KU LEUVEN

Fast, Furious and Insecure

Lennert Wouters, Eduard Marin, Tomer Ashur, Benedikt Gierlichs and Bart Preneel

COSIC

an imec research group at KU Leuven

Passive Keyless Entry and Start

Challenge

Response

The Tesla Model S key fob

PCB back

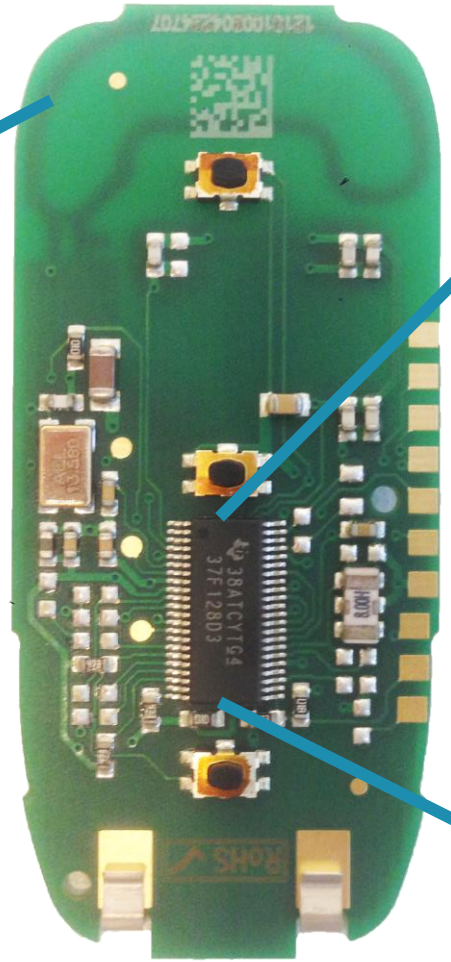
PCB front

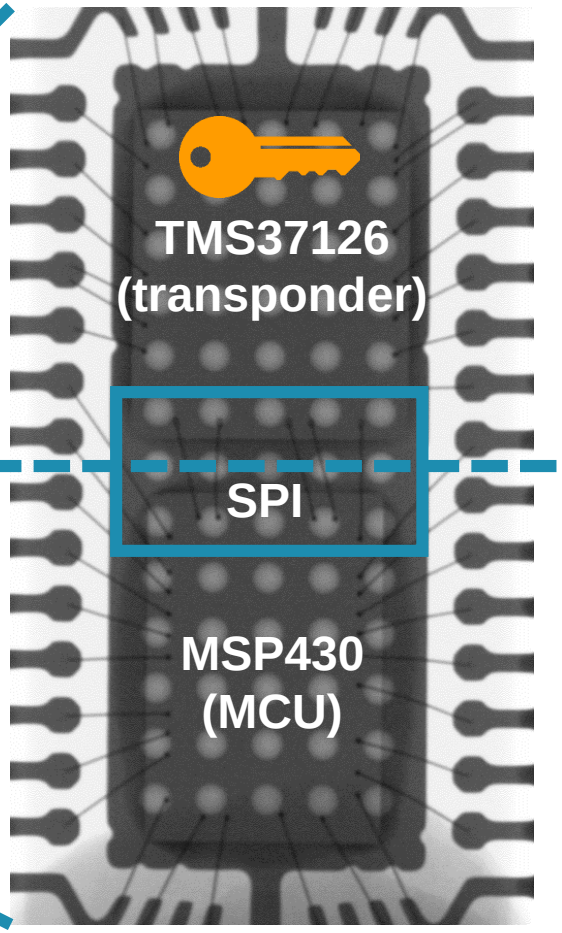
TI TMS37F128 (X-Ray)

UHF antenna

3D LF antenna

MicRF112 transmitter IC



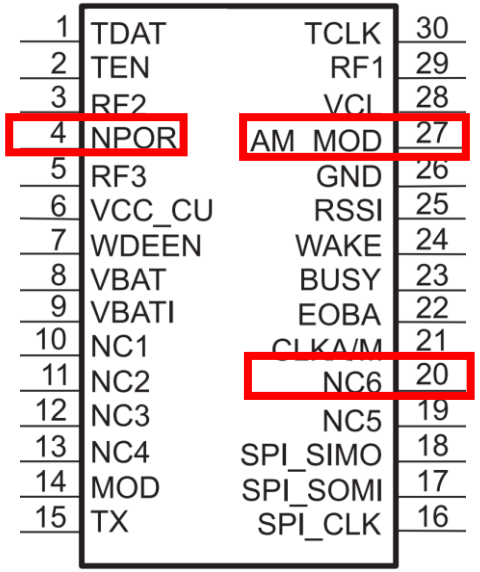


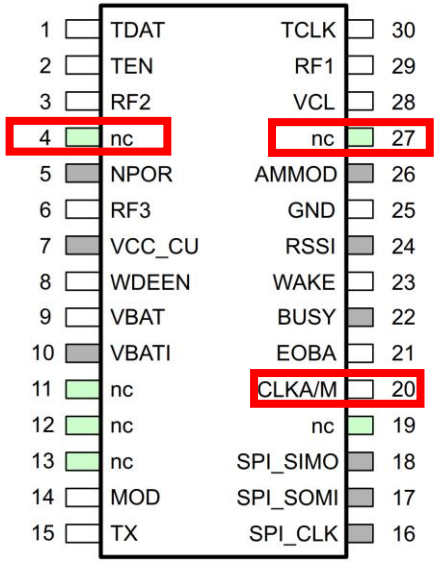
COSIC

KU LEUVEN

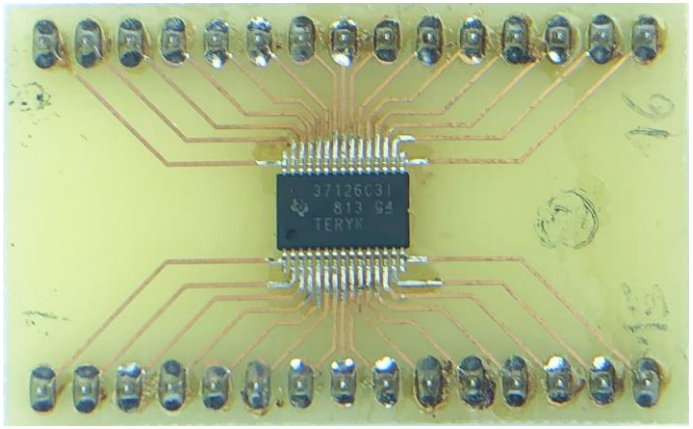
Getting started

- Cannot order the IC's from Farnell/Digikey
- Uncommon package (30 pin TSSOP – 0.5mm pitch)
- Almost no public information on these chips (NDA)
  - The information that is available is inconsistent



