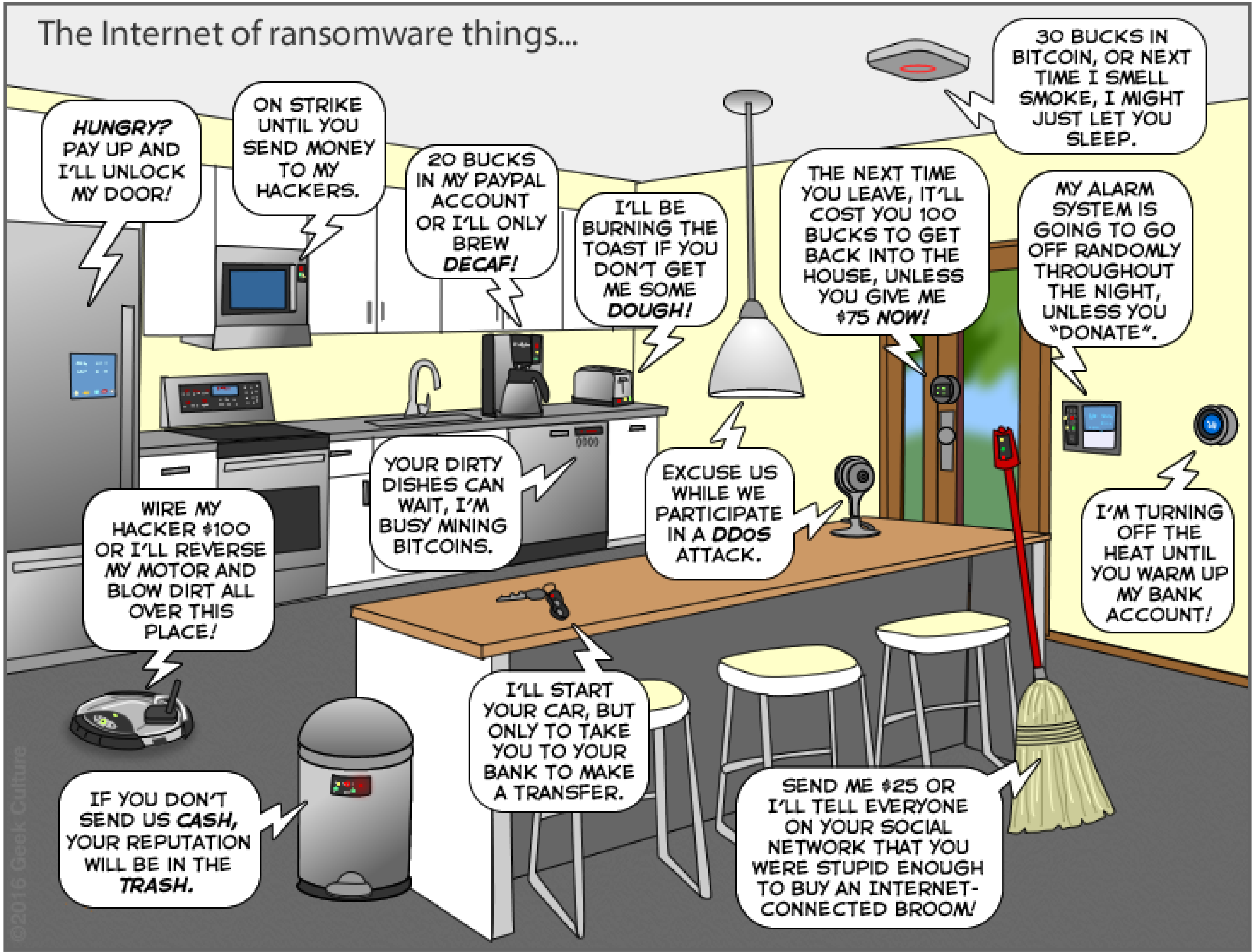
IoT Goes Nuclear: Creating a ZigBee Chain Reaction

