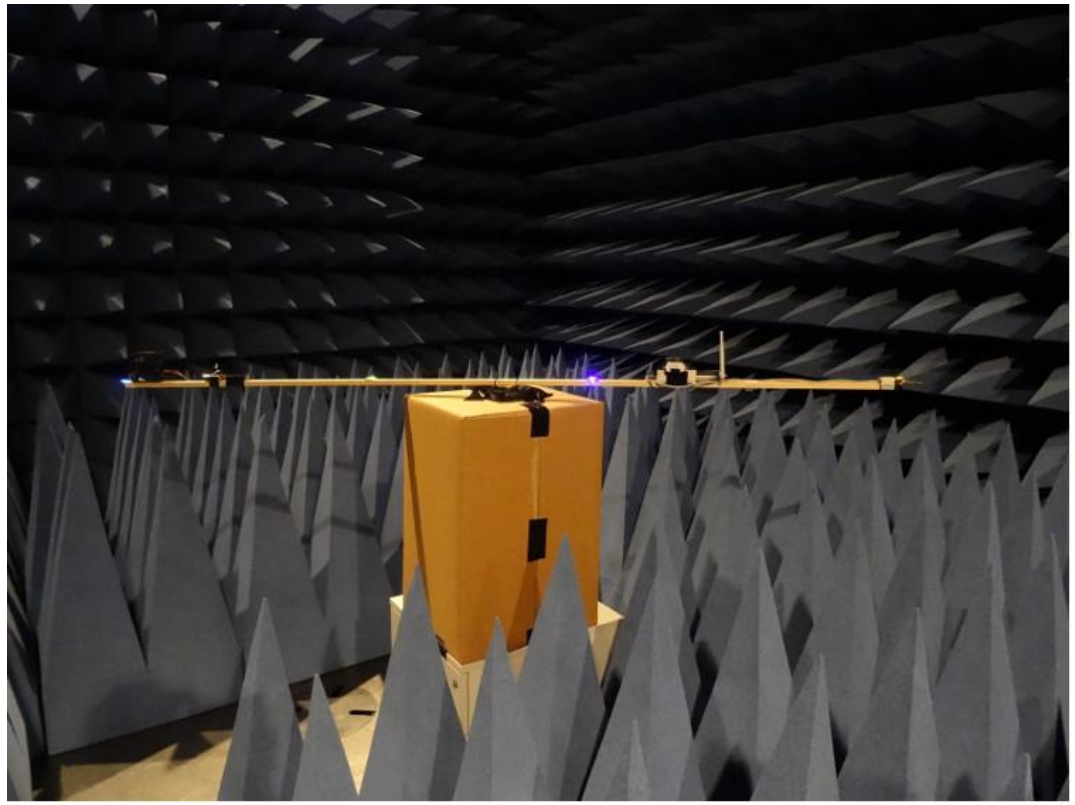
Contents and Schedule

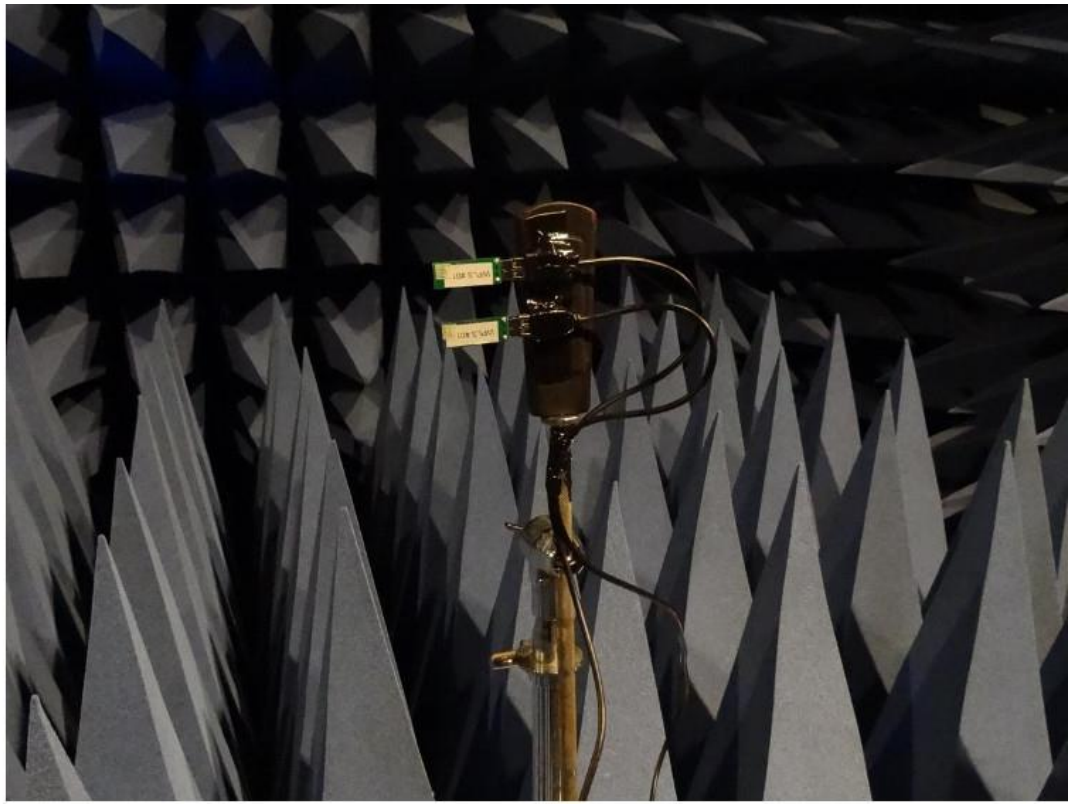
05.04.23	Orga + Motivation + Basics
19.04.23	Introduction SDR + Practice with GRC
10.05.23	Spectrum sensing + Electronic Warfare
24.05.23	Physical Layer Secruity Theory + Basics
14.06.23	Keys exctraction from the wireless channel
28.06.23	PLS Attacks and Virtual Proofs of Reality + Machine Learning

April			May			June			July		
1	Sat		1	Mon		1	Thu	Pfingstferien	1	Sat	
2	Sun		2	Tue		2	Fri		2	Sun	
3	Mon		3	Wed		3	Sat		3	Mon	
4	Tue		4	Thu		4	Sun		4	Tue	
5	Wed	Kick-Off	5	Fri		5	Mon	Absorberhalle	5	Wed	UB 5
6	Thu		6	Sat		6	Tue		6	Thu	
7	Fri		7	Sun		7	Wed	UB 3	7	Fri	
8	Sat		8	Mon		8	Thu	Absorberhalle	8	Sat	
9	Sun		9	Tue		9	Fri		9	Sun	
10	Mon		10	Wed	VL 2	10	Sat		10	Mon	
11	Tue		11	Thu		11	Sun		11	Tue	
12	Wed	Hardwarevergabe	12	Fri		12	Mon		12	Wed	
13	Thu		13	Sat		13	Tue		13	Thu	
14	Fri		14	Sun		14	Wed	VL 4	14	Fri	
15	Sat		15	Mon		15	Thu		15	Sat	
16	Sun		16	Tue		16	Fri		16	Sun	
17	Mon		17	Wed	UB 2	17	Sat		17	Mon	
18	Tue		18	Thu		18	Sun		18	Tue	
19	Wed	VL 1	19	Fri		19	Mon		19	Wed	
20	Thu		20	Sat		20	Tue		20	Thu	
21	Fri		21	Sun		21	Wed	UB 4	21	Fri	
22	Sat		22	Mon		22	Thu		22	Sat	
23	Sun		23	Tue		23	Fri		23	Sun	
24	Mon		24	Wed	VL 3	24	Sat		24	Mon	
25	Tue		25	Thu		25	Sun		25	Tue	
26	Wed	UB 1	26	Fri		26	Mon		26	Wed	
27	Thu		27	Sat		27	Tue		27	Thu	
28	Fri		28	Sun		28	Wed	VL 5 (Schug, Tobisch)	28	Fri	
29	Sat		29	Mon	Pfingstferien	29	Thu		29	Sat	
30	Sun		30	Tue		30	Fri		30	Sun	
			31	Wed					31	Mon	

SDR – Software Defined Radio
GRC – GNU Radio Companion

Anechoic Chamber Assignment (ID 04/445)





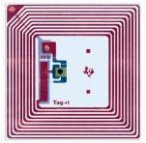
05.-09.06.23 – Every Groups gets a Timeslot (Moodle)

Motivation

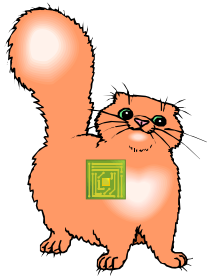
IoT, Attacks and Countermeasures

Motivation

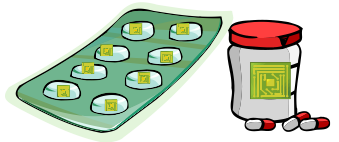
U.S. credit cards („tap-and-go“)



Housepets

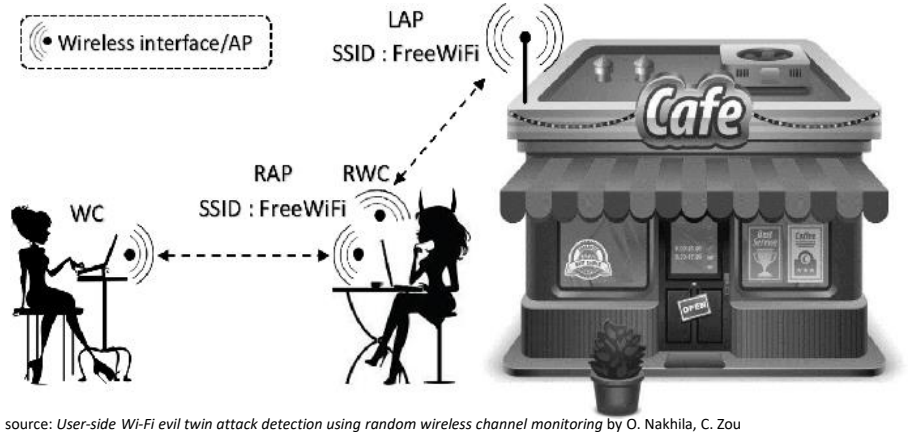


NFC

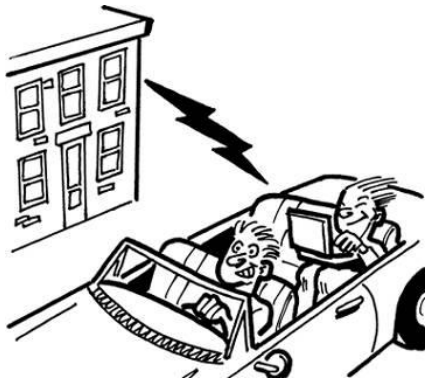


Anti-counterfeiting of products

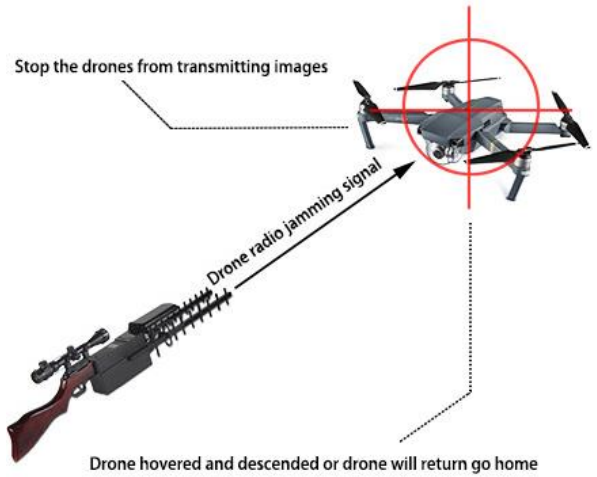
Types of RF Attacks



source: *User-side Wi-Fi evil twin attack detection using random wireless channel monitoring* by O. Nakhila, C. Zou



source: https://www.secjuice.com/modern-wardriving-an-analysis/



source: https://www.perfectjammer.com/gun-type-drones-uav-jammers-high-power.html

- **Sniffing**: The passive observation of wireless network traffic, noteworthy as wireless domain enables truly promiscuous sniffing with no direct physical access.
- **Wardriving**: Wardriving is type of sniffing that refers to discovering of non-802.11 RF networks. Example: killerbee 802.15.4 framework.
- **Evil-twin Attack**: Standing up a decoy device or rogue access point that mimics trusted infrastructure, such that it tricks victims into connecting into it.
- **Replay Attack**: Involve retransmitting a previously captured raw PHY-layer payload or the synthesis of a new frame based on decoded data.
- **Jamming**: Can be conducted by transmitting noise within the target network's RF channel with sufficient bandwidth and power.

But nobody would do this, right?

So leicht dringen Hacker in Ihr Smart Home ein

Veröffentlicht am 04.09.2018 | Lesedauer: 9 Minuten

Von **Florian Gehm**
Redakteur Wirtschaft und Finanzen

Gehackt! Wenn das Smarthome nicht sicher ist, funktioniert bald gar nichts mehr

Quelle: picture alliance / dpa Themendie

Fehlalarm

Replay-Attacke öffnet Alarmsysteme

„Ich bin drin" – so sollte sich eigentlich nur der legitime Nutzer eines Alarmsystems nach dessen Entschärfung freuen. Doch wer ungeschützte Funkfernbedienungen nutzt, öffnet auch Einbrechern Tür und Tor.

Von Thomas Detert

But nobody would do this, right?

The New York Times

Keeping Your Car Safe From Electronic Thieves

Disruptions
By NICK BILTON APRIL 15, 2015

Last week, I started keeping my car keys in the freezer, and I may be at the forefront of a new digital safety trend.

Let me explain: In recent months, there has been a slew of mysterious car break-ins in my Los Feliz neighborhood in Los Angeles. What's odd is that there have been no signs of forced entry. There are no pools of broken glass on the pavement and no scratches on the doors from jimmied locks.

But these break-ins seem to happen only to cars that use remote keyless systems, which replace traditional keys with wireless fobs. It happened to our neighbor Heidi, who lives up the hill and has a Mazda 3. It happened to Simon, who lives across the street from me and has a Toyota Prius.

And it happened to our Prius, not once, but three times in the last month.

Source: http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html

But nobody would do this, right?

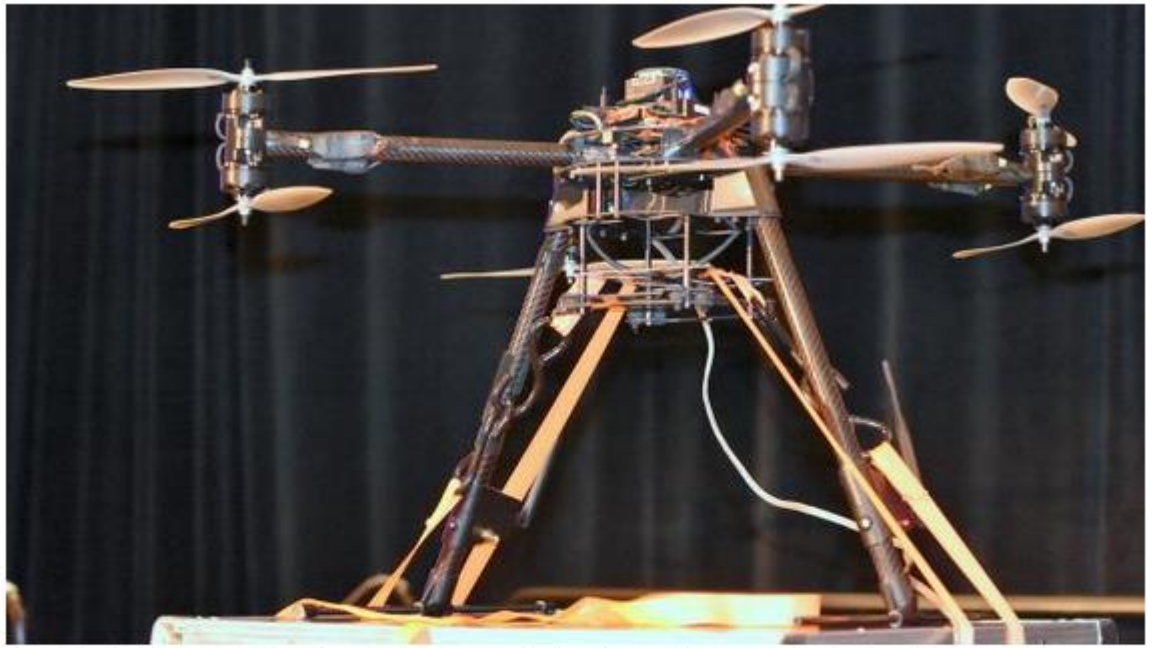
30.000-Euro-Drohne mit 45-Euro-Hardware gehackt

03.03.2016 10:42 Uhr – Uli Ries

Funk als Einfallstor

Zielgruppe für die Drohne, die bis zu drei Kilogramm schwere Lasten transportieren und bis zu 45 Minuten in der Luft bleiben kann, sollen unter anderem Feuerwehren und Polizeiorganisationen sein. Das wohl schwerwiegendste Sicherheitsproblem steckt in der Funktechnik: Die Drohne lässt sich nicht nur mit einer im 2,4-GHz-Bereich funkenden manuellen Fernbedienung steuern, sondern auch mittels einer Telemetriebox.

Diese dient als Mittler zwischen einer Android-App zur Flugplanung und dem Flugobjekt. In diesem Fall kommt anstelle der auf knapp 100 Meter Reichweite beschränkten 2,4-GHz-Technik Hardware auf Basis der proprietären XBee-Chips (868LP) zum Einsatz, deren Reichweite bis zu zwei Kilometer betragen soll. Auf diesem Weg finden auch die von der Drohne erfassten Daten – durch Erweiterungen erfasst das Modell beispielsweise Hitzesignaturen per Infrarot-Kamera oder entdeckt Gase mittels entsprechender Sensoren – den Weg zurück zum Tablet.



