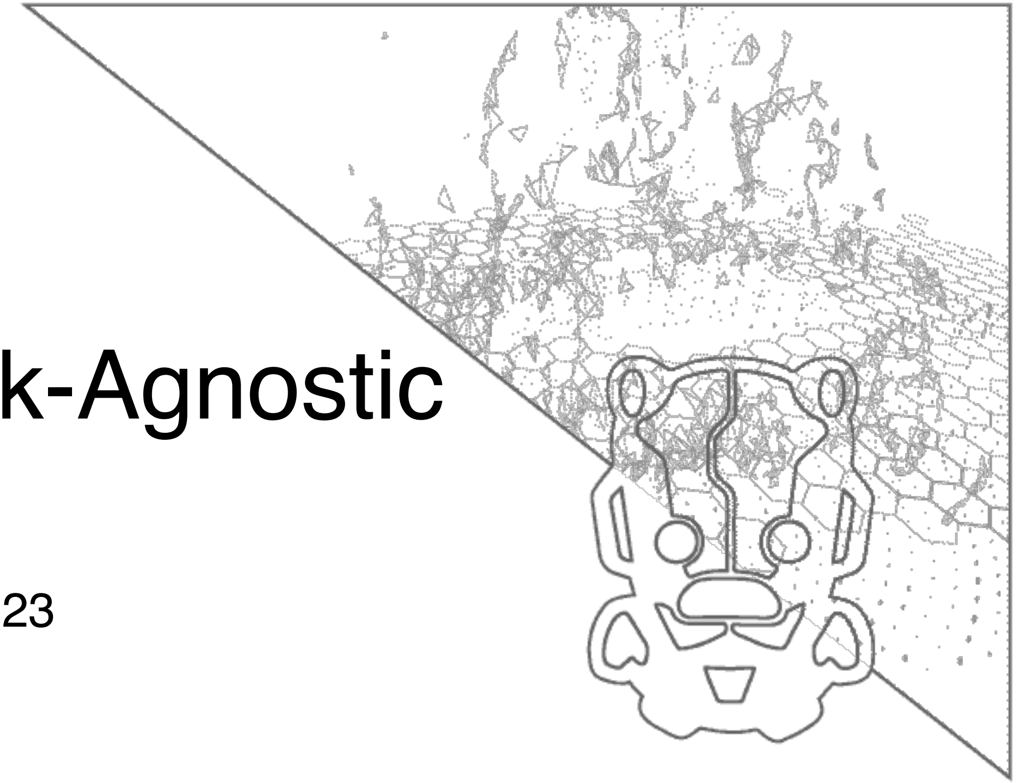
#HITB2023AMS

Upgrading Rollback-Agnostic Replay Attacks

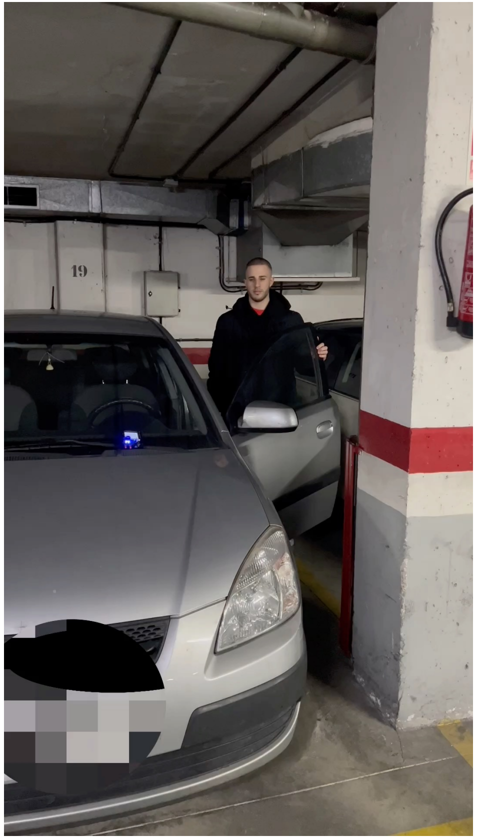
HITB2023, Amsterdam 20-21 April 2023



Carlos Gómez Quintana
Associate Security Consultant

IOActive®

Teaser



👀

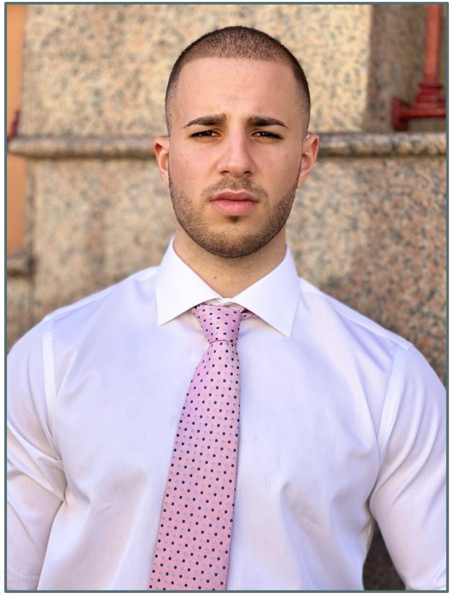
Agenda

- # Whoami #
- Introduction
  - Software Defined Radio (SDR)
  - Arsenal
  - Radio Frequency Analysis
  - Modulation
  - Rolling Codes
- Attacks
  - Rolljam
  - Rollback
    - Upgrade
- Questions & Contact

Disclaimer

- All tests carried out have been under the permission and supervision of the legitimate owners
- Performing any of the above techniques is considered **ILLEGAL** if the necessary permission is not obtained
- All captured signals have been **erased** after the end of the investigation
- The tests comply with data protection law and the right to personal privacy

# Whoami



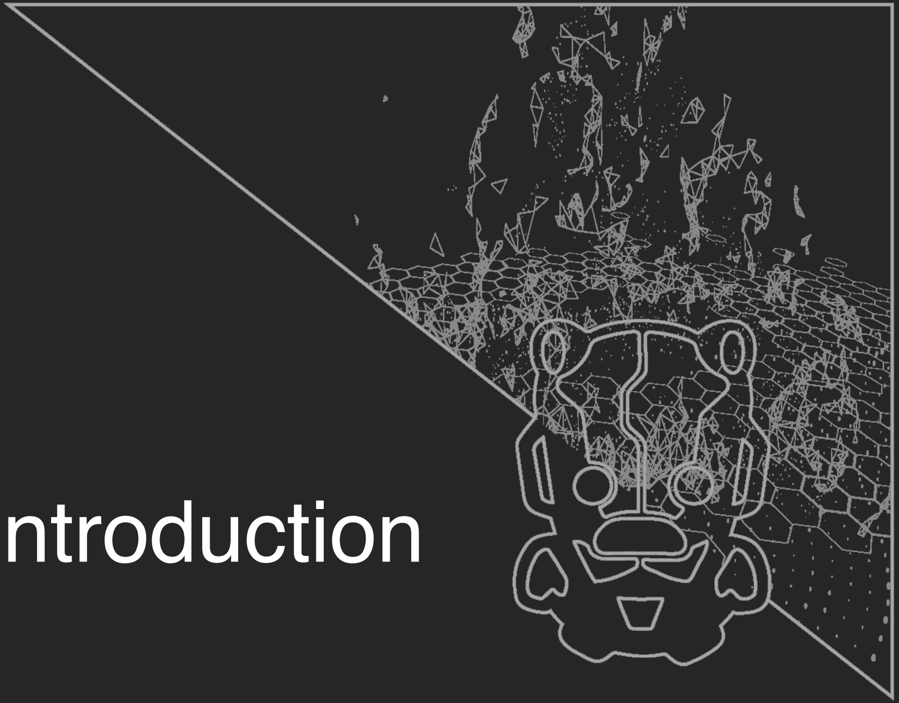
- Associate Security Consultant at IOActive
- Software engineering
- Love cars, evade and breaks things =)

✉ carlos.gomez@ioactive.com

@cgomezz_23

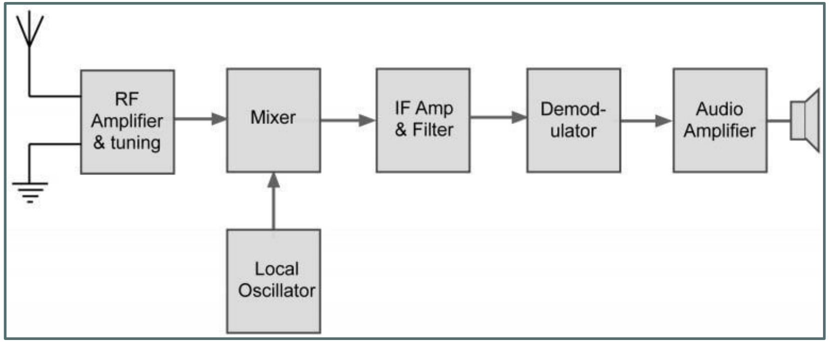
in @cgomezquintana

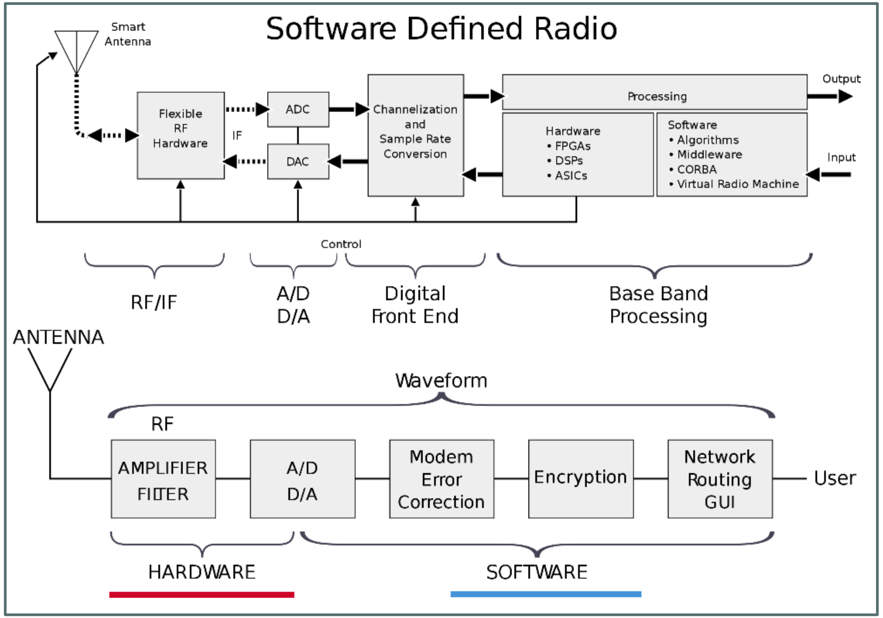
Radio Frequency Introduction



SDR Introduction

Traditional Radio





Arsenal

~~Which SDR should I buy?~~

What do I want to do?

- Signal reception
- Emitting signals
- Reception of a certain band
- Professional use

USRP: $1000

BladeRF: $700

Ubertooth: $130

RTL-SDR: $30

HackRF: $300

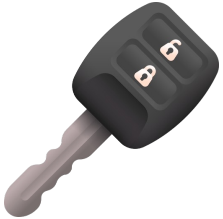
Yard Stick One: $150

Disclaimer 2.0

JAMMING IS ILLEGAL

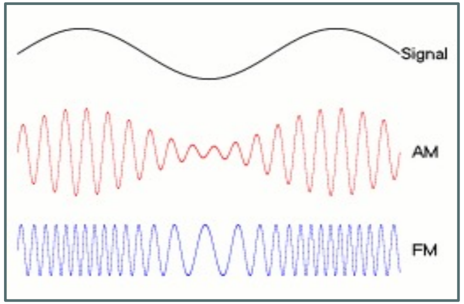
What is RKE?

- Remote Keyless Entry system
- Operate by radio frequencies
  - European, Asian, and British cars on 433.92 MHz
  - North American and Japanese cars on 315 MHz
- Lock/unlock doors, turn on the vehicle, etc.
- Chips with cyphers

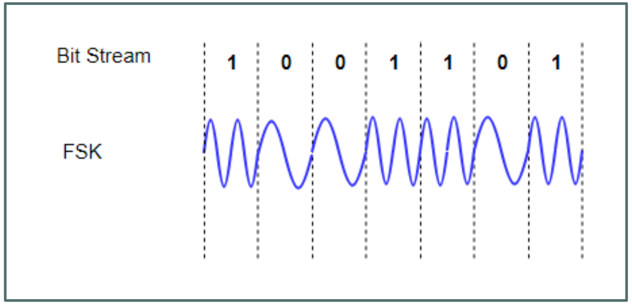


Modulation

- Process of modifying an information signal so that it can be transmitted over a communication channel
- The modulating signal contains the information to be transmitted, such as voice, music or data



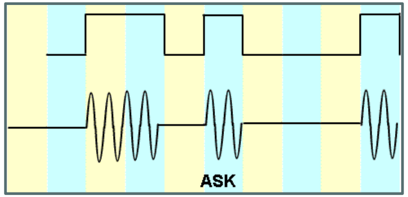
Analog Modulation



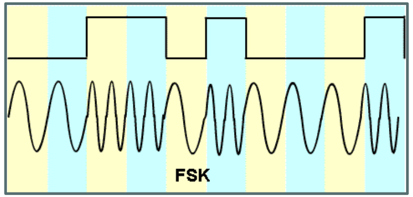
Digital Modulation

Modulation (continued)