Eyal Ronen, Colin O’Flynn,
Adi Shamir, Achi-Or Weingarten

מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE

DALHOUSIE UNIVERSITY

The Joy of Tech™ by Nitrozac & Snaggy



Typical IoT devices: Philips Hue Smart Lights

Typical IoT devices: Philips Hue Smart Lights

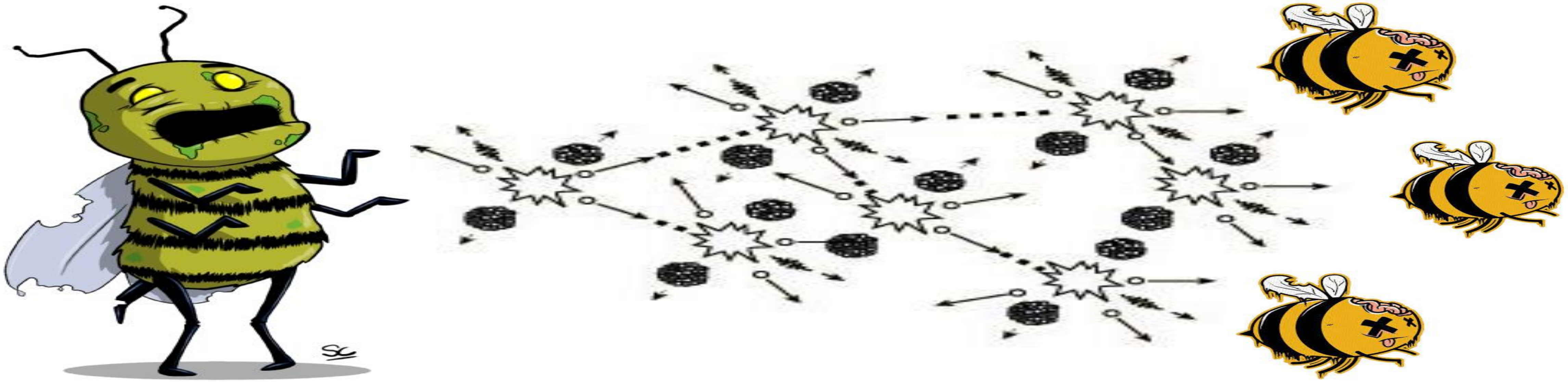
- Mature technology and standards, a relatively simple system

Typical IoT devices: Philips Hue Smart Lights

- Mature technology and standards, a relatively simple system
- A high end product with high end security, but…

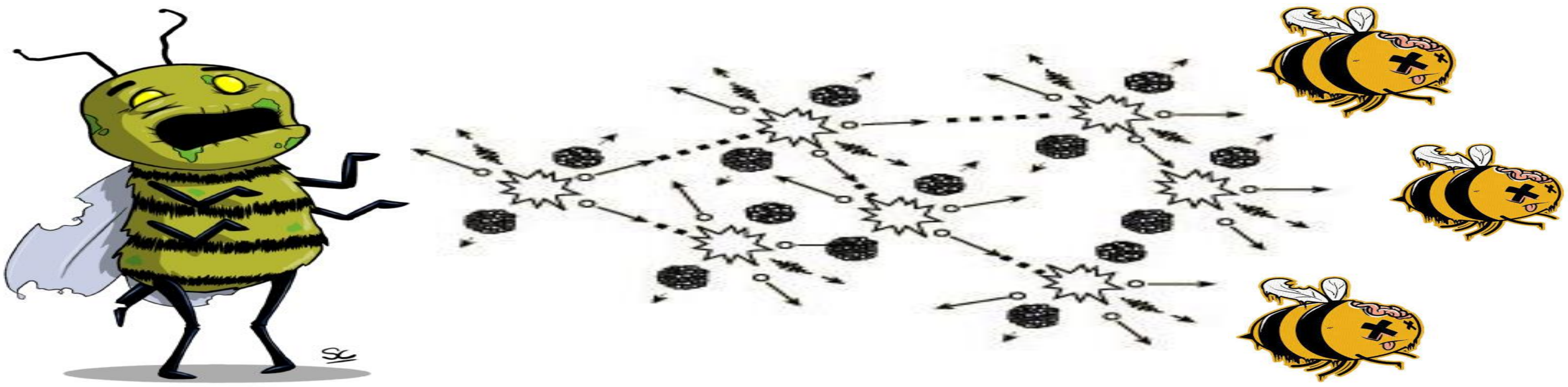
Creating a lightbulb worm

- We have proven the possibility of creating a worm which spreads using only the standard ZigBee wireless interface