Diese für den kommerziellen Einsatz konzipierte Drohne bringt diverse Sicherheitsprobleme mit, die Hackern leicht Zugriff erlauben. (Bild: heise online)

Eine unter anderem für den Feuerwehr- und Polizeieinsatz gedachte Drohne funkt vergleichsweise leicht angreifbar und kann mit wenigen Handgriffen von potentiellen Angreifern ferngesteuert werden.

Source: http://heise.de/-3126838

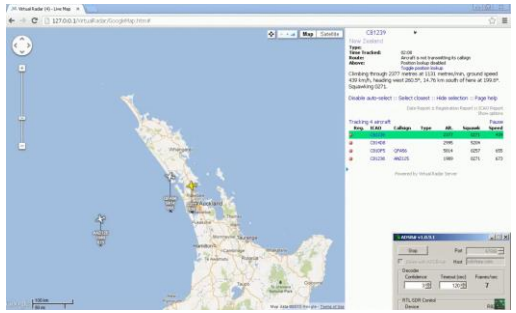
Some Concrete Examples of what you can do with an SDR

Stereo FM with RDS
Radio transmitter

Replay Attack Analysis on
Food-Pagers

TMC Security Analysis

All-you-can-eat
Security Analysis

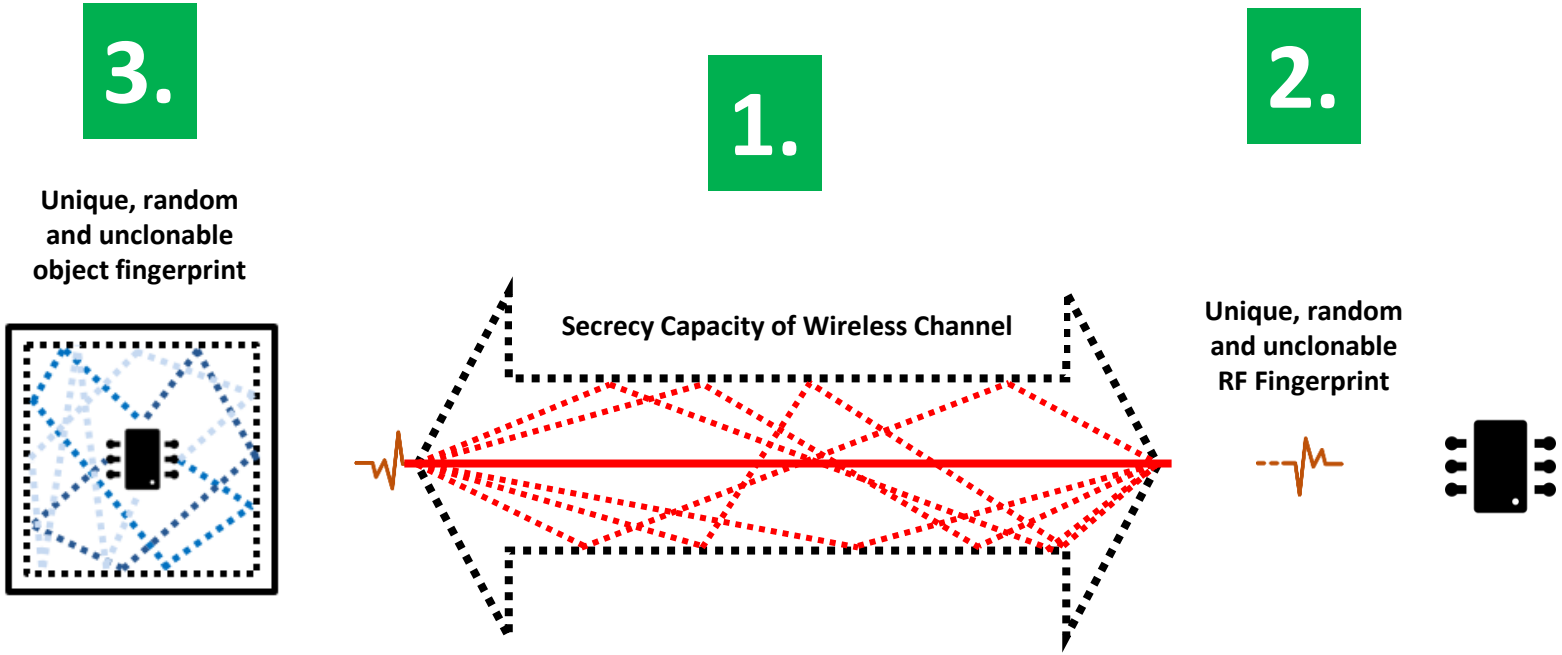


Building a Cheap ADS-B
Aircraft RADAR (ADS-B)

[1] Balint Seeber, "Hacking the wireless World with SDR – 2.0"
[2] https://kasper-oswald.de/forschung/kontaktlose-smartcards/
[3] https://www.rtl-sdr.com/adsb-aircraft-radar-with-rtl-sdr/

Physical-Layer Security…

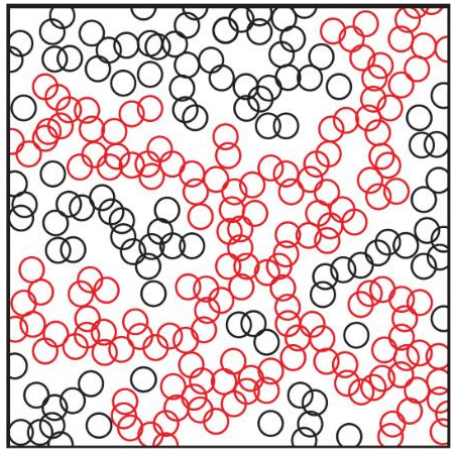
- … as countermeasure against advanced wireless attackers



The New Security Paradigm for the Internet of Things

IoT Goes Nuclear: Creating a ZigBee Chain Reaction [1]

- Goal:
  - worm that can automatically spread in a chain reaction
- Requirements:
  - Persistence of code execution on a lightbulb.
  - Lateral movement
- Why did this work?
  - single symmetric encryption key
  - Hardware vulnerable to side-channel analysis
  - Errors in the implementation
- What else could they do?
  - Bricking attack (irreversible)
  - Wireless network jamming (DoS)
  - Epileptic seizures



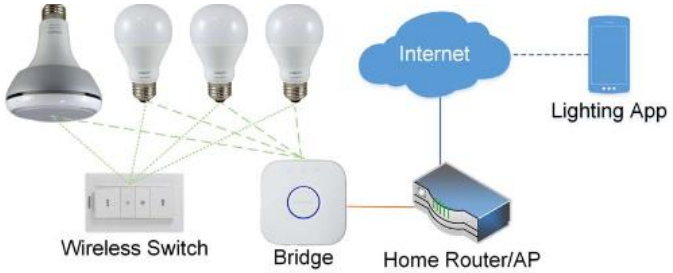


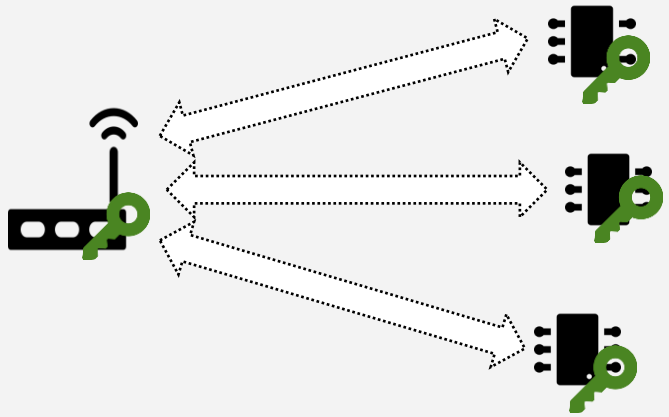
Figure 2. The ZLL architecture.

Figure 3. Philips Hue bridge (gateway), lamps, and wireless switch.

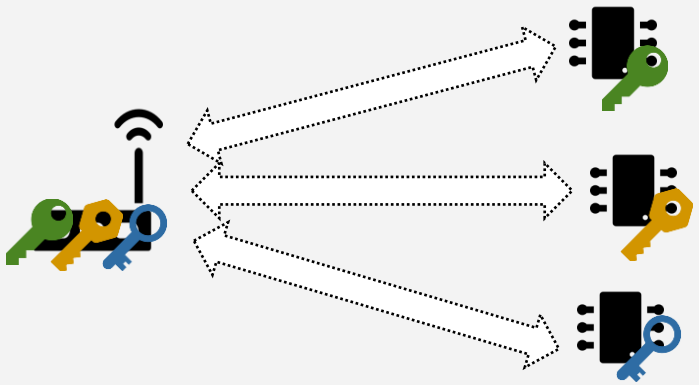
[1] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7958578

Key Distribution with WPLS

1. Initially: Devices use the same key



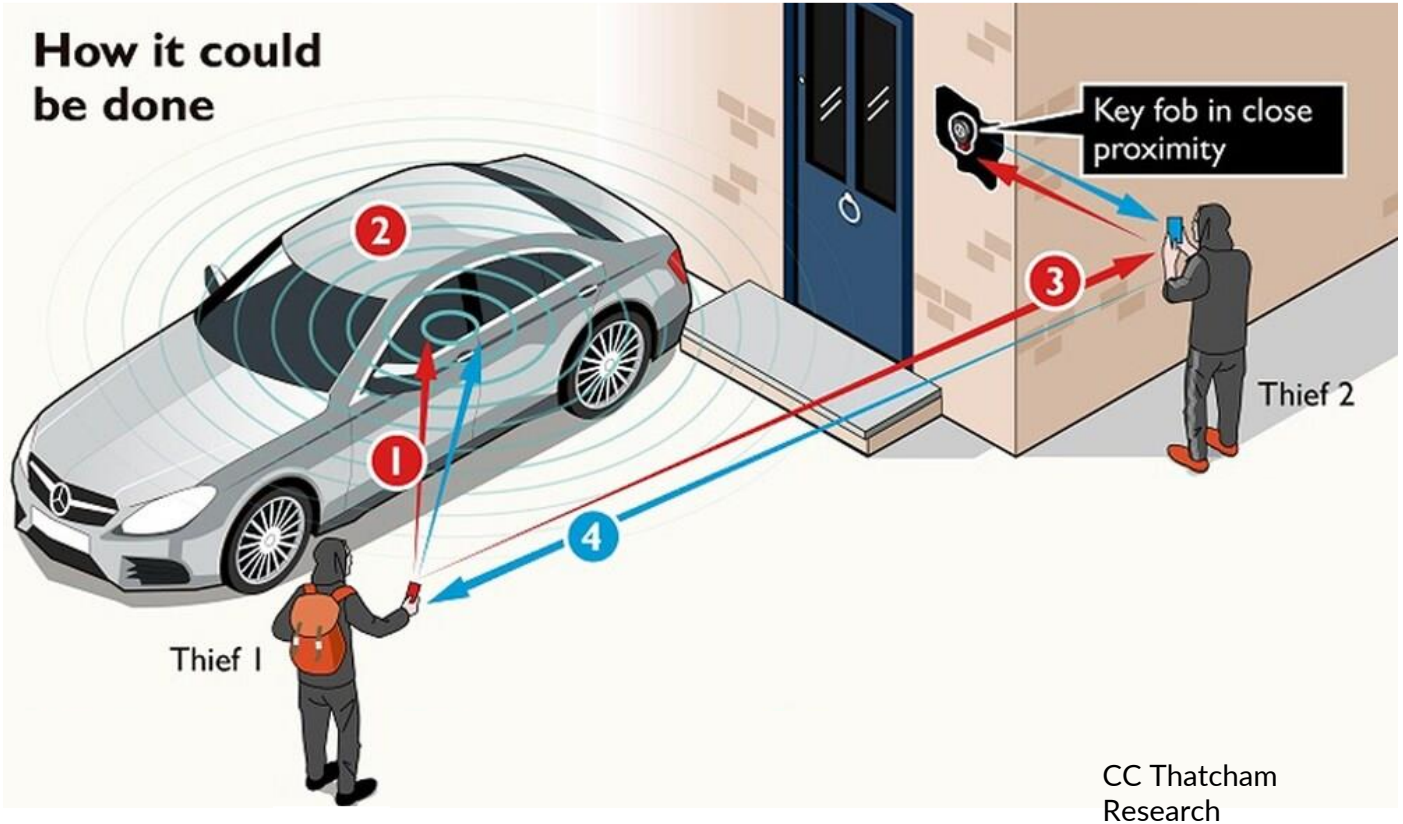
Later: Keys fully differentiated



- Manufacturers often use a single master key for encryption
  - Simplicity for user and integrator
  - Low-cost solution
- WPLS-based technology allows to continuously diversify keys in the field
  - Software-only solution
- Short-lived keys eliminate security hardware
  - Attacks on keys less attractive
  - Attacks less effective

Trending Topics: Relay Attack on Keyless Go

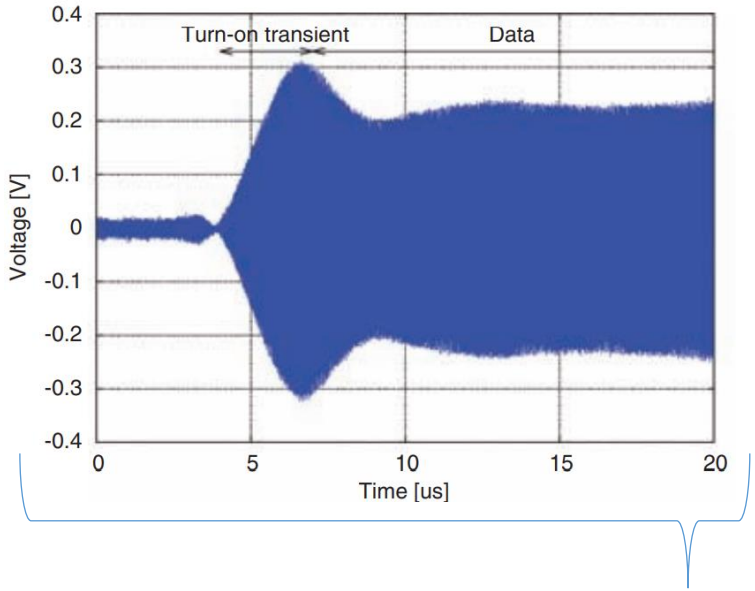
1. Thief waits for the car to send an inquiry for the key.
2. Car releases signals asking for the key fob to authenticate the driver.
3. Thief I relays that inquiry signal to Thief 2.
4. Thief 2 transmits the signal to the key, which in turn answers directly to the car, or gets transmitted via the signal relay.