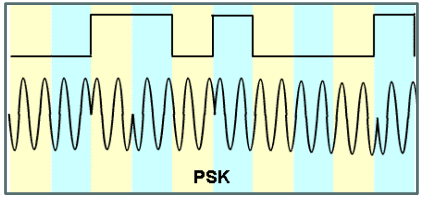
MOST COMMON MODULATIONS



Amplitude Shift Keying



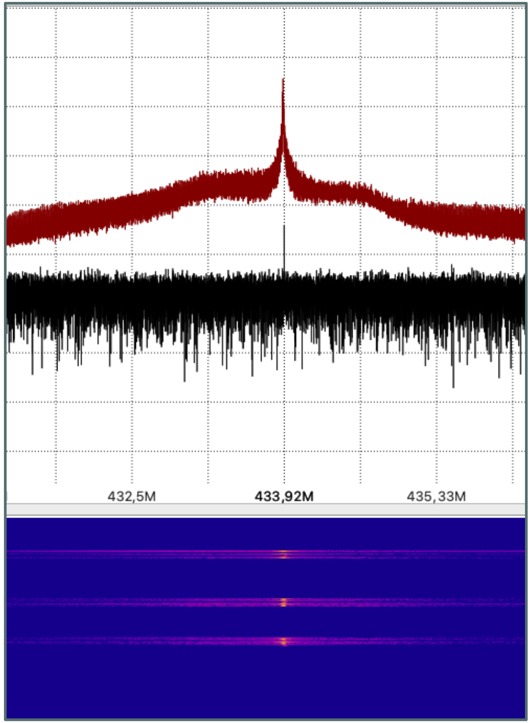
Frequency Shift Keying



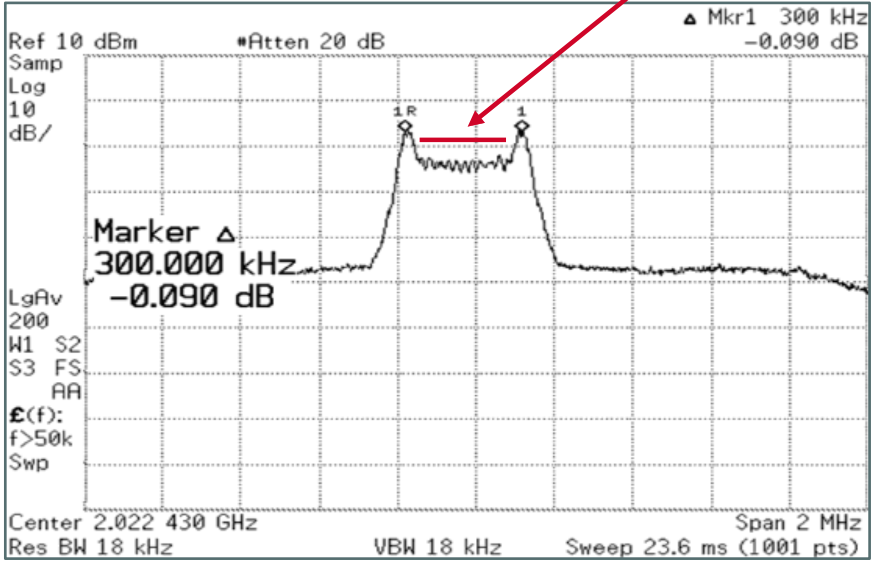
Phase Shift Keying

Modulation (continued)

ASK



2-FSK



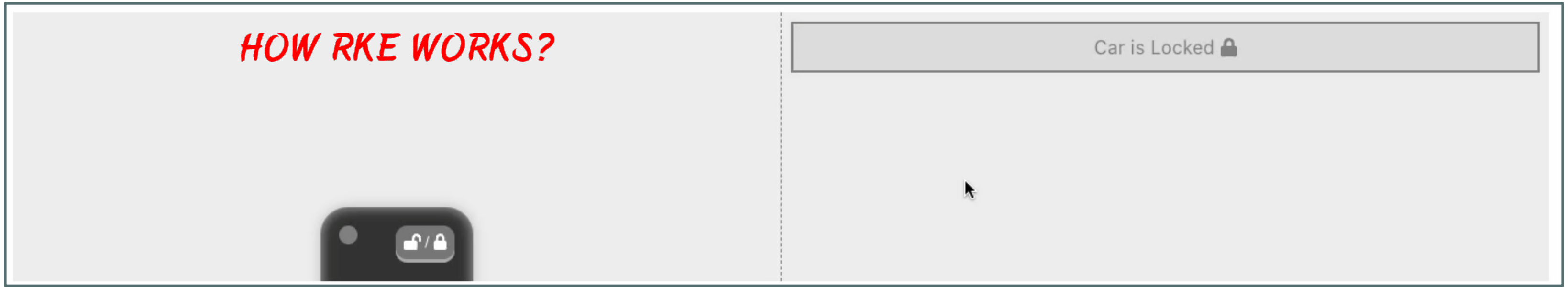
Ref 10 dBm   #Atten 20 dB   Δ Mkr1 300 kHz
−0.090 dB
Samp
Log
10
dB/
Marker Δ
300.000 kHz
−0.090 dB
LgAv
200
W1 S2
S3 FS
AA
£(f):
f>50k
Swp
Center 2.022 430 GHz   Span 2 MHz
Res BW 18 kHz   VBW 18 kHz   Sweep 23.6 ms (1001 pts)

Frequency deviation

How do rolling codes work exactly?

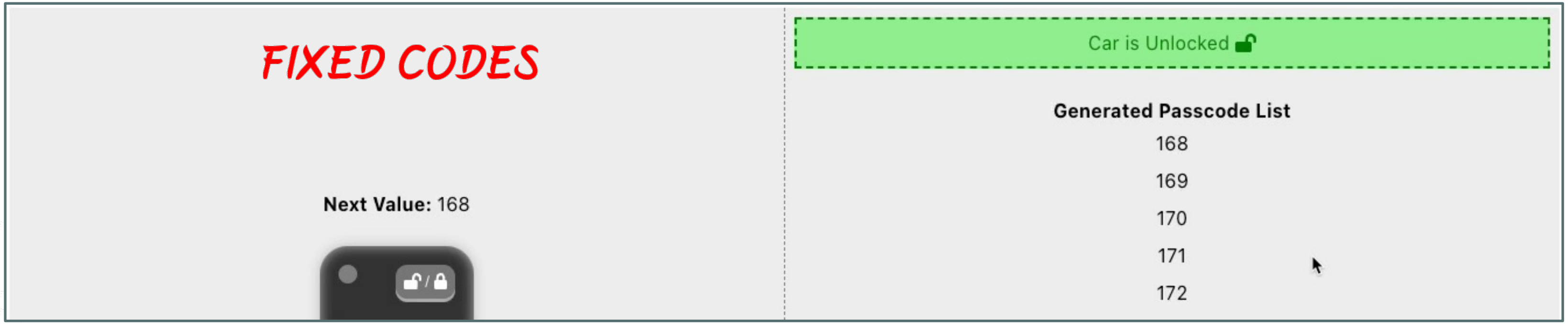
#HITB2023AMS

Rolling Codes



HOW RKE WORKS?

Car is Locked 🔒



FIXED CODES

Next Value: 168

Car is Unlocked 🔓

Generated Passcode List

168

169

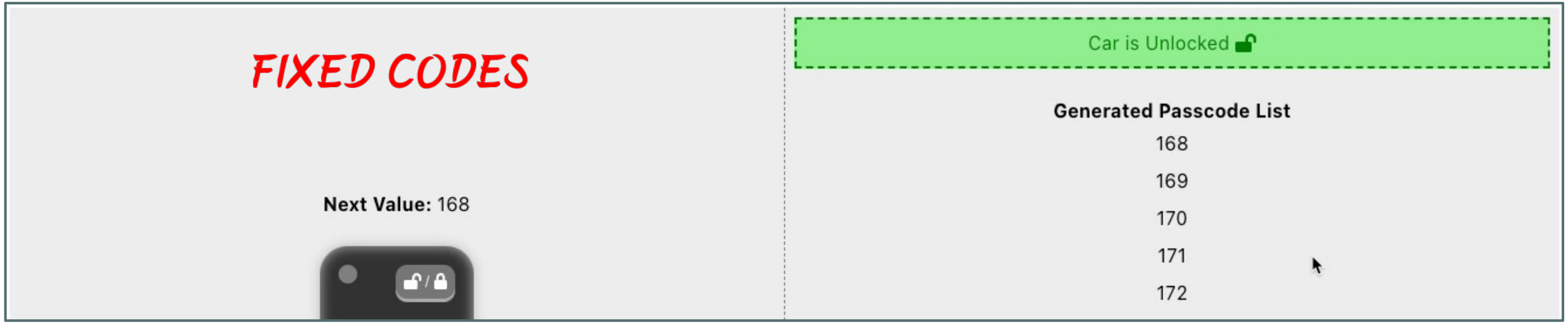
170

171

172

https://harryli0088.github.io/rolling-code/

Rolling Codes (continued)



FIXED CODES

Next Value: 168

Car is Unlocked

Generated Passcode List

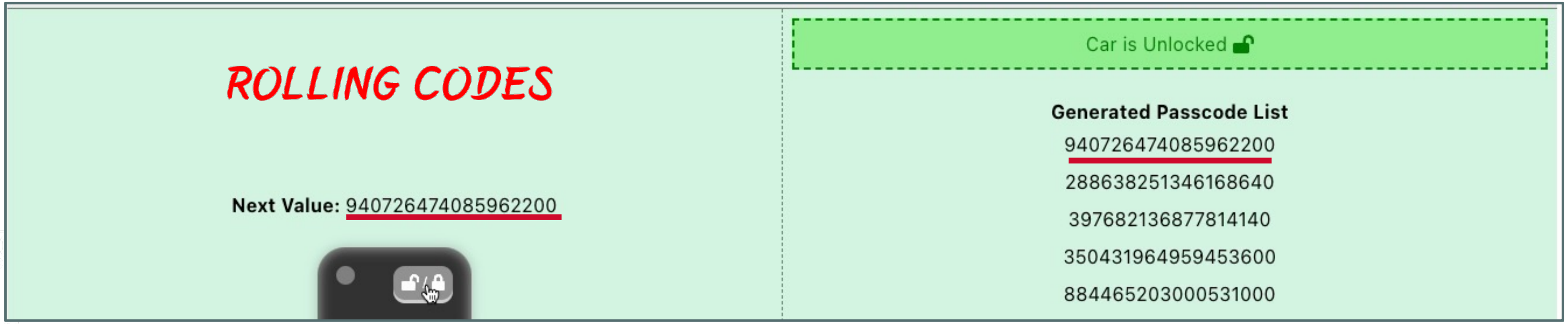
168

169

170

171

172



ROLLING CODES

Next Value: 940726474085962200

Car is Unlocked

Generated Passcode List

940726474085962200

288638251346168640

397682136877814140

350431964959453600

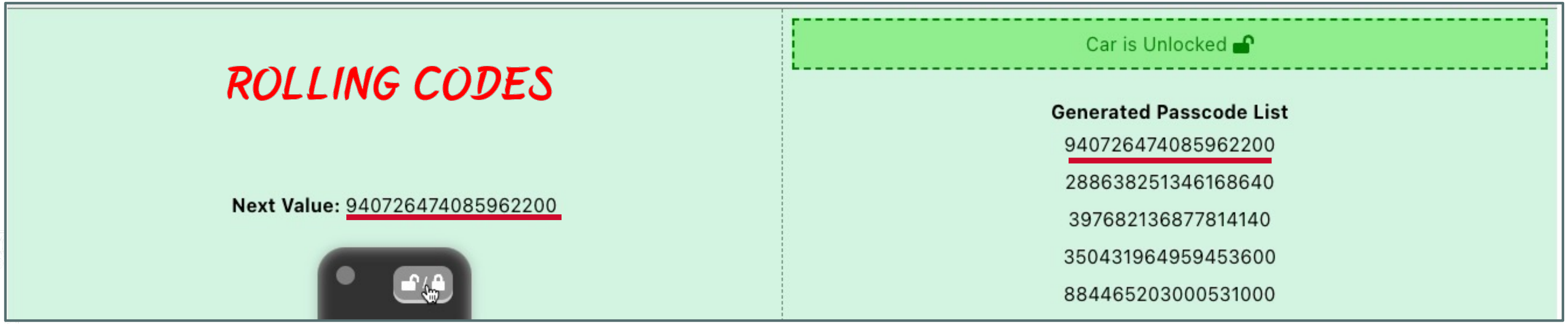
884465203000531000

https://harryli0088.github.io/rolling-code/

Rolling Codes (continued)

