# Unlocking Keeloq

Rogan Dawes – Researcher
Orange Cyberdefense

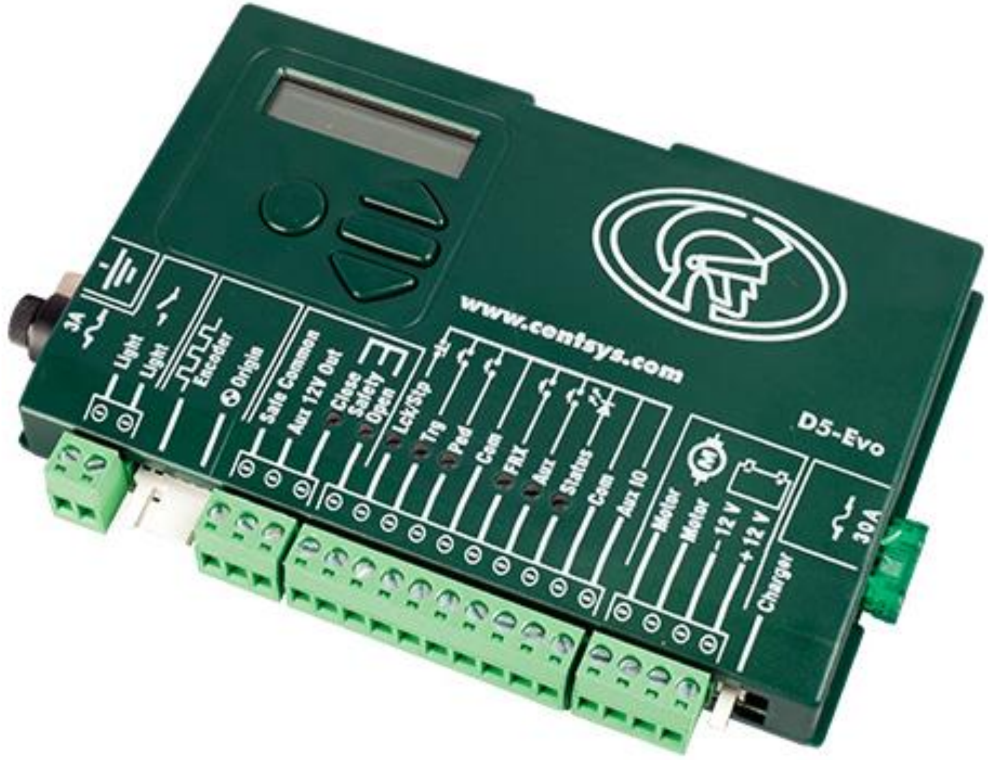
FENCE
COIN
STOP
COIN

AndrewNohawk

Coding Radio RTLSDR Security

# HACKING FIXED KEY REMOTES

CENTURION
D5 Evo


www.centsys.com
D5-Evo
3A
Light
Light
Encoder
Origin
Safe Common
Aux 12V Out
Close
Safety
Open
Lck/Stp
Trg
Ped
Com
FRX
Aux
Status
Com
Aux IO
Motor
Motor
- 12 V
+ 12 V
Charger
30A

## 11. Remote controls

⚠ Press button of valid transmitter *(if menu locked)*

11.1. Add remotes

11.2. Delete remotes ........ 11.2.1.Delete remote by ID

11.2.2.Delete remote button

11.2.3.Delete remote by button

11.2.4.Delete not present

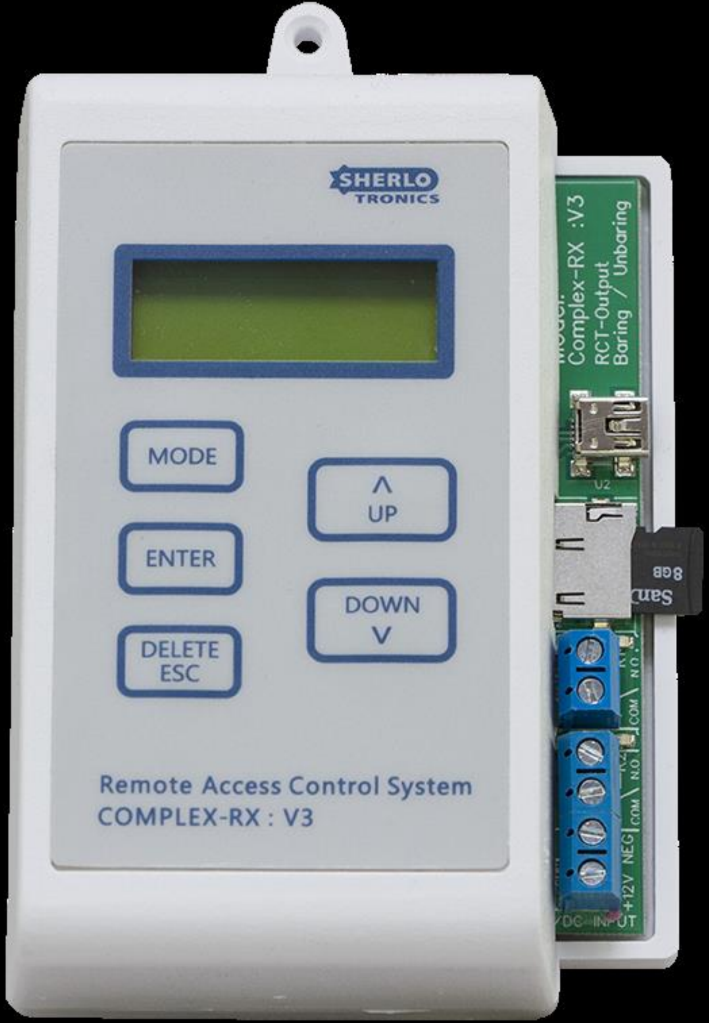
11.2.5.Delete all remotes

11.3. Edit remote button

11.4. Autolearn

11.5. Lock Tx menu

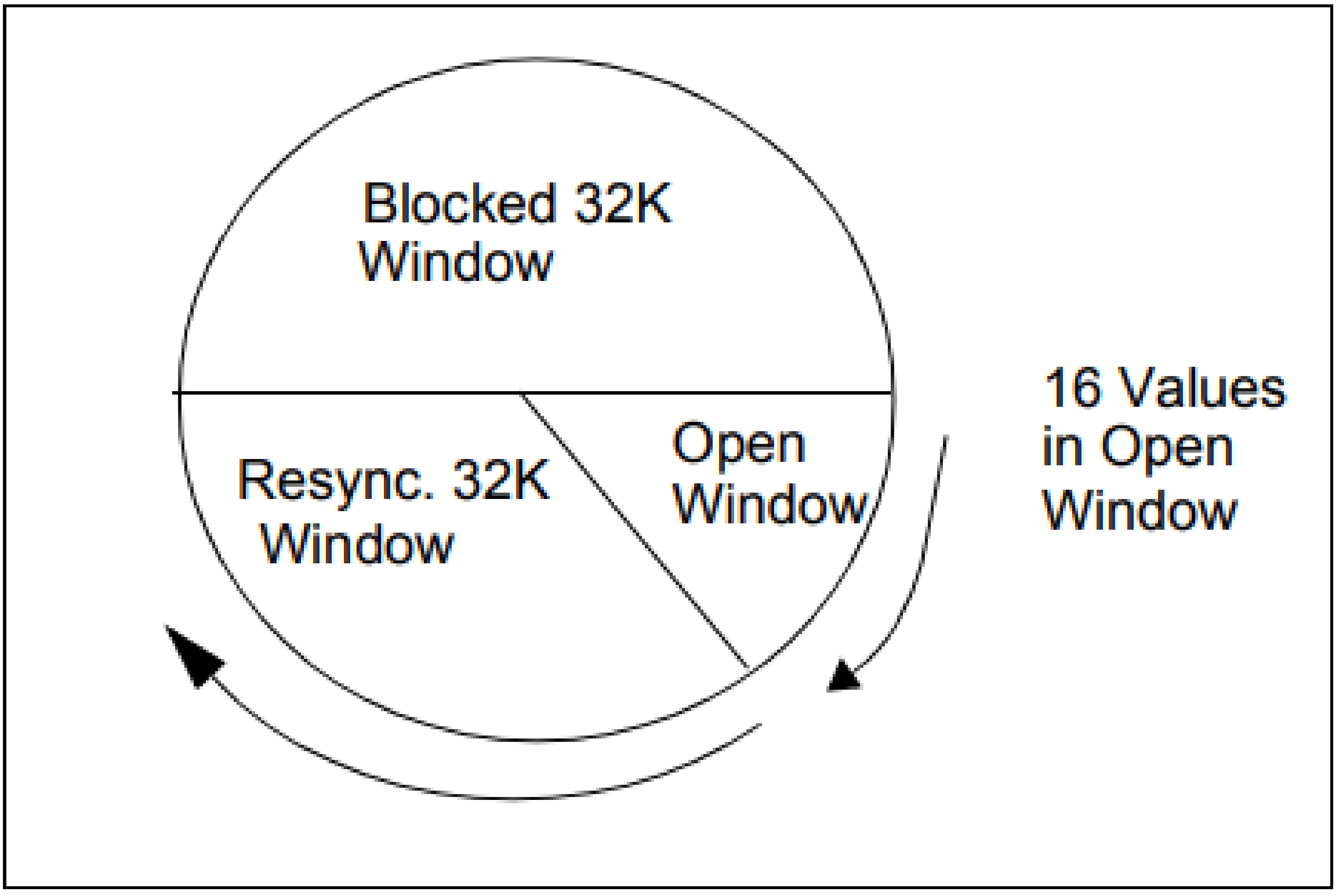
11.6. Onboard receiver enable/disable


SHERLO TRONICS
MODE
ENTER
DELETE ESC
^ UP
DOWN V
Remote Access Control System
COMPLEX-RX : V3
Model: Complex-RX :V3
RCT-Output
Baring / Unbaring
U2
8GB
SanD
DC INPUT
+12V NEG COM N.O. COM N.O.