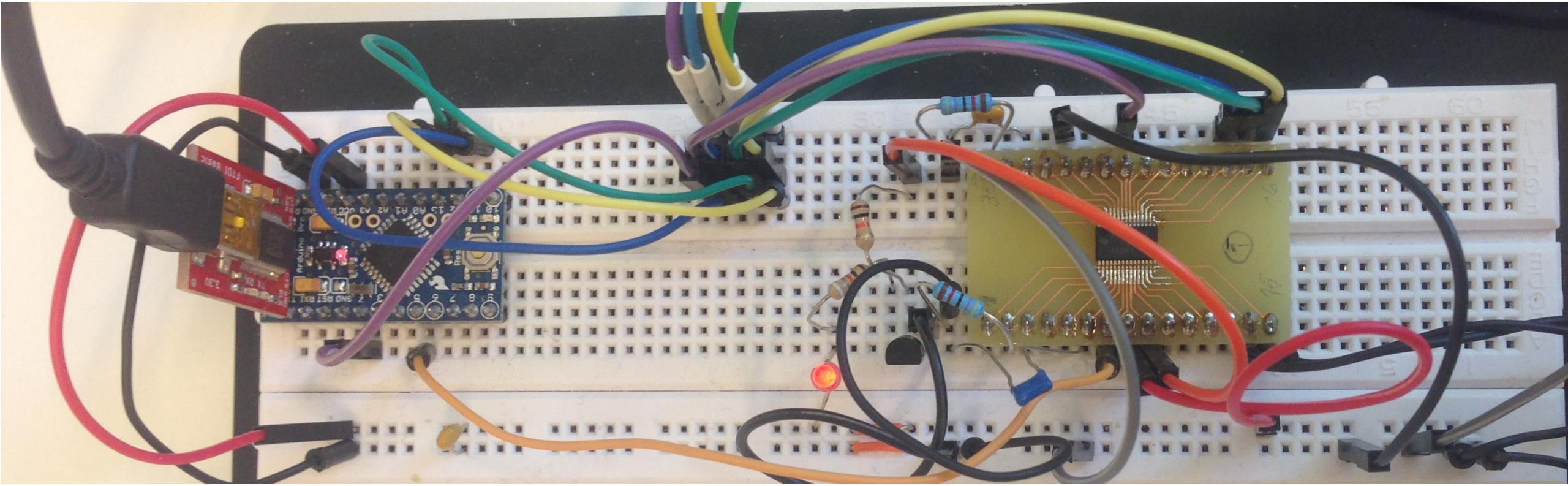


淘宝网
Taobao.com

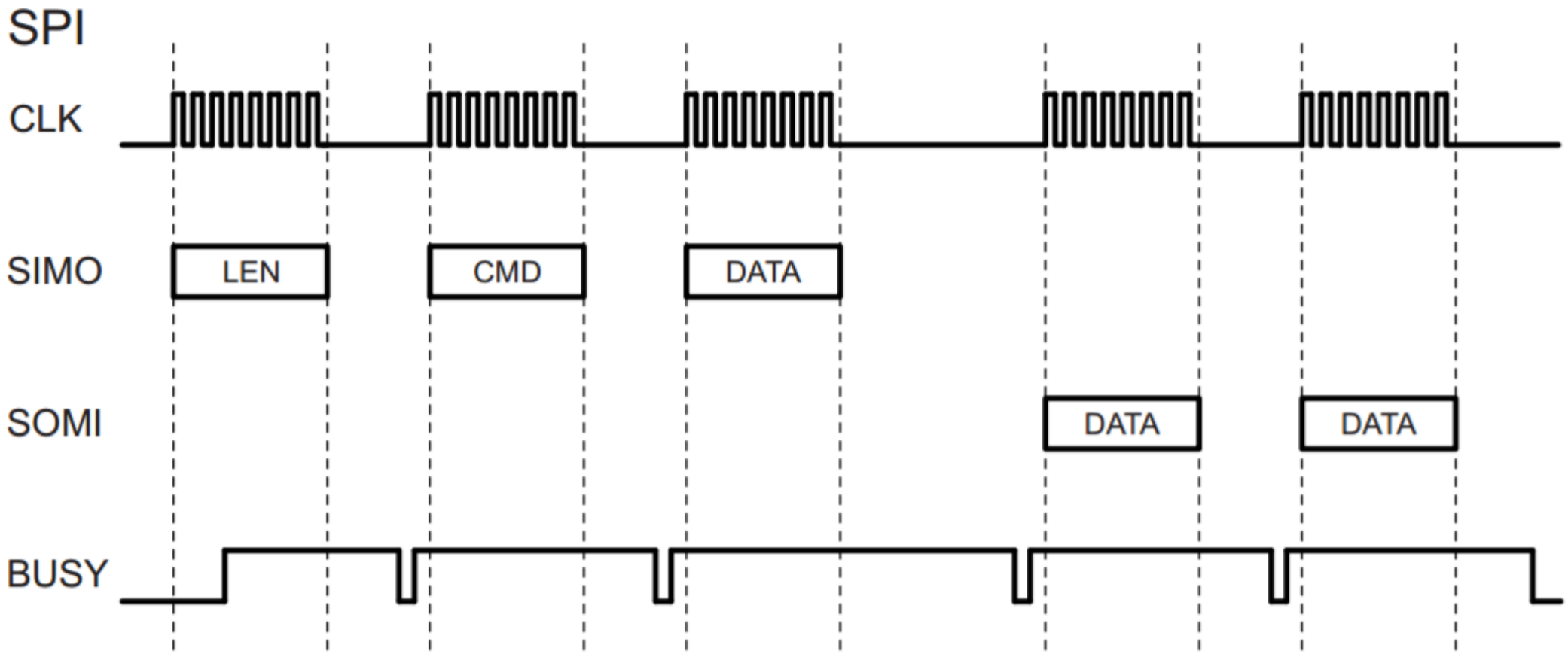


COSIC KU LEUVEN

Connecting to the TMS37126



The Serial Peripheral Interface (SPI)



Source: http://www.ti.com/lit/an/spna147/spna147.pdf

Uncovering undocumented SPI commands

- SPI BUSY line indicates when the slave is ready for the next byte
  - The transponder indicates an error by pulling busy high or low for a long period

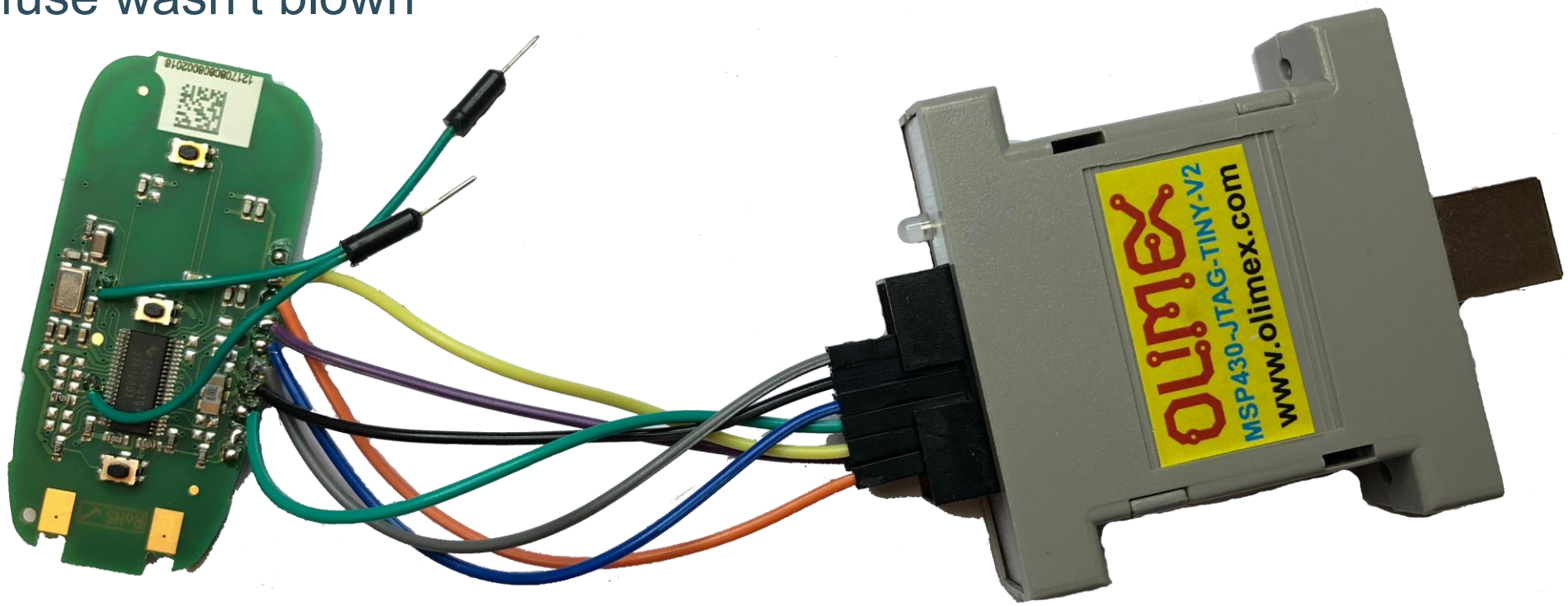
- Observation 1:
  - Error if CMD value is incorrect
- Observation 2:
  - If LEN is 0xFF and the CMD value is correct we get an error after the correct number of bytes (LEN) has been sent

Uncovering undocumented SPI commands

Action	LEN	CMD	WA
DST40(C, K1)	0x06	0x84	NA
DST_UNK(C, K1)	0x06	0x85	NA
DST40(C, K2)	0x06	0x86	NA
DST_UNK(C, K2)	0x06	0x87	NA
Change K1	0x07	0x01	0x11
Change K2	0x07	0x01	0x12