169 + (RANDOM HASH) = 9123183451763l724

ROLLING CODE GENERATED



ROLLING CODES

Next Value: 9407264740859622OO

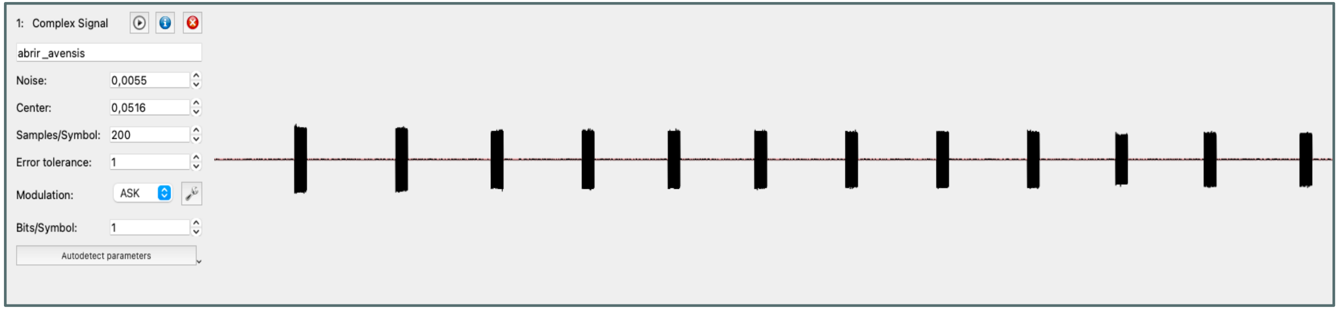
Car is Unlocked

Generated Passcode List

9407264740859622OO
2886382513461686 40
397682136877814140
350431964959453600
884465203000531000

https://harryli0088.github.io/rolling-code/

Analysis



1: Complex Signal

abrir_avensis

Noise: 0,0055

Center: 0,0516

Samples/Symbol: 200

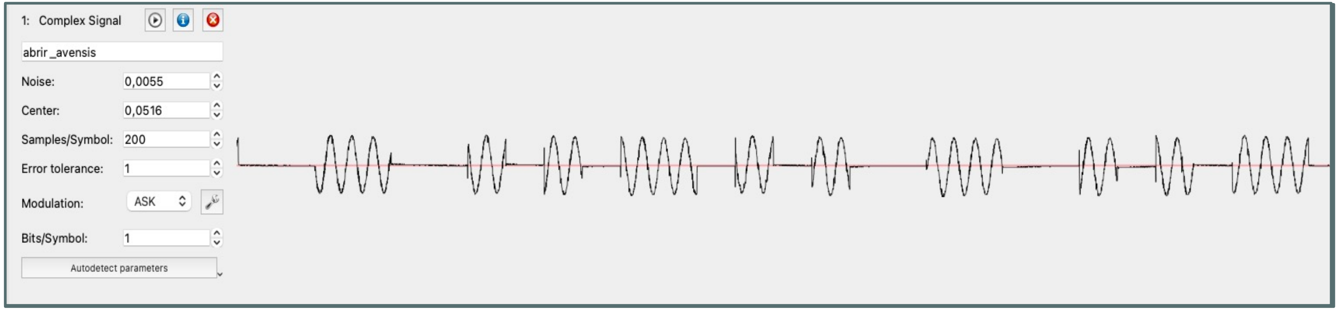
Error tolerance: 1

Modulation: ASK

Bits/Symbol: 1

- **CHIP Codec**: 4D70

Analysis



1: Complex Signal

abrir_avensis

Noise: 0,0055

Center: 0,0516

Samples/Symbol: 200

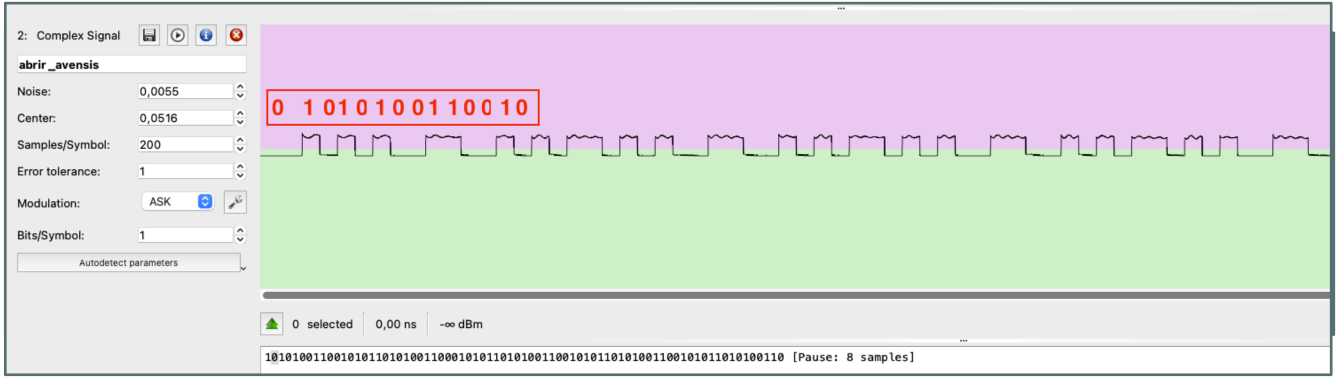
Error tolerance: 1

Modulation: ASK

Bits/Symbol: 1

- **CHIP Codec**: 4D70
- ASK modulation

Analysis



abrir_avensis

Noise: 0,0055

Center: 0,0516

Samples/Symbol: 200

Error tolerance: 1

Modulation: ASK

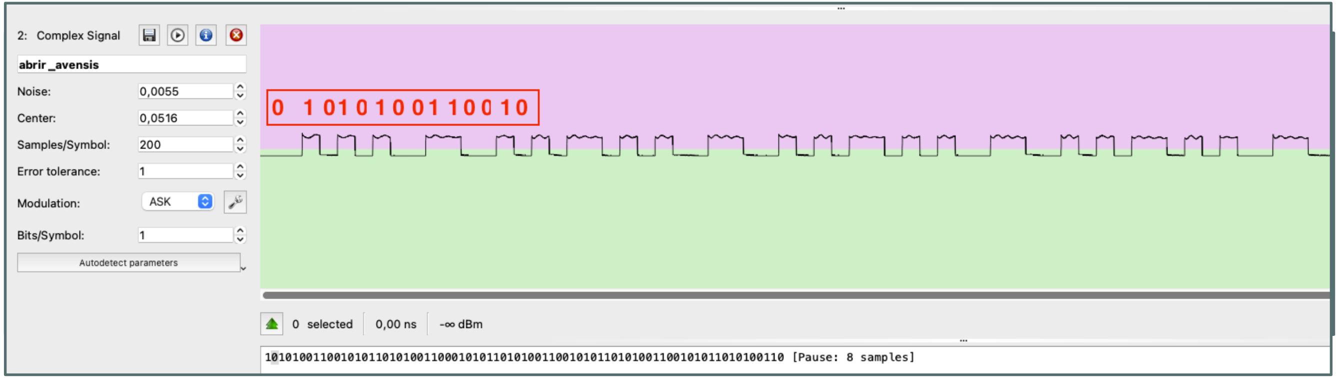
Bits/Symbol: 1

```
101010011001010110101001100010101101010011001010110101001100101011010100110 [Pause: 8 samples]
```

- **CHIP Codec**: 4D70
- ASK modulation
- Not bit codification

#HITB2023AMS

Analysis



2: Complex Signal

abrir_avensis

Noise: 0,0055

Center: 0,0516

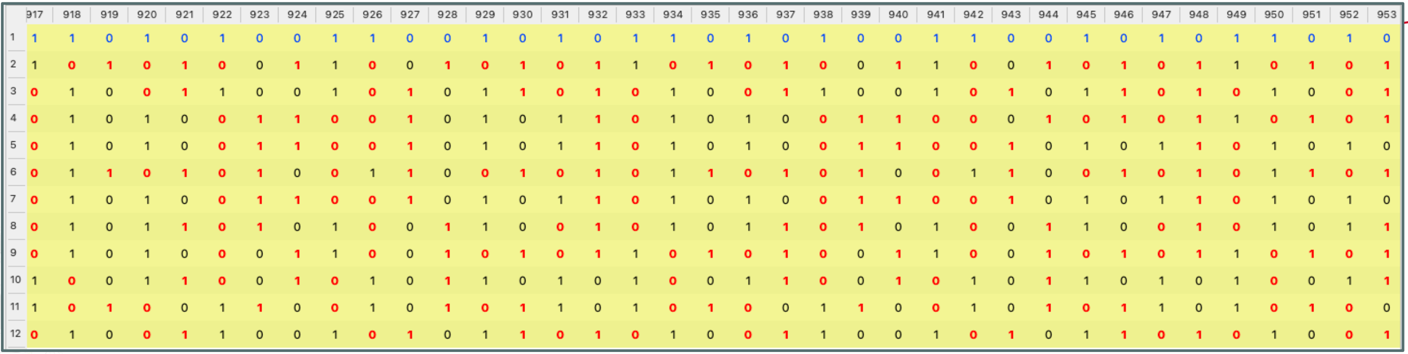
Samples/Symbol: 200

Error tolerance: 1

Modulation: ASK

Bits/Symbol: 1

```
101010011001010110101001100010101101010011001010110101001100101011010100110 [Pause: 8 samples]
```



	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953
1	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0
2	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1
3	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1
4	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	0	1	0	1	0	1	1	0	1	0	1
5	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0
6	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1
7	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0
8	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1
9	0	1	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1
10	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1
11	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0
12	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1

- **CHIP Codec**: 4D70
- ASK modulation
- Not bit codification

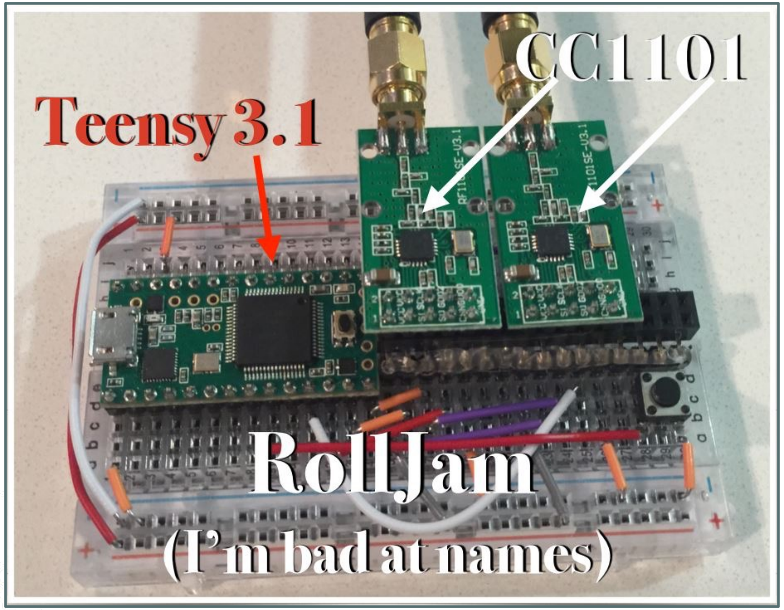
Rolling Codes

#HITB2023AMS

RollJam
Wireless Vehicle Entry Attack

Rolljam

ROLLJAM DEVICE

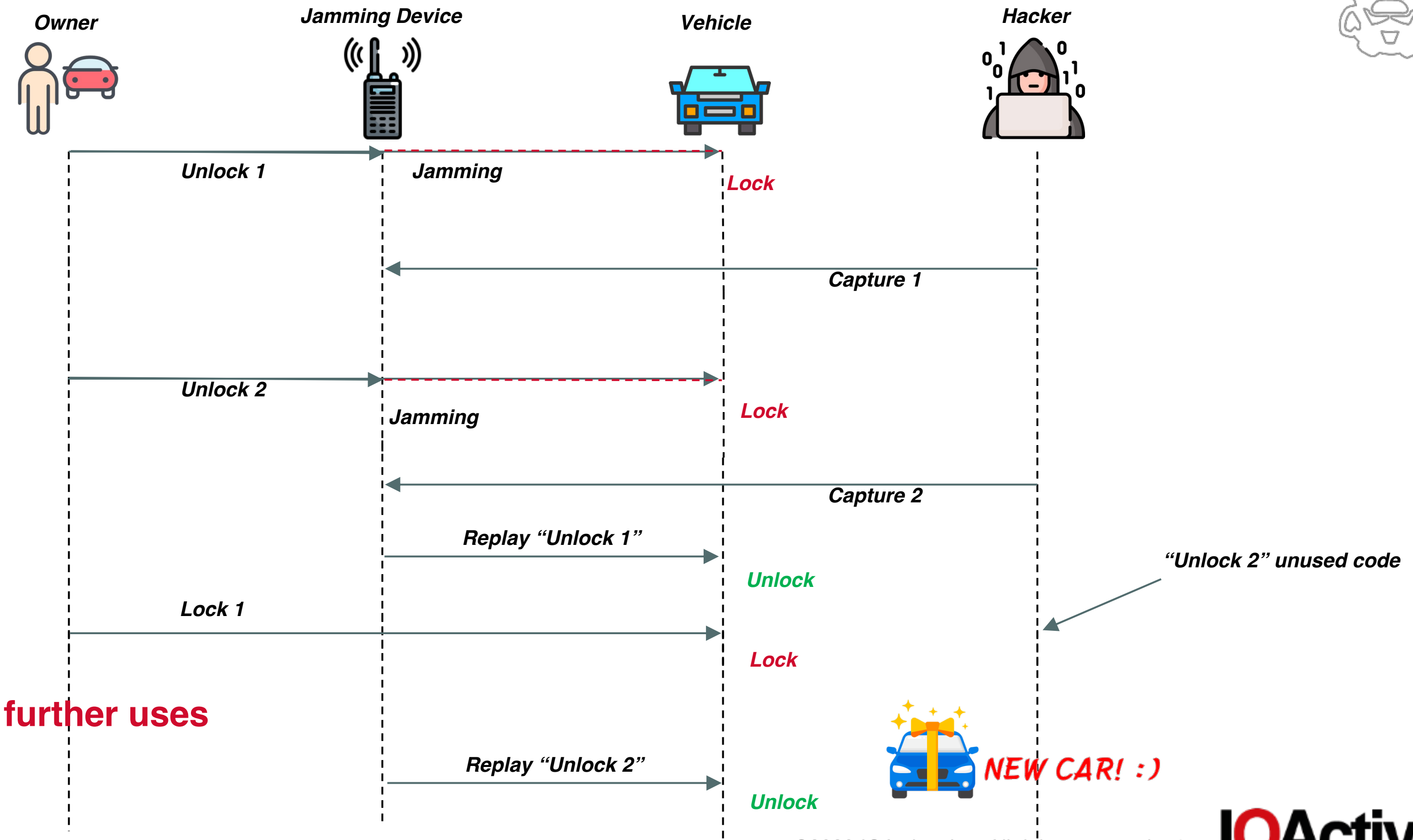


Samy Kamkar

@samykamkar

https://samy.pl/

How Rolljam Works



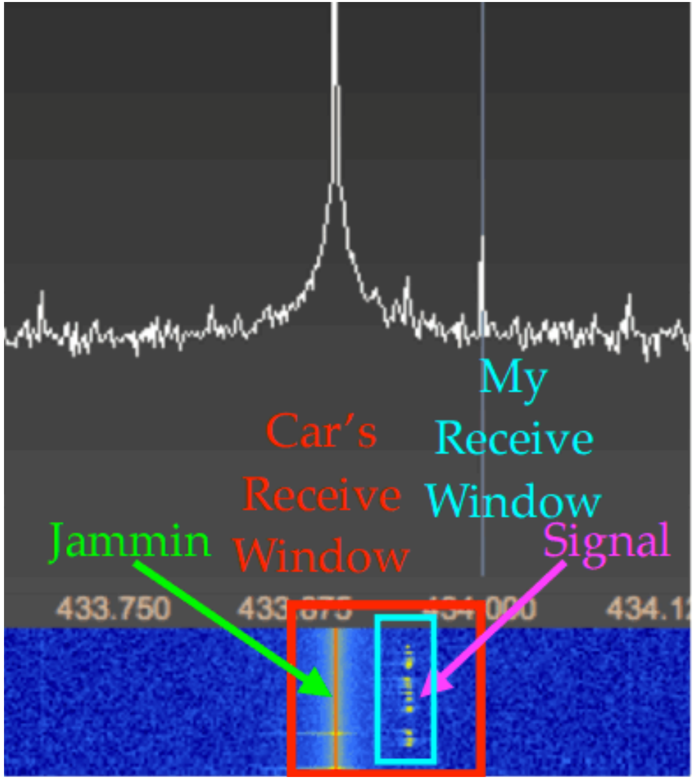
No further uses

#HITB2023AMS

How Rolljam Works (continued)