Creating a lightbulb worm

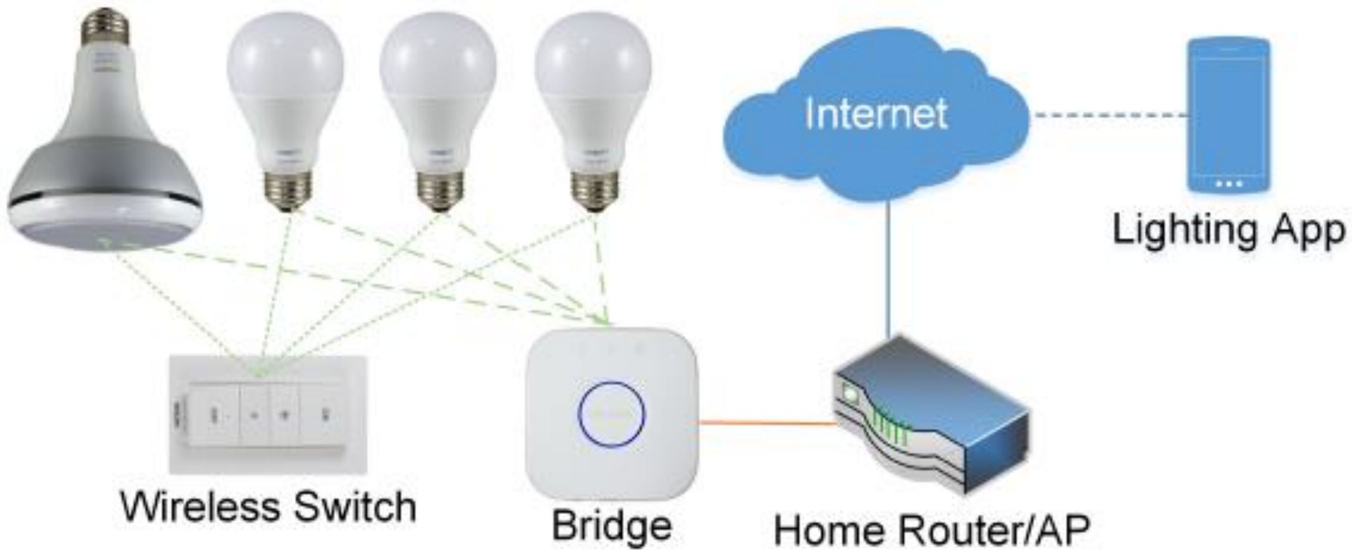
- We have proven the possibility of creating a worm which spreads using only the standard ZigBee wireless interface
  - Taking over a preinstalled smart light