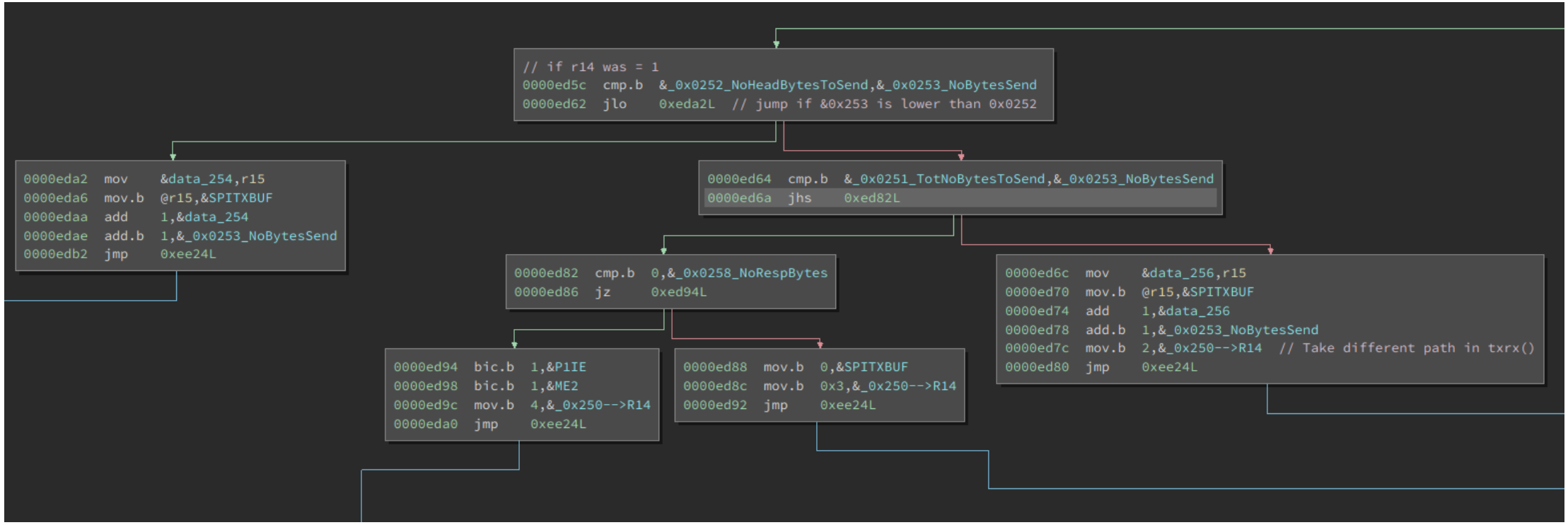
Obtaining MSP430 firmware

- Olimex MSP430-JTAG-TINY-V2 programmer
- JTAG fuse wasn’t blown



MSP430 Static firmware analysis

- Interrupt Vector Table (IVT)
- References to Special Function Registers (SFR)
  - SPI transmit and receive buffers



More info: POC||GTFO 0x11: A TOURIST'S GUIDE TO MSP430

MSP430 Dynamic firmware analysis

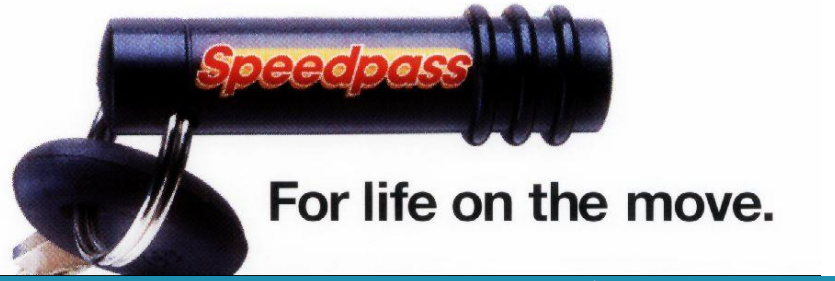
- MSPDebug + Olimex MSP430-JTAG-TINY-V2
- MSP430F1232 supports up to two breakpoints
- Caveat: some debug pins are shared with IO and can trigger interrupts

- Inspect interesting routines + dump RAM and register values
  - Retrieve bytes exchanged over SPI

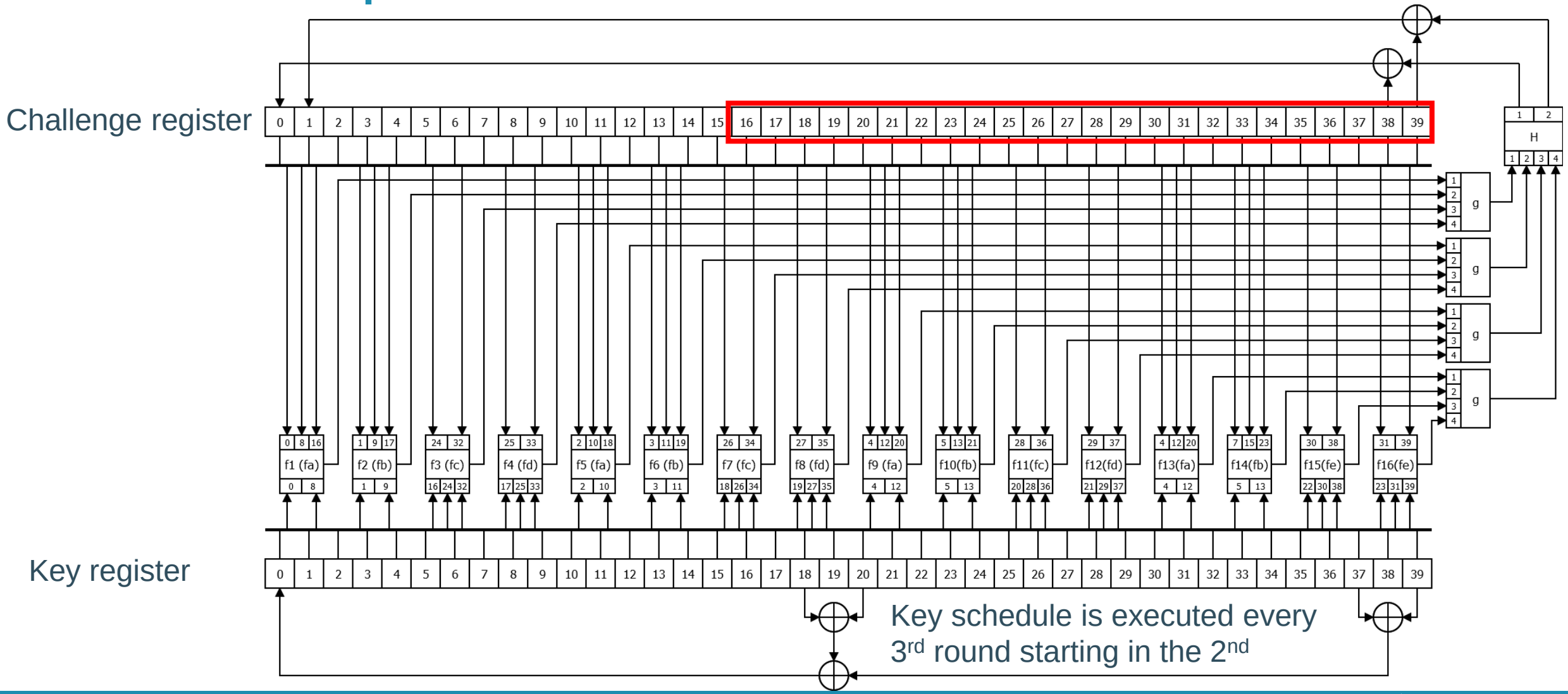
- The firmware is only using CMD 0x86 (DST40) during normal operation

Texas Instruments
Digital Signature Transponder (DST)

- DST40
  - Introduced in 2000
  - 40-bit key
  - Security Analysis of a Cryptographically-Enabled RFID Device (2005)
    - S Bono, M Green, A Stubblefield, A Juels, AD Rubin
  - Used for immobilizer by Ford, Lincoln, Mercury, Nissan and Toyota
  - Exxon-Mobil's Speedpass payment system



DST40 Cipher



COSIC

KU LEUVEN

RF reverse engineering

Key fob RF operation

- Two separate systems:
  - Remote Keyless Entry (RKE)
    - Actions are performed by pressing a button
    - One way communication
  - Passive Keyless Entry and Start (PKES)
    - The car is unlocked automatically if the key fob is in proximity of the vehicle
    - Two way communication