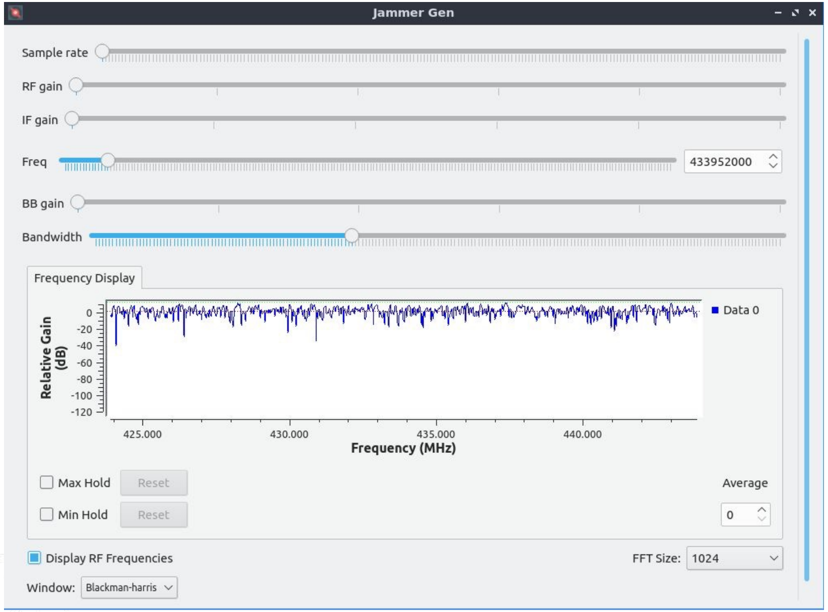
ATTACK METHODOLOGY

1. Jamming + listening signal 1
2. Jamming + listening signal 2
3. Stop the jamming device + send signal 1
4. Signal 2 valid to use ☺



Executing Rolljam

Jammer


Jammer Gen

Sample rate

RF gain

IF gain

Freq 433952000

BB gain

Bandwidth

Frequency Display

□ Max Hold Reset

□ Min Hold Reset

Average 0

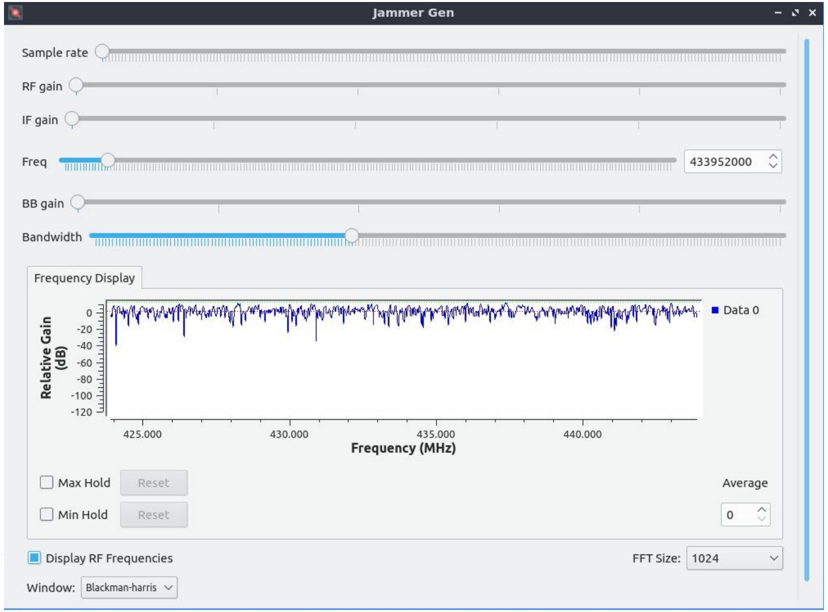
☑ Display RF Frequencies

FFT Size: 1024

Window: Blackman-harris

Executing Rolljam

Jammer



Jammer Gen

Sample rate

RF gain

IF gain

Freq 433952000

BB gain

Bandwidth

Frequency Display

□ Max Hold Reset

□ Min Hold Reset

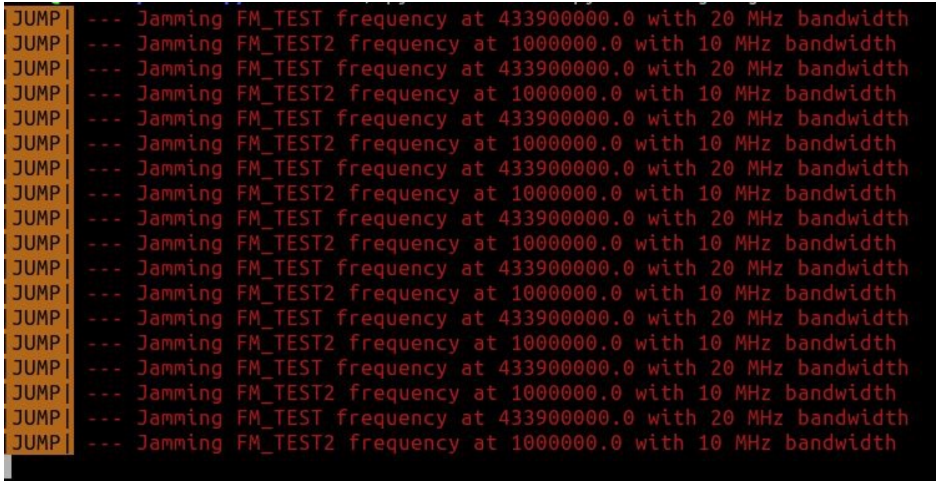
Average 0

☑ Display RF Frequencies

FFT Size: 1024

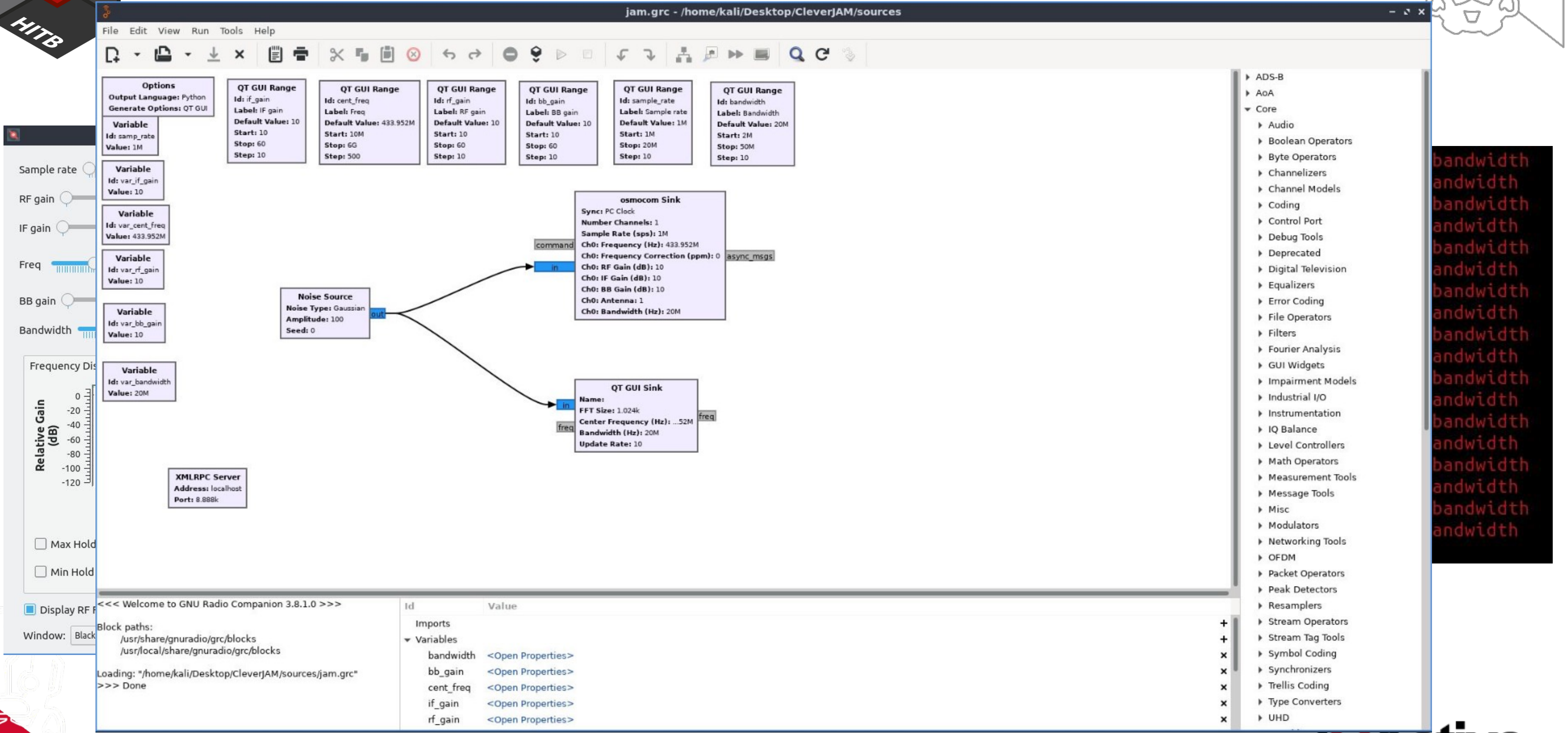
Window: Blackman-harris

Hopping Program



```
|JUMP| --- Jamming FM_TEST frequency at 433900000.0 with 20 MHz bandwidth
|JUMP| --- Jamming FM_TEST2 frequency at 1000000.0 with 10 MHz bandwidth
|JUMP| --- Jamming FM_TEST frequency at 433900000.0 with 20 MHz bandwidth
|JUMP| --- Jamming FM_TEST2 frequency at 1000000.0 with 10 MHz bandwidth
|JUMP| --- Jamming FM_TEST frequency at 433900000.0 with 20 MHz bandwidth
|JUMP| --- Jamming FM_TEST2 frequency at 1000000.0 with 10 MHz bandwidth
|JUMP| --- Jamming FM_TEST frequency at 433900000.0 with 20 MHz bandwidth
|JUMP| --- Jamming FM_TEST2 frequency at 1000000.0 with 10 MHz bandwidth
|JUMP| --- Jamming FM_TEST frequency at 433900000.0 with 20 MHz bandwidth
|JUMP| --- Jamming FM_TEST2 frequency at 1000000.0 with 10 MHz bandwidth
|JUMP| --- Jamming FM_TEST frequency at 433900000.0 with 20 MHz bandwidth
|JUMP| --- Jamming FM_TEST2 frequency at 1000000.0 with 10 MHz bandwidth
|JUMP| --- Jamming FM_TEST frequency at 433900000.0 with 20 MHz bandwidth
|JUMP| --- Jamming FM_TEST2 frequency at 1000000.0 with 10 MHz bandwidth
|JUMP| --- Jamming FM_TEST frequency at 433900000.0 with 20 MHz bandwidth
|JUMP| --- Jamming FM_TEST2 frequency at 1000000.0 with 10 MHz bandwidth
|JUMP| --- Jamming FM_TEST frequency at 433900000.0 with 20 MHz bandwidth
|JUMP| --- Jamming FM_TEST2 frequency at 1000000.0 with 10 MHz bandwidth
```

Executing Rolljam



Options
Output Language: Python
Generate Options: QT GUI

Variable
Id: samp_rate
Value: 1M

Variable
Id: var_if_gain
Value: 10

Variable
Id: var_cent_freq
Value: 433.952M

Variable
Id: var_rf_gain
Value: 10

Variable
Id: var_bb_gain
Value: 10

Variable
Id: var_bandwidth
Value: 20M

QT GUI Range
Id: if_gain
Label: IF gain
Default Value: 10
Start: 10
Stop: 60
Step: 10

QT GUI Range
Id: cent_freq
Label: Freq
Default Value: 433.952M
Start: 10M
Stop: 6G
Step: 500

QT GUI Range
Id: rf_gain
Label: RF gain
Default Value: 10
Start: 10
Stop: 60
Step: 10

QT GUI Range
Id: bb_gain
Label: BB gain
Default Value: 10
Start: 10
Stop: 60
Step: 10

QT GUI Range
Id: sample_rate
Label: Sample rate
Default Value: 1M
Start: 1M
Stop: 20M
Step: 10

QT GUI Range
Id: bandwidth
Label: Bandwidth
Default Value: 20M
Start: 2M
Stop: 50M
Step: 10

osmocom Sink
Sync: PC Clock
Number Channels: 1
Sample Rate (sps): 1M
Ch0: Frequency (Hz): 433.952M
Ch0: Frequency Correction (ppm): 0
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 10
Ch0: BB Gain (dB): 10
Ch0: Antenna: 1
Ch0: Bandwidth (Hz): 20M

Noise Source
Noise Type: Gaussian
Amplitude: 100
Seed: 0

QT GUI Sink
Name:
FFT Size: 1.024k
Center Frequency (Hz): ...52M
Bandwidth (Hz): 20M
Update Rate: 10