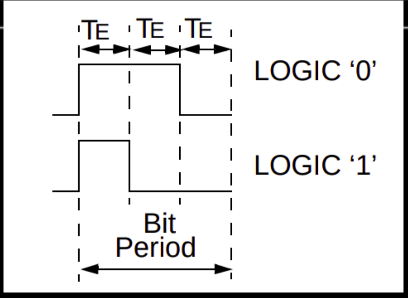
# Keeloq

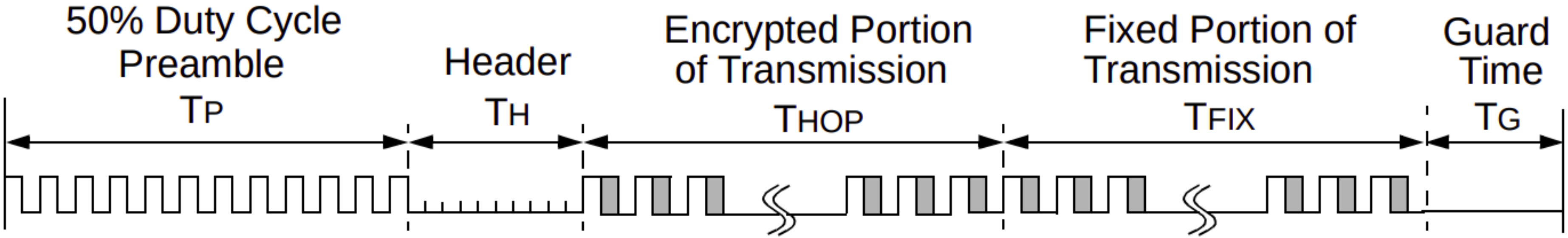
- Secure remote control systems can only be implemented if two conditions are met.

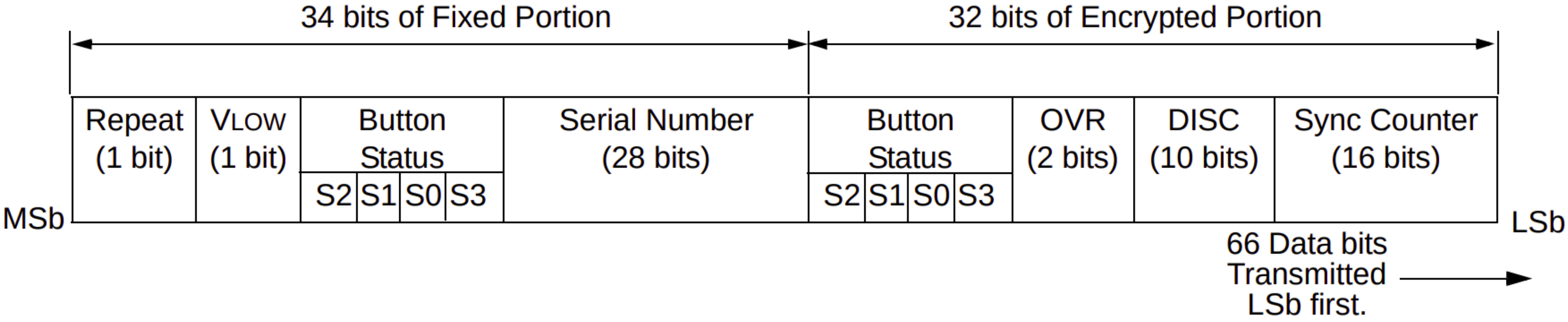
- A large number of possible combinations must be available
- The system may never respond twice to the same transmitted code


Blocked 32K
Window
Resync. 32K
Window
Open
Window
16 Values
in Open
Window

# Over the air (ASK/OOK)




50% Duty Cycle Preamble
TP
Header
TH
Encrypted Portion of Transmission
THOP
Fixed Portion of Transmission
TFIX
Guard Time
TG


34 bits of Fixed Portion
32 bits of Encrypted Portion
MSb
LSb
66 Data bits Transmitted LSb first.

| Repeat (1 bit) | VLOW (1 bit) | Button Status | Serial Number (28 bits) | Button Status | OVR (2 bits) | DISC (10 bits) | Sync Counter (16 bits) |
|---|---|---|---|---|---|---|---|
| | | S2 S1 S0 S3 | | S2 S1 S0 S3 | | | |