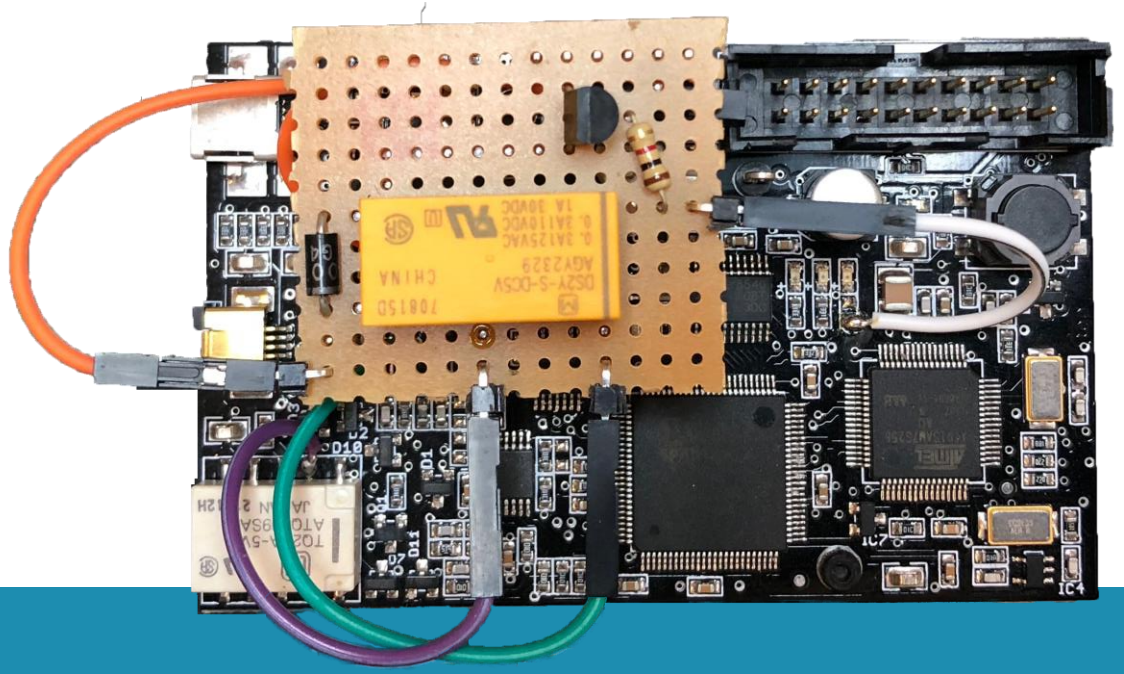
Passive Keyless Entry and Start

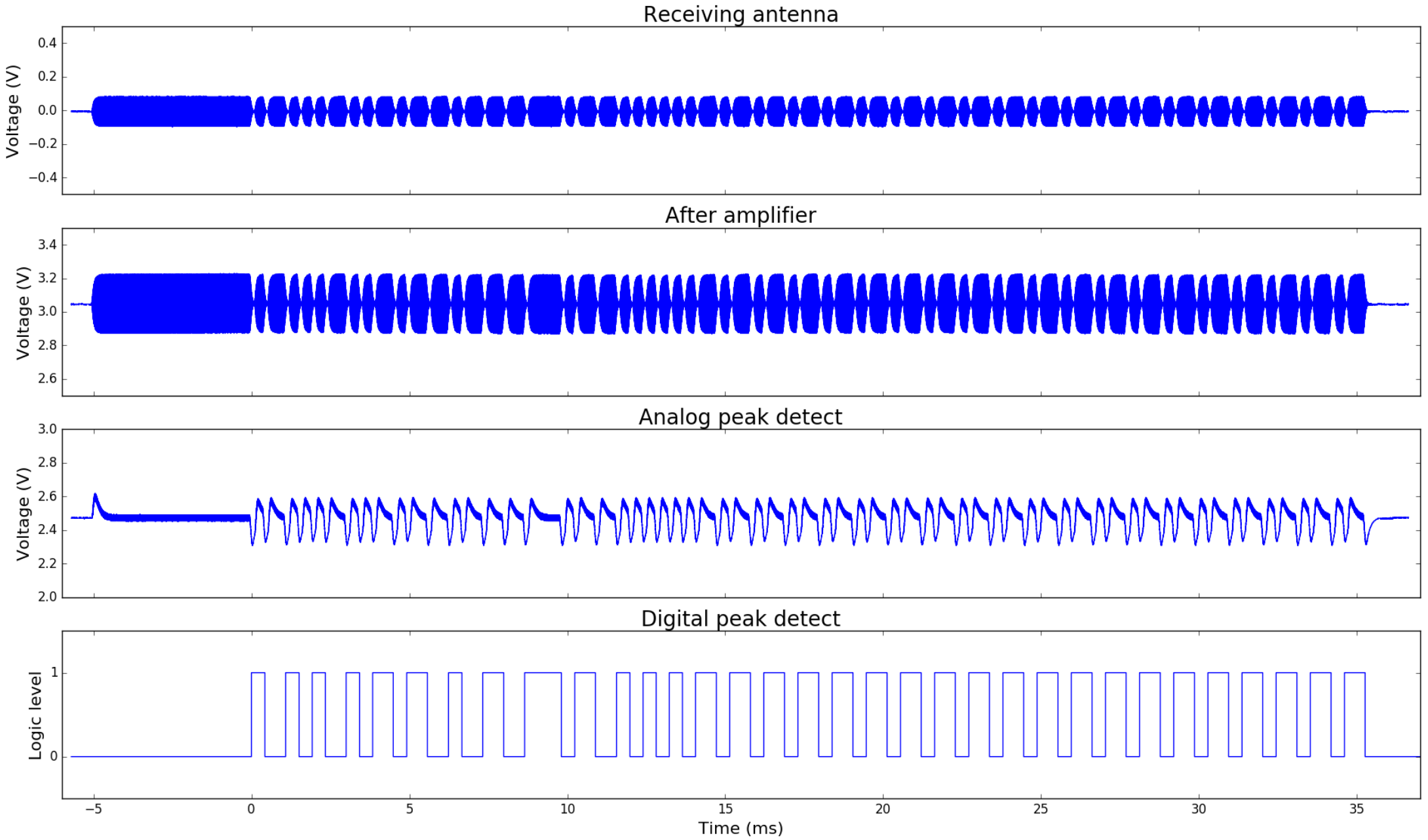
- Ultra High Frequency (433.92 MHz)
  - From key fob to car
  - Easy to receive using widely available tools
    - SDR or Yard Stick One (CC1111)

- Low Frequency (134.2 kHz)
  - From car to key fob
  - More challenging to receive

Low Frequency

- Proxmark3
  - Added DST transponder code for the AT91SAM microcontroller
  - Hardware modification to boost receiver range
  - Custom peak detect code for the FPGA