XMLRPC Server
Address: localhost
Port: 8.888k

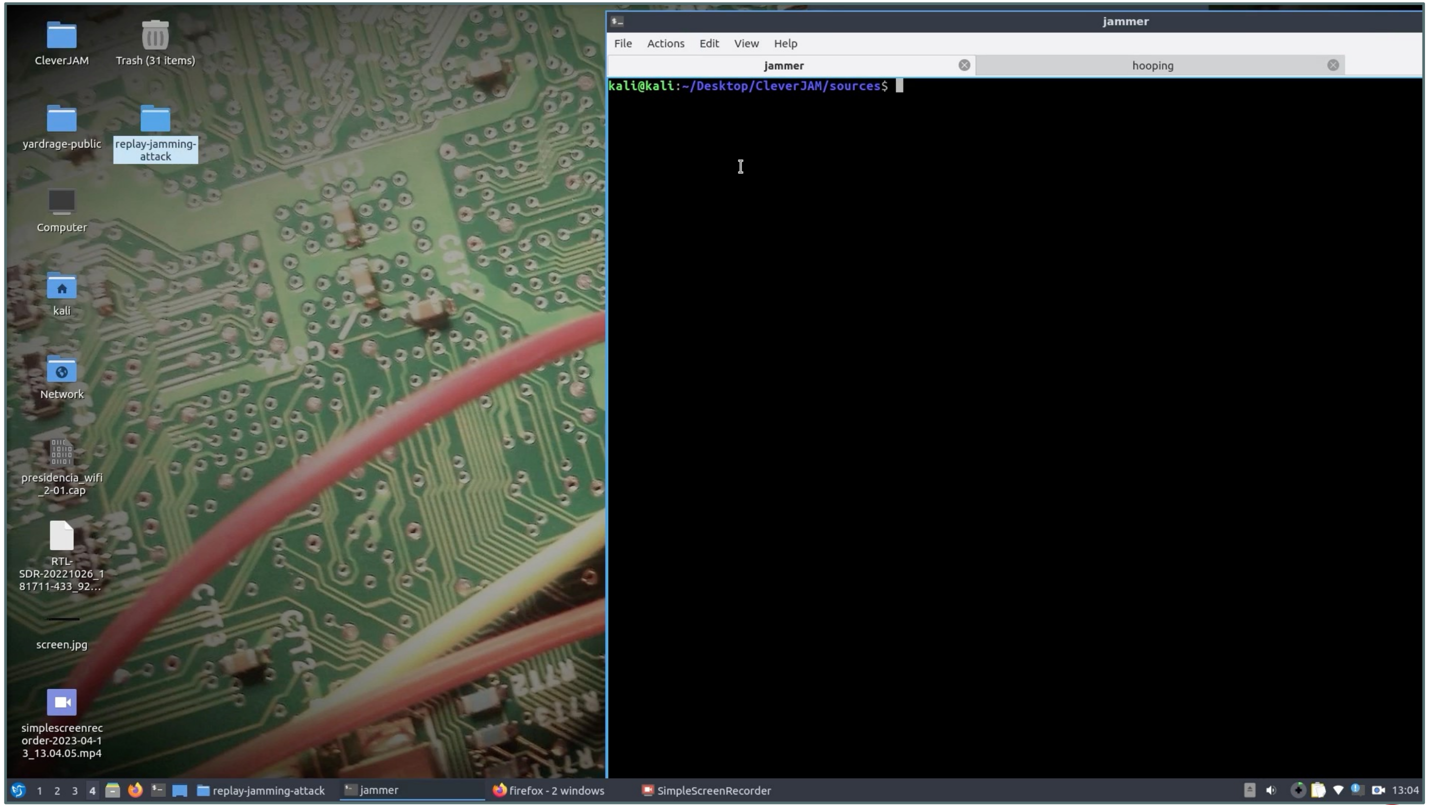
```
<<< Welcome to GNU Radio Companion 3.8.1.0 >>>

Block paths:
	/usr/share/gnuradio/grc/blocks
	/usr/local/share/gnuradio/grc/blocks

Loading: "/home/kali/Desktop/CleverJAM/sources/jam.grc"
>>> Done
```

Id	Value
Imports	
Variables	
bandwidth	<Open Properties>
bb_gain	<Open Properties>
cent_freq	<Open Properties>
if_gain	<Open Properties>
rf_gain	<Open Properties>

Executing Rolljam (continued)



```
kali@kali:~/Desktop/CleverJAM/sources$
```

#HITB2023AMS

Rollback
Time-Agnostic Re-Synchronization
Replay Attack

CVE-2022-36945

CVE-2022-37305

CVE-2022-37418

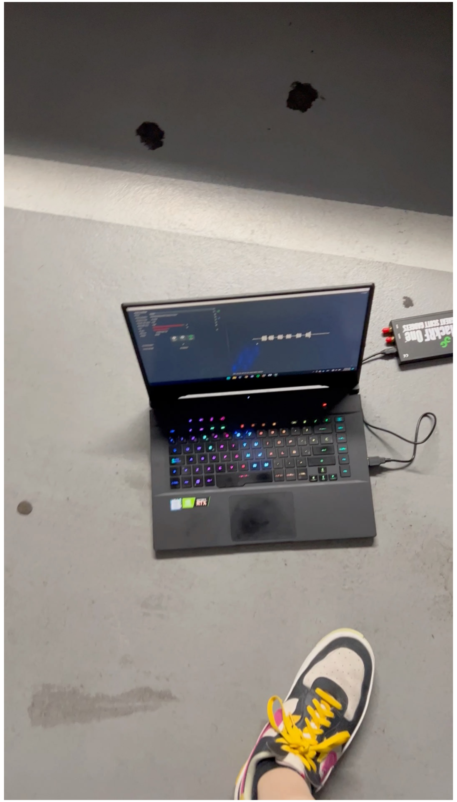
Original Disclosure

- Presented at **Blackhat USA 2022**
  - Authors: Levente Csikor & Hoon Wei Lim
  - US-22-Csikor-RollBack-A-New-Time-Agnostic-Replay-Attack
- Official paper
  - Rollback Paper

Demo Time

LOOSE ATTACK

👀

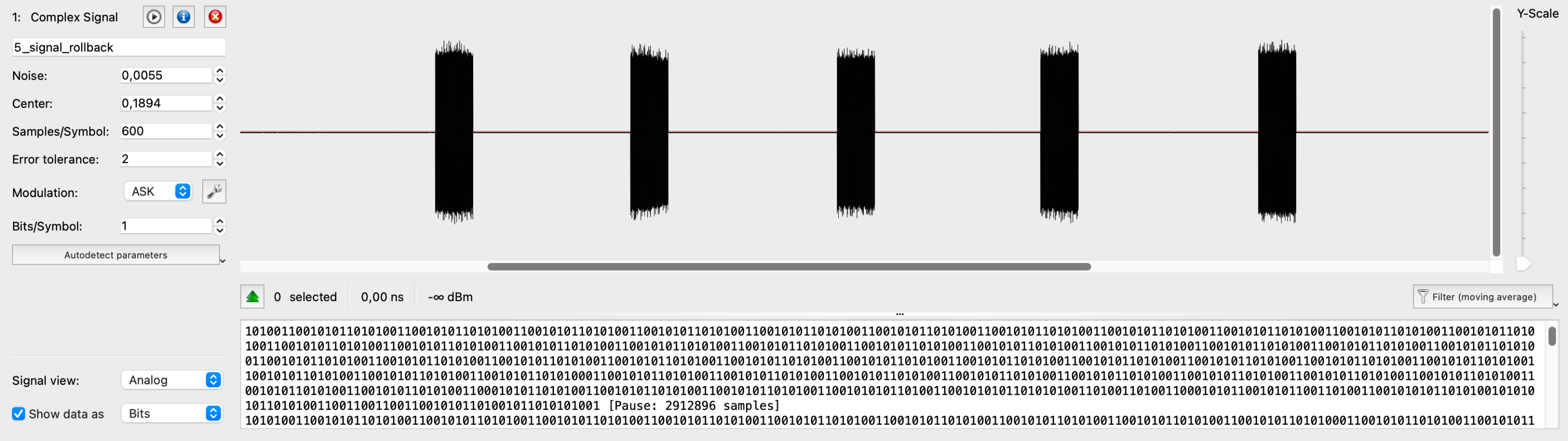


ROLLBACK TIME!

What is Rollback Exactly?

- Rollback is **DIFFERENT** than Rolljam
- Don't need to **JAM** any signal
- Owner uses the vehicle/key fob as usual
  - Vehicle acts as **intended**, can **receive** the signals as usual
- Attack → Re-synchronize the car with **used** codes
  - 2 to 3 codes for resync
- Original affected vehicles: Kia, Hyundai, Mazda, Nissan, and Toyota
  - New discoveries: ~~censored~~ (2013), ~~censored~~ (2019) and ~~censored~~ (2022)

How Rollback Works



5_signal_rollback

Noise: 0,0055

Center: 0,1894

Samples/Symbol: 600

Error tolerance: 2

Modulation: ASK

Bits/Symbol: 1

Signal view: Analog

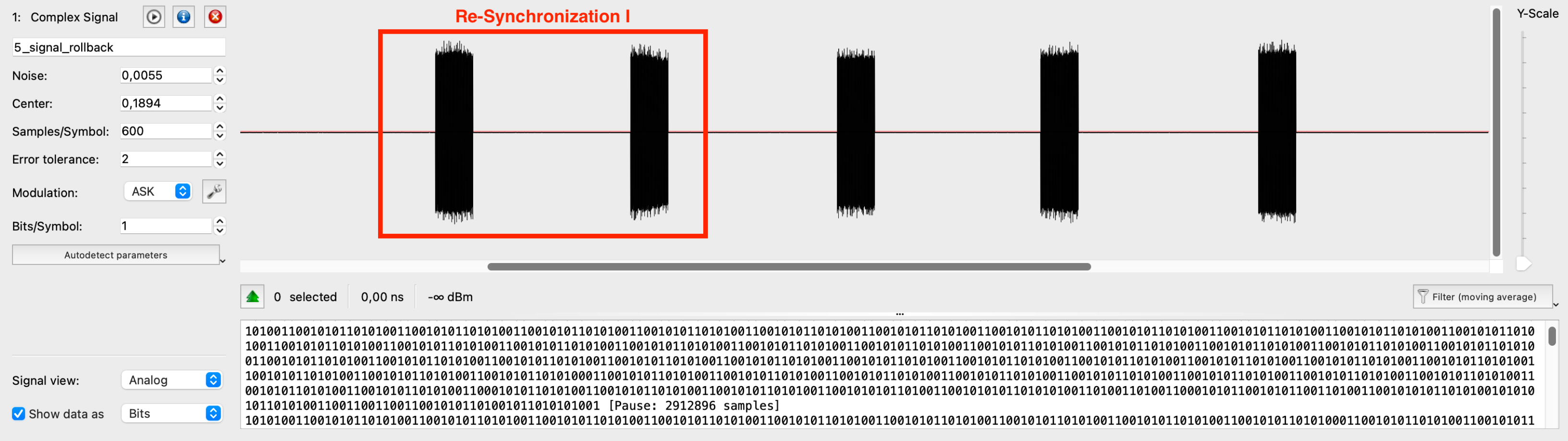
☑ Show data as Bits

0 selected 0,00 ns -∞ dBm

```
1010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010
1001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010
0110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001
1001010110101001100101011010100110010101101010001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011
0010101101010011001010110101001100010101101010011001010110101001100101011010100110010101101001100101010110100110010101011010101001101001101001100010101100101011001101001100101010110101001010
10110101001100110011001100101011010010110101001 [Pause: 2912896 samples]
1010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100011001010110101001100101011
```

- Bag of 5 old codes

How Rollback Works



1: Complex Signal

5_signal_rollback

Noise: 0,0055

Center: 0,1894

Samples/Symbol: 600

Error tolerance: 2

Modulation: ASK

Bits/Symbol: 1

Signal view: Analog

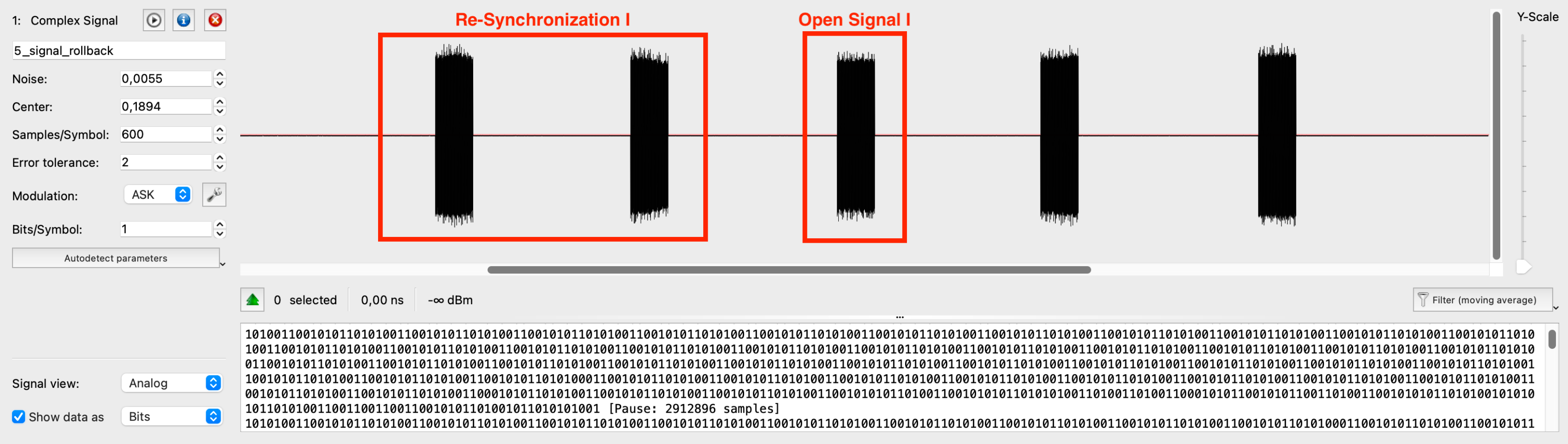
☑ Show data as Bits

0 selected | 0,00 ns | -∞ dBm

```
1010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010
1001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010
0110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001
1001010110101001100101011010100110010101101010001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011
0010101101010011001010110101001100010101101010011001010110101001100101011010100110010101011010011001010101101010100110100110100110001010110010101100110100110010101011010100101010
1011010100110011001100110010101101001011010101001 [Pause: 2912896 samples]
1010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100011001010110101001100101011
```