# Key Derivation Function (KDF) – Normal Learn

Manufacturer knows

- KDF
- Manufacturer key

Transmitter contains

- Shared key

Sends with each transmission

- Transmitter serial number
- Encrypted counter

Receiver contains

- KDF
- Manufacturer key

Receives

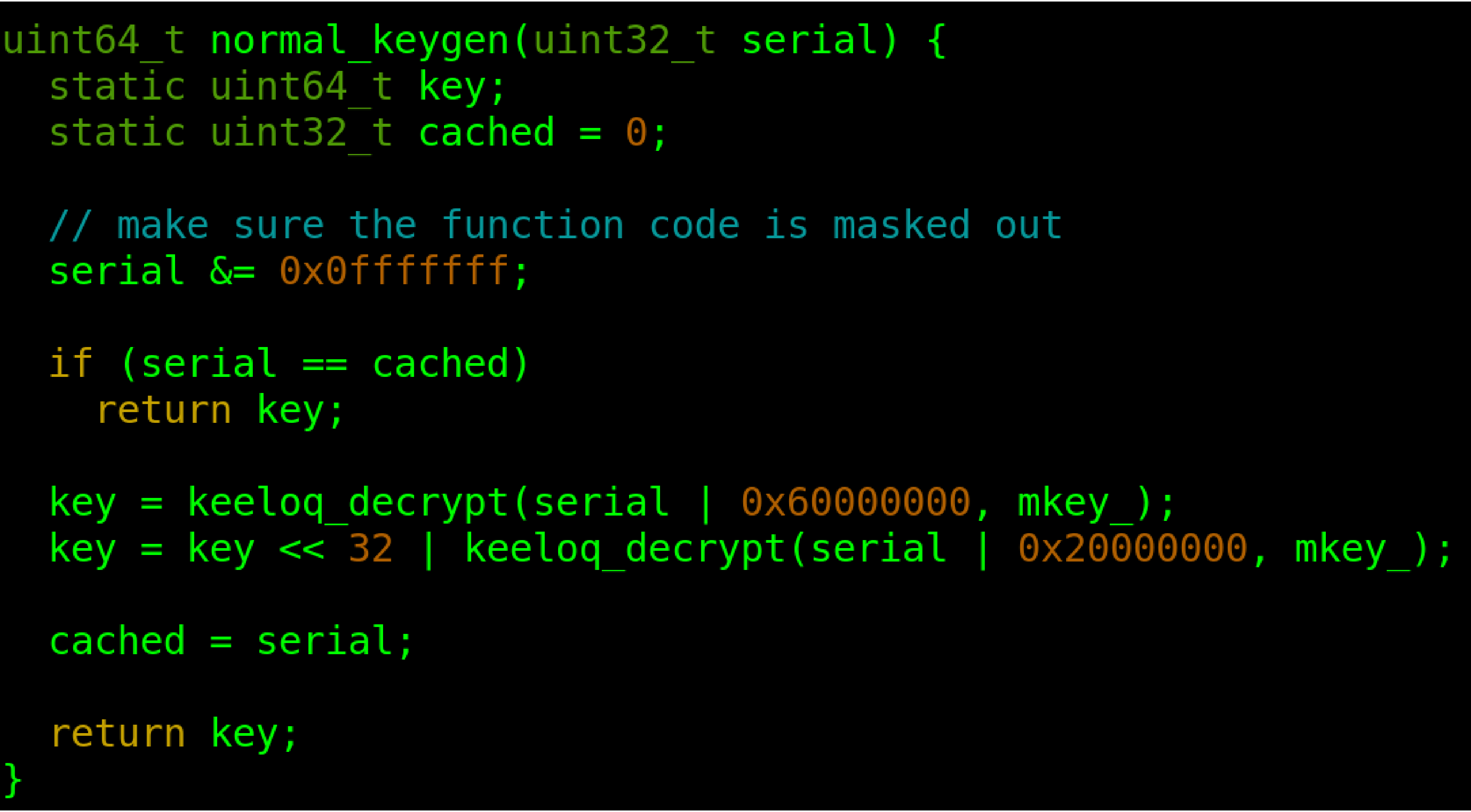
- Transmitter serial number

Derives

- Shared key

Checks

- Counter

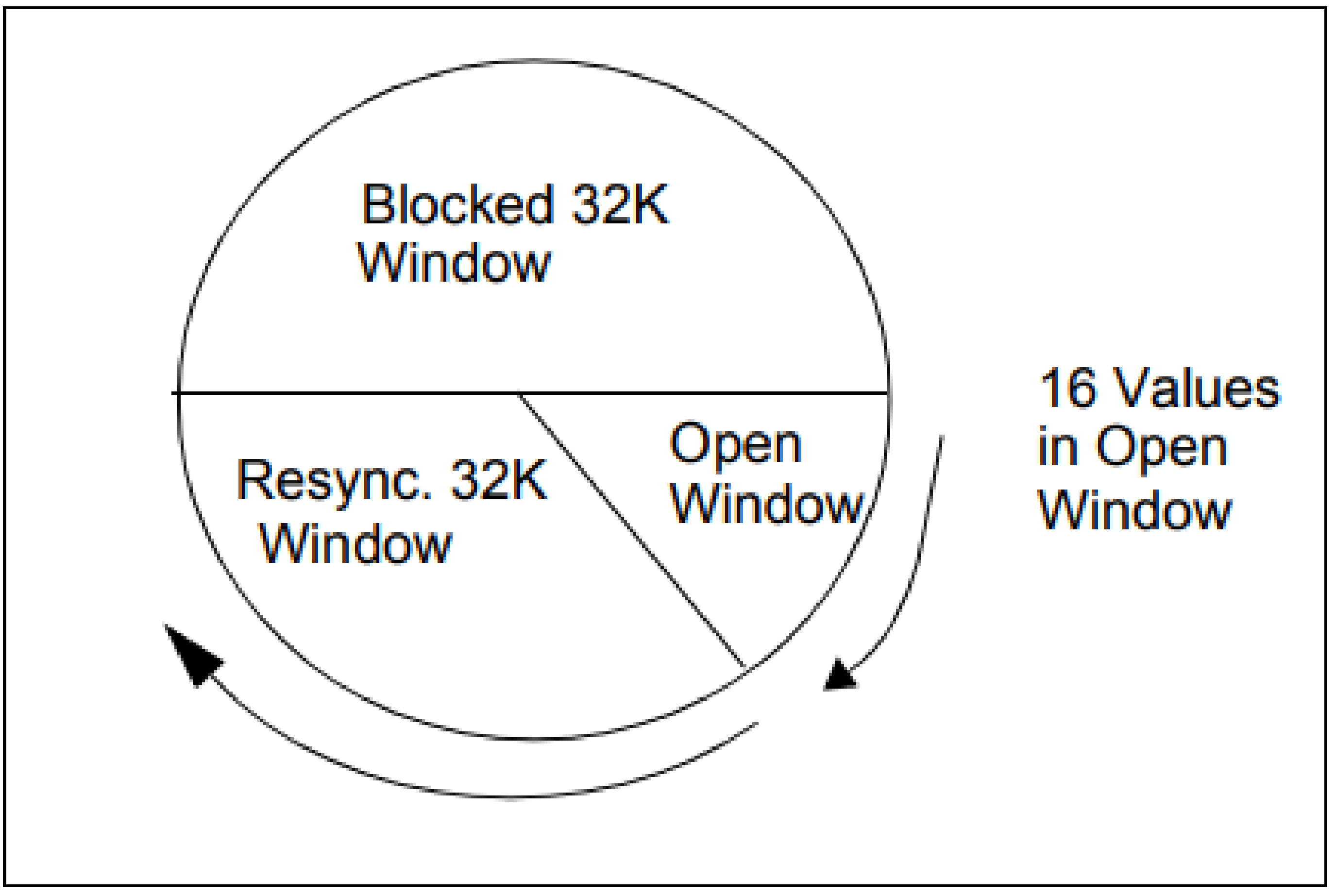


```c
uint64_t normal_keygen(uint32_t serial) {
  static uint64_t key;
  static uint32_t cached = 0;

  // make sure the function code is masked out
  serial &= 0x0fffffff;

  if (serial == cached)
    return key;

  key = keeloq_decrypt(serial | 0x60000000, mkey_);
  key = key << 32 | keeloq_decrypt(serial | 0x20000000, mkey_);

  cached = serial;

  return key;
}
```

# What attacks have been tried?

- Cryptanalysis
  - Specific weaknesses due to implementation flaws
- Side Channel
  - Recover key material from transmitter or receiver through power analysis
- Replay
  - Jam one transmission while recording it
  - Jam (and record) a second transmission while replaying the first

# Ro y Attack
# Ag ss Entry
# Sy



Cy lackHat USA
202 st key fob
sig

FAIL

1 BIT SQUARED

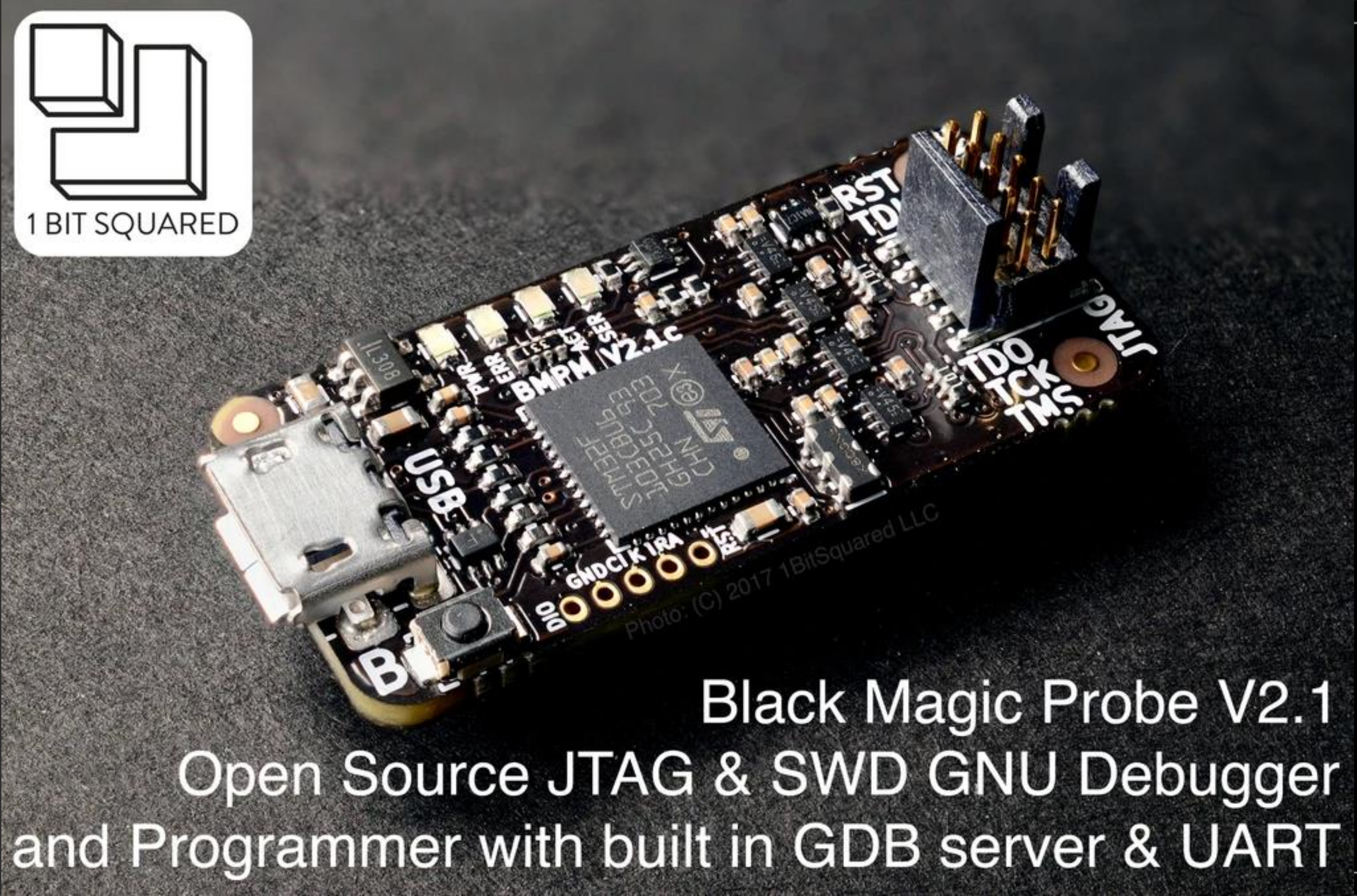


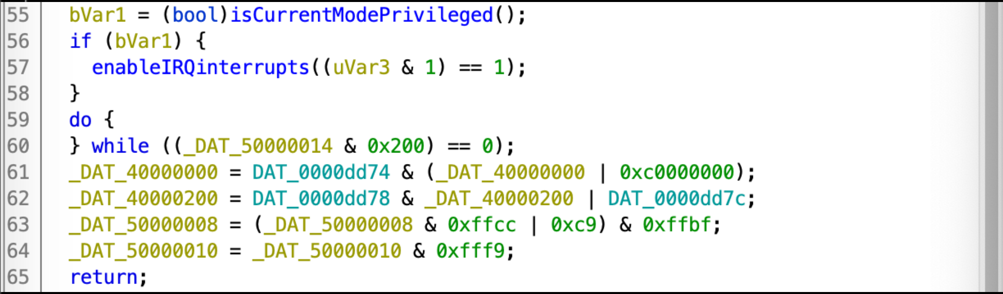
Photo: (C) 2017 1BitSquared LLC

Black Magic Probe V2.1
Open Source JTAG & SWD GNU Debugger
and Programmer with built in GDB server & UART