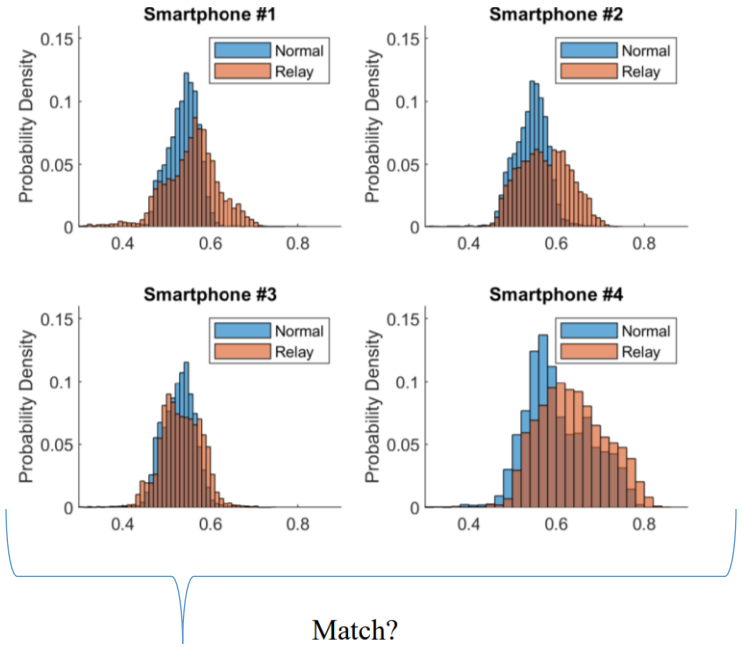


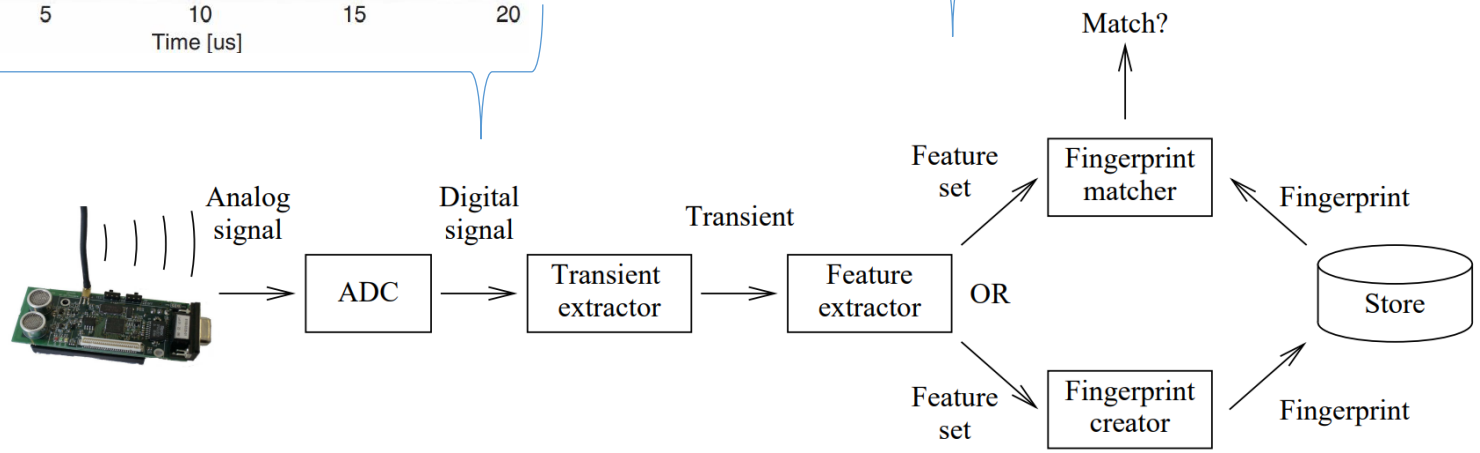
CC Thatcham Research

RF Fingerprinting

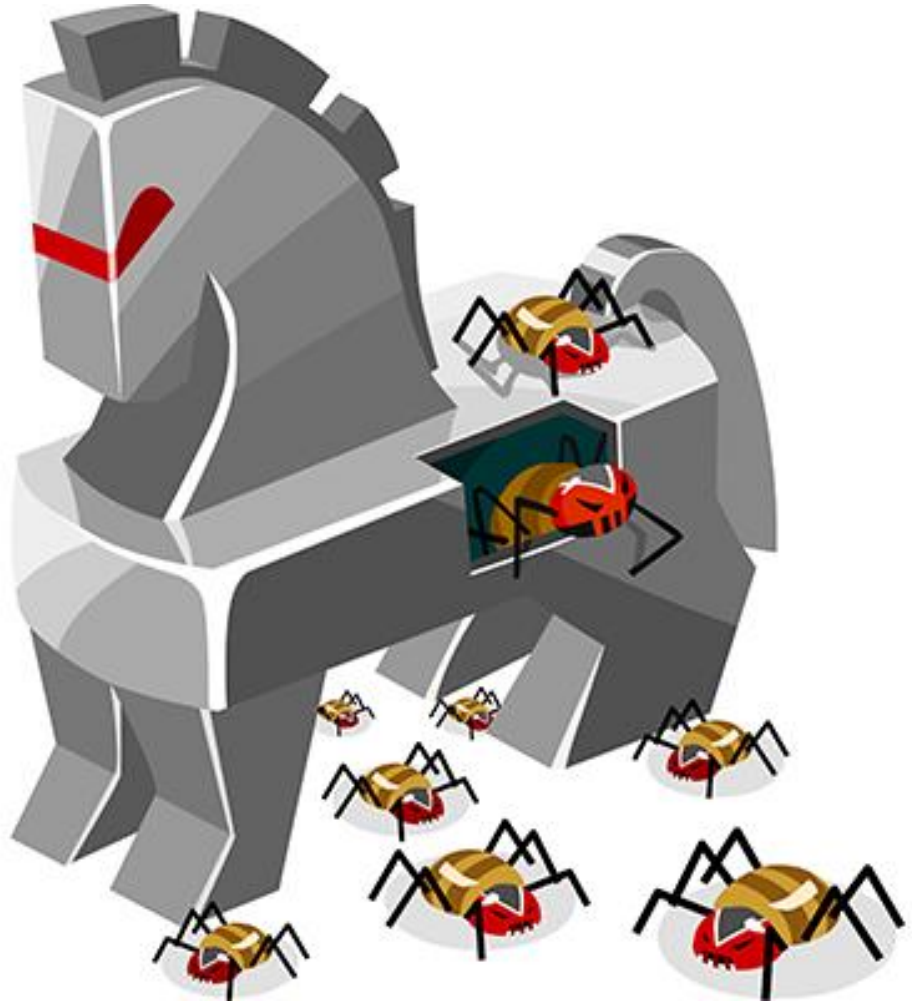
2.

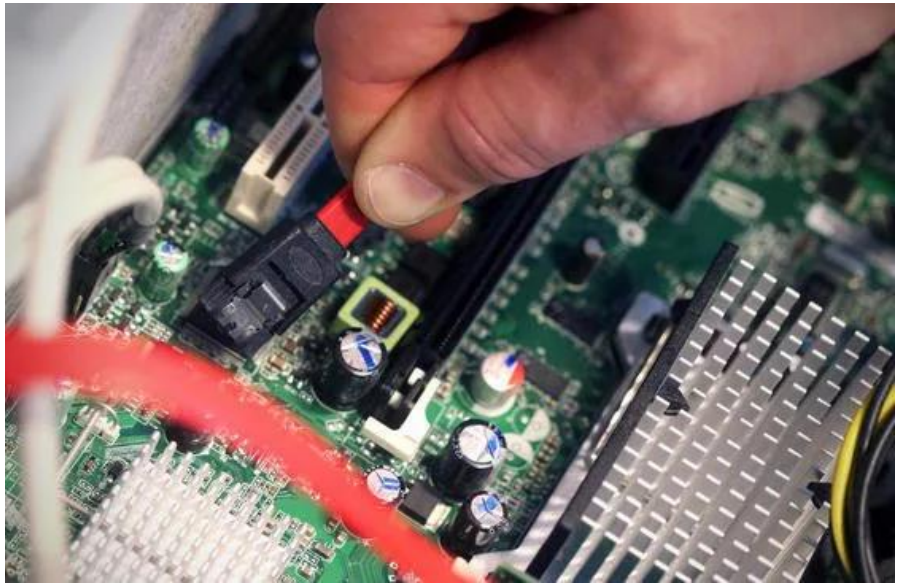


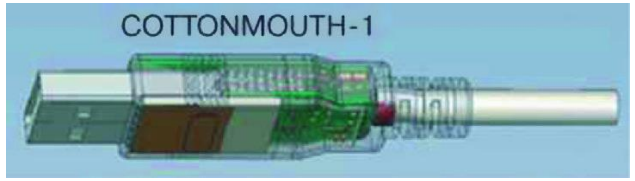




Hardware Trojans and Manipulations



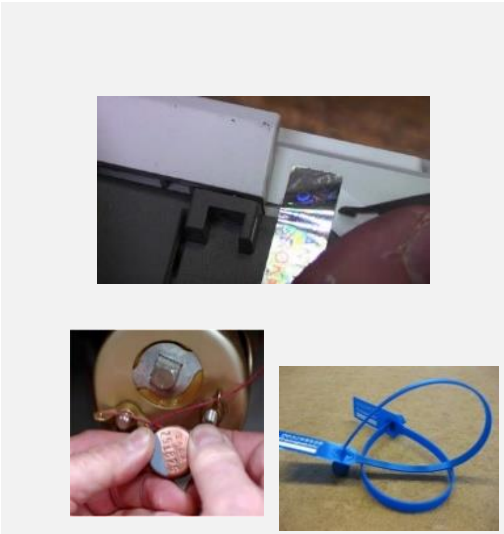


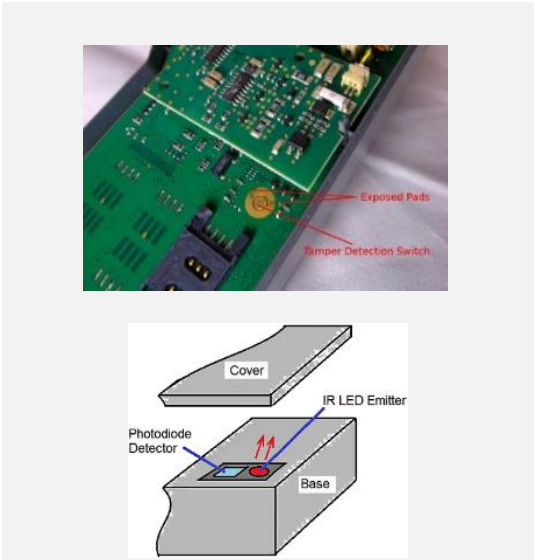


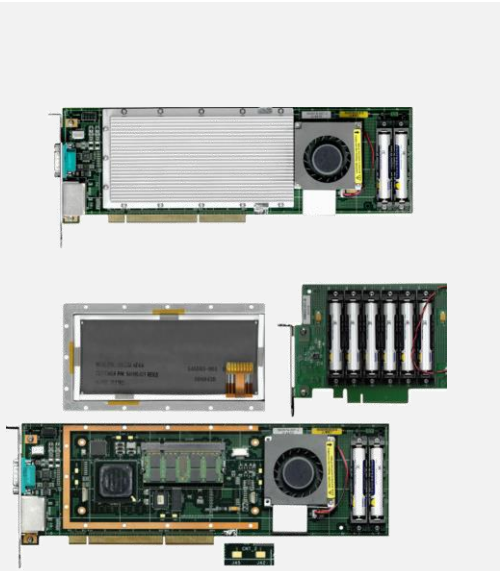
Hardware Trojaner in USB-Stecker
(NSA)

Trending Topics: Physical Integrity Assessment

- Four different approaches of Tamper Resilience exist:
  1. Tamper Resistance: Tamper is made difficult
  2. Tamper Evidence: Intrusion (attempts) must be evident
  3. Tamper Detection: The user is notified about tamper attacks
  4. Tamper Responsiveness: Countermeasures are engaged when tamper occurs



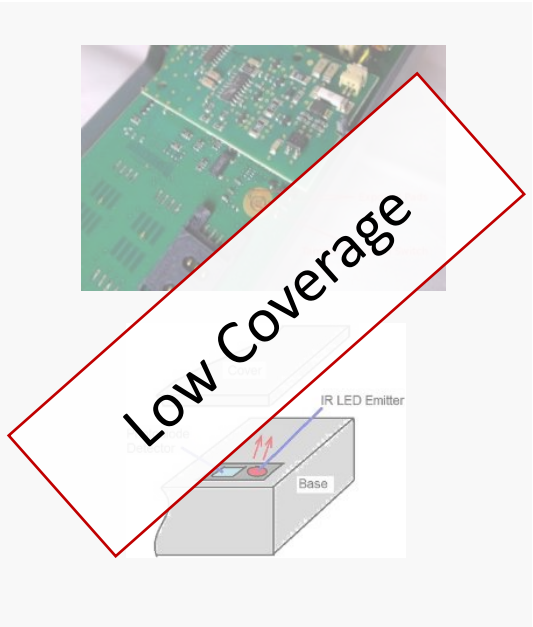


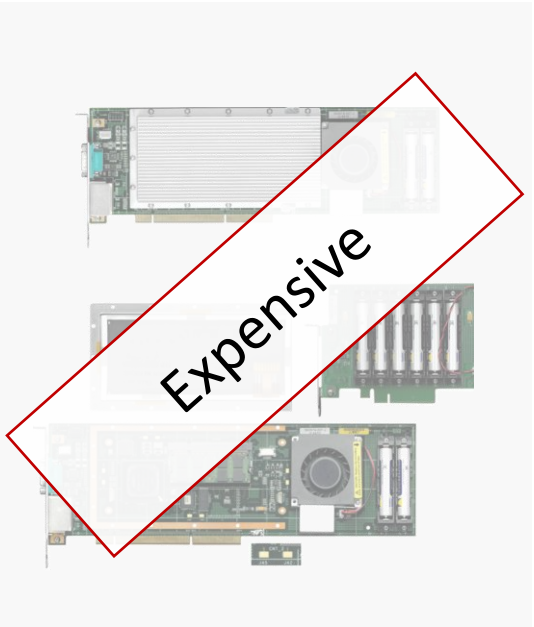


Trending Topics: Physical Integrity Assessment

- Four different approaches of Tamper Resilience exist:
  1. Tamper Resistance: Tamper is made difficult
  2. Tamper Evidence: Intrusion (attempts) must be evident
  3. Tamper Detection: The user is notified about tamper attacks
  4. Tamper Responsiveness: Countermeasures are engaged when tamper occurs
  5. Enclosure-PUF

And WPLS-based Countermeasures

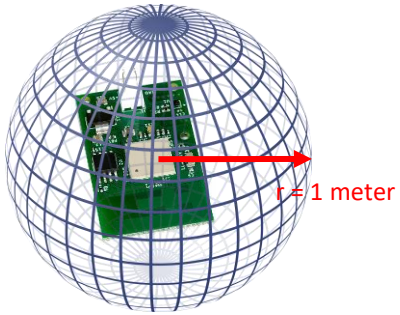




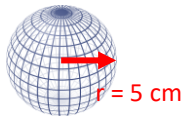
Anti Tamper Radio

3.

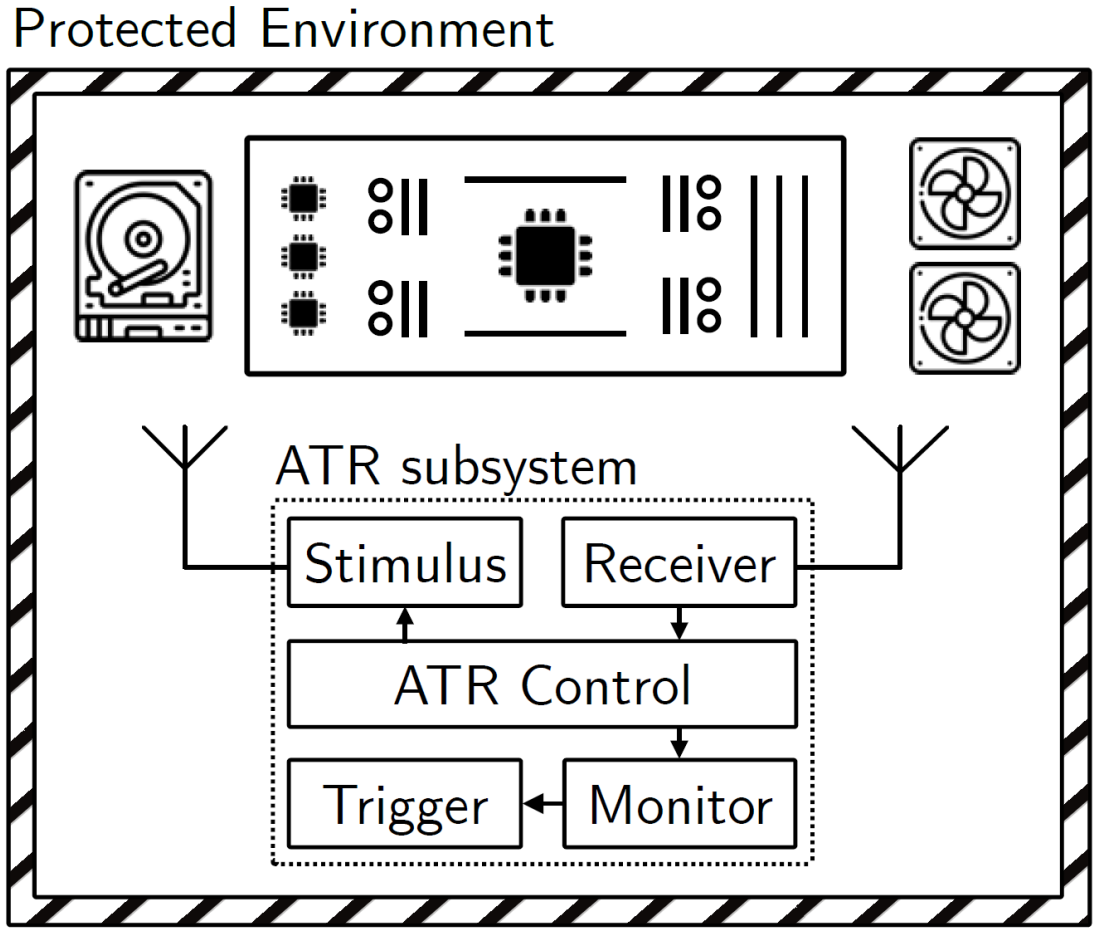
- Anti Tamper Radio
  - Ubiquitous and scalable sensor
  - Millimeter accuracy through radar technology
  - Multipurpose sensor through software defined tuning
  - Low power and advanced power management
  - Small size/PCB footprint:
  - Ease of integration (component like accelerometer)



Perimeter equivalent security
Δc = 1mm Changes

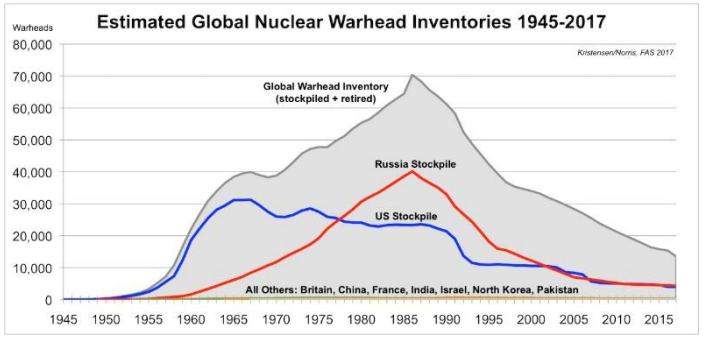


High security
(FIP140 Level 4)
Δc = 60µm Changes

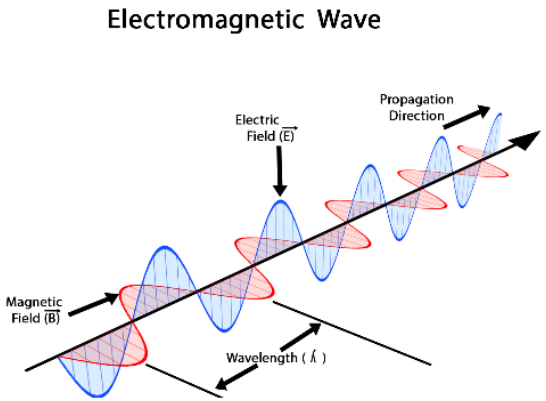


Trending Topics: Virtual Proof of Reality

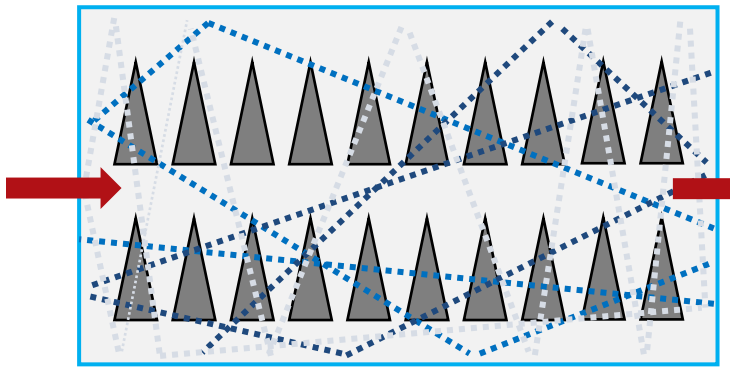
3.



Proving physical statements remotely without using classical tamper-resistant hardware and cryptographic keys.