Creating a lightbulb worm

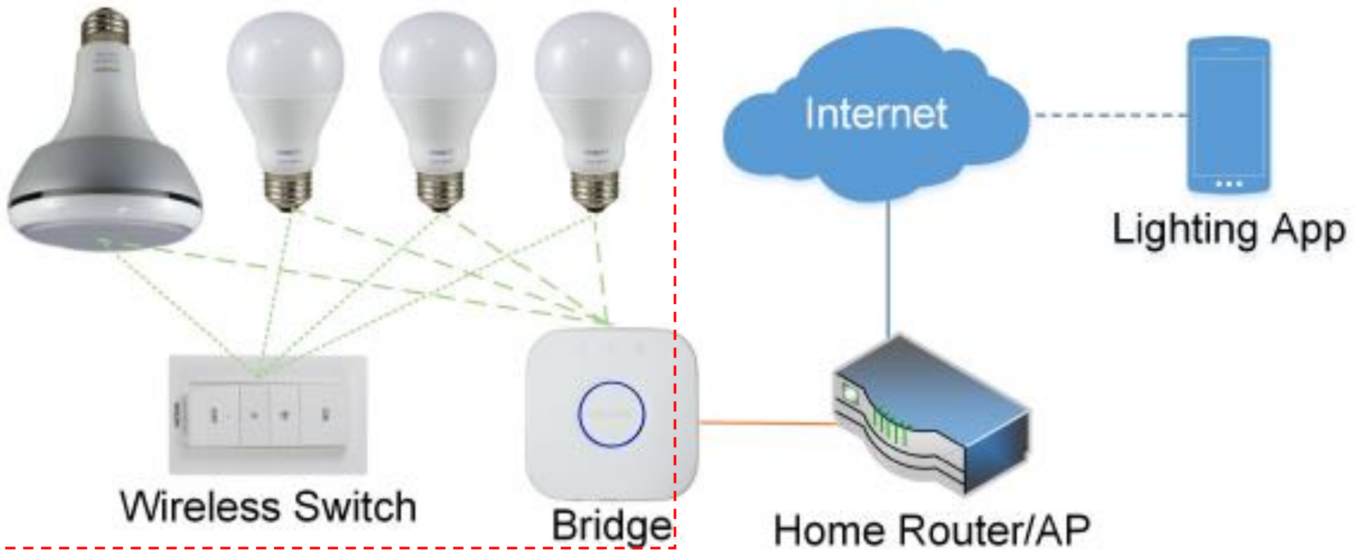
- We have proven the possibility of creating a worm which spreads using only the standard ZigBee wireless interface
  - Taking over a preinstalled smart light
  - Spreading everywhere