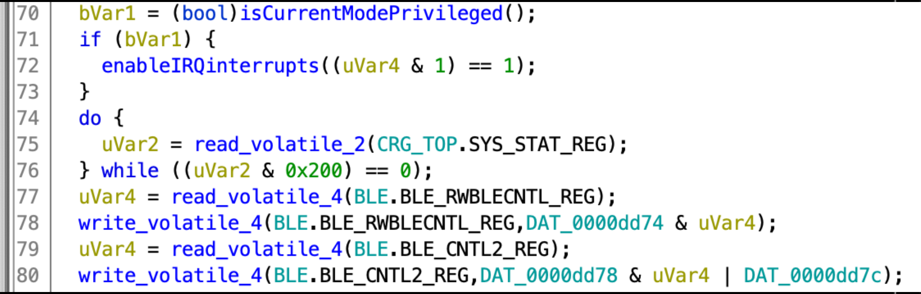
0
1
00
1000
0110
010
1011
0110
00110
11000
11011
110010
000001
010111
011011
1101110
0100110
11000110
01000010
0001

# SVD Loader

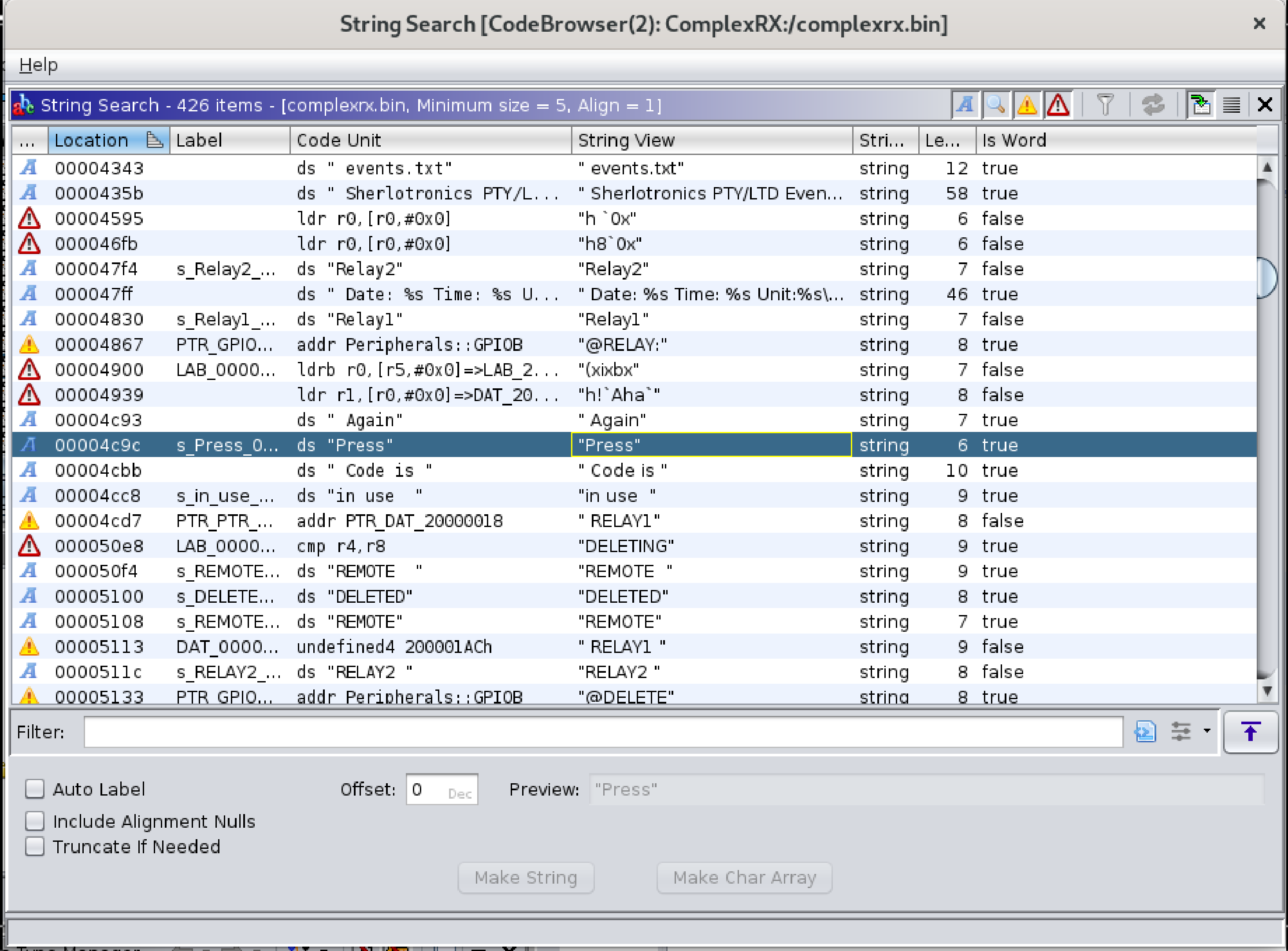
SVD-Loader for Ghidra automates the entire generation of peripheral structs and memory maps for over **650 different microcontrollers**: By parsing so-called SVD files (CMSIS **S**ystem **V**iew **D**escription) SVD-Loader is able to automatically annotate all peripherals of the controller, simplifying reverse-engineering of ARM firmwares significantly.



```
  bVar1 = (bool)isCurrentModePrivileged();
  if (bVar1) {
    enableIRQinterrupts((uVar3 & 1) == 1);
  }
  do {
  } while ((_DAT_50000014 & 0x200) == 0);
  _DAT_40000000 = DAT_0000dd74 & (_DAT_40000000 | 0xc0000000);
  _DAT_40000200 = DAT_0000dd78 & _DAT_40000200 | DAT_0000dd7c;
  _DAT_50000008 = (_DAT_50000008 & 0xffcc | 0xc9) & 0xffbf;
  _DAT_50000010 = _DAT_50000010 & 0xfff9;
  return;
```



```
  bVar1 = (bool)isCurrentModePrivileged();
  if (bVar1) {
    enableIRQinterrupts((uVar4 & 1) == 1);
  }
  do {
    uVar2 = read_volatile_2(CRG_TOP.SYS_STAT_REG);
  } while ((uVar2 & 0x200) == 0);
  uVar4 = read_volatile_4(BLE.BLE_RWBLECNTL_REG);
  write_volatile_4(BLE.BLE_RWBLECNTL_REG,DAT_0000dd74 & uVar4);
  uVar4 = read_volatile_4(BLE.BLE_CNTL2_REG);
  write_volatile_4(BLE.BLE_CNTL2_REG,DAT_0000dd78 & uVar4 | DAT_0000dd7c);
```



String Search [CodeBrowser(2): ComplexRX:/complexrx.bin]

String Search - 426 items - [complexrx.bin, Minimum size = 5, Align = 1]

| ... | Location | Label | Code Unit | String View | Stri... | Le... | Is Word |
|---|---|---|---|---|---|---|---|
| A | 00004343 | | ds " events.txt" | " events.txt" | string | 12 | true |
| A | 0000435b | | ds " Sherlotronics PTY/L... | " Sherlotronics PTY/LTD Even... | string | 58 | true |
| ⚠ | 00004595 | | ldr r0,[r0,#0x0] | "h `0x" | string | 6 | false |
| ⚠ | 000046fb | | ldr r0,[r0,#0x0] | "h8`0x" | string | 6 | false |
| A | 000047f4 | s_Relay2_... | ds "Relay2" | "Relay2" | string | 7 | false |
| A | 000047ff | | ds " Date: %s Time: %s U... | " Date: %s Time: %s Unit:%s\... | string | 46 | true |
| A | 00004830 | s_Relay1_... | ds "Relay1" | "Relay1" | string | 7 | false |
| ⚠ | 00004867 | PTR_GPIO... | addr Peripherals::GPIOB | "@RELAY:" | string | 8 | true |
| ⚠ | 00004900 | LAB_0000... | ldrb r0,[r5,#0x0]=>LAB_2... | "(xixbx" | string | 7 | false |
| ⚠ | 00004939 | | ldr r1,[r0,#0x0]=>DAT_20... | "h!`Aha`" | string | 8 | false |
| A | 00004c93 | | ds " Again" | " Again" | string | 7 | true |
| A | 00004c9c | s_Press_0... | ds "Press" | "Press" | string | 6 | true |
| A | 00004cbb | | ds " Code is " | " Code is " | string | 10 | true |
| A | 00004cc8 | s_in_use_... | ds "in use " | "in use " | string | 9 | true |
| ⚠ | 00004cd7 | PTR_PTR_... | addr PTR_DAT_20000018 | " RELAY1" | string | 8 | false |
| ⚠ | 000050e8 | LAB_0000... | cmp r4,r8 | "DELETING" | string | 9 | true |
| A | 000050f4 | s_REMOTE... | ds "REMOTE " | "REMOTE " | string | 9 | true |
| A | 00005100 | s_DELETE... | ds "DELETED" | "DELETED" | string | 8 | true |
| A | 00005108 | s_REMOTE... | ds "REMOTE" | "REMOTE" | string | 7 | true |
| ⚠ | 00005113 | DAT_0000... | undefined4 200001ACh | " RELAY1 " | string | 9 | false |
| A | 0000511c | s_RELAY2_... | ds "RELAY2 " | "RELAY2 " | string | 8 | false |
| ⚠ | 00005133 | PTR_GPIO... | addr Peripherals::GPIOB | "@DELETE" | string | 8 | true |