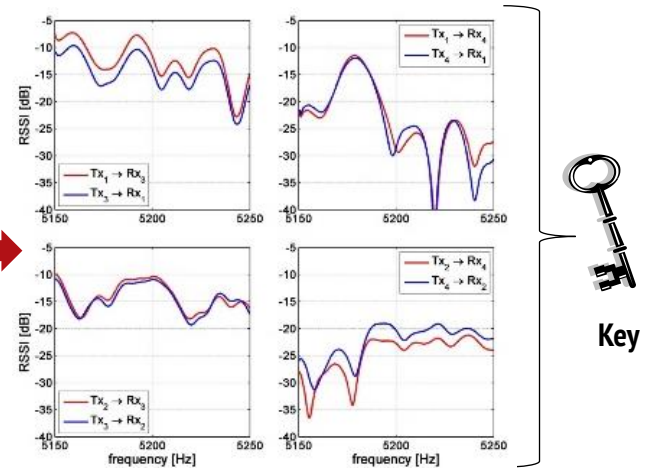


Challenges C_i



Physical Unclonable Function

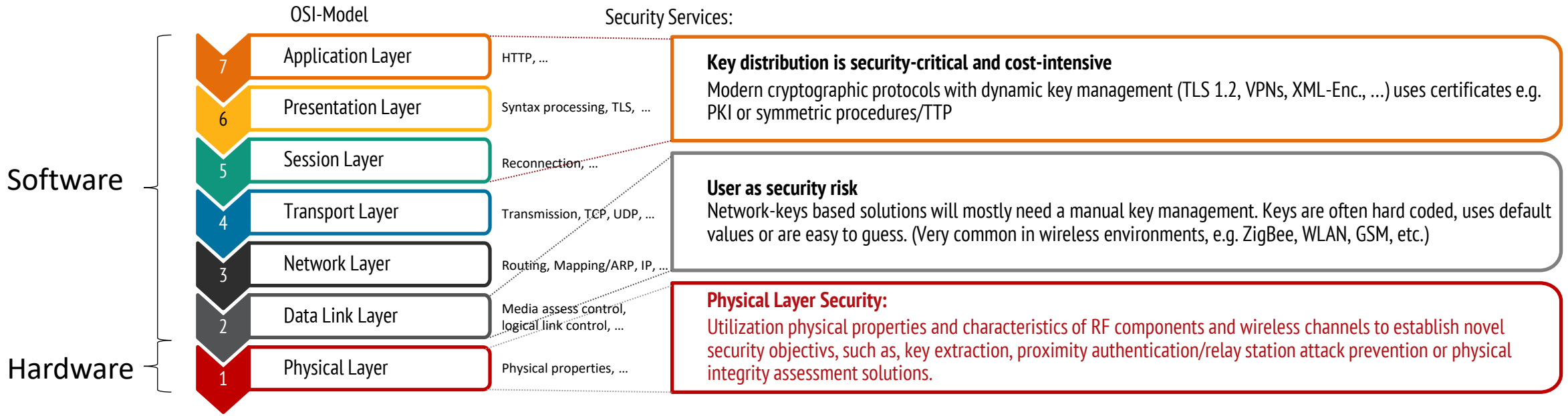
$R_i = PUF(C_i)$



Responses R_i (≈Fingerprint)

Open System Interconnection (OSI) Model

- None of the other layers work without the **physical layer (PL)**
- PL defines transmission and receiving hardware (physical machines)
- PL encodes bits into a physical signal (and vice versa)
- Physical link (cable or wireless)
  - Electromagnetic wave (travels with speed of light)
  - Sound, vibrations, pneumatics, …

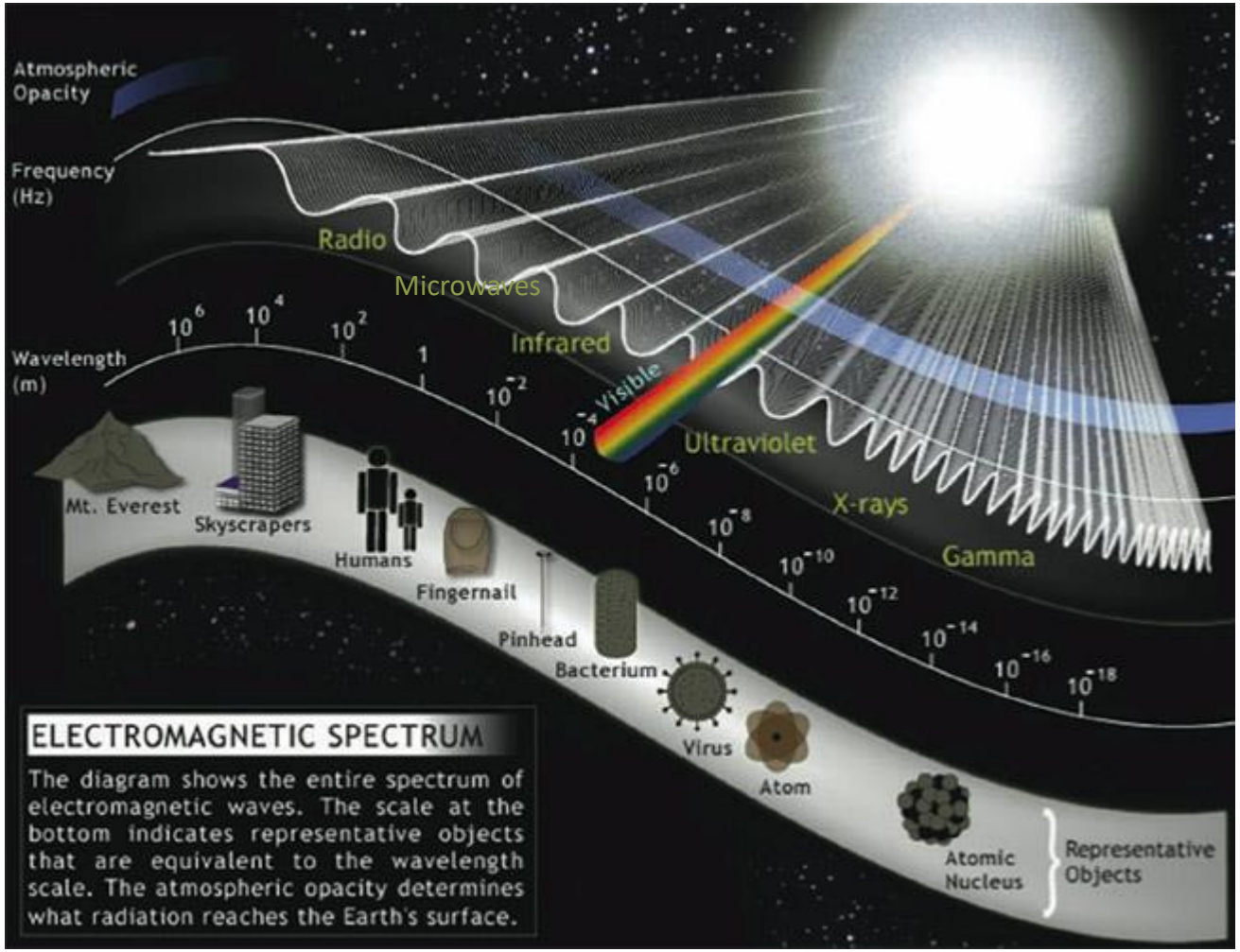


Some Basics

or

How to open garage doors?

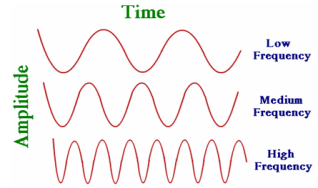
Electromagnetic Spectrum (many types of radiation)



https://www.windows2universe.org/sun/spectrum/multispectral_sun_overview.html

What we see as light is only a small part of the EM spectrum.

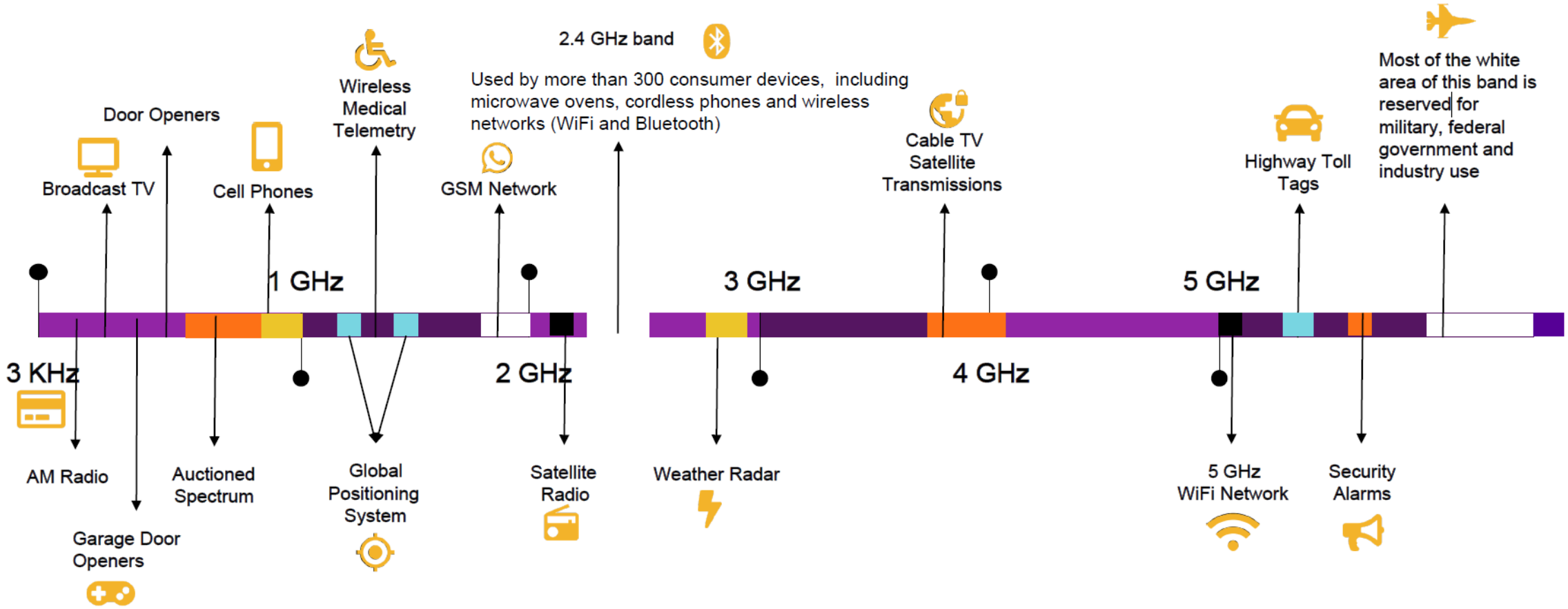
EM radiation travels in waves. Frequency describes how many waves per second a wavelength produces. Wavelength measures the length of an individual wave in meters.



Scientists describe the EM spectrum as a long line. At one end with radio waves with longest wavelength and lowest frequencies in the spectrum.

- Radio waves (football field size)
- **Microwaves**
- Infrared light
- Visible light
- X-Ray
- Gamma Rays (atom nuclei size)

Inside the radio wave spectrum?