The underlying ZLL protocol



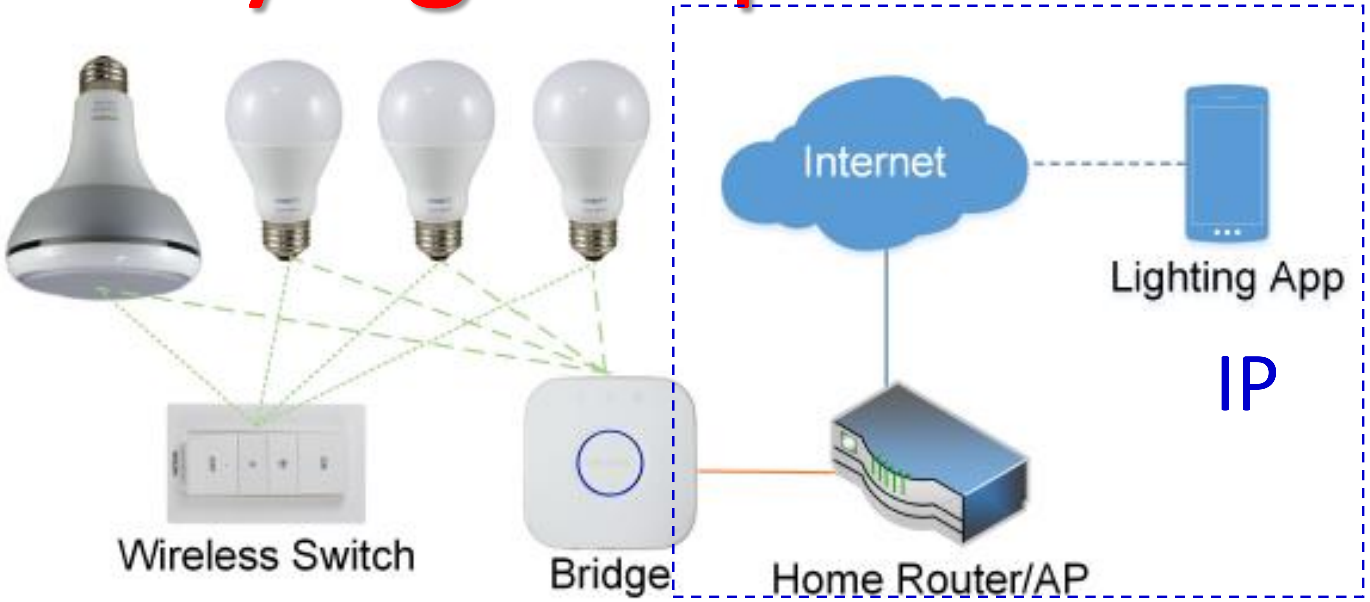
The underlying ZLL protocol

Zigbee
Personal
Area
Network



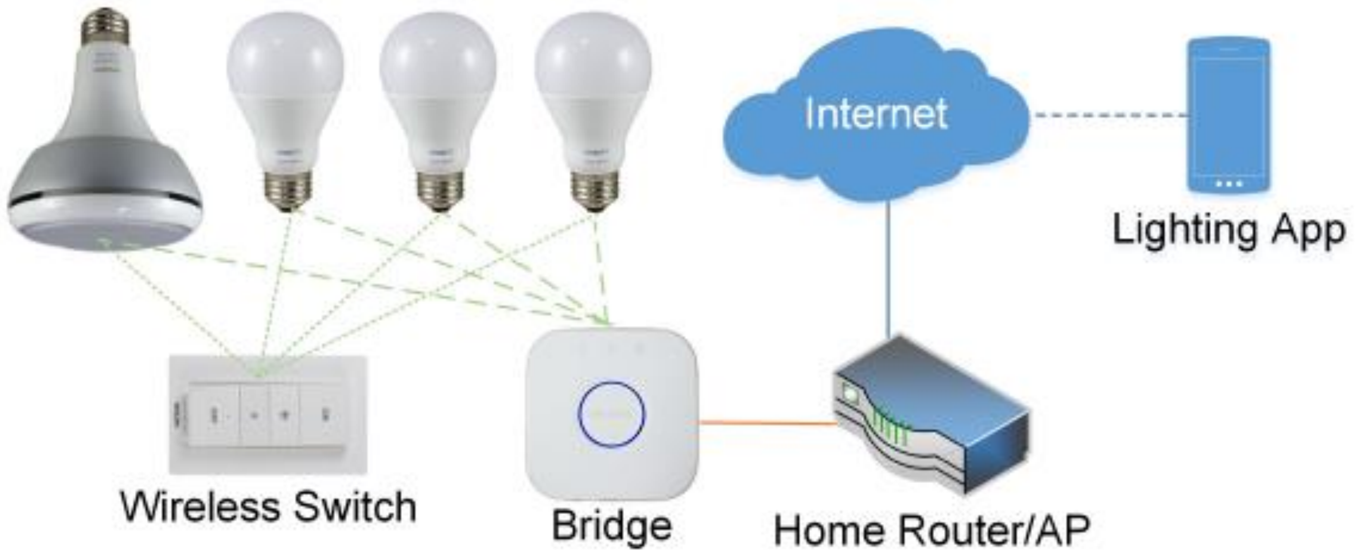
- Each installed light is connected to a central controller using the ZigBee Light Link (ZLL) wireless protocol in a Personal Area Network (PAN)

The underlying ZLL protocol



- Each installed light is connected to a central controller using the ZigBee Light Link (ZLL) wireless protocol in a Personal Area Network (PAN)
- The bridge is connected to a secure home/ office network, and is controlled by a smartphone app via IP

The underlying ZLL protocol



- Each installed light is connected to a central controller using the ZigBee Light Link (ZLL) wireless protocol in a Personal Area Network (PAN)
- The bridge is connected to a secure home/ office network, and is controlled by a smartphone app via IP
- It enables each authorized user to turn each light on or off, to change the light intensity, and to set its color