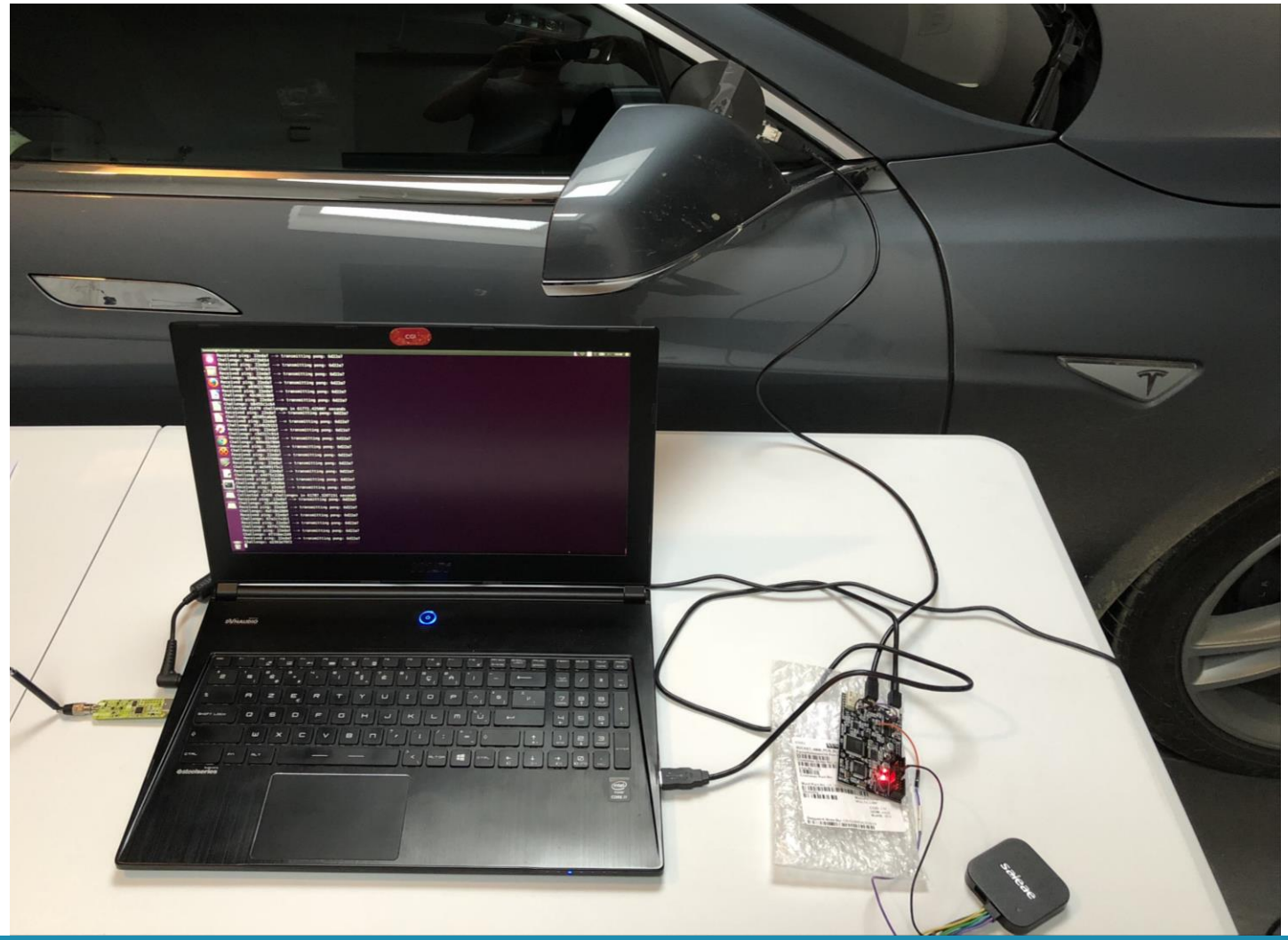


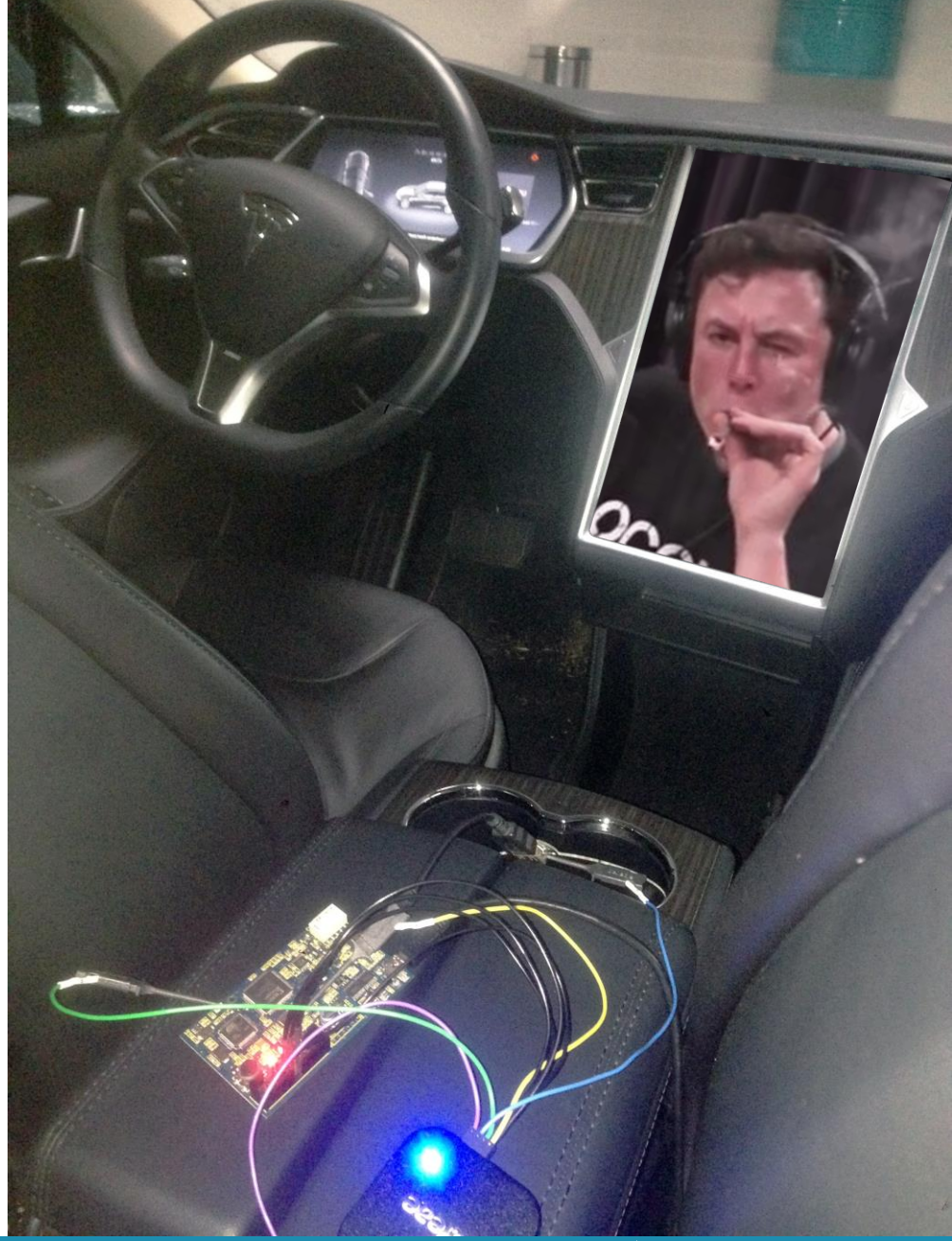


COSIC

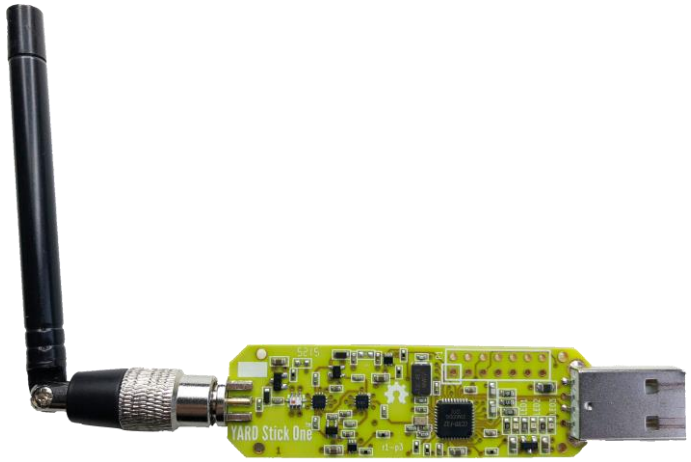
KU LEUVEN

Receiving LF signals

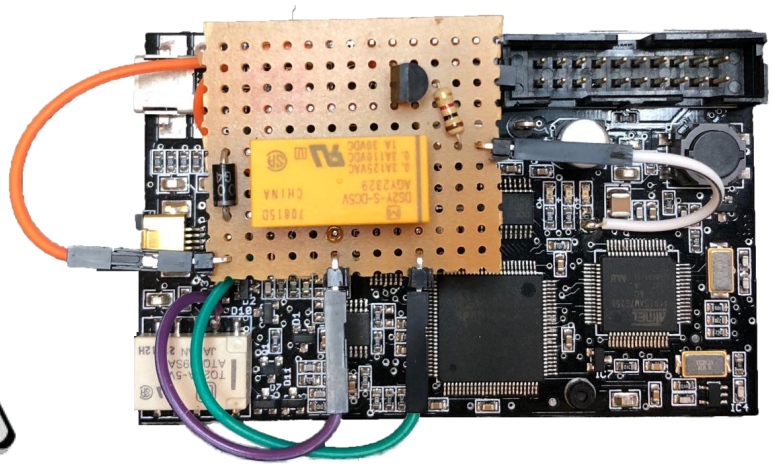




PKES Protocol analyzer

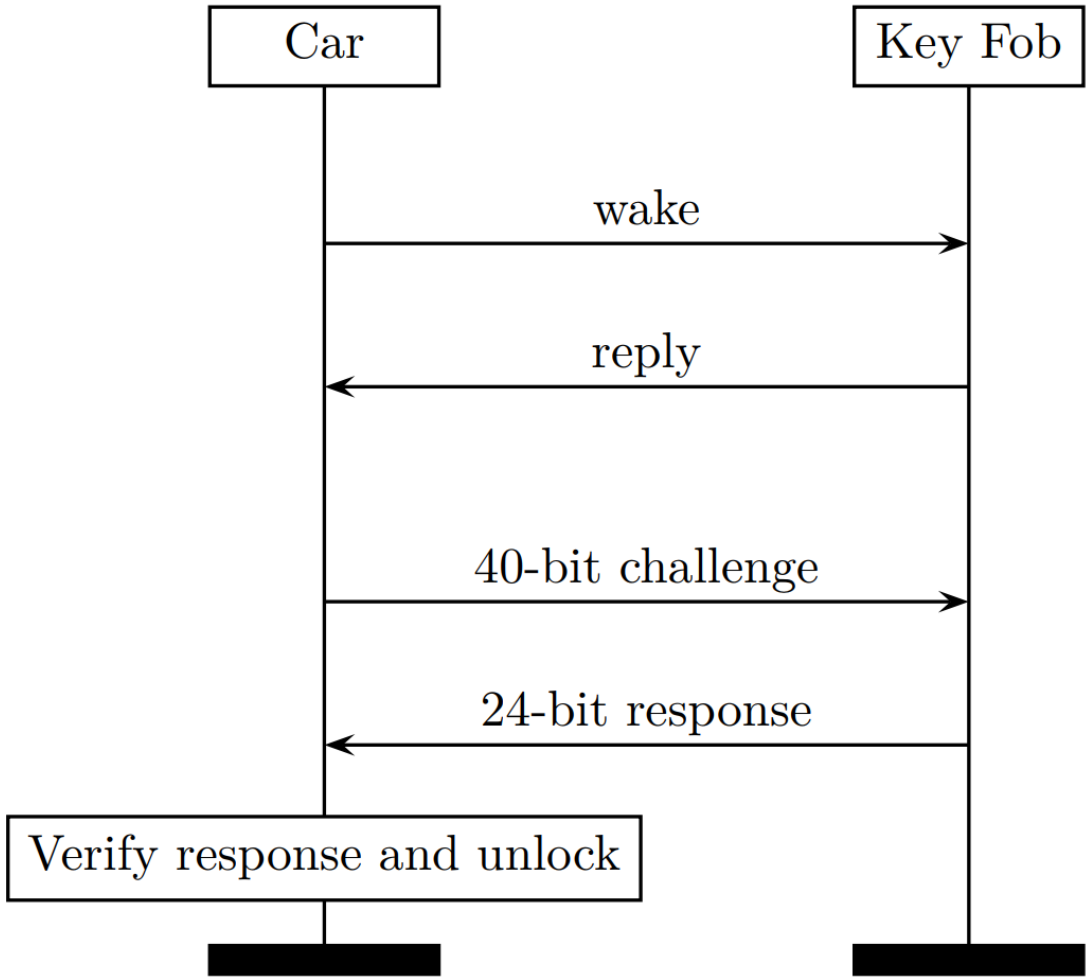


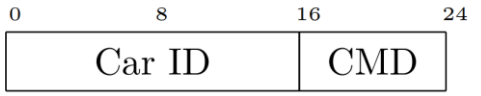
Yard Stick One (UHF)