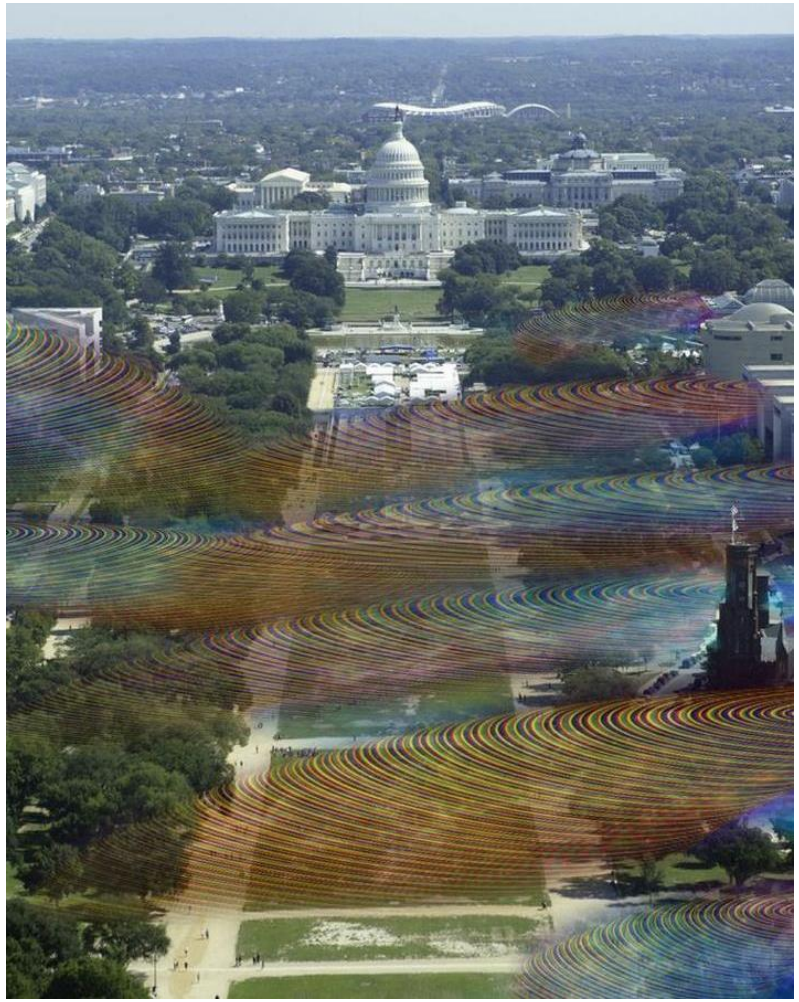


Mehta et al., RF Exploitation: IoT/OT Hacking with SDR, RSA Conference 2019

microwaves

Motivation

We are surrounded by wireless signals almost every second



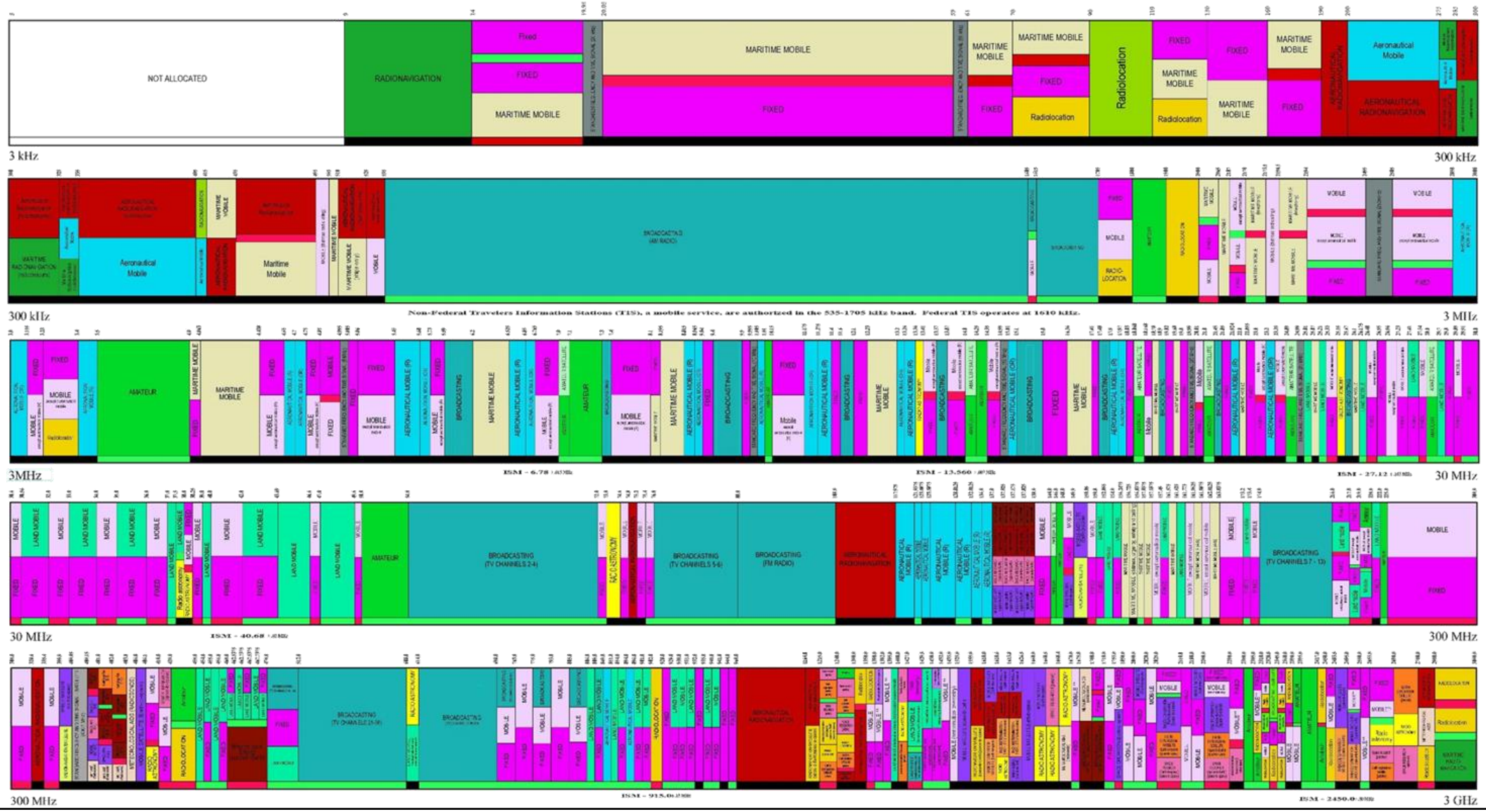
Images: Nickolay Lamm

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

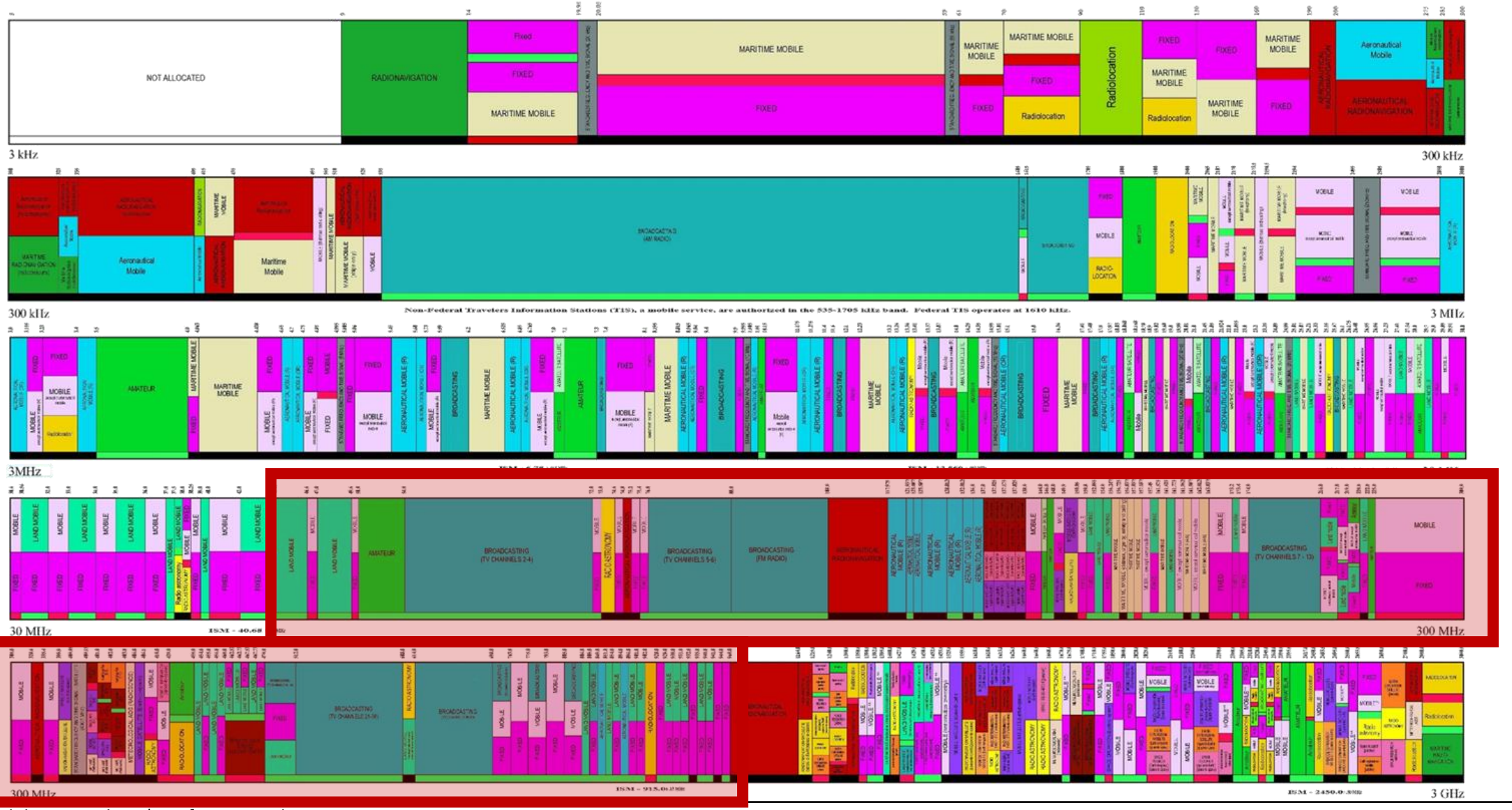
[Frequency Allocations – WiKi]

Radio Spectrum

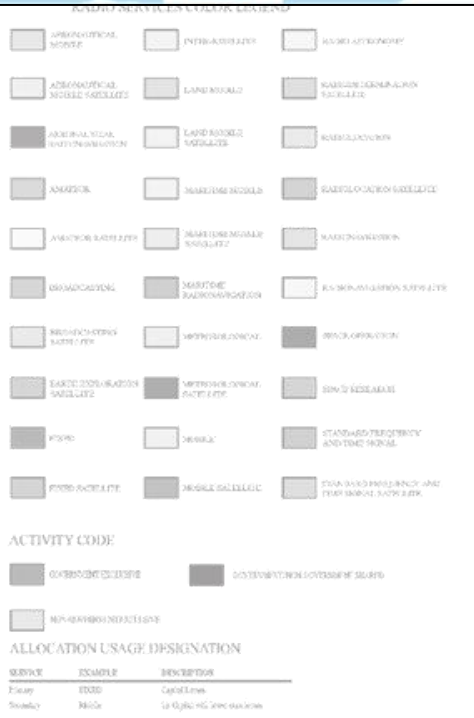


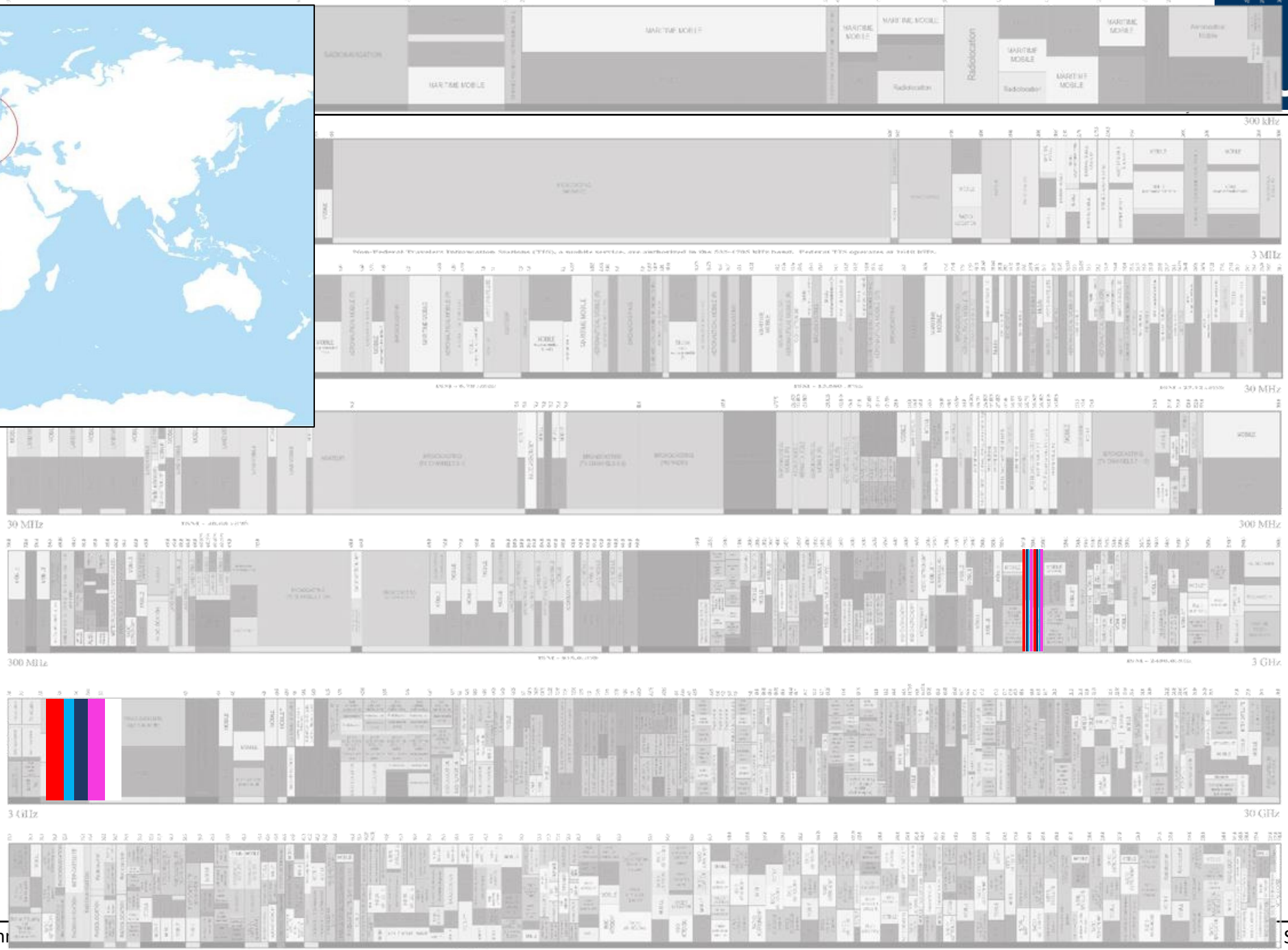
[Frequency Allocations – WiKi]

Radio Spectrum



[Frequency Allocations – WiKi]





[Frequency Allocations – WiKi]

Motivation 5G

In 2019 the German Bundesnetzagentur has put up exclusive right of frequency usage to auction:

Company	Bandwidth		Costs
1und1 Drillisch	2000 MHz 3600 MHz	4x 5 MHz 5x 10 MHz	???
O2 Telefónica	2000 MHz 3600 MHz	4x 5 MHz 7x 10 MHz	???
Vodafone	2000 MHz 3600 MHz	8x 5 MHz 7x 10 MHz + 20 MHz	???
Dt. Telekom	2000 MHz 3600 MHz	8x 5 MHz 9x 10 MHz	???
Total	**420 MHz**		**???**

497 auction rounds

Motivation 5G

In 2019 the German Bundesnetzagentur has put up exclusive right of frequency usage to auction:

Company	Bandwidth		Costs
1und1 Drillisch	2000 MHz 3600 MHz	4x 5 MHz 5x 10 MHz	1.070.187.000
O2 Telefónica	2000 MHz 3600 MHz	4x 5 MHz 7x 10 MHz	1.424.832.000
Vodafone	2000 MHz 3600 MHz	8x 5 MHz 7x 10 MHz + 20 MHz	1.879.689.000
Dt. Telekom	2000 MHz 3600 MHz	8x 5 MHz 9x 10 MHz	2.174.943.000
Total	**420 MHz**		**6.549.651.000**

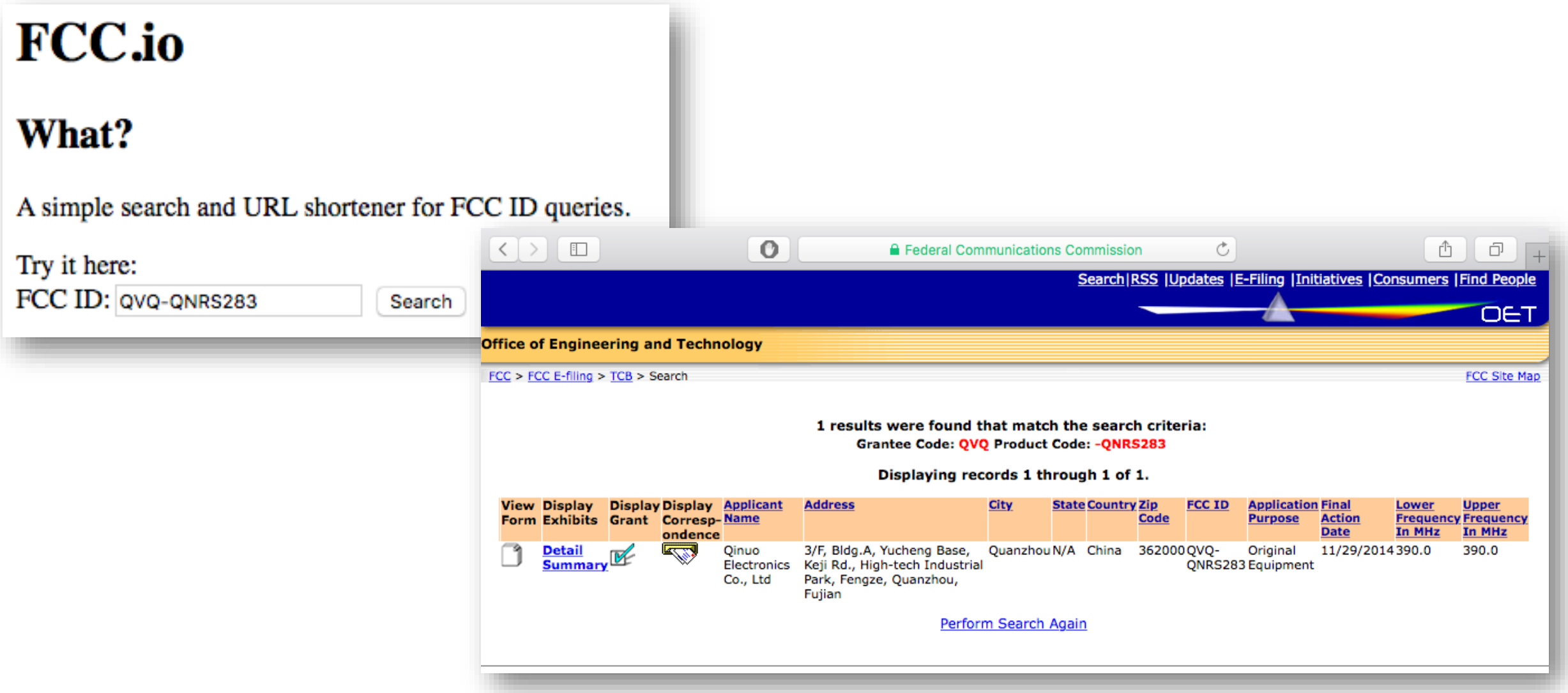
497 auction rounds
Costs/MHz: 15.594.407 €

FCC IDs

FCC ID - What is this?

- Unique number, that identifies every device capable of wireless communication
- Gain information about the device by using **FCC.io**
- US devices only
  - Most devices are sold worldwide

FCC IDs


FCC.io
What?
A simple search and URL shortener for FCC ID queries.
Try it here:
FCC ID: QVQ-QNRS283
Search
Federal Communications Commission
Search | RSS | Updates | E-Filing | Initiatives | Consumers | Find People
OET
Office of Engineering and Technology
FCC > FCC E-filing > TCB > Search
FCC Site Map
1 results were found that match the search criteria:
Grantee Code: QVQ Product Code: -QNRS283
Displaying records 1 through 1 of 1.
View Form
Display Exhibits
Display Grant
Display Correspondence
Applicant Name
Address
City
State
Country
Zip Code
FCC ID
Application Purpose
Final Action Date
Lower Frequency In MHz
Upper Frequency In MHz
Detail Summary
Qinuo Electronics Co., Ltd
3/F, Bldg.A, Yucheng Base, Keji Rd., High-tech Industrial Park, Fengze, Quanzhou, Fujian
Quanzhou
N/A
China
362000
QVQ-QNRS283
Original Equipment
11/29/2014
390.0
390.0
Perform Search Again

FCC IDs

OET Exhibits List

8 Matches found for FCC ID QVQ-QNRS283

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Cover letter	Cover Letter(s)	11/29/2014	pdf	11/29/2014
Cover letter	Cover Letter(s)	11/29/2014	pdf	11/29/2014
External photos	External Photos	11/29/2014	pdf	11/29/2014
Label	ID Label/Location Info	11/29/2014	pdf	11/29/2014
Internal photos	Internal Photos	11/29/2014	pdf	11/29/2014
Test report	Test Report	11/29/2014	pdf	11/29/2014
Test setup	Test Setup Photos	11/29/2014	pdf	11/29/2014
User manual	Users Manual	11/29/2014	pdf	11/29/2014

Instruction Manual of QN-RS283

---to Compatible with original Genie Remote

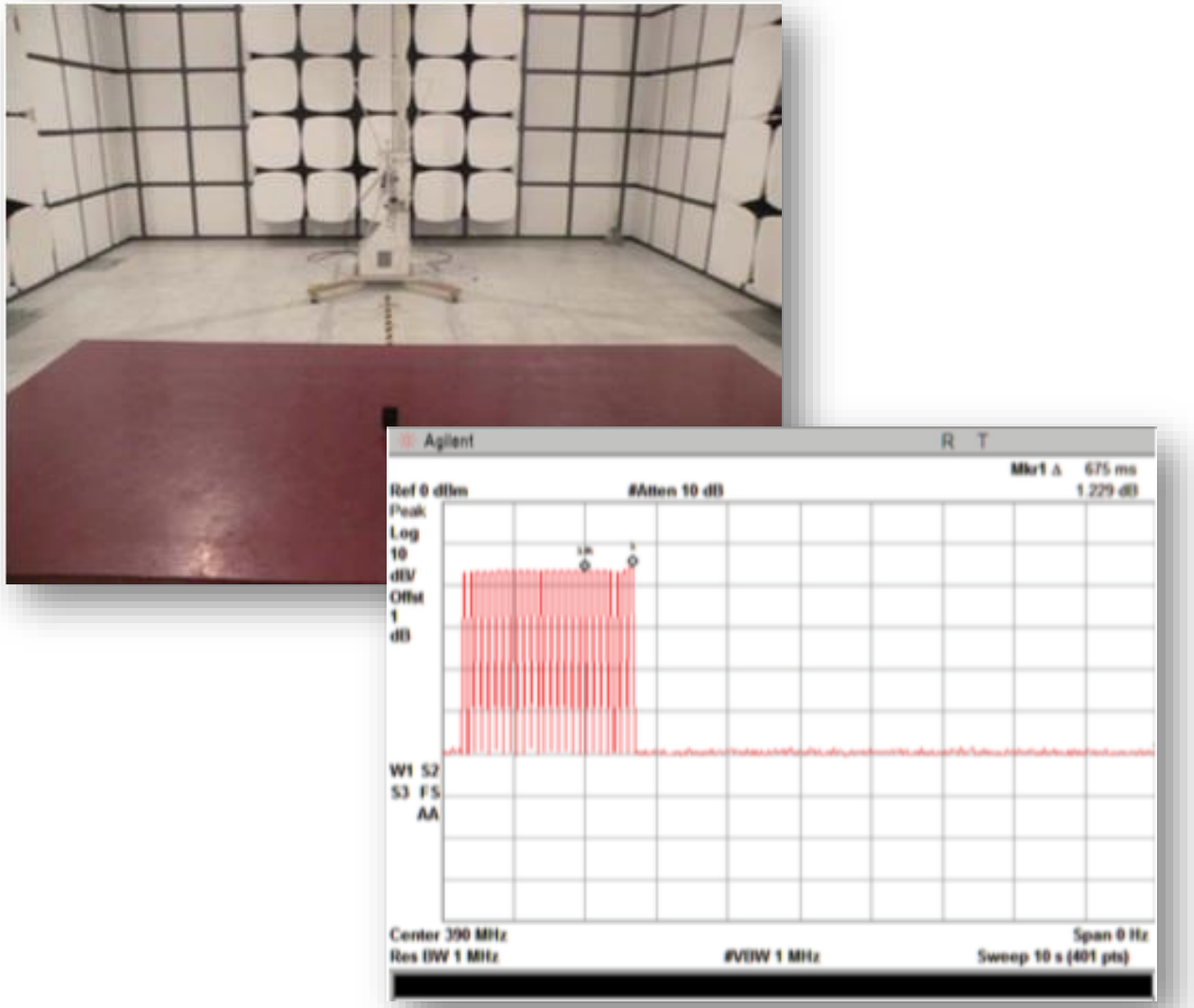
Introduction of original Genie remote and compatible remote control

FCC IDs

1 General Information

1.1 Description of Device (EUT)

Trade Name	:	Ucontrol
EUT	:	Rolling Code Remote Control to C Remote
Model No.	:	QN-RS283
Type of Antenna	:	PCB antenna, Max Gain 0dBi.
Operation Frequency	:	390 MHz
Channel number	:	1
Modulation type	:	ASK
Power Supply	:	DC 3V Supply by battery



RTL-SDR and Hack RF

- 1 MHz – 6 GHz
- Half-duplex transceiver
- Raw I/Q samples
- Open software / hardware
- GNU Radio, SDR# and more

- 24 MHz –1766 MHz
- Raw I/Q samples
- Receive only
- RTL2832U – Realtek Chip

Hack RF Replay Attacks

Hack RF can receive **and** send signals!