- Replay the first 2 codes

How Rollback Works



Re-Synchronization I

Open Signal I

1: Complex Signal

5_signal_rollback

Noise: 0,0055

Center: 0,1894

Samples/Symbol: 600

Error tolerance: 2

Modulation: ASK

Bits/Symbol: 1

Signal view: Analog

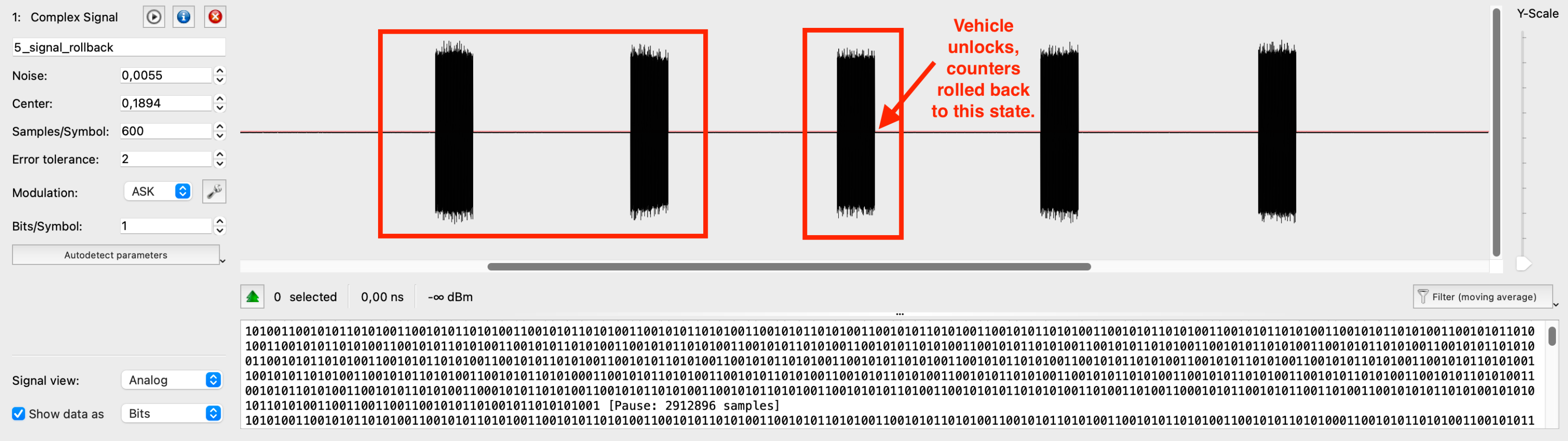
☑ Show data as Bits

0 selected | 0,00 ns | -∞ dBm

```
101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010
100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010
011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001
100101011010100110010101101010011001010110101000110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011
001010110101001100101011010100110001010110101001100101011010100110010101101010011001010110101001100101010110100110010101011010101001101001101001100110100110100110001010110010101100110100110010101011010100101010
1011010100110011001100110010101101001011010101001 [Pause: 2912896 samples]
101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100011001010110101001100101011
```

- Replay the first 2 codes
  - The vehicle is unlocked with the next code sent, the counters return to this state

How Rollback Works



1: Complex Signal

5_signal_rollback

Noise: 0,0055

Center: 0,1894

Samples/Symbol: 600

Error tolerance: 2

Modulation: ASK

Bits/Symbol: 1

Signal view: Analog

☑ Show data as Bits

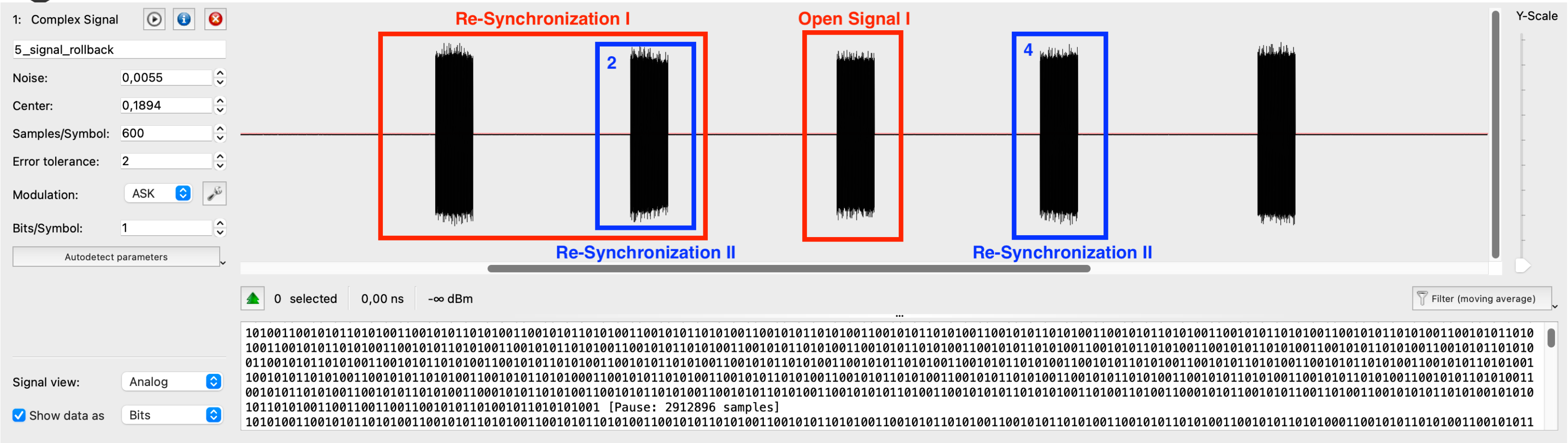
0 selected 0,00 ns -∞ dBm

```
1010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010
1001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010
0110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001
1001010110101001100101011010100110010101101010001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011
0010101101010011001010110101001100010101101010011001010110101001100101011010100110010101011010011001010101101010100110100110100110001010110010101100110100110010101011010100101010
1011010100110011001100110010101101001011010101001 [Pause: 2912896 samples]
1010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100011001010110101001100101011
```

Vehicle unlocks, counters rolled back to this state.

- Replay the first 2 codes
  - The vehicle is unlocked with the next code sent, the counters return to this state

How Rollback Works (continued)



1: Complex Signal

5_signal_rollback

Noise: 0,0055

Center: 0,1894

Samples/Symbol: 600

Error tolerance: 2

Modulation: ASK

Bits/Symbol: 1

Signal view: Analog

☑ Show data as Bits

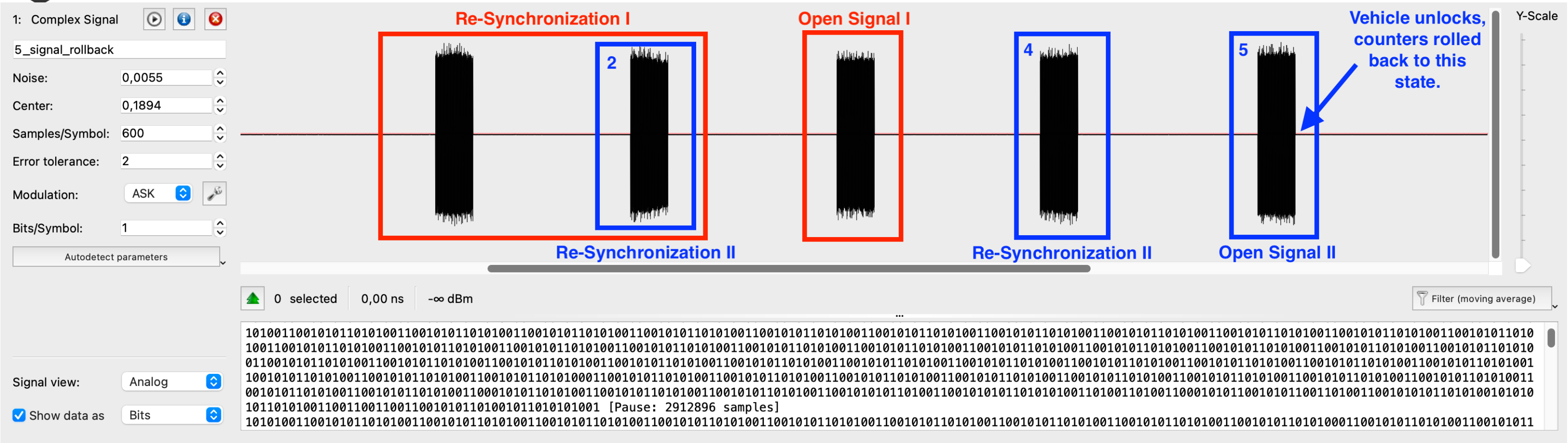
0 selected 0,00 ns -∞ dBm

```
1010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010
1001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010
0110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001
1001010110101001100101011010100110010101101010001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011
0010101101010011001010110101001100010101101010011001010110101001100101011010100110010101011010011001010101101010100110100110100110001010110010101100110100110010101011010100101010
10111010100110011001100110010101101001011010101001 [Pause: 2912896 samples]
1010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010001100101011010100110010101
```

- Send intercalated signals, in this case 2 and 4, to re-synchronise the vehicle

#HITB2023AMS

How Rollback Works (continued)



1: Complex Signal

5_signal_rollback

Noise: 0,0055

Center: 0,1894

Samples/Symbol: 600

Error tolerance: 2

Modulation: ASK

Bits/Symbol: 1

Signal view: Analog

☑ Show data as Bits

Re-Synchronization I

Re-Synchronization II

2

Open Signal I

4

Re-Synchronization II

5

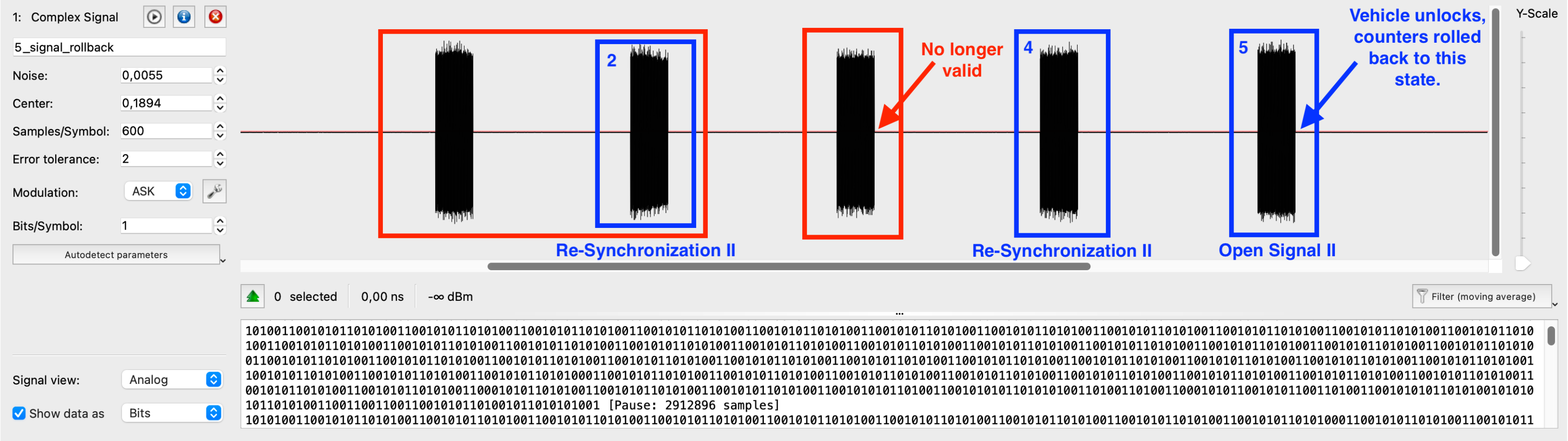
Open Signal II

Vehicle unlocks, counters rolled back to this state.

```
1010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010
1001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010
0110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001
1001010110101001100101011010100110010101101010001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011
0010101101010011001010110101001100010101101010011001010110101001100101011010100110010101011010011001010101101010100110100110100110001010110010101100110100110010101011010100101010
101101010011001100110011001010110100101101010101001 [Pause: 2912896 samples]
1010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010001100101011010100110010101101010011001010110101001100101011
```

- Send intercalated signals, in this case 2 and 4, to re-synchronise the vehicle
- Rollback on signal 5

How Rollback Works (continued)



1: Complex Signal

5_signal_rollback

Noise: 0,0055

Center: 0,1894

Samples/Symbol: 600

Error tolerance: 2

Modulation: ASK

Bits/Symbol: 1

Signal view: Analog

☑ Show data as Bits

0 selected | 0,00 ns | -∞ dBm

No longer valid

Vehicle unlocks, counters rolled back to this state.

```
1010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010
1001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010
0110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001
1001010110101001100101011010100110010101101010001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011
0010101101010011001010110101001100010101101010011001010110101001100101011010100110010101101010011001010101101001100101010110101001101001101001100010101100101011001101001100101010110101001010
1011010100110011001100110010101101001011010101001 [Pause: 2912896 samples]
1010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010011001010110101001100101011010100110010101101010001100101011010100110010101101010011001010110101001100101011
```

- Send intercalated signals, in this case 2 and 4, to re-synchronise the vehicle
- Rollback on signal 5
- Red sync no longer valid

What is new here?

Rollback

Providing a fresh and profound alternative perspective

Rollback

- Is it possible to carry out a rollback attack on different days?

- Is it possible to execute the attack with obsolete codes collected on different days?

Rollback

- Is it possible to carry out a rollback attack on different days?