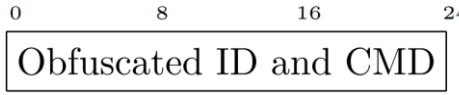


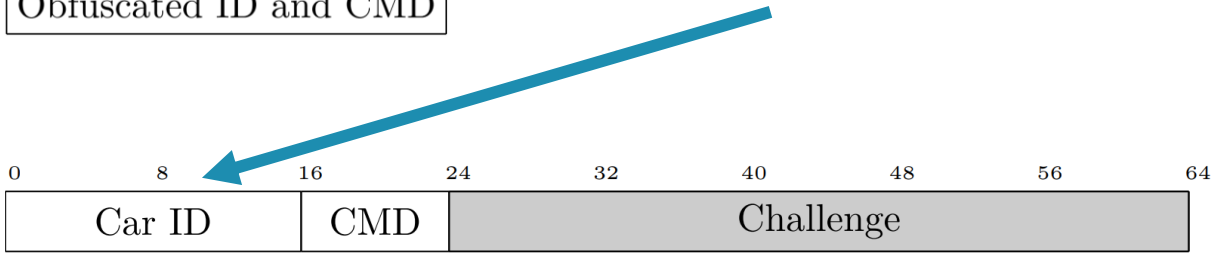
Proxmark 3 (LF)

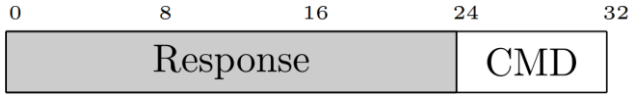
PKES protocol











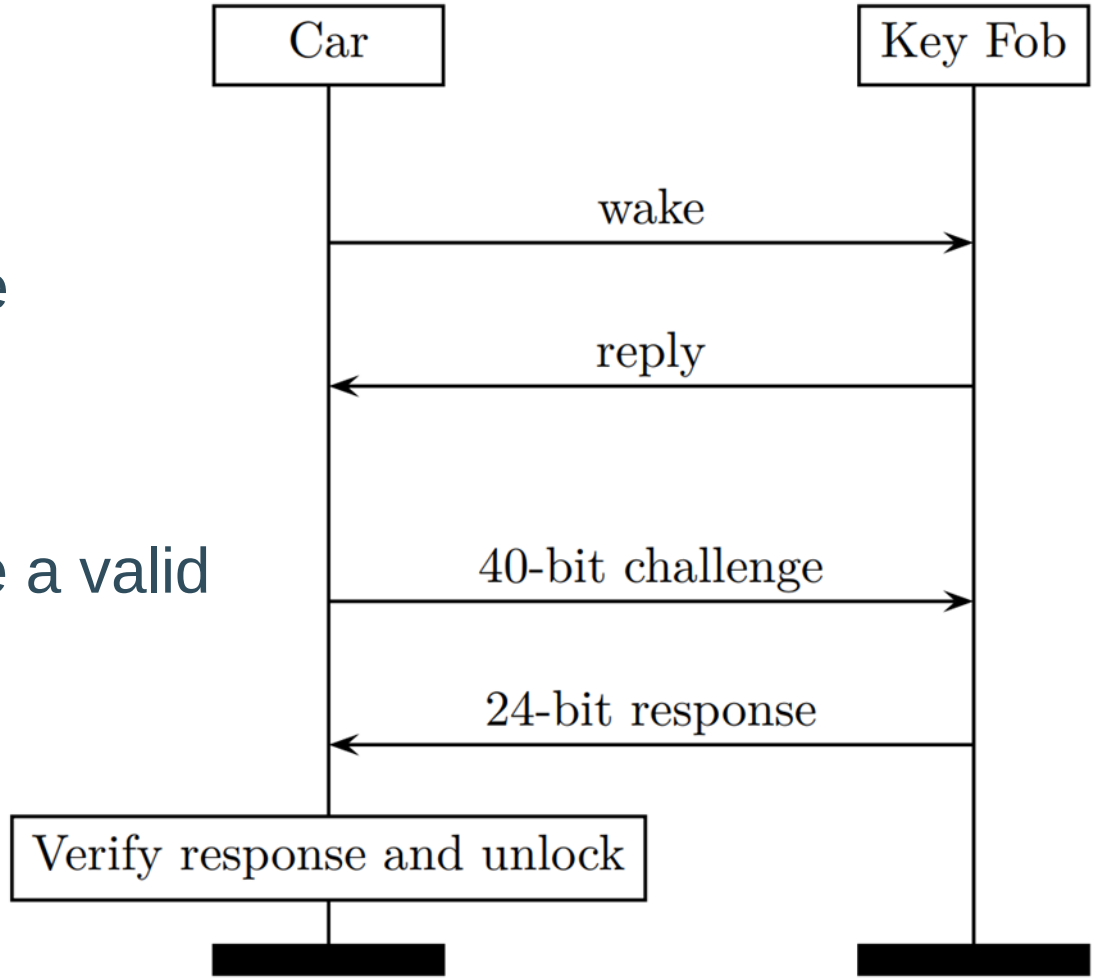
COSIC

KU LEUVEN

A car only attack

- Receive the 40-bit challenge
  - ~2^{16} keys produce the correct response
  - Guess a key and transmit the response