- **hackrf_transfer -r 390_data.raw -f 390000000 # listen**
- **hackrf_transfer -t 390_data.raw -f 390000000 # transmit**
- No modulation/demodulation needed
- Can be within 20 MHz

Costs: ca 270€

https://greatscottgadgets.com/hackrf/one/

Hack RF Replay Attacks

Hack RF can receive **and** send signals!

- **hackrf_transfer -r 390_data.raw -f 390000000 # listen**
- **hackrf_transfer -t 390_data.raw -f 390000000 # transmit**
- No modulation/demodulation needed
- Can be within 20 MHz

Costs: ca 270€

You can easily receive and send captured Signals -> Simple Replay Attacks possible!

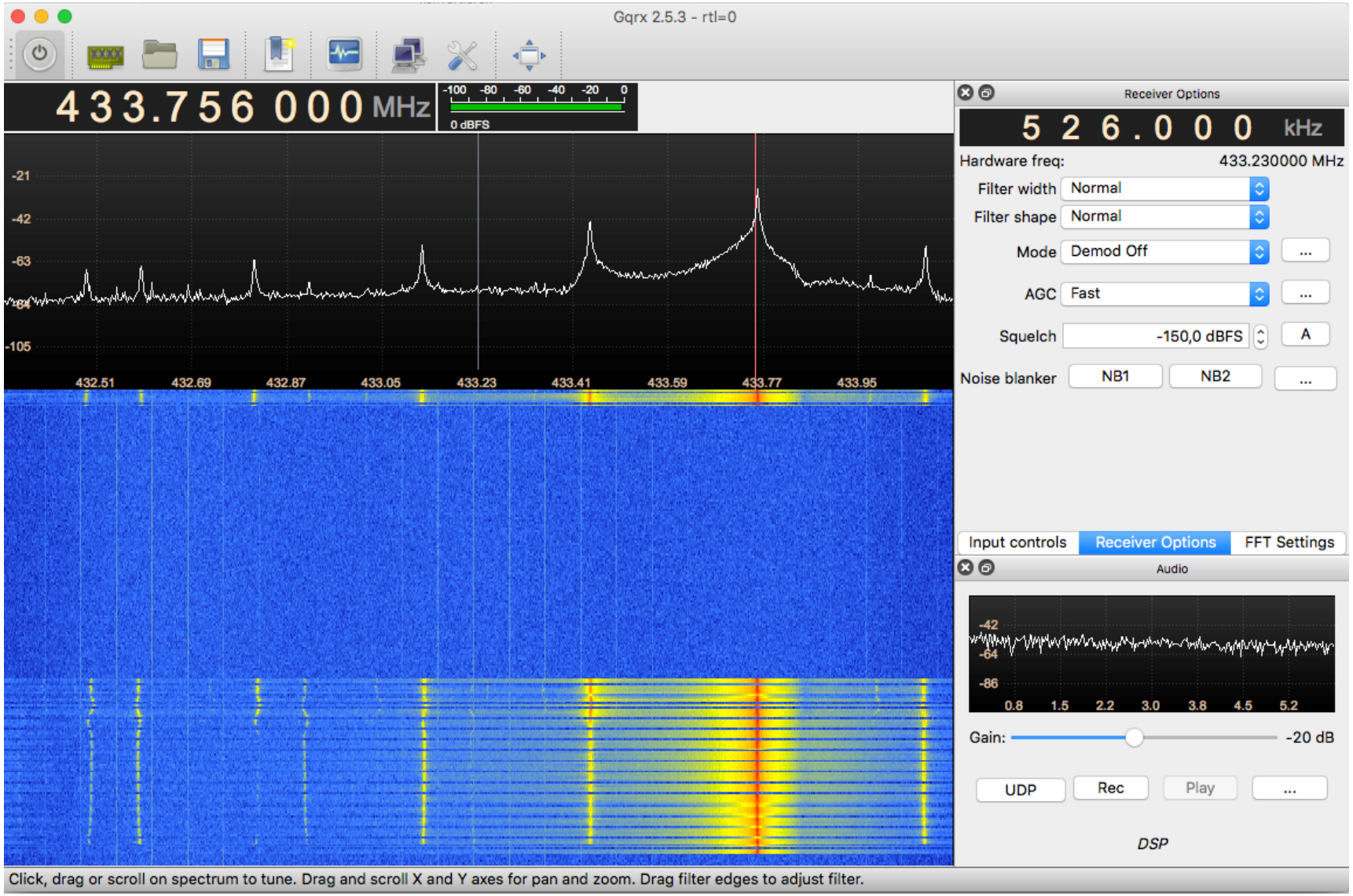
RTL-SDR

RTL-SDR can only receive signals!

- Signal analysis and processing possible
- Huge variety of (mostly free) software

Costs: ca 20€

RTL-SDR: GQRX

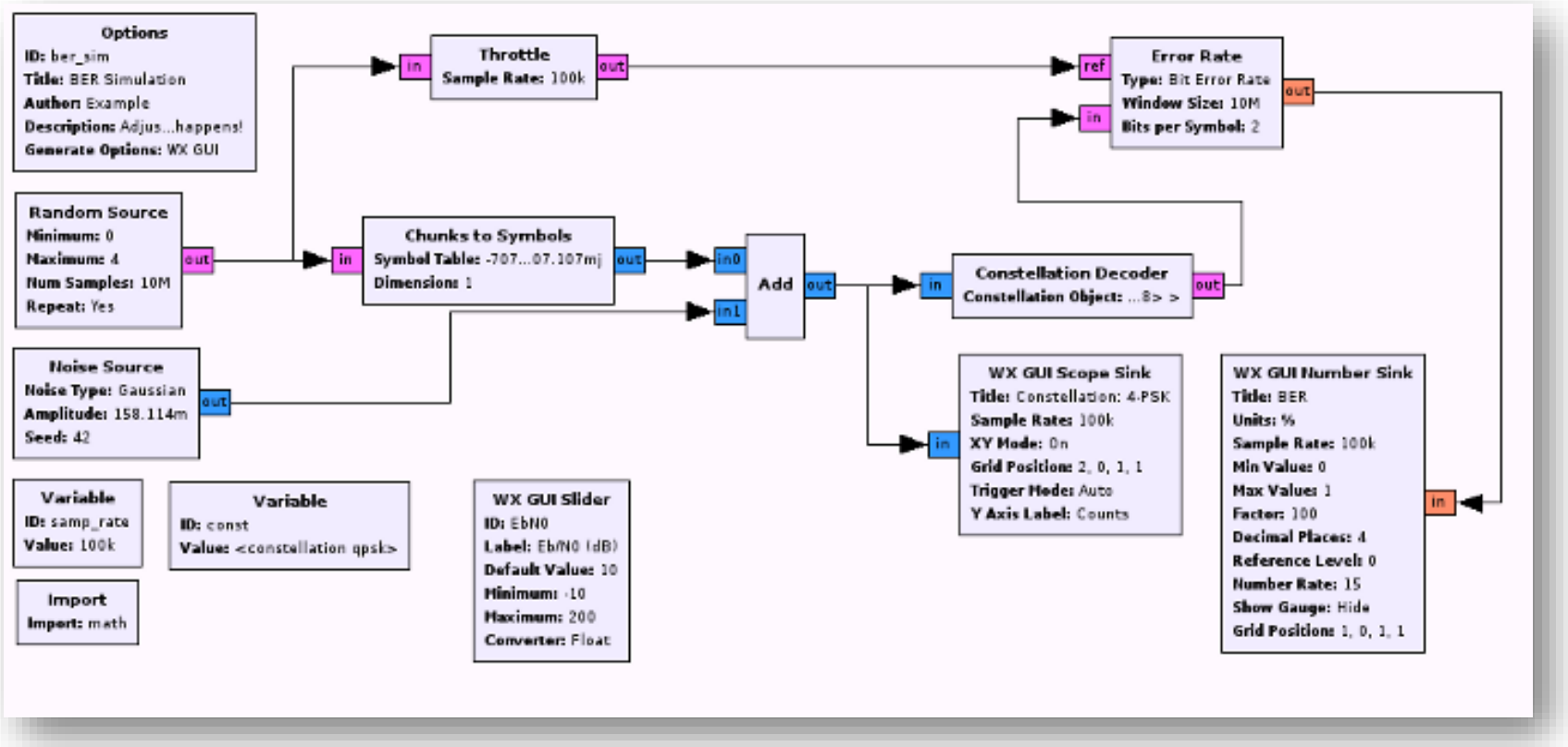


GQRX:

- Waterfall view, demodulation, save to .WAV
- OSX and Linux only

On Windows you might want to use **SDR#**

RTL-SDR: GnuRadio



GnuRadio:

- „Easy“ processing of signals
- Very usefull for modulation / demodulation of signals
- Windows, Linux, OSX

RTL-SDR: rtl_fm

SYNOPSIS

rtl_fm [-f freq] [-options] [filename]

OPTIONS

-f frequency_to_tune_to [Hz]
(use multiple -f for scanning, requires squelch)
(ranges supported, -f 118M:137M:25k)

-s sample_rate (default: 24k)

-d device_index (default: 0)

-g tuner_gain (default: automatic)

-l squelch_level (default: 0/off)

-o oversampling (default: 1, 4 recommended)

-p ppm_error (default: 0)

-E sets lower edge tuning (default: center)

-N enables NBFM mode (default: on)

-W enables WBFM mode (default: off)
(-N -s 170k -o 4 -A fast -r 32k -l 0 -D)

filename
(a '-' dumps samples to stdout)
(omitting the filename also uses stdout)

Rtl_fm:

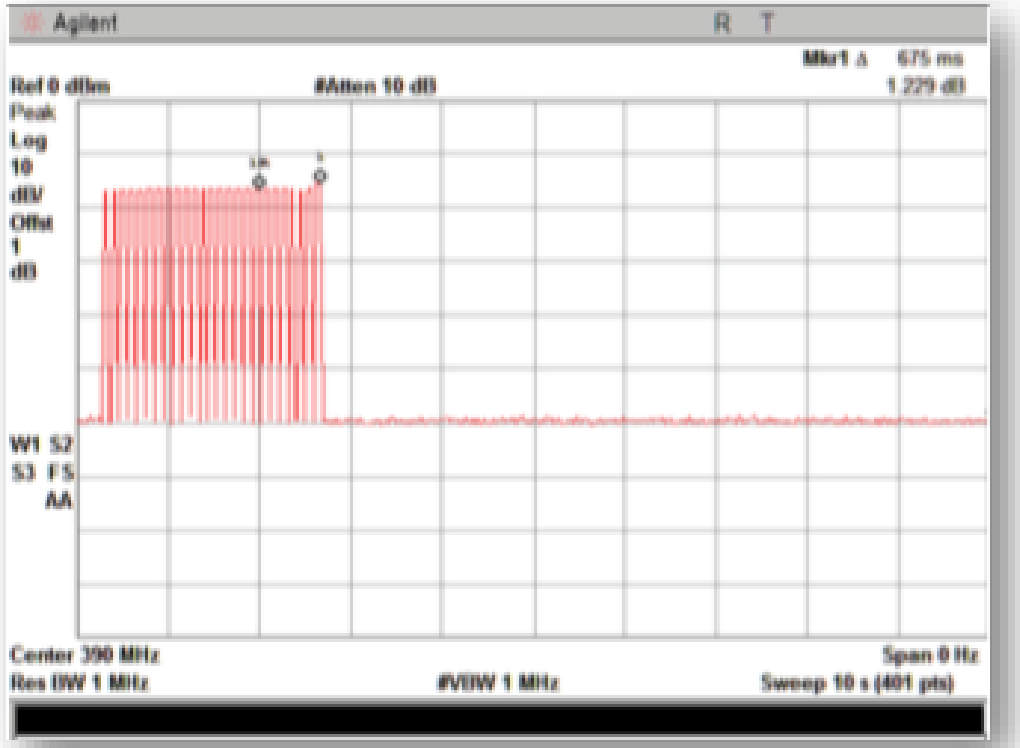
- Terminal based
- Simple
- Demodulation tool
- OSX and Linux only

Test Report

1 General Information

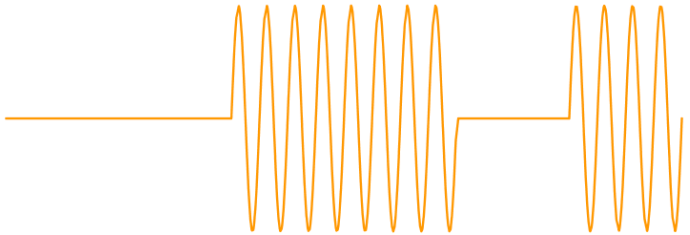
1.1 Description of Device (EUT)

Trade Name	:	Ucontrol
EUT	:	Rolling Code Remote Control to C Remote
Model No.	:	QN-RS283
Type of Antenna	:	PCB antenna, Max Gain 0dBi.
Operation Frequency	:	390 MHz
Channel number	:	1
Modulation type	:	ASK
Power Supply	:	DC 3V Supply by battery

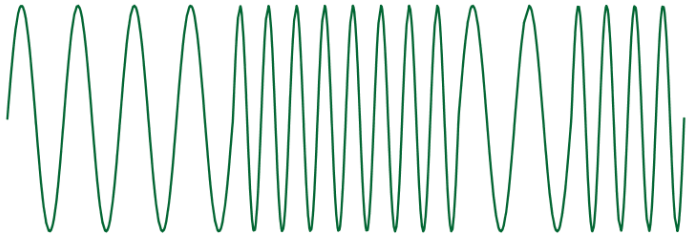


Recap: Modulation Schemes

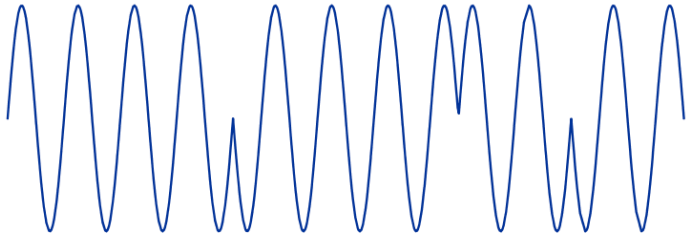
Discrete signal (001101)