- Is it possible to execute the attack with obsolete codes collected on different days?
- Perform Rollback on different days
- Perform Rollback on a run of 50 old codes

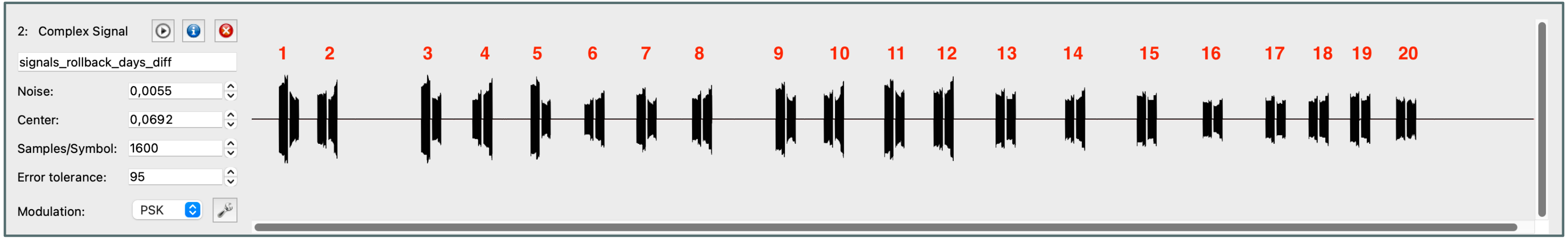
Rollback Principles

What is new here?

- We **do not need** jamming
- Signals **do not need** to be sequential
  - In some cases they need to be strictly sequential
- Signals **persit** over time
- **Loose**, **strict**, and **timeframes**

Rollback: First New Scenario

HOW POWERFUL IS?!



2: Complex Signal

signals_rollback_days_diff

Noise: 0,0055

Center: 0,0692

Samples/Symbol: 1600

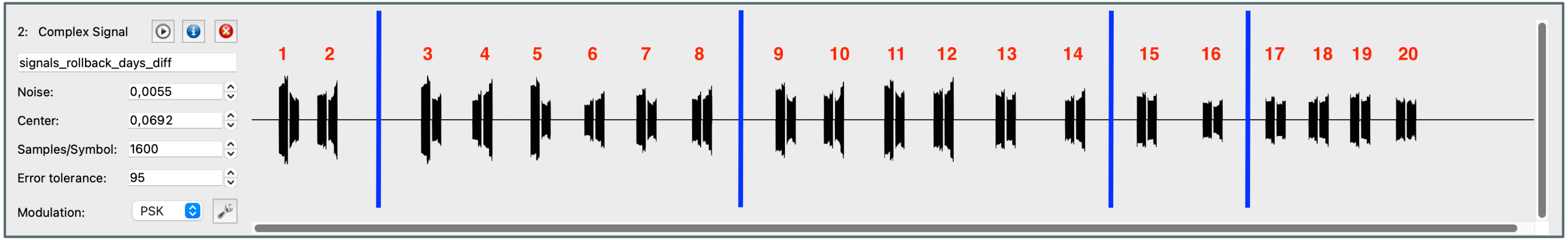
Error tolerance: 95

Modulation: PSK

- Bag of 20 old codes

Rollback: First New Scenario

HOW POWERFUL IS?!



2: Complex Signal

signals_rollback_days_diff

Noise: 0,0055

Center: 0,0692

Samples/Symbol: 1600

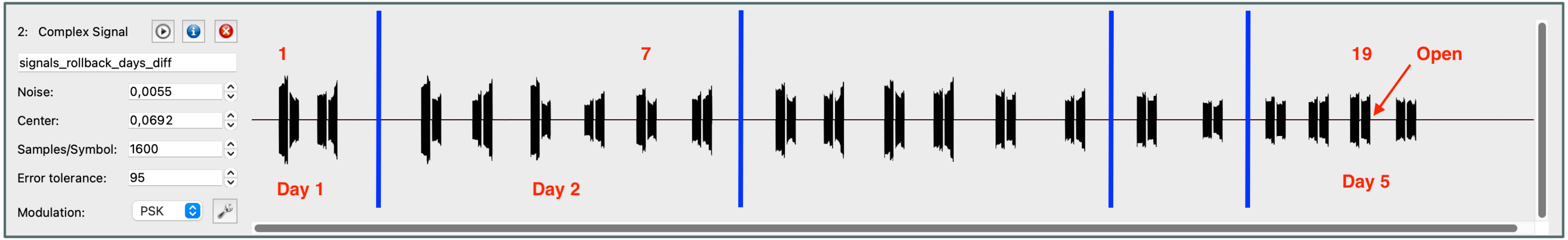
Error tolerance: 95

Modulation: PSK

- Bag of 20 old codes
- Five days of grabbing

Rollback: First New Scenario

HOW POWERFUL IS?!



2: Complex Signal

signals_rollback_days_diff

Noise: 0,0055

Center: 0,0692

Samples/Symbol: 1600

Error tolerance: 95

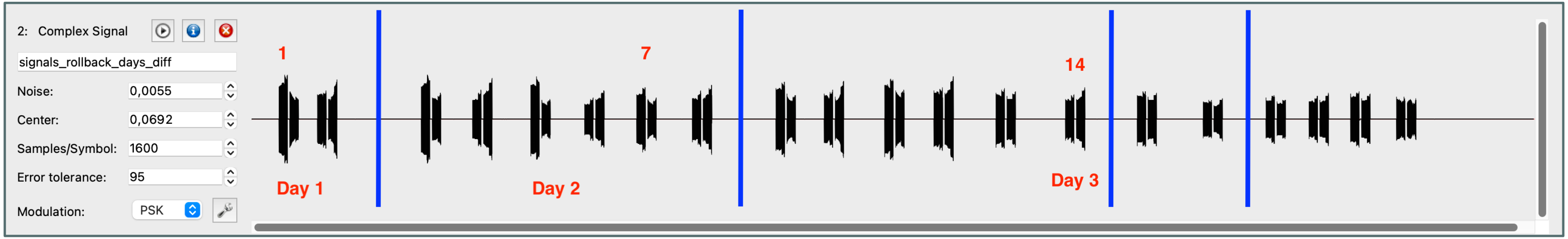
Modulation: PSK

- Bag of 20 old codes
- Five days of grabbing
- Replay 1, 7, and 19 → **Open**

Rollback: First New Scenario (continued)

FAIL VERSION

HOW POWERFUL IS?!



2: Complex Signal

signals_rollback_days_diff

Noise: 0,0055

Center: 0,0692

Samples/Symbol: 1600

Error tolerance: 95

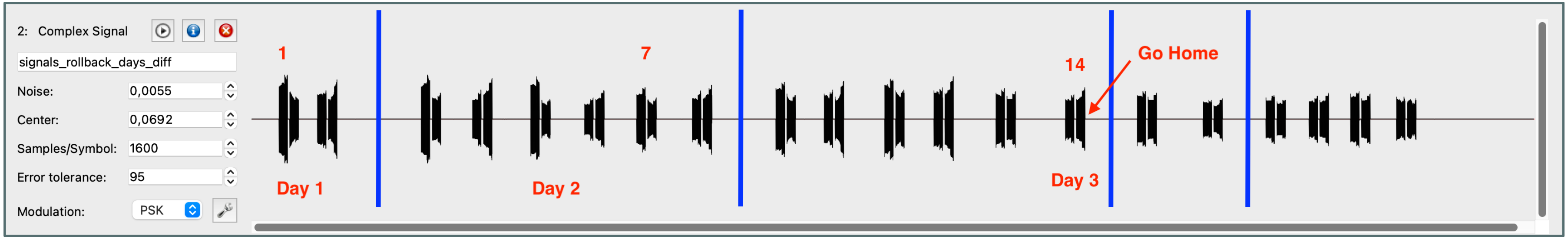
Modulation: PSK

- Replay 1, 7, and 14

Rollback: First New Scenario (continued)

FAIL VERSION

HOW POWERFUL IS?!



2: Complex Signal

signals_rollback_days_diff

Noise: 0,0055

Center: 0,0692

Samples/Symbol: 1600

Error tolerance: 95

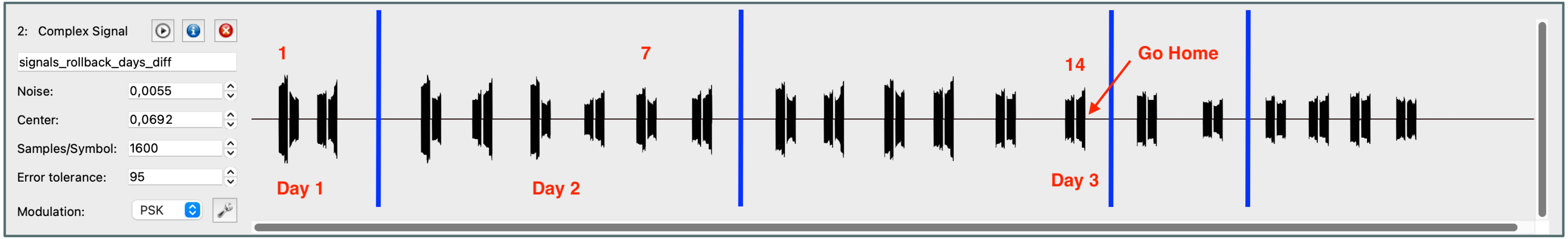
Modulation: PSK

- Replay 1, 7, and 14 → **Go Home**

Rollback: First New Scenario (continued)

FAIL VERSION

HOW POWERFUL IS?!



2: Complex Signal

signals_rollback_days_diff

Noise: 0,0055

Center: 0,0692

Samples/Symbol: 1600

Error tolerance: 95

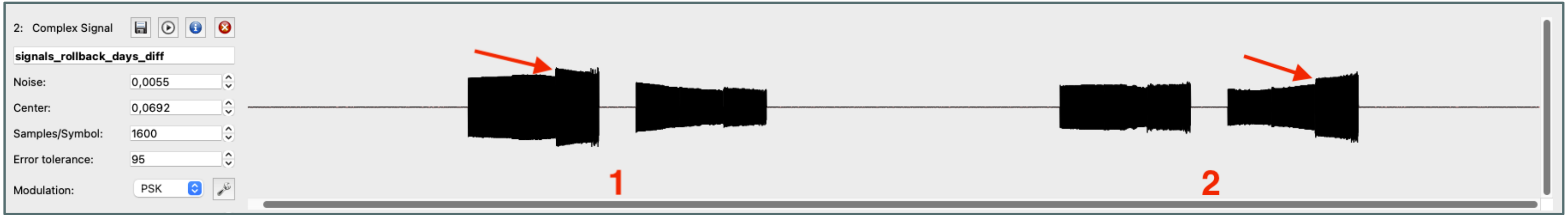
Modulation: PSK

- Replay 1, 7, and 14 → Go Home

Rollback: First New Scenario (continued)

FAIL VERSION

HOW POWERFUL IS?!



2: Complex Signal

signals_rollback_days_diff

Noise: 0,0055

Center: 0,0692

Samples/Symbol: 1600

Error tolerance: 95

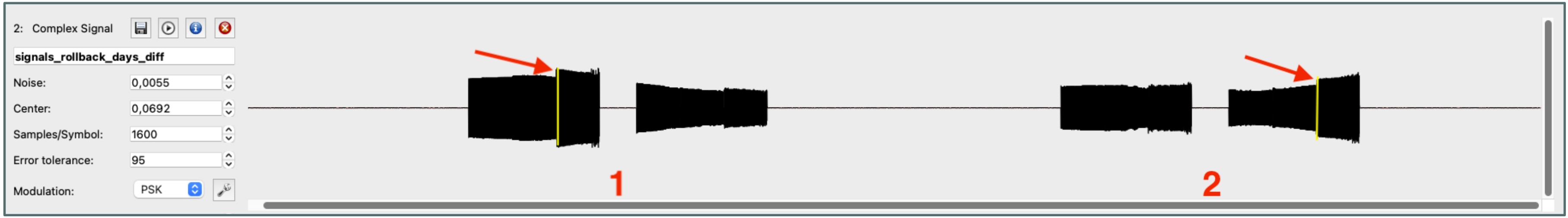
Modulation: PSK

- Even signal: 1
- Odd signal: 2

Rollback: First New Scenario (continued)

FAIL VERSION

HOW POWERFUL IS?!



2: Complex Signal

signals_rollback_days_diff

Noise: 0,0055

Center: 0,0692

Samples/Symbol: 1600

Error tolerance: 95

Modulation: PSK

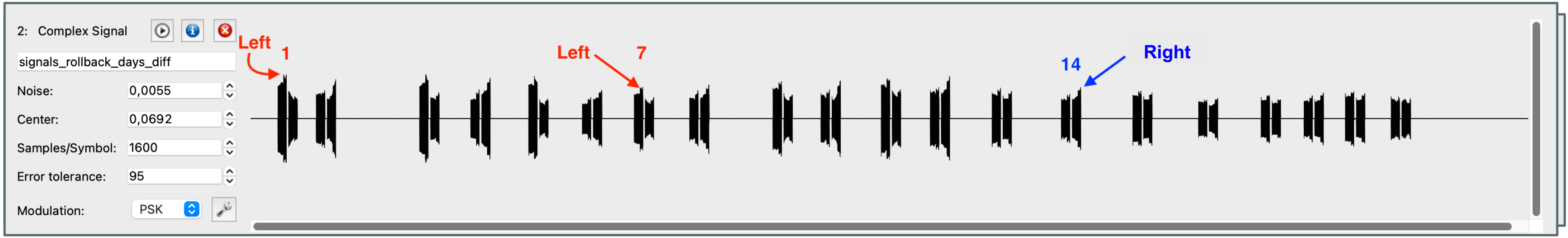
- Even signal: 1
- Odd signal: 2

- Displacement of the peak

Rollback: First New Scenario (continued)

FAIL VERSION

HOW POWERFUL IS?!



2: Complex Signal

signals_rollback_days_diff

Noise: 0,0055

Center: 0,0692

Samples/Symbol: 1600

Error tolerance: 95

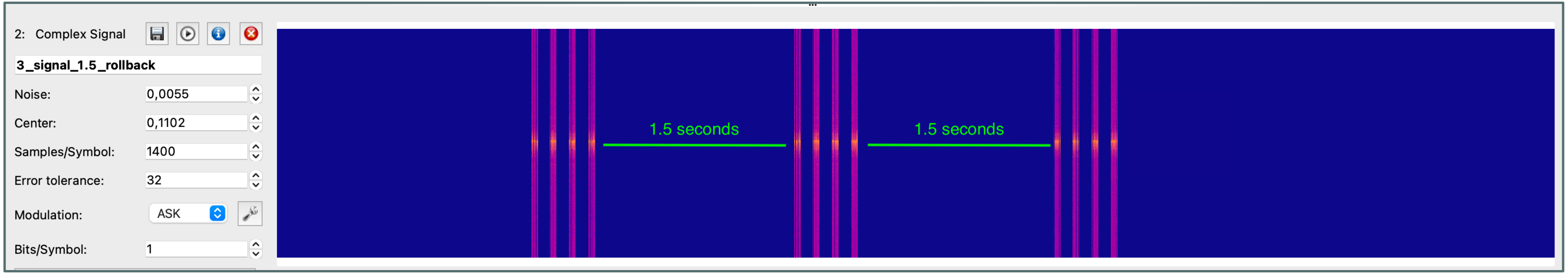
Modulation: PSK

- Odd + odd = open
- Even + even = open
- Odd + even = go home

Rollback: Second New Scenario

TIMING TIME :D

STRICT SEQUENCE!