Starting the attack

Starting the attack

- Write a full python based ZLL stack, using Eval Board as RF transmitter

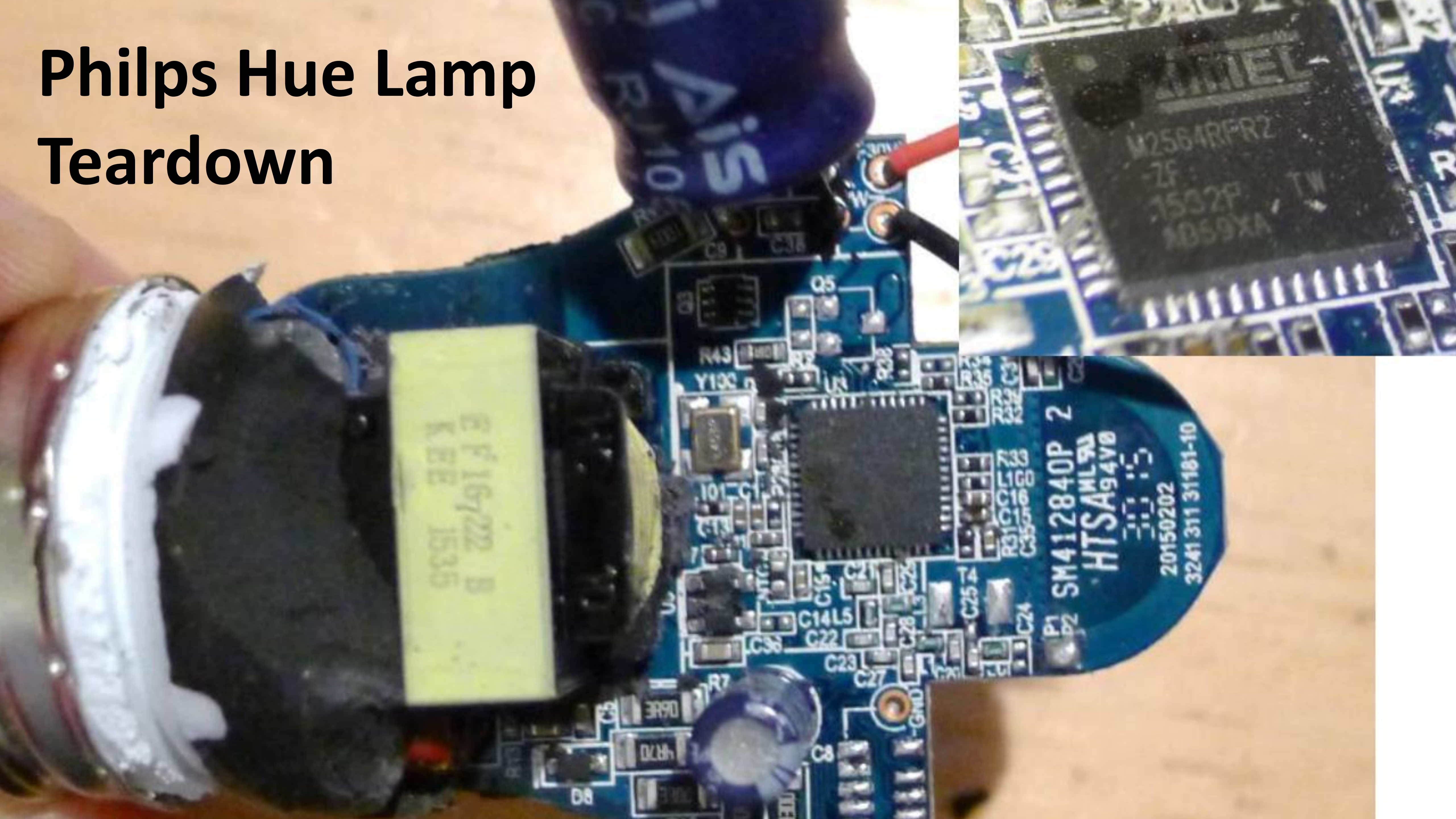
Starting the attack

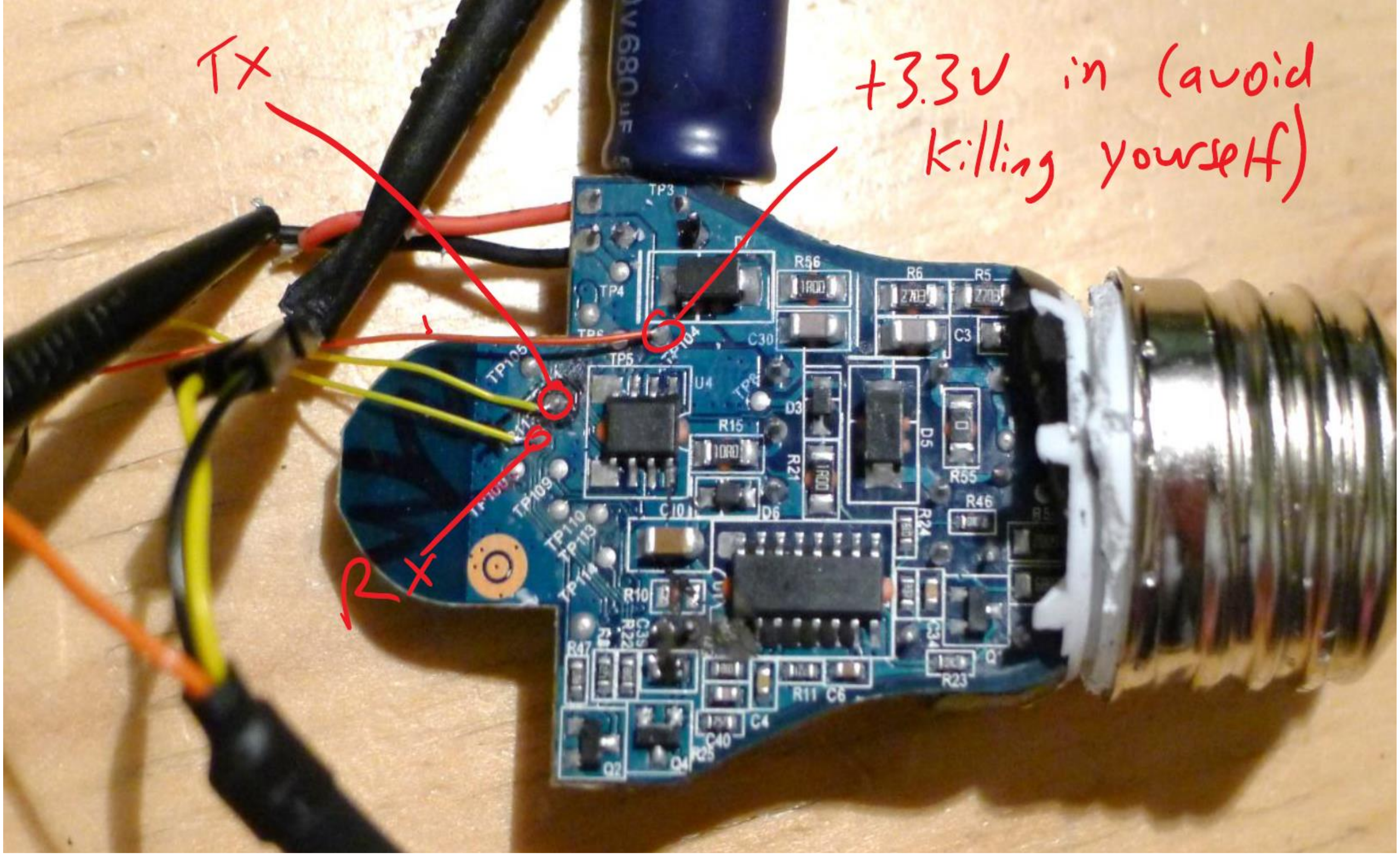
- Write a full python based ZLL stack, using Eval Board as RF transmitter
- Buy many lamps, sniff traffic, and break (physically) some lamps

Starting the attack

- Write a full python based ZLL stack, using Eval Board as RF transmitter
- Buy many lamps, sniff traffic, and break (physically) some lamps
- Start connecting wires

Philps Hue Lamp Teardown




Tx
+3.3V in (avoid killing yourself)
Rx

Boot sequence debug printout

Locked

```
[Log,Info,ConnectedLamp,MCUCR=0x00,LockBits=0xFC,LowFuse=0xF6,HighFuse=0x9
A,ExtFuse=0xFE]
[Log,Info,ConnectedLamp,devsig=0x1EA803]
[Log,Info,S_DeviceInfo,Booting into normal mode...]
[Log,Info,S_DeviceInfo,DeviceId: Bulb_A19_DimmableWhite_v2]
[Log,Info,N_Security,LIB4.5.75]
[Log,Info,N_Security,KeyBitMask,0x0012]
[Log,Info,ConnectedLamp,Platform version 0.41.0.1,package_ZigBee
117,package_BC_Stack 104,svn 26632]
[Log,Info,ConnectedLamp,Product version WhiteLamp-Atmel 5.38.1.15095,built
by LouvreZLL]
[Log,Info,A_Commissioning,Factory New at Ch: 11]
[TH,Ready,0]
```