ASK – Amplitude-shift keying



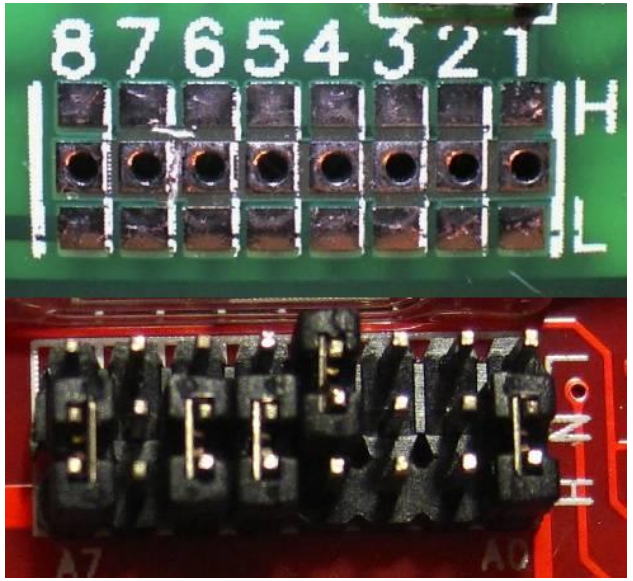
FSK – Frequency-shift keying



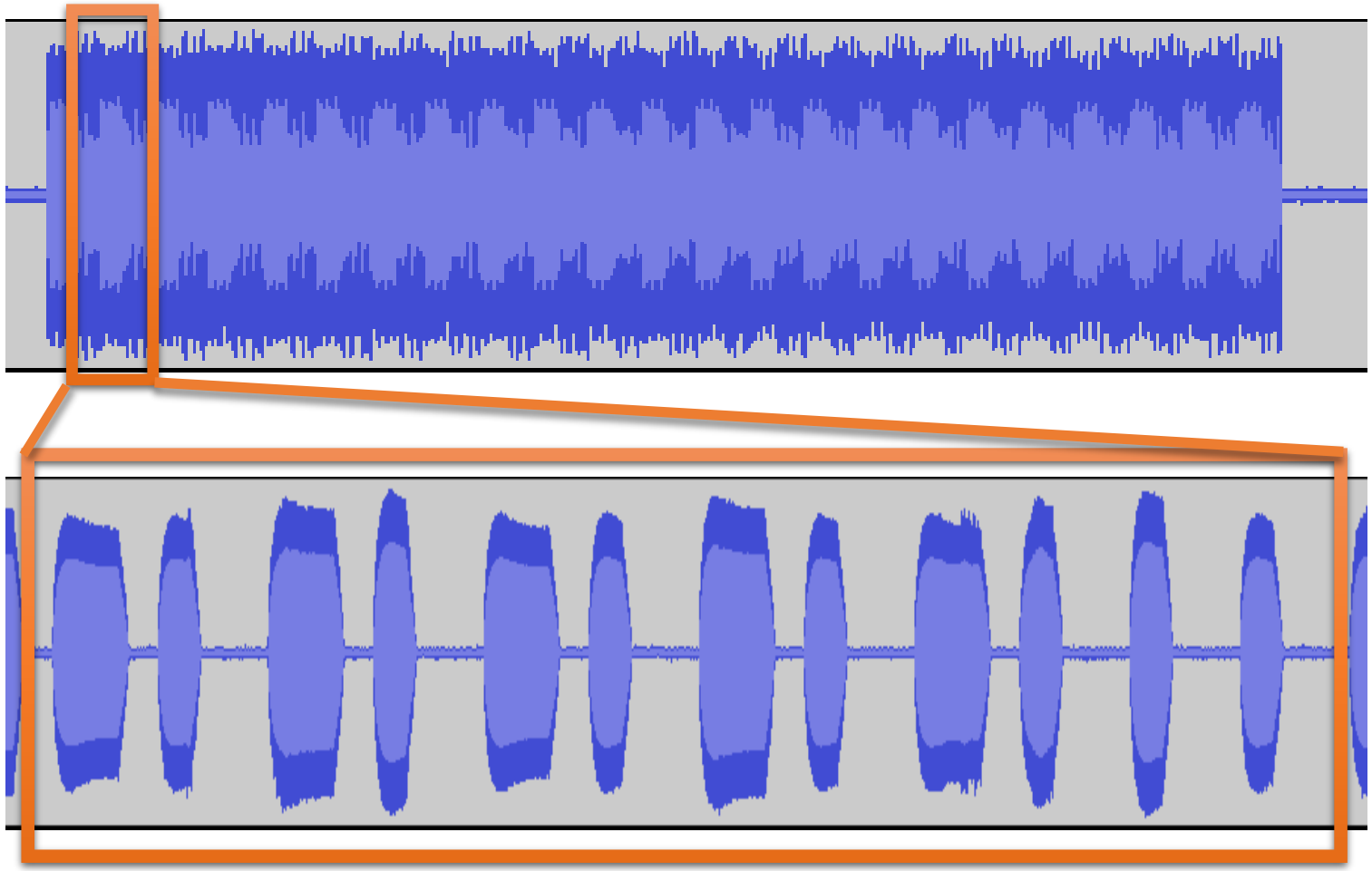
PSK – Phase-shift keying

Brute Force Attack on Fixed Code Garage Doors

8-12 bit code



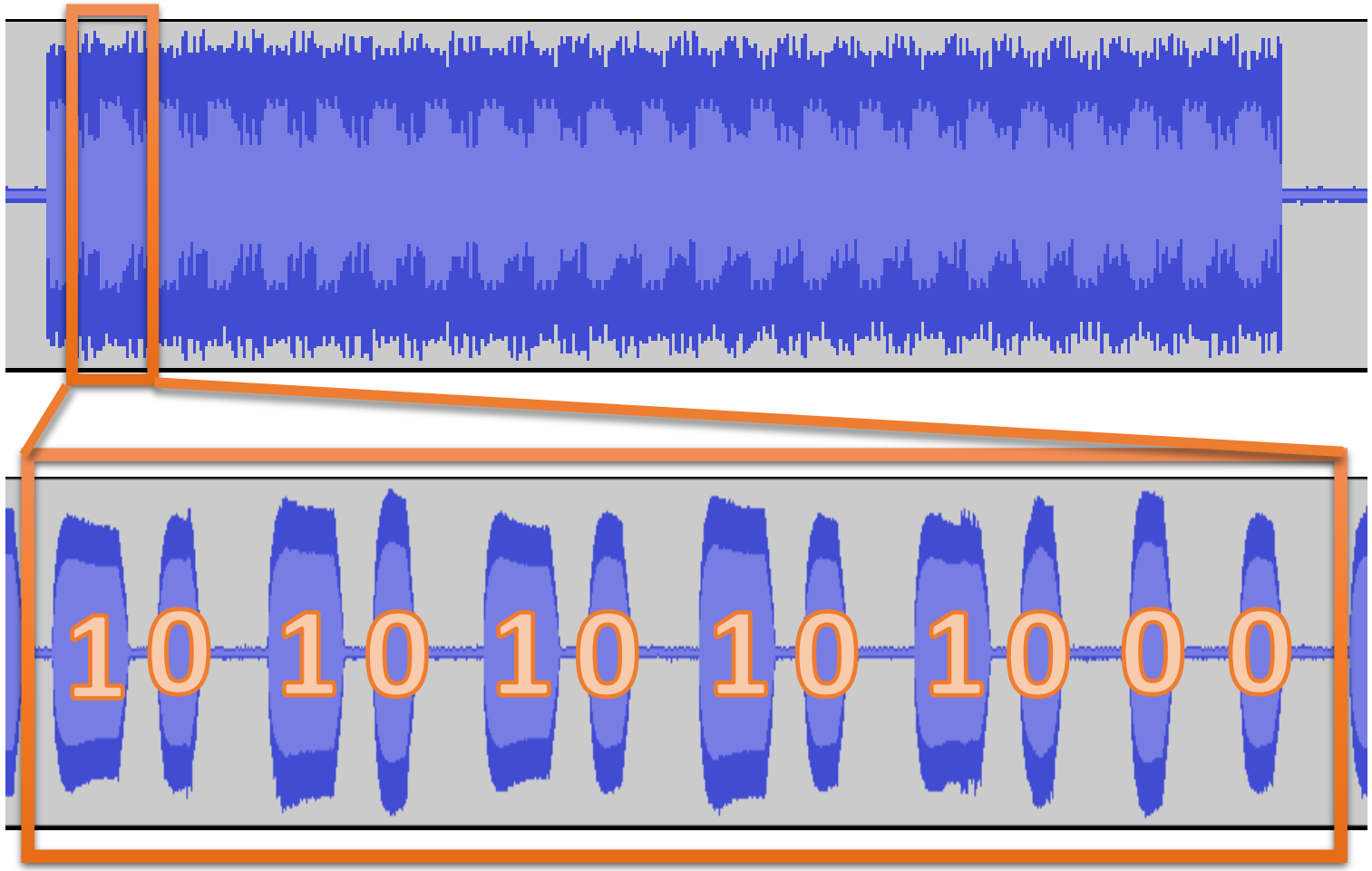
Fixed Code Garage Doors



- 12 Bit Garage door
- Fixed Code is send to open the door
- ASK OOK Modulation

Assumption: We know that this signal tarnsmits the message *101010101000*

Fixed Code Garage Doors



- 12 Bit Garage door
- Fixed Code is send to open the door
- ASK OOK Modulation

Assumption: We know that this signal tarnsmits the message *101010101000*

Brute Force Attack on Fixed Code Garage Doors

8-12 bit code
~2ms per bit + ~2ms delay
5 signals per transmission

$$12 * 2^{12} + 11 * 2^{11} + 10 * 2^{10} + 9 * 2^{9} + 8 * 2^{8} = 88576\ Bits$$

$$88576\ Bits * (2ms\ signal + 2ms\ delay) * 5\ transmissions = 177152 0ms = \mathbf{29.5\ minutes}$$

Brute Force Attack on Fixed Code Garage Doors

8-12 bit code

~2ms per bit + ~2ms delay

5 signals per

$12 * 2^{12} + 1$

$+ 9 * 2^{9} + 8$

$88576\ Bits$

$* (2ms\ signa$

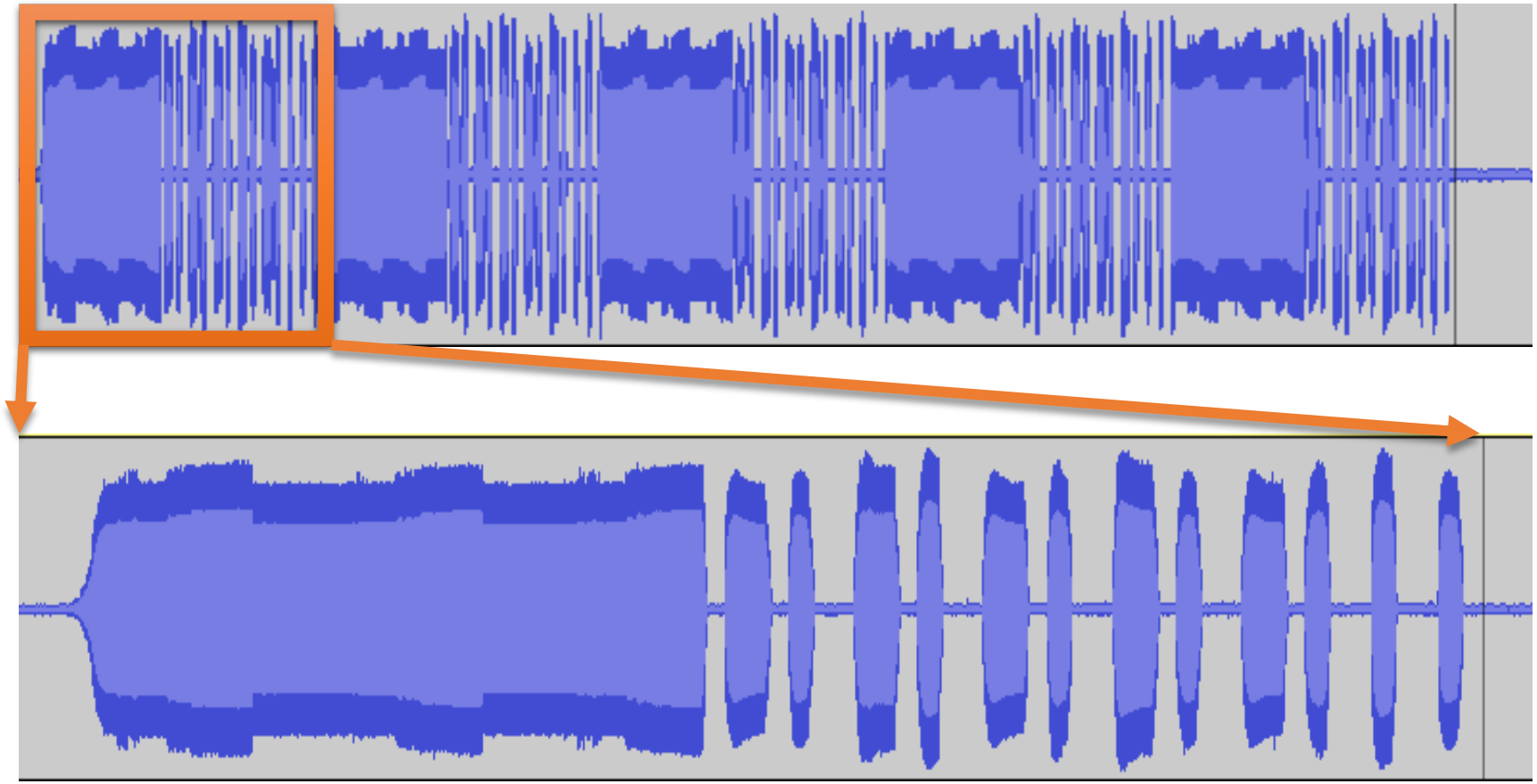
$* 5\ transmissions$

$= 177152 0ms = \mathbf{29.5\ minutes}$

This is an average of 15 minutes to open any fixed code garage door with 8-12 Bit code length!

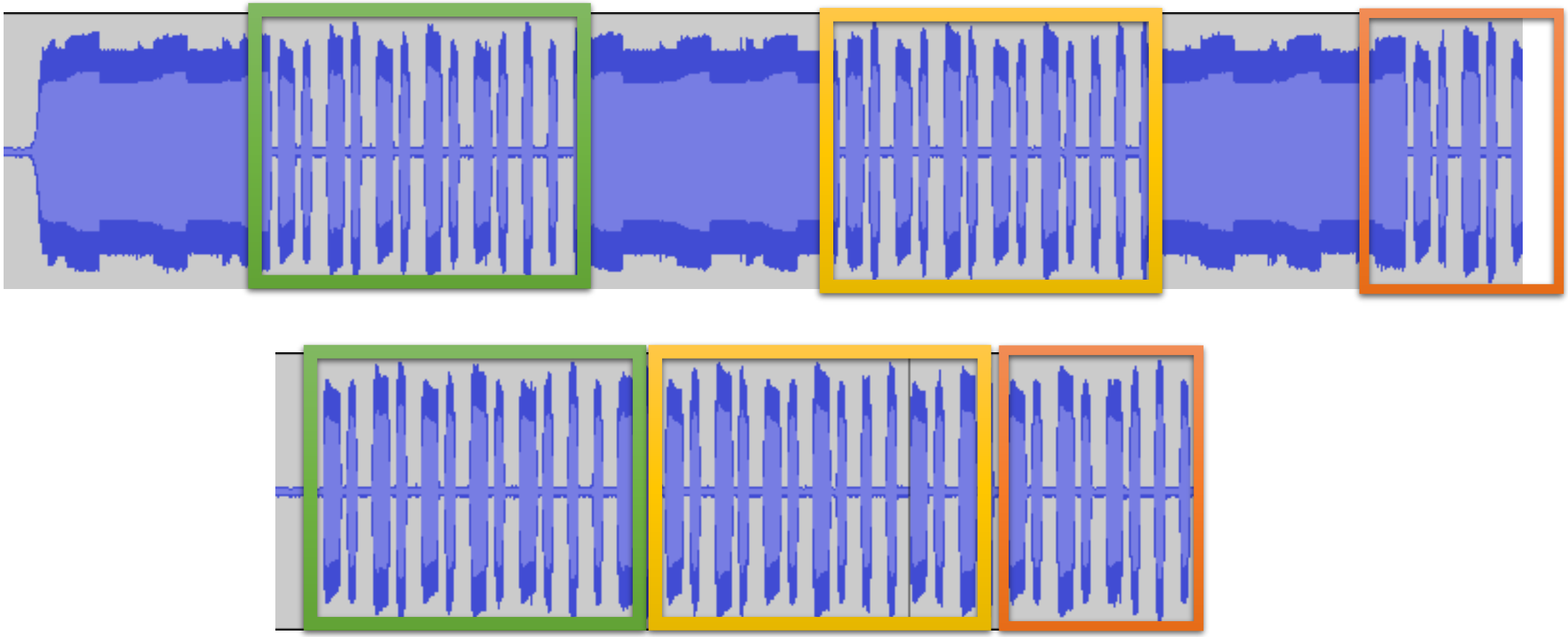
Can we get better?

Brute Force Attack on Fixed Code Garage Doors



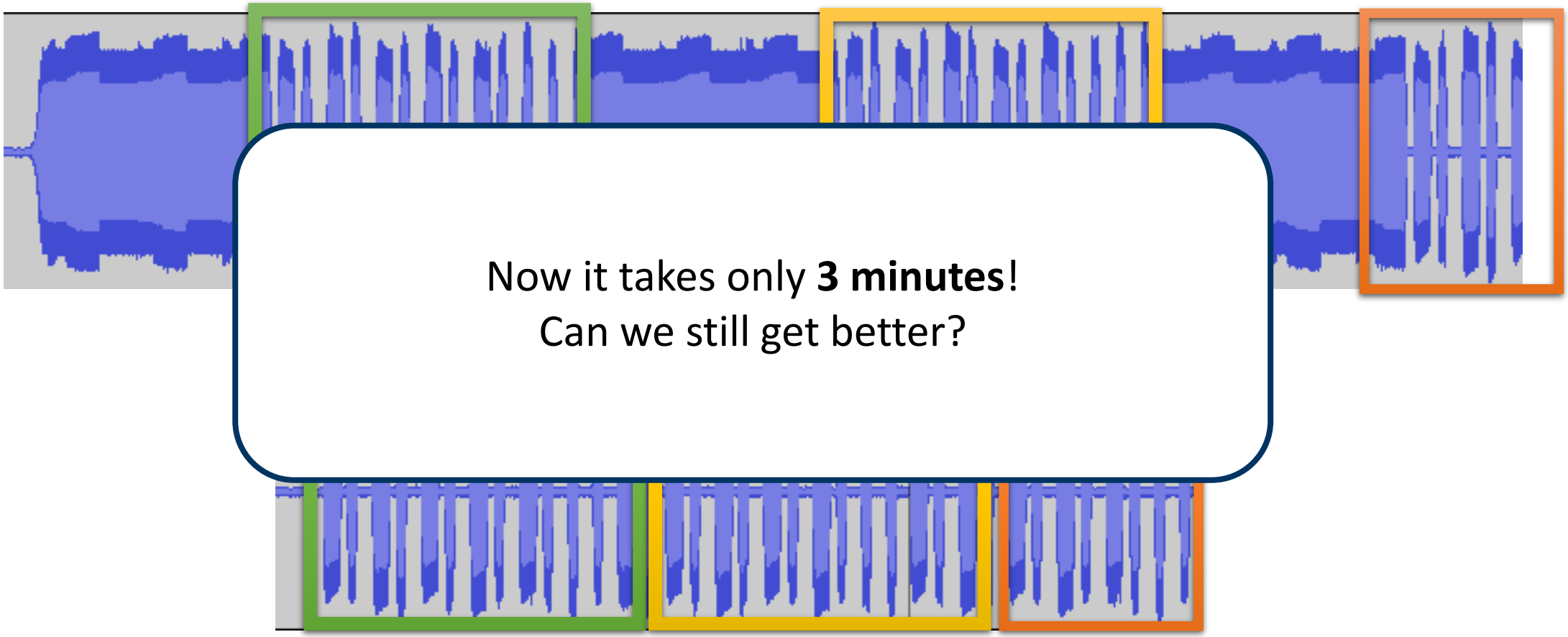
$$\frac{1771520ms}{5} = 354304\,ms \approx 6\,minutes$$