- After on average 2^{23} guesses you will have a valid challenge response pair
- Assuming 1 guess per second → 97 days
- Can be automated



Proof of Concept

DST40 key recovery

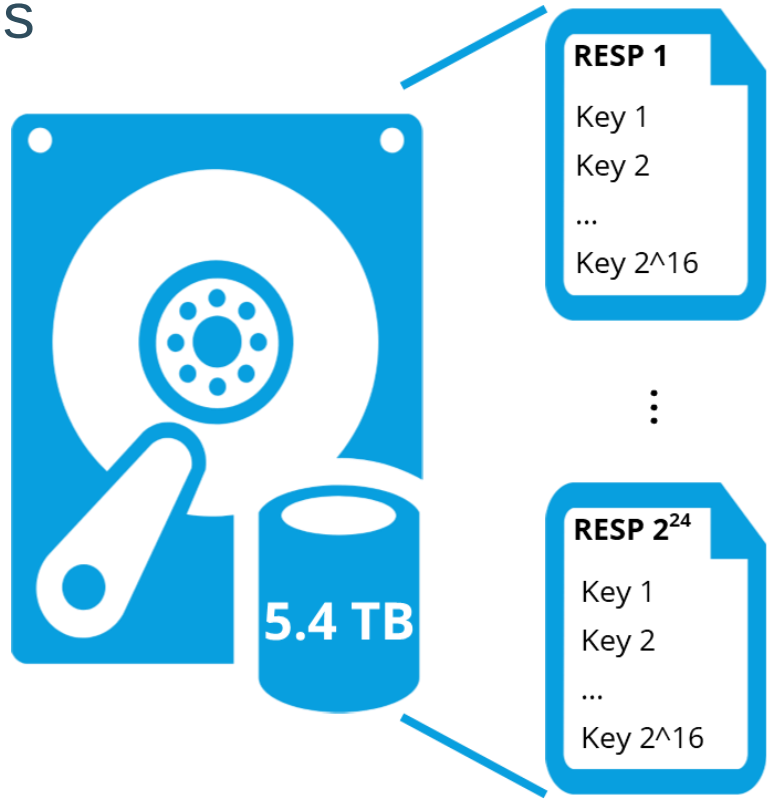
- 40-bit challenge is combined with a 40-bit key resulting in a 24-bit response
- For each 40-bit challenge multiple keys produce the same response
  - Need two challenge response pairs to recover the key

DST40 key recovery

- The key fob cannot verify the sender of a challenge
  - The key fob replies to any challenge it receives as long as the car ID is correct
- Time-Memory Trade-Off Table
  - Simplified pseudocode:

```
challenge = 0x636f736963
for key in range (0, 2^40):
        response = DST40(challenge, key)
        responseFile.append(key)
```

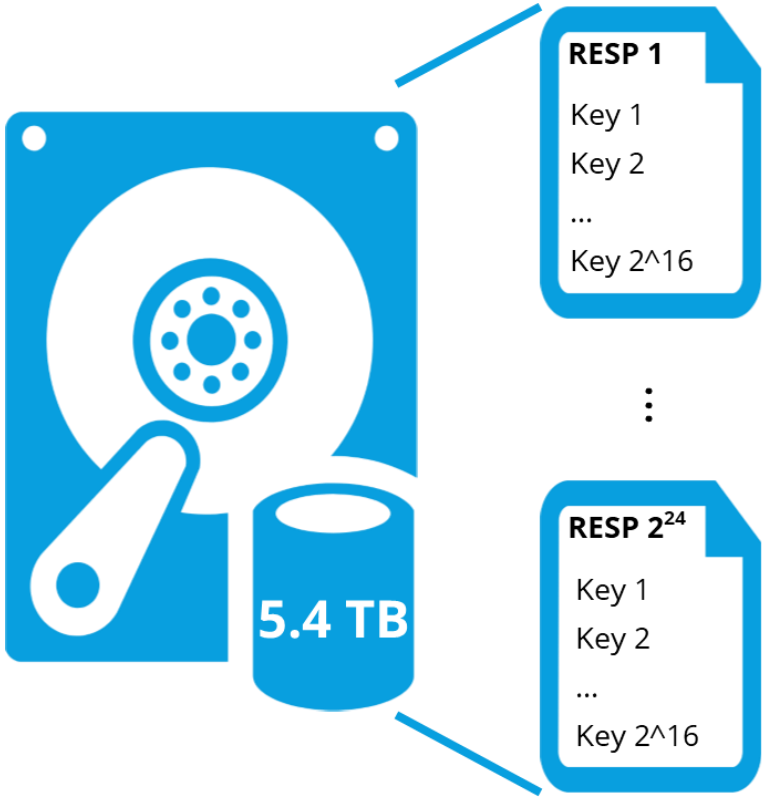
  - 2^{24} files each containing ~2^{16} 40-bit keys



Cloning a key fob

- Retrieve the 2-byte car ID (sniff or brute force)
- Send challenge 0x636f736963 to the key fob
- Use the response to select the correct TMTO file
- Send a different challenge and record the response
- Test the remaining ~2^{16} keys

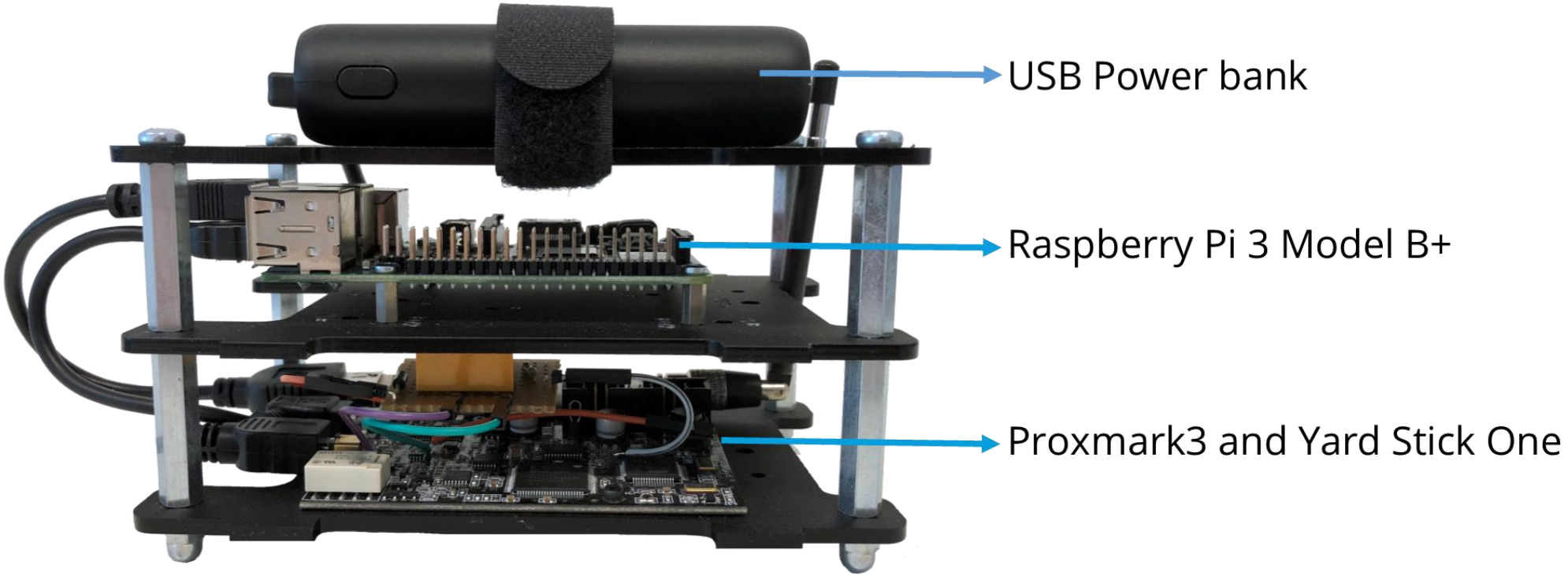
```
for key in TMTO_File:
        resp = DST40(challenge2, key)
        if resp == response2:
                return key
```