2: Complex Signal

3_signal_1.5_rollback

Noise: 0,0055

Center: 0,1102

Samples/Symbol: 1400

Error tolerance: 32

Modulation: ASK

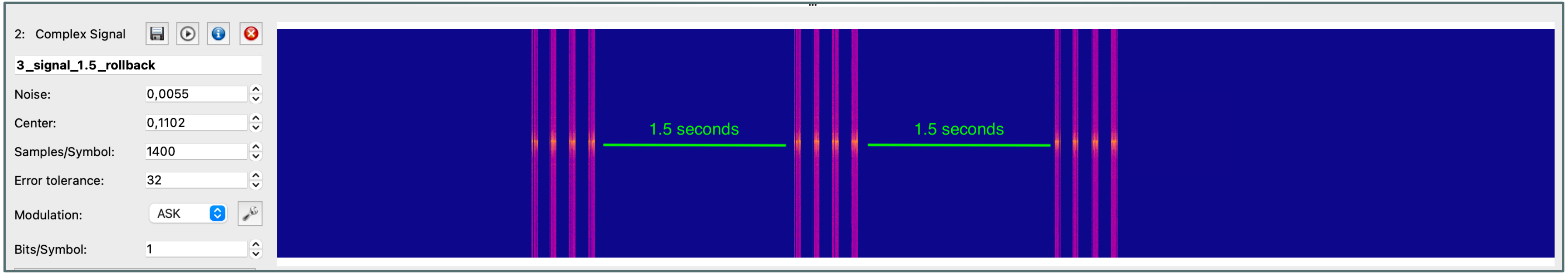
Bits/Symbol: 1

- 3 different signals

Rollback: Second New Scenario

TIMING TIME :D

STRICT SEQUENCE!



2: Complex Signal

3_signal_1.5_rollback

Noise: 0,0055

Center: 0,1102

Samples/Symbol: 1400

Error tolerance: 32

Modulation: ASK

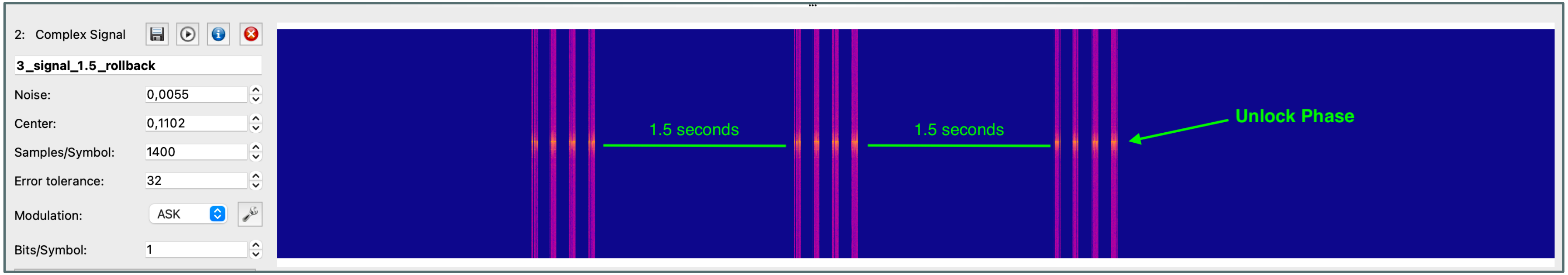
Bits/Symbol: 1

- 3 different signals
- Timeframe of 1.5 between signals

Rollback: Second New Scenario

TIMING TIME :D

STRICT SEQUENCE!



2: Complex Signal

3_signal_1.5_rollback

Noise: 0,0055

Center: 0,1102

Samples/Symbol: 1400

Error tolerance: 32

Modulation: ASK

Bits/Symbol: 1

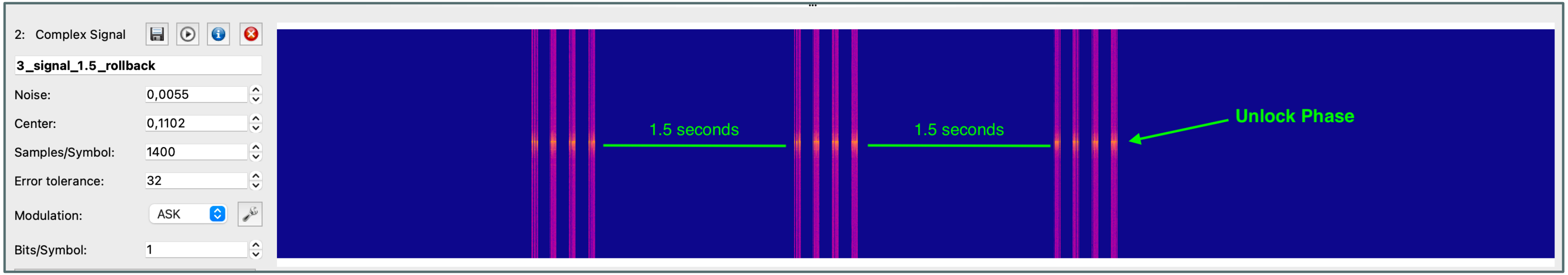
- 3 different signals
- Timeframe of 1.5 between signals

#HITB2023AMS

Rollback: Second New Scenario

TIMING TIME :D

STRICT SEQUENCE!



2: Complex Signal

3_signal_1.5_rollback

Noise: 0,0055

Center: 0,1102

Samples/Symbol: 1400

Error tolerance: 32

Modulation: ASK

Bits/Symbol: 1

- 3 different signals
- Timeframe of 1.5 between signals

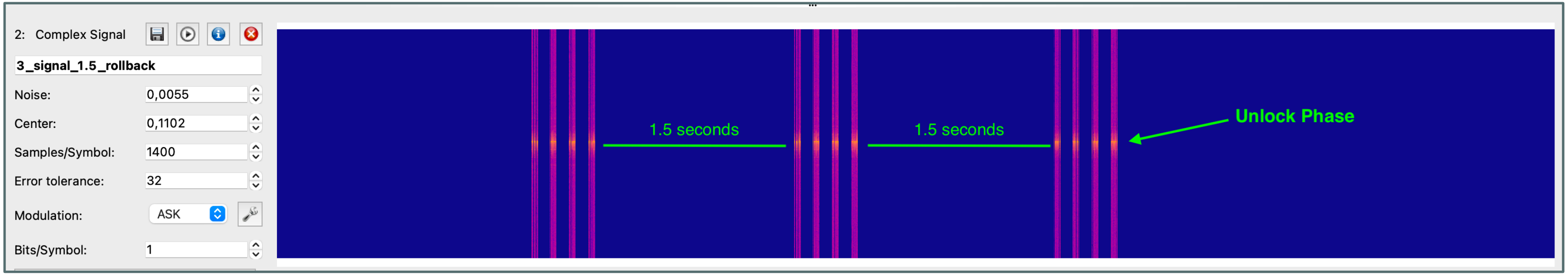
WHAT'S NEW?

IOActive.

Rollback: Second New Scenario

TIMING TIME :D

STRICT SEQUENCE!



2: Complex Signal

3_signal_1.5_rollback

Noise: 0,0055

Center: 0,1102

Samples/Symbol: 1400

Error tolerance: 32

Modulation: ASK

Bits/Symbol: 1

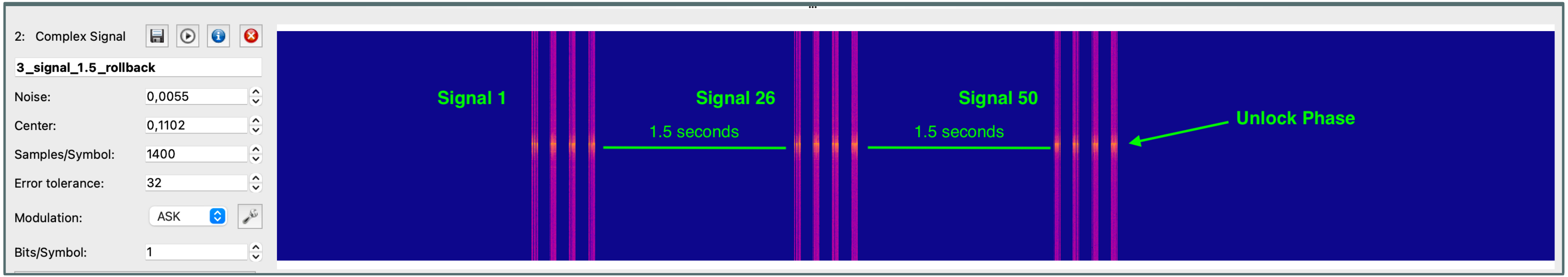
- 3 different signals
- Timeframe of 1.5 between signals
- Four days of signal capturing

WHAT'S NEW?

#HITB2023AMS

Rollback: Second New Scenario

TIMING TIME :D HACKED :) STRICT SEQUENCE!



2: Complex Signal

3_signal_1.5_rollback

Noise: 0,0055

Center: 0,1102

Samples/Symbol: 1400

Error tolerance: 32

Modulation: ASK

Bits/Symbol: 1

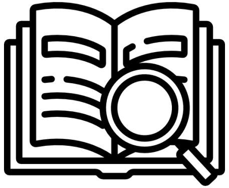
- 3 different signals
- Timeframe of 1.5 between signals
- Four days of signal capturing
- Bag of 50 codes!

WHAT'S NEW?

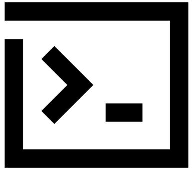
Trust the Process

- No methodology
- No a priori indications
- Not access to official documentation

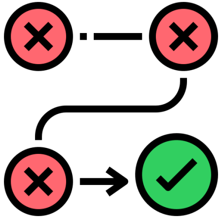
1



2

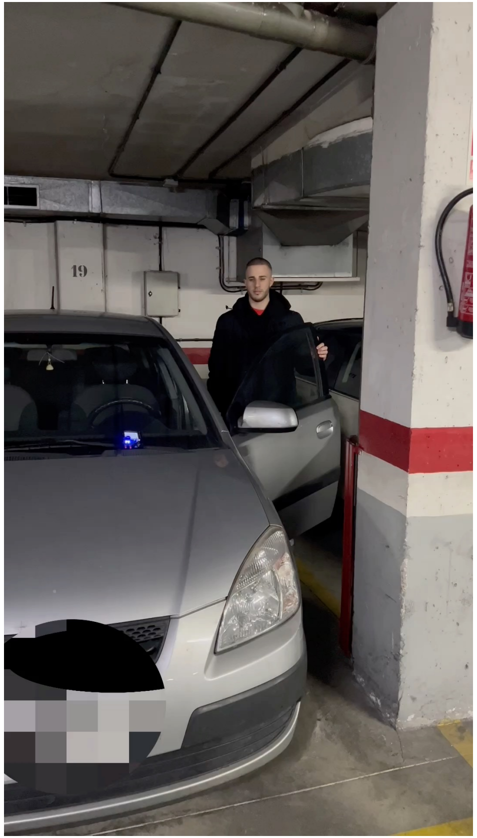


3



Demo Time

STRICT + TIMEFRAME

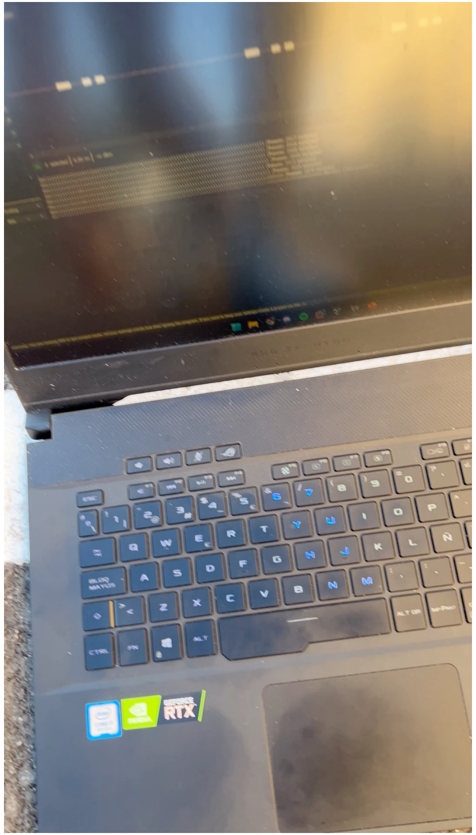


ROLLBACK TIME!

👀

Demo Time

LOOSE ATTACK 👀



ROLLBACK TIME!

Findings

- Modern vehicles still affected
- Jamming is not necessary
- Design flaw in some manufacturers
  - Can be "*fixed*" by vehicle manufacturers with software/firmware updates
- More powerful than we thought
  - Repeatable with jumps of up to 50 old codes!
- Depends on code hoping, not days hoping

Mitigations

- Discard old codes used by vehicle manufacturers
- Mandatory physical resynchronisation of the RKEs
- Precautionary measures for most-based jamming attacks
- Establish anti-jamming technology by manufacturers (detect jamming of signals for example)

Q & A

- IOActive ❤
  - Alfredo Pironti
  - Jose Antonio Maldonado
- Hack In The Box
- Eduardo Arriols (@_Hykeos)
- Joel Serna (@JoelSernaMoreno)

✉ carlos.gomez@ioactive.com

@cgomezz_23

in @cgomezquintana