Filter:

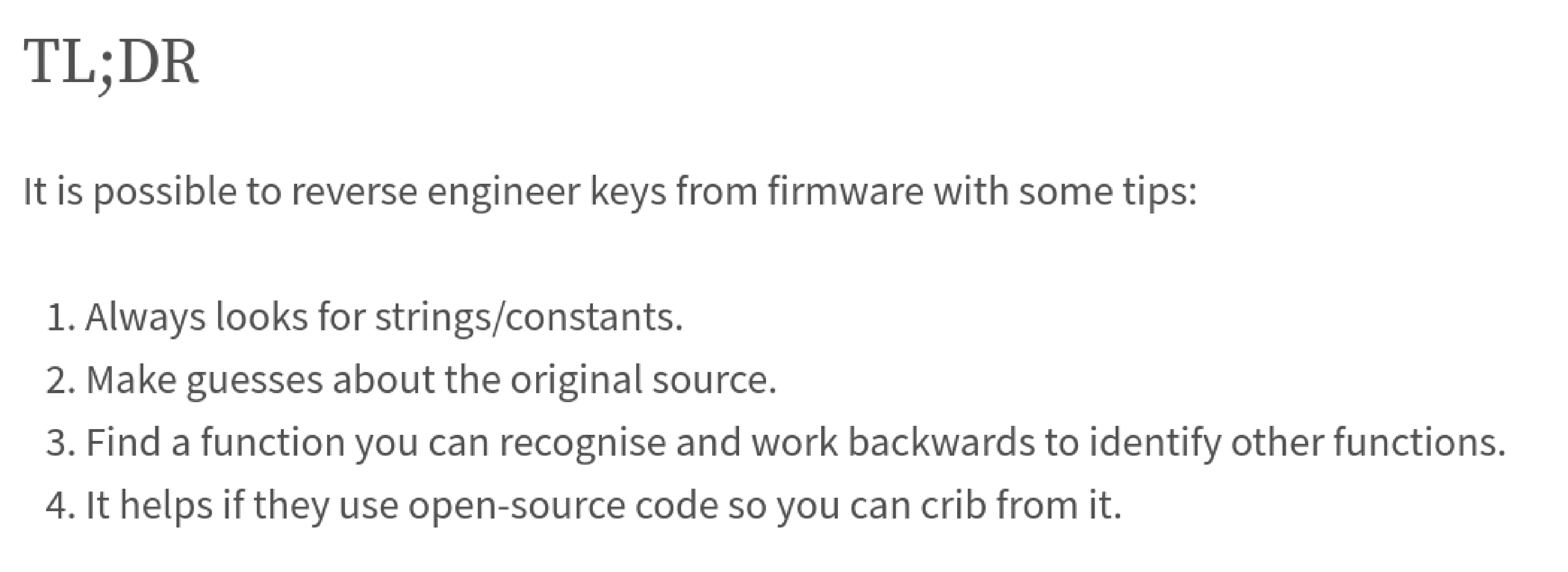
☐ Auto Label
☐ Include Alignment Nulls
☐ Truncate If Needed

Offset: 0 Dec

Preview: "Press"

# Tips for reverse engineering crypto code – David Lodge

https://www.pentestpartners.com/security-blog/reverse-engineering-keys-from-firmware-a-how-to/

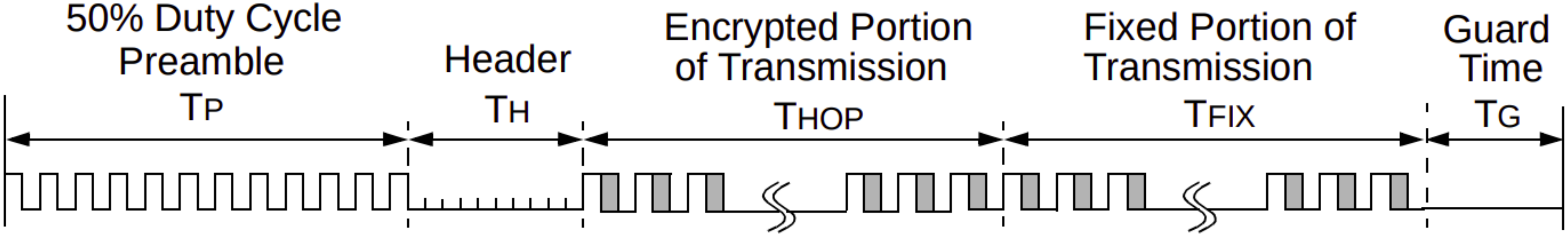


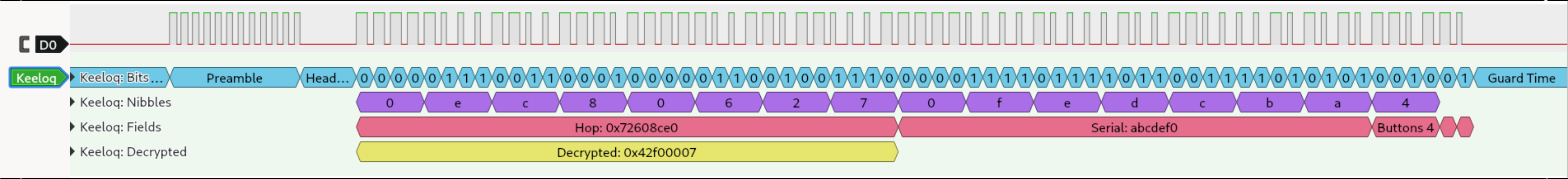
## TL;DR

It is possible to reverse engineer keys from firmware with some tips:

1. Always looks for strings/constants.
2. Make guesses about the original source.
3. Find a function you can recognise and work backwards to identify other functions.
4. It helps if they use open-source code so you can crib from it.

# Decoding the Keeloq code word

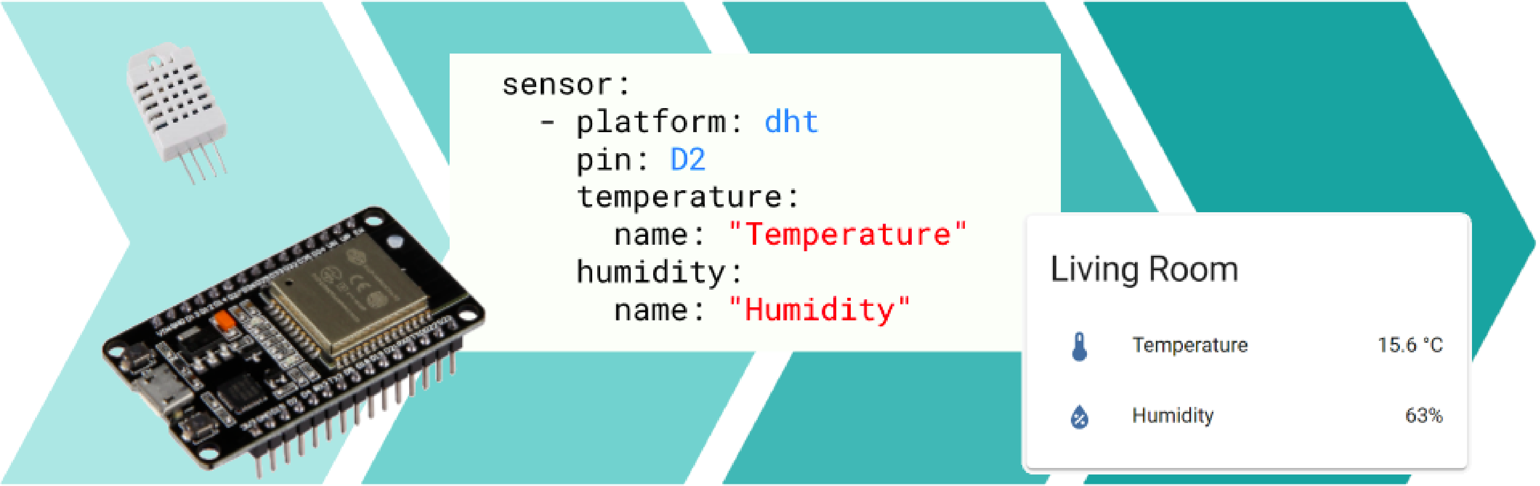

50% Duty Cycle Preamble
TP
Header
TH
Encrypted Portion of Transmission
THOP
Fixed Portion of Transmission
TFIX
Guard Time
TG



```
Keeloq: Bits ...   Preamble   Head...   0 0 0 0 0 1 1 1 0 0 1 1 0 0 0 1 0 0 0 0 0 1 1 0 0 1 0 0 1 1 1 0 0 0 0 0 1 1 1 1 0 1 1 1 1 0 1 1 0 0 1 1 1 0 1 1 0 1 0 1 0 0 1 0 0 1   Guard Time
Keeloq: Nibbles   0   e   c   8   0   6   2   7   0   f   e   d   c   b   a   4
Keeloq: Fields   Hop: 0x72608ce0   Serial: abcdef0   Buttons 4
Keeloq: Decrypted   Decrypted: 0x42f00007
```

# ESPHome

ESPHome is a system to control your ESP8266/ESP32 by simple yet powerful configuration files and control them remotely through Home Automation systems.