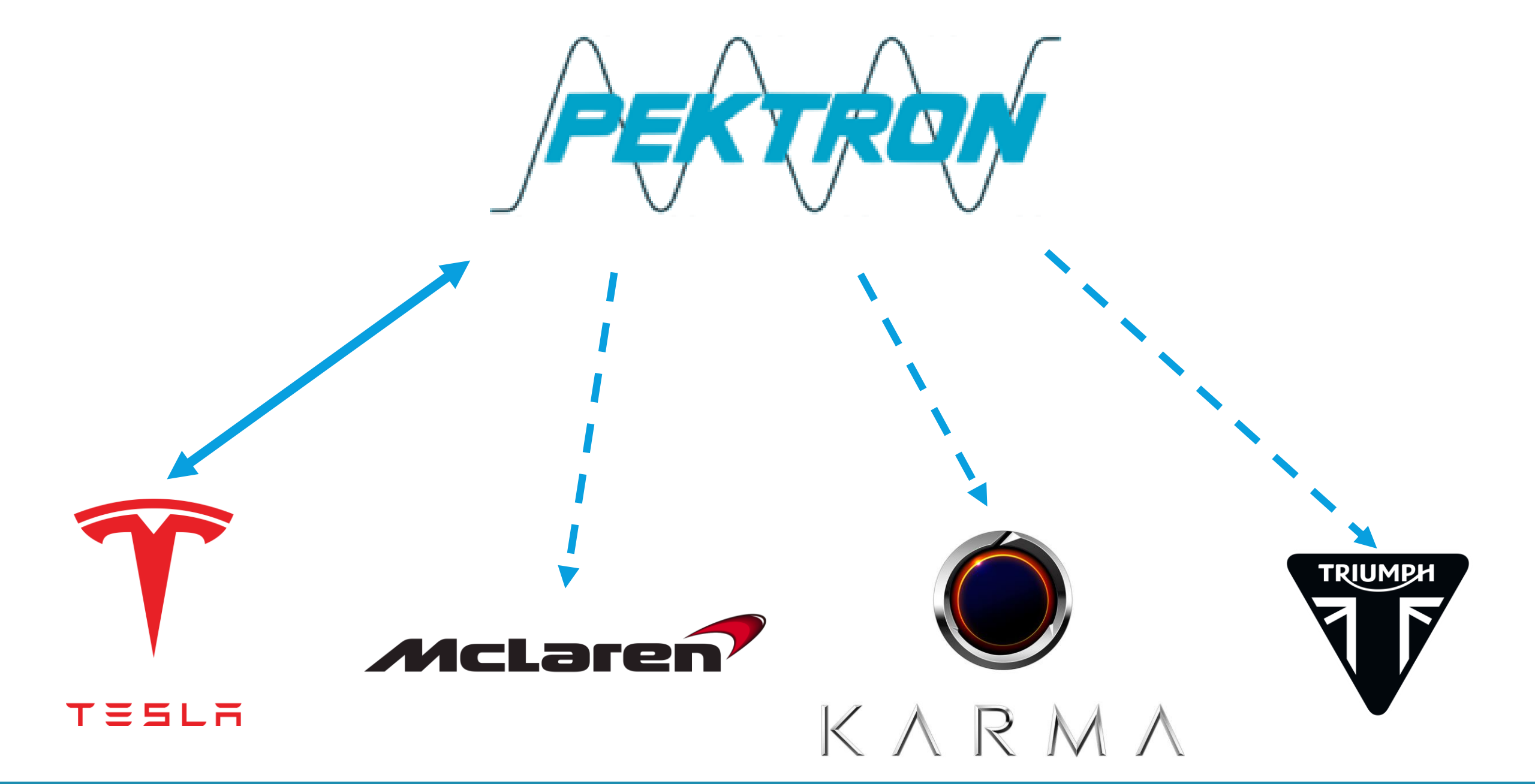
COSIC

KU LEUVEN

Proof of Concept attack

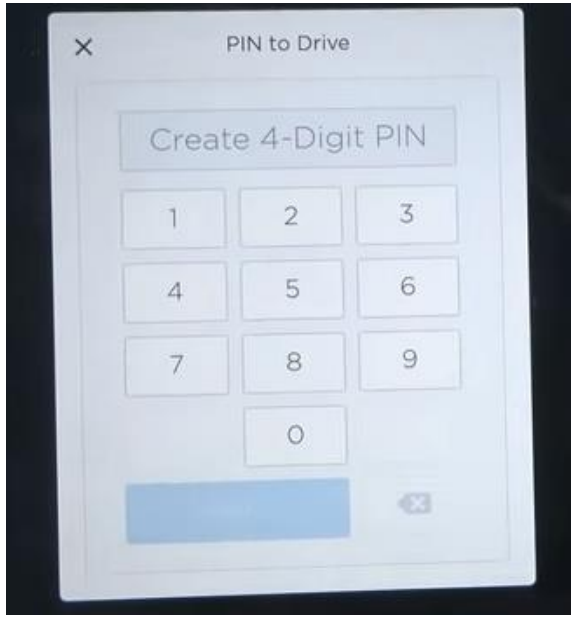


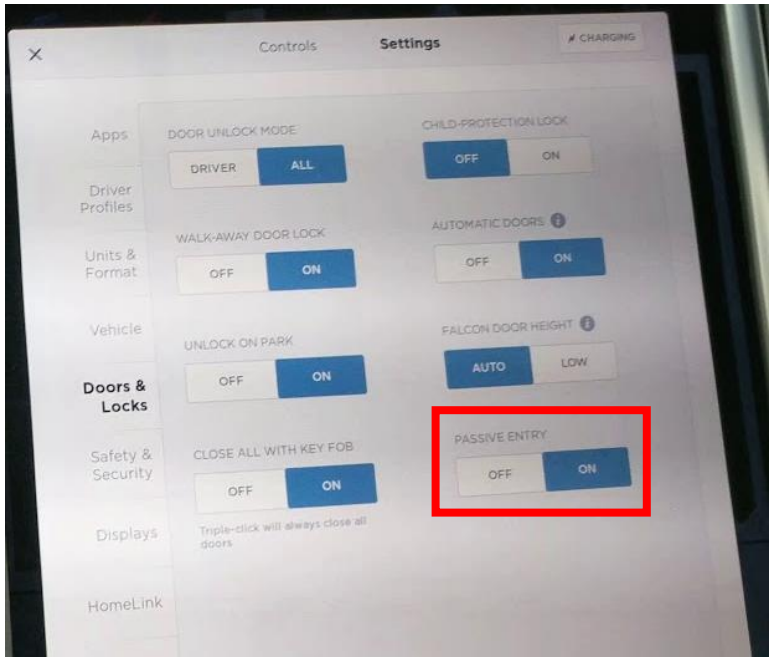
Responsible disclosure


PEKTRON
TESLA
McLaren
KARMA
TRIUMPH

Responsible disclosure

- First notified Tesla on 31/08/2017
  - Tesla vehicles produced from June 2018 onwards use a new key fob
  - OTA update includes a Pin to Drive feature and the ability to disable PKE





COSIC

KU LEUVEN

Conclusions (yes, this is 2019)

- Some manufacturers and chip vendors still rely on:
  - proprietary cryptography
  - NDAs and secrecy of datasheets
    - (See also Helena Handschuh's talk)
  - tier 1 or tier 2 suppliers to get security right
  - secrecy of firmware

Conclusions

Cryp·tomer
@TomerAshur

Just one more thing. Everybody is making fun of Tesla for using a 40-bit key (and rightly so). But Tesla at least had a mechanism we could report to and fixed the problem once informed. @McLarenAuto, @KarmaAutomotive, and @UKTriumph use the same system and ignored us.

6:12 PM - 10 Sep 2018

243 Retweets **601** Likes

10 243 601

Demo video:
https://www.youtube.com/watch?v=aVlYuPzmJoY

Oops!... I did it again.

The new key fob

- Hardware looks identical, JTAG is locked and the key fob is using DST80
- Trick the key fob into computing DST40 using only half of the 80-bit key!
  - Allows to recover the DST80 key with twice the amount of resources
    - 2 x 5,4TB and 2 x 2s
  - The attack requires close range to the fob, making it more difficult to execute
- Cars being produced today are already using a new (new) key fob
- Tesla has already begun to roll out a software update to applicable customers!

Picture source: TrevP, https://teslaownersonline.com/threads/software-update-2019-32.13901/

Questions?

@LennertWo
@CosicBe
lennert.wouters@esat.kuleuven.be