Brute Force Attack on Fixed Code Garage Doors



$$\frac{354304ms}{2} = 177152\,ms \approx 3\,minutes$$

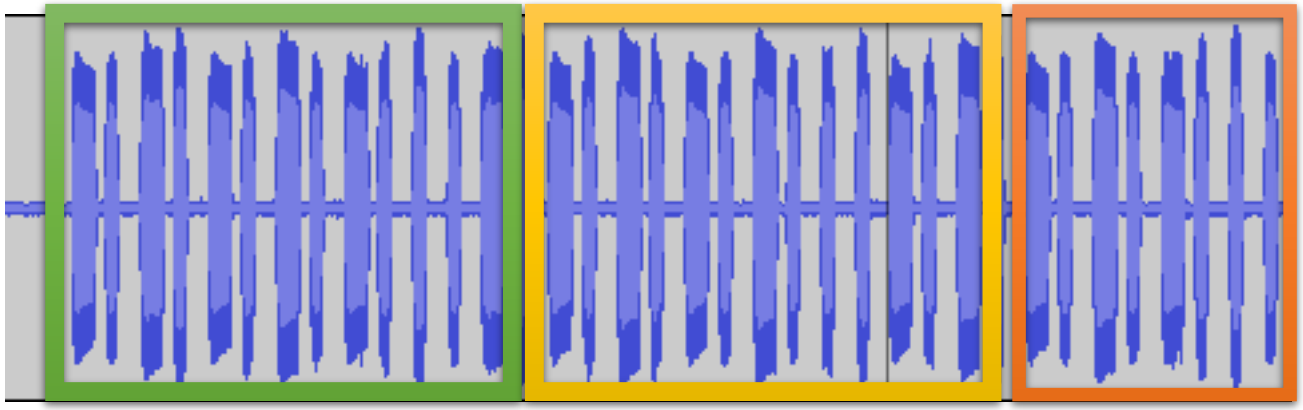
Brute Force Attack on Fixed Code Garage Doors



Now it takes only **3 minutes**!
Can we still get better?

$$\frac{354304ms}{2} = 177152\ ms \approx 3\ minutes$$

Bit shift register and De Bruijn Sequence

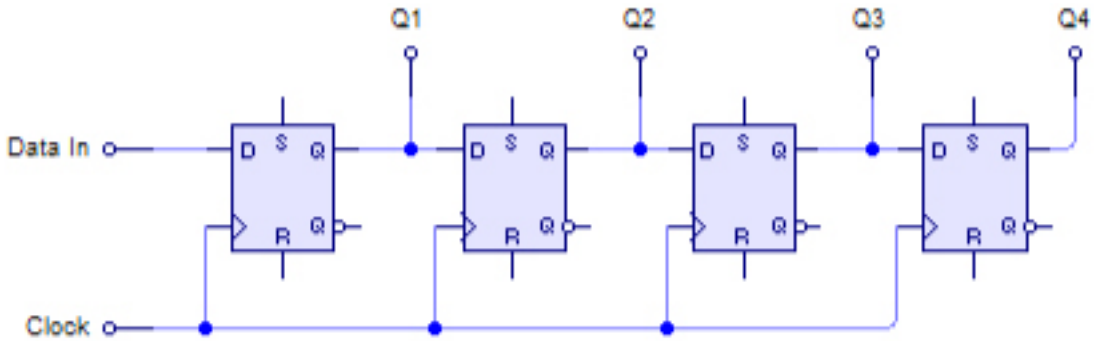


Where does one code end and the other begin?

Bit shift register

4 Bit shift register
Data in: **10010**

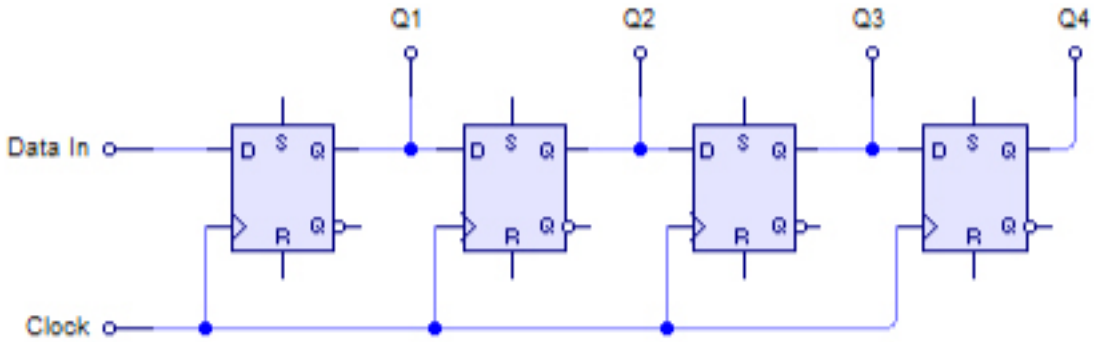
Clock	Flip Flop 1	Flip Flop 2	Flip Flop 3	Flip Flop 4
0	-	-	-	-
1	1	-	-	-
2	0	1	-	-
3	0	0	1	-
4	1	0	0	1
5	0	1	0	0
6	-	0	1	0



Bit shift register

4 Bit shift register
Data in: **10010**

Clock	Flip Flop 1	Flip Flop 2	Flip Flop 3	Flip Flop 4
0	-	-	-	-
1	1	-	-	-
2	0	1	-	-
3	0	0	1	-
4	1	0	0	1
5	0	1	0	0
6	-	0	1	0



A 5 Bit input tests two different 4 Bit Codes!

Bit shift register and De Bruijn Sequence

De Bruijn Sequence:

- Sequenz length: $k^n + (n-1)$
- $\frac{(k!)^{k^{n-1}}}{k^n}$ possible De Bruijn Sequences
  - k: number of possible symbols (e.g., binary k=2)
  - n: number of bits (e.g., key length)

Prof. N.G. de Bruijn (1918-2012)

Bit shift register and De Bruijn Sequence

De Bruijn Sequence:

00110 (5 Bits sequence) tests all different **2-Bit** sequences instead of 8 bits total

00110
00110
00110
00110

Instead of 00 01 11 10

Prof. N.G. de Bruijn (1918-2012)

Bit shift register and De Bruijn Sequence

De Bruijn Sequence:

0001011100 (10 Bits) tests all different **3-Bit** sequences instead of 24 bits total

*000*1011100
*0001*011100
*00010*11100
*000101*1100
*0001011*100
*00010111*00
*000101110*0
0001011100

Instead of 000 001 010 101 011 111 110 100

Prof. N.G. de Bruijn (1918-2012)

Bit shift register and De Bruijn Sequence

De Bruijn Sequence:

000010011010111000 (19 Bits) tests all different **4-Bit** sequences instead of 64 bits total

0000100110101111000
0000100110101111000
0000100110101111000
0000100110101111000
0000100110101111000
0000100110101111000
0000100110101111000
0000100110101111000

0000100110101111000
0000100110101111000
0000100110101111000
0000100110101111000
0000100110101111000
0000100110101111000
0000100110101111000
0000100110101111000

Prof. N.G. de Bruijn (1918-2012)

Instead of 0000 0001 0010 0100 … 1111 1110 1100 1000

Bit shift register and De Bruijn Sequence

De Bruijn Sequence:

000001000110010100111010110111110000 (36 Bits) tests all different **5-Bit** sequences instead of 160 bits total

*00000*1000110010100111010110111110000
*0*00001000110010100111010110111110000
*00*00010001100101001110101101111110000
*000*00100011001010011101011011111000 0
...
0000010001100101001110101101111100 00
0000010001100101001110101101111 10000
0000010001100101001110101101111 10000

Instead of 00000 00001 00010 00100 … 11100 11000 10000

Prof. N.G. de Bruijn (1918-2012)

Bit shift register and De Bruijn Sequence

De Bruijn Sequence:

0000010000110001010001110010010110011010011110101011 101101111100000 (69 Bits) tests all different **6-Bit** sequences instead of 384 bits total

000000100001100010100…11110101011101101111100000
000001000011000101000…11110101011101101111100000
000000100001100010100…11110101011101101111100000
…
000001000011000101000…11110101011101101111100000
000001000011000101000…11110101011101101111100000
000001000011000101000…11110101011101101111100000

Instead of 000000 000001 000010 … 111000 110000 100000

Prof. N.G. de Bruijn (1918-2012)

Bit shift register and De Bruijn Sequence

De Bruijn Sequence:

00000001000001100001010000111000100100010110001101000
11110010011001010100101110011011001110100111110101011
01011110110111011111111000000 (134 Bits) tests all different **7-Bit** sequences instead of 896 bits total

Prof. N.G. de Bruijn (1918-2012)

0000000100000110000101000011100010010001011000110100011110010011001010100101110011011001110100111110101011010111101101110111111110000000
0000000100000110000101000011100010010001011000110100011110010011001010100101110011011001110100111110101011010111101101110111111110000000
0000000100000110000101000011100010010001011000110100011110010011001010100101110011011001110100111110101011010111101101110111111110000000
...
0000000100000110000101000011100010010001011000110100011110010011001010100101110011011001110100111110101011010111101101110111111110000000
0000000100000110000101000011100010010001011000110100011110010011001010100101110011011001110100111110101011010111101101110111111110000000

Instead of 0000000 0000001 0000010 … 1100000 1000000

Bit shift register and De Bruijn Sequence

De Bruijn Sequen

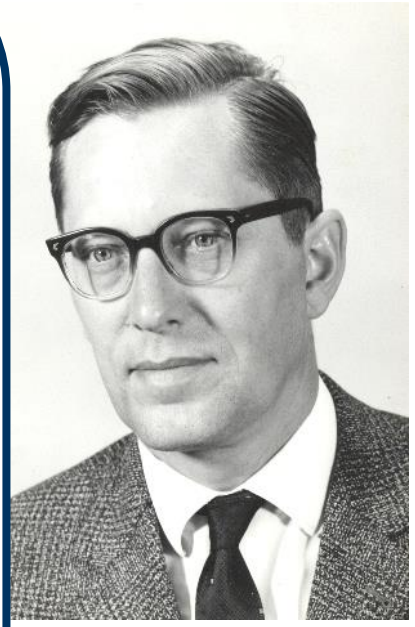
0000000100000
1111001001100
0101111011011
Bit sequences in

0000000100000
0000000100000
0000000100000
…
0000001000001100001010000111…1101101110111111000000

Instead of 0000000 0000001 0000010 … 1100000 1000000

We can use this for our Brute Force Attack. For **every** 8-12 Bit garage door:

$$(2^{12} + 11) * \frac{4ms}{2} = 8214ms = \mathbf{8,214\ sec}$$



N.G. de Bruijn (1918-2012)

Countermeasures

- Use a large key space
  - Brute forcing the key takes more time
- Require a preamble/postamble word for each key
  - Sending De Bruijn Sequences won‘t work anymore
- **Use rolling codes!**
  - More on that later

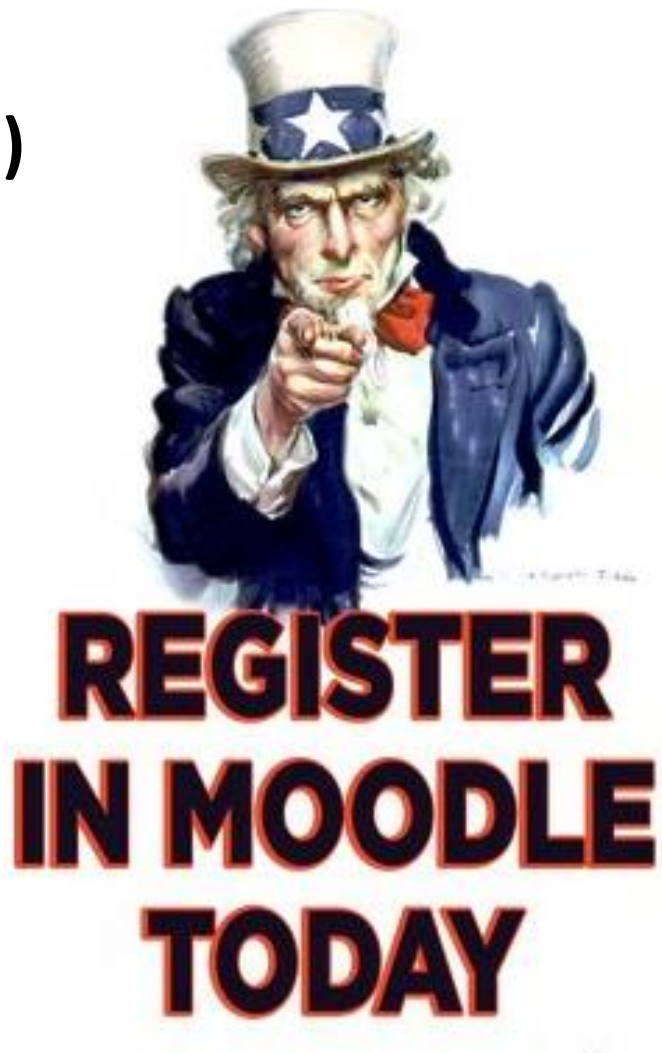
Opening the car

The garage is now open...

Next time in WPLS:
How do we open the car?

Moodle Course

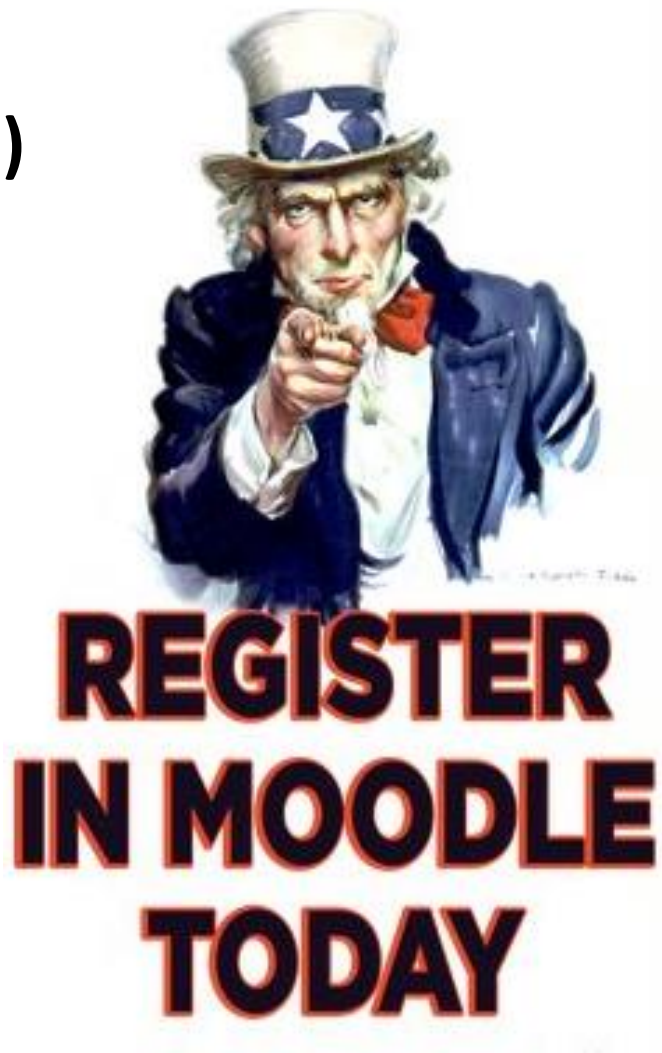
Bachelor/Master-Praktikum
Wireless Physical Layer Security (SS 2023)



Moodle Course
Passwort: wpls2023

Questions?

Bachelor/Master-Praktikum
Wireless Physical Layer Security (SS 2023)



Many thanks for your attention!

Questions?

… or maybe later:

christian.zenger@rub.de
johannes.kortz@rub.de
jonathan.mazyrko@rub.de

Copyright Notice

- Parts of this lectures are based on the lecture “Drive it like you hacked it” by Samy Kamkar (DefCon 2016)
- Parts of this lectures are based on the lecture “Physical Layer Security for Wireless Systems (PhySec)” at TU Darmstadt (Winter Term 2015)
- This document has been distributed by the contributing authors as a means to ensure timely dissemination of scholarly and technical work on a non-commercial basis.
- Copyright and all rights therein are maintained by the authors or by other copyright holders

Pics

- https://upload.wikimedia.org/wikipedia/commons/thumb/c/c9/FCC_New_Logo.svg/2000px-FCC_New_Logo.svg.png
- http://www.idownloadblog.com/2014/07/13/fcc-loosens-label-restrictions/
- https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=2458843
- https://greatscottgadgets.com/hackrf/
- http://gnuradio.org/redmine/attachments/download/399/screenshot-grc-bersimu.png
- https://www.garagen-welt.de/sites/garagenwelt/files/styles/hero_unit/public/Z-Line-Garage_1124x520_2_0.jpg?itok=18ViWZqZ
- https://upload.wikimedia.org/wikipedia/commons/a/a1/4-Bit_SIPO_Shift_Register.png
- http://www.win.tue.nl/automath/images/deBruijn.gif
- http://rennlist.com/wp-content/uploads/2015/12/Garage1.jpg
- Samy Kamkar – Dirve it like you hacked it slides
- http://p5.focus.de/img/incoming/origs4551096/2888514346-w630-h472-o-q75-p5/urn-newsml-dpa-com-20090101-141205-99-01789-large-4-3.jpg
- https://supportforums.cisco.com/sites/default/files/legacy/7/5/1/90157-26.png
- https://upload.wikimedia.org/wikipedia/commons/thumb/4/44/BMW.svg/2000px-BMW.svg.png
- http://i.ebayimg.com/images/g/eb0AAOxyVLNS9iMS/s-l300.jpg
- http://images.newcars.com/images/car-pictures/original/2016-BMW-M3-Sedan-Base-4dr-Rear-wheel-Drive-Sedan-Photo-2.png
- http://www.clker.com/cliparts/k/D/I/H/j/2/plainwifiright-hi.png
- https://vmcdn.ca/old/sootoday/userfiles/images/Police/Crime/door-been-easily-kicked-in.jpg
- https://www.wired.com/wp-content/uploads/2015/08/rolljam3.jpg
- http://www.icpdf.com/icpdf_datasheet_8_datasheet/NM24C03U_pdf_1809029/NM24C03U_571.html
- https://creators.vice.com/en_uk/article/9an9m7/heres-what-wi-fi-would-look-like-if-we-could-see-it
- https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OeffentlicheNetze/Mobilfunknetze/mobilfunknetze-node.html