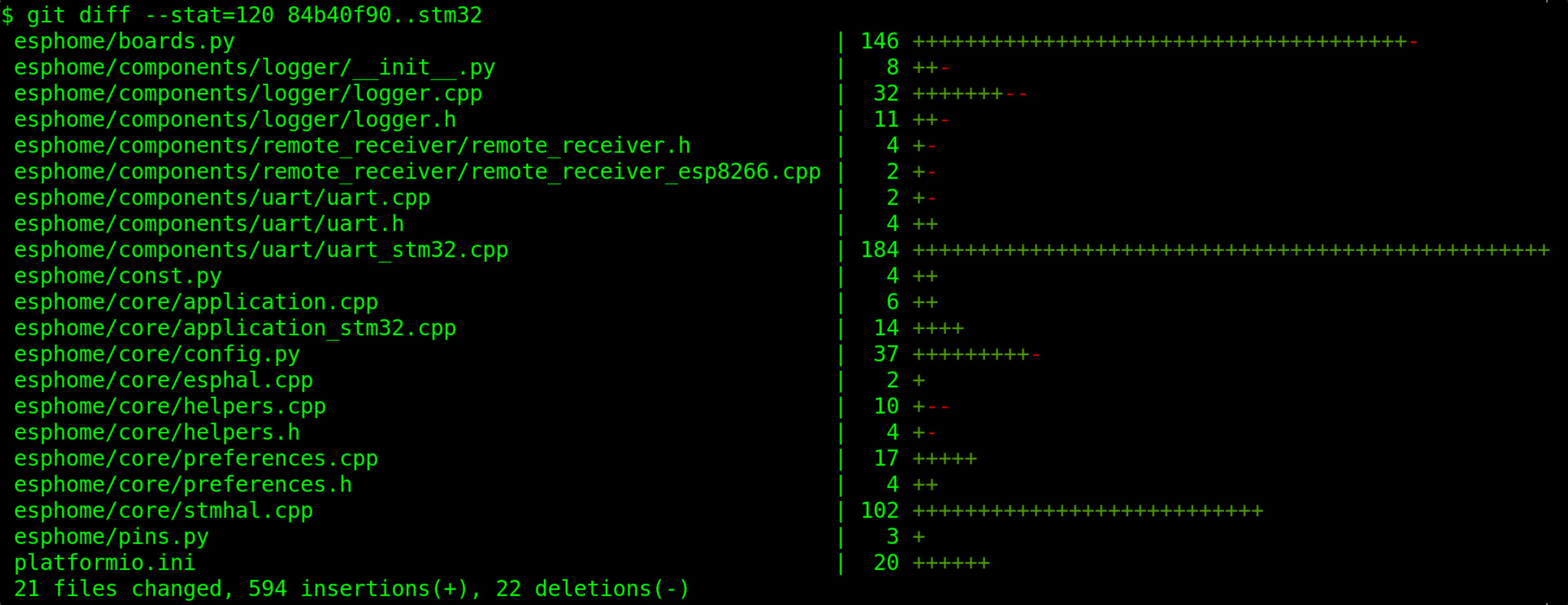


```yaml
sensor:
  - platform: dht
    pin: D2
    temperature:
      name: "Temperature"
    humidity:
      name: "Humidity"
```

Living Room

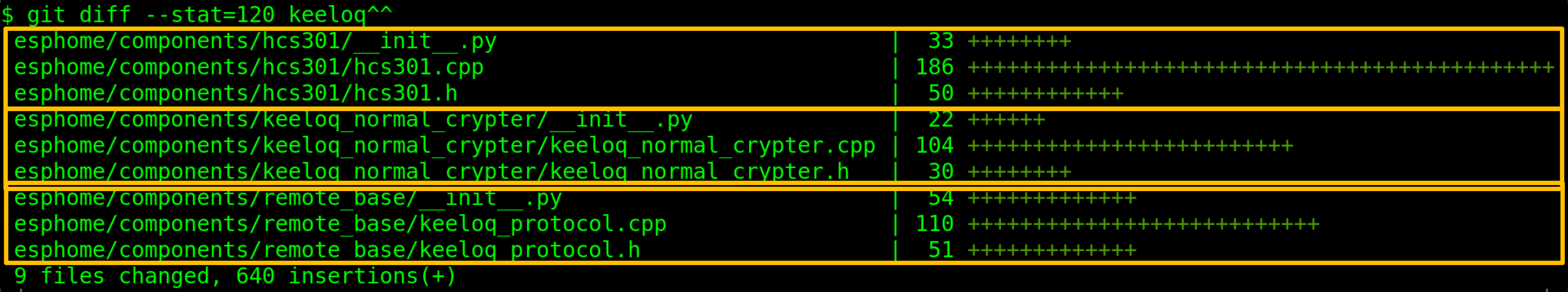
| | | |
|---|---|---|
| 🌡 | Temperature | 15.6 °C |
| 💧 | Humidity | 63% |

# Porting to STM32



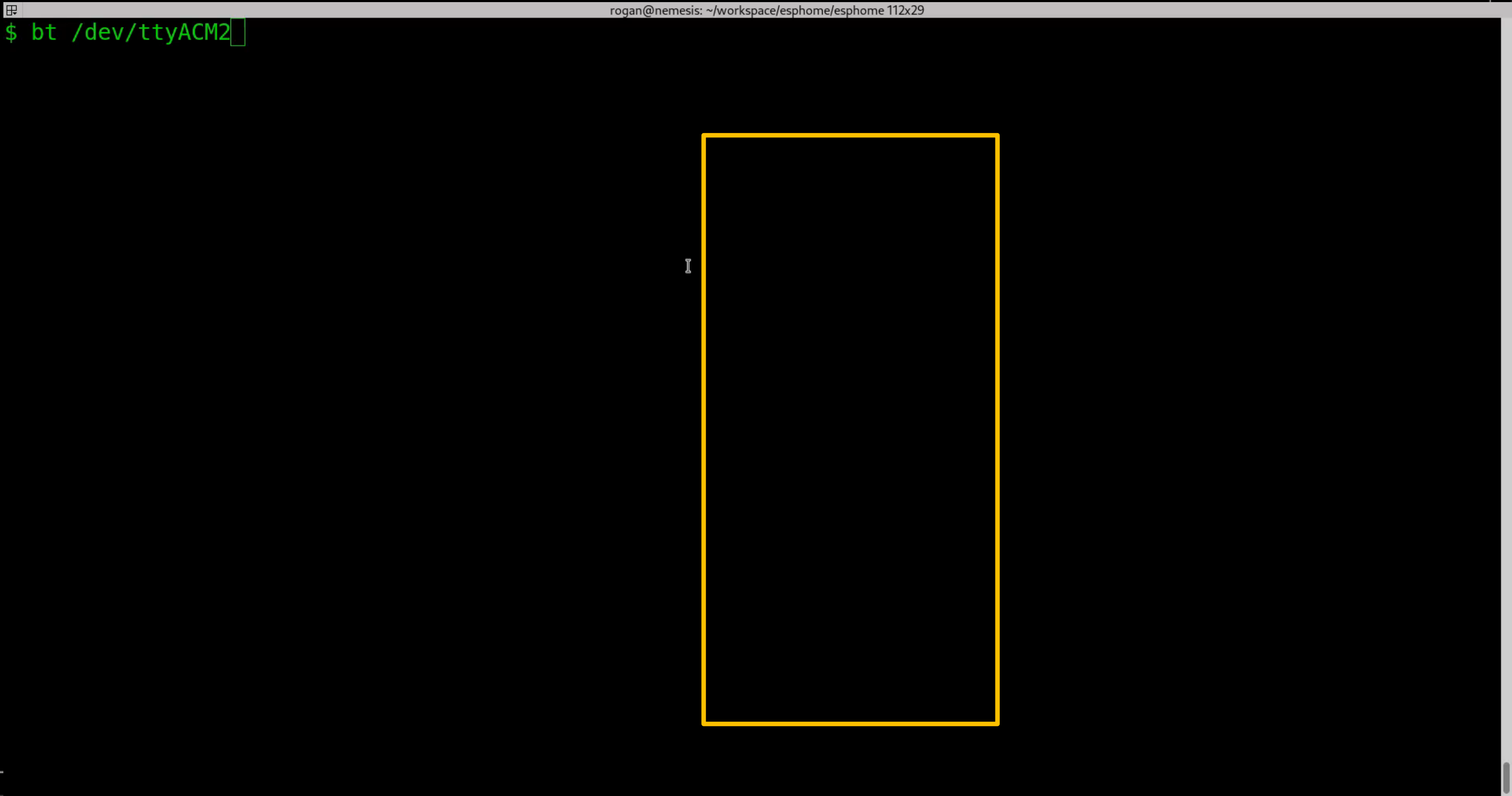
```
$ git diff --stat=120 84b40f90..stm32
 esphome/boards.py                                              | 146 ++++++++++++++++++++++++++++++++++++++-
 esphome/components/logger/__init__.py                          |   8 ++-
 esphome/components/logger/logger.cpp                           |  32 +++++++--
 esphome/components/logger/logger.h                             |  11 ++-
 esphome/components/remote_receiver/remote_receiver.h           |   4 +-
 esphome/components/remote_receiver/remote_receiver_esp8266.cpp |   2 +-
 esphome/components/uart/uart.cpp                               |   2 +-
 esphome/components/uart/uart.h                                 |   4 ++
 esphome/components/uart/uart_stm32.cpp                         | 184 +++++++++++++++++++++++++++++++++++++++++++++++++
 esphome/const.py                                               |   4 ++
 esphome/core/application.cpp                                   |   6 ++
 esphome/core/application_stm32.cpp                             |  14 ++++
 esphome/core/config.py                                         |  37 +++++++++-
 esphome/core/esphal.cpp                                        |   2 +
 esphome/core/helpers.cpp                                       |  10 +--
 esphome/core/helpers.h                                         |   4 +-
 esphome/core/preferences.cpp                                   |  17 +++++
 esphome/core/preferences.h                                     |   4 ++
 esphome/core/stmhal.cpp                                        | 102 +++++++++++++++++++++++++++
 esphome/pins.py                                                |   3 +
 platformio.ini                                                 |  20 ++++++
 21 files changed, 594 insertions(+), 22 deletions(-)
```

# Implementing Keeloq and Normal KDF



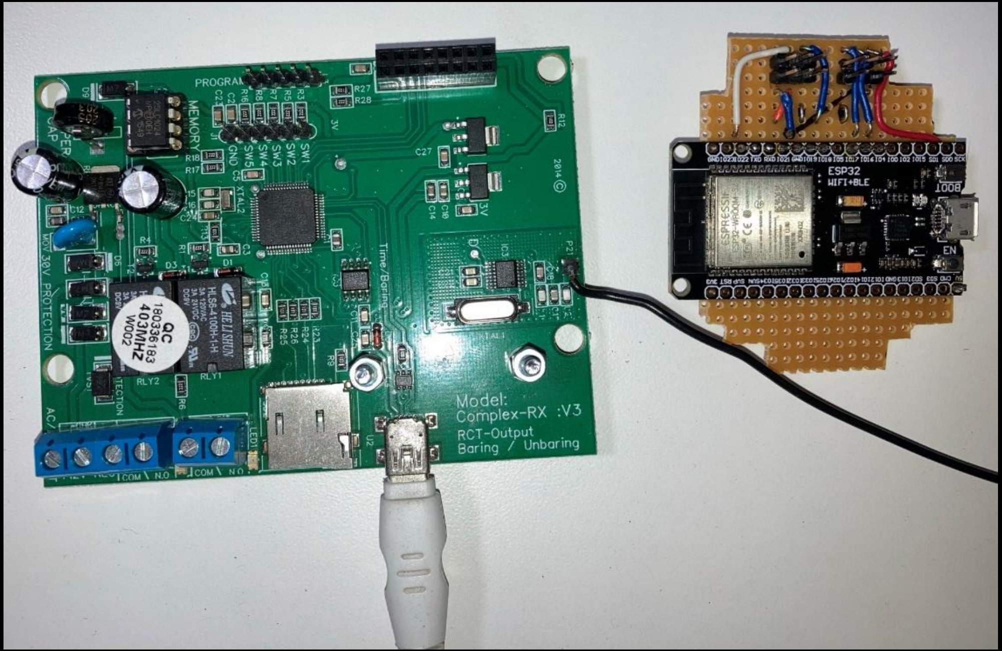
```
$ git diff --stat=120 keeloq^^
 esphome/components/hcs301/__init__.py                              |  33 ++++++++
 esphome/components/hcs301/hcs301.cpp                               | 186 +++++++++++++++++++++++++++++++++++++++++++++
 esphome/components/hcs301/hcs301.h                                 |  50 ++++++++++++
 esphome/components/keeloq_normal_crypter/__init__.py               |  22 ++++++
 esphome/components/keeloq_normal_crypter/keeloq_normal_crypter.cpp | 104 +++++++++++++++++++++++++
 esphome/components/keeloq_normal_crypter/keeloq_normal_crypter.h   |  30 ++++++++
 esphome/components/remote_base/__init__.py                         |  54 +++++++++++++
 esphome/components/remote_base/keeloq_protocol.cpp                 | 110 +++++++++++++++++++++++++++
 esphome/components/remote_base/keeloq_protocol.h                   |  51 +++++++++++++
 9 files changed, 640 insertions(+)
```

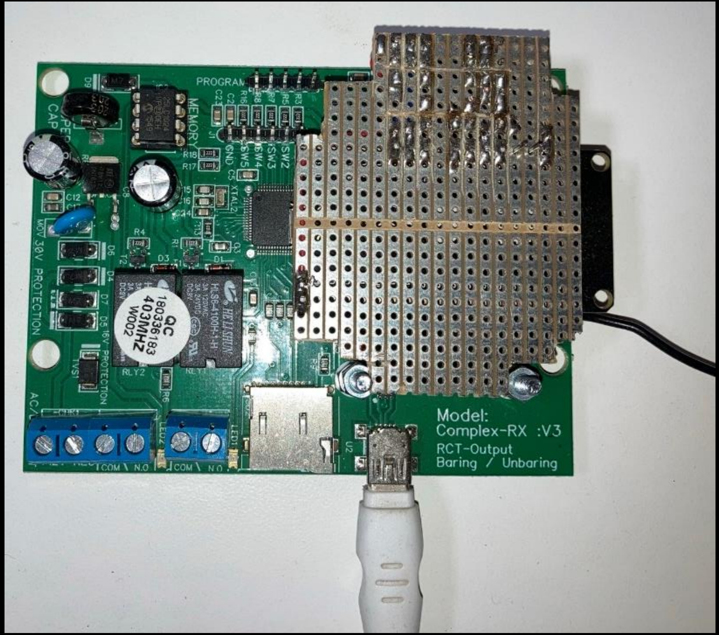
# Demonstration of ESPHome/Keeloq



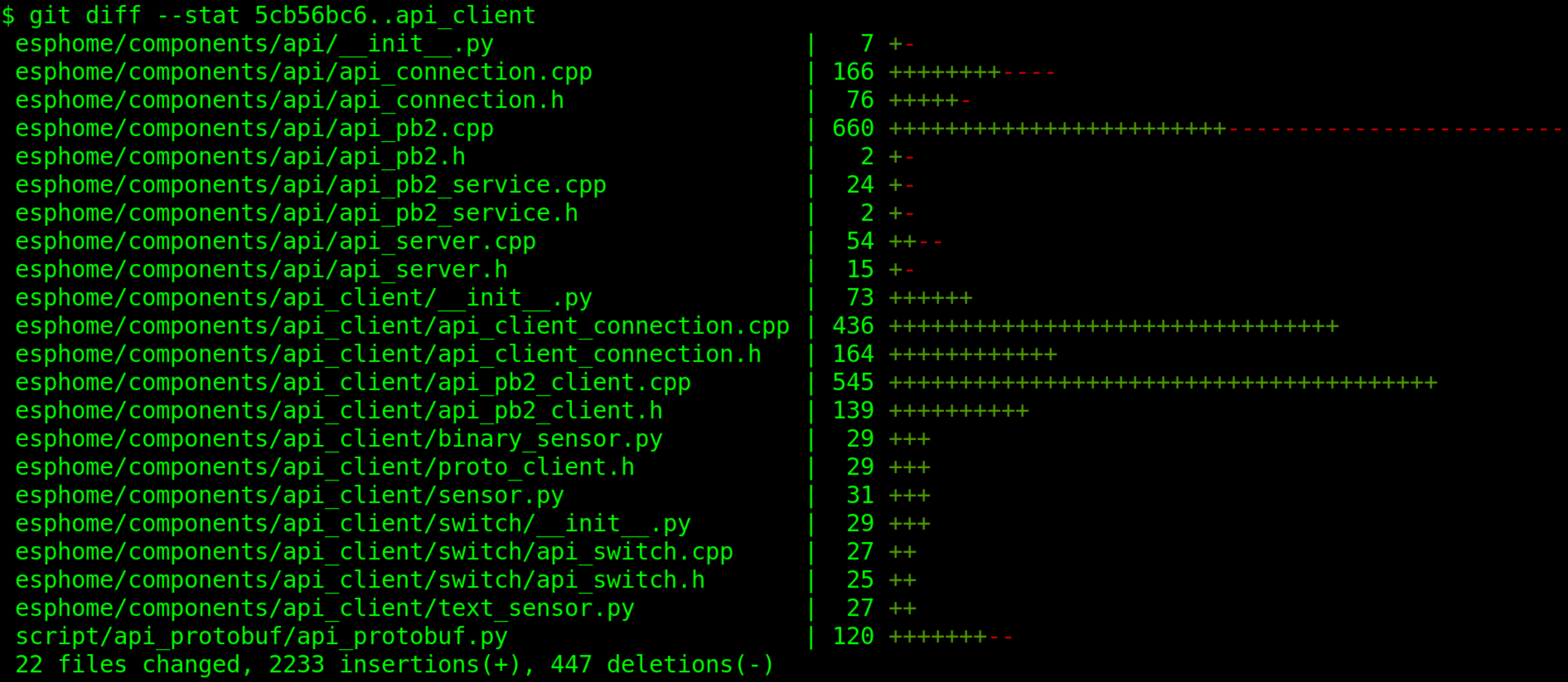
```
$ bt /dev/ttyACM2
```

# Bringing it all online



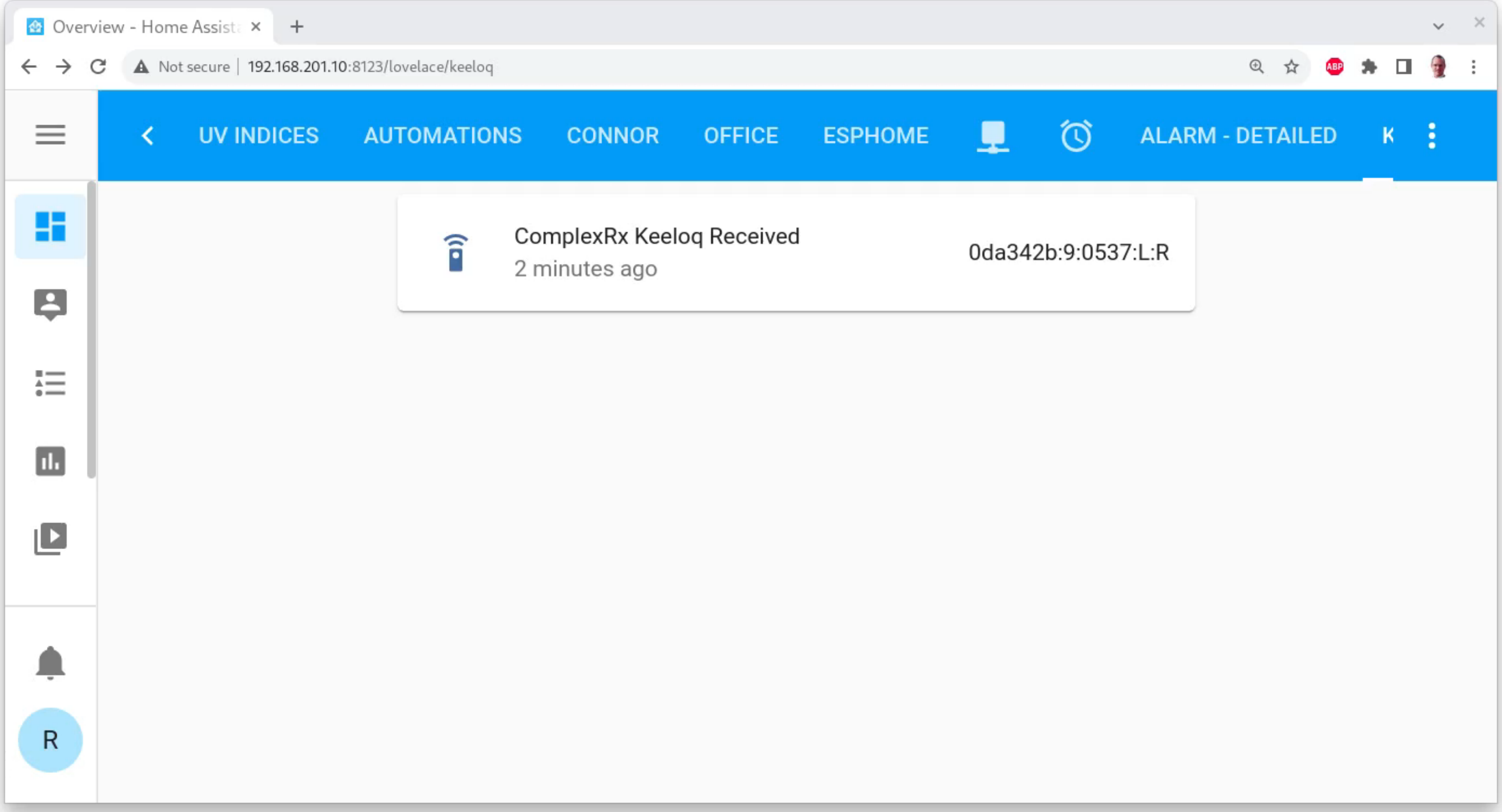


# ESPHome Client API



```
$ git diff --stat 5cb56bc6..api_client
 esphome/components/api/__init__.py                      |   7 +-
 esphome/components/api/api_connection.cpp               | 166 ++++++++----
 esphome/components/api/api_connection.h                 |  76 +++++-
 esphome/components/api/api_pb2.cpp                      | 660 ++++++++++++++++++++++++------------------------
 esphome/components/api/api_pb2.h                        |   2 +-
 esphome/components/api/api_pb2_service.cpp              |  24 +-
 esphome/components/api/api_pb2_service.h                |   2 +-
 esphome/components/api/api_server.cpp                   |  54 ++--
 esphome/components/api/api_server.h                     |  15 +-
 esphome/components/api_client/__init__.py               |  73 ++++++
 esphome/components/api_client/api_client_connection.cpp | 436 ++++++++++++++++++++++++++++++++
 esphome/components/api_client/api_client_connection.h   | 164 ++++++++++++
 esphome/components/api_client/api_pb2_client.cpp        | 545 +++++++++++++++++++++++++++++++++++++++
 esphome/components/api_client/api_pb2_client.h          | 139 ++++++++++
 esphome/components/api_client/binary_sensor.py          |  29 +++
 esphome/components/api_client/proto_client.h            |  29 +++
 esphome/components/api_client/sensor.py                 |  31 +++
 esphome/components/api_client/switch/__init__.py        |  29 +++
 esphome/components/api_client/switch/api_switch.cpp     |  27 ++
 esphome/components/api_client/switch/api_switch.h       |  25 ++
 esphome/components/api_client/text_sensor.py            |  27 ++
 script/api_protobuf/api_protobuf.py                     | 120 +++++++--
 22 files changed, 2233 insertions(+), 447 deletions(-)
```

# Home Assistant and Keeloq Remotes



Overview - Home Assista ×
Not secure | 192.168.201.10:8123/lovelace/keeloq
UV INDICES
AUTOMATIONS
CONNOR
OFFICE
ESPHOME
ALARM - DETAILED
K
R

ComplexRx Keeloq Received
2 minutes ago
0da342b:9:0537:L:R

```
remote_receiver:
  id: receiver
  pin:
    number: PA_3
    mode: INPUT
  buffer_size: 200
  tolerance: 30%
  on_keeloq:
    then:
      - lambda: |-
          char buff[20];
          if (id(keeloq_crypter).decrypt(x)) {
            snprintf(buff, sizeof(buff), "%07x:%1x:%04X:%c:%c",
                     x.serial, x.button, x.sync, x.low ? 'L' : 'N', x.repeat ? 'R' : 'F');
          } else {
            snprintf(buff, sizeof(buff), "%07x:%1x::%c:%c",
                     x.serial, x.button, x.low ? 'L' : 'N', x.repeat ? 'R' : 'F');
          }
          std::string buffAsStdStr = buff;
          id(keeloq_remote).publish_state(buff);
```

```
hcs301:
  id: hcs301_id
  power_pin: PB_15
  clock_pin: PB_14
  pwm_pin: PB_13

script:
  - id: program_hcs301
    mode: single
    then:
      - lambda: |-
          uint64_t hcs301_key = id(keeloq_crypter).normal_keygen(0x0DA342B);
          if (id(hcs301_id).program(0x0DA342B, 0x0, hcs301_key)) {
            ESP_LOGD("hcs301", "Successfully programmed");
          }
```

# Outstanding features

- Persistent recording of counters and replay detection
- Desynchronisation recovery in the client API
- Implementation of other entity types in client API

- HCS301 initial sequence no

# Code

- ESPHome

- https://github.com/rogandawes/esphome
- Branches stm32, keeloq and api_client

# Thank You!

Rogan Dawes
@RoganDawes
rogan.dawes@orangecyberdefense.com

# Questions?