Challenges in taking over a preinstalled smart light

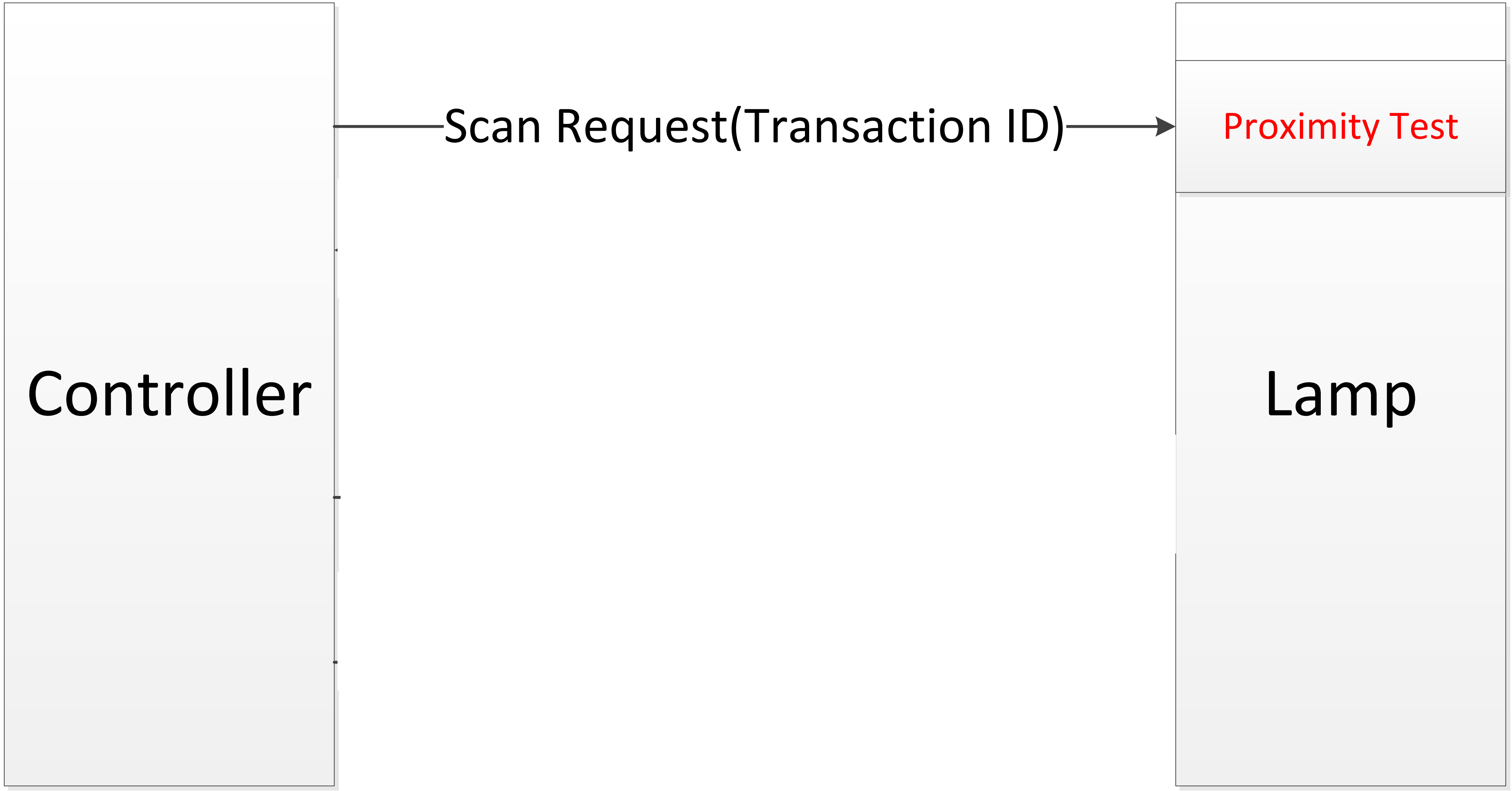
Challenges in taking over a preinstalled smart light

- ZigBee Light Link standard uses multiple cryptographic and security protocols to prevent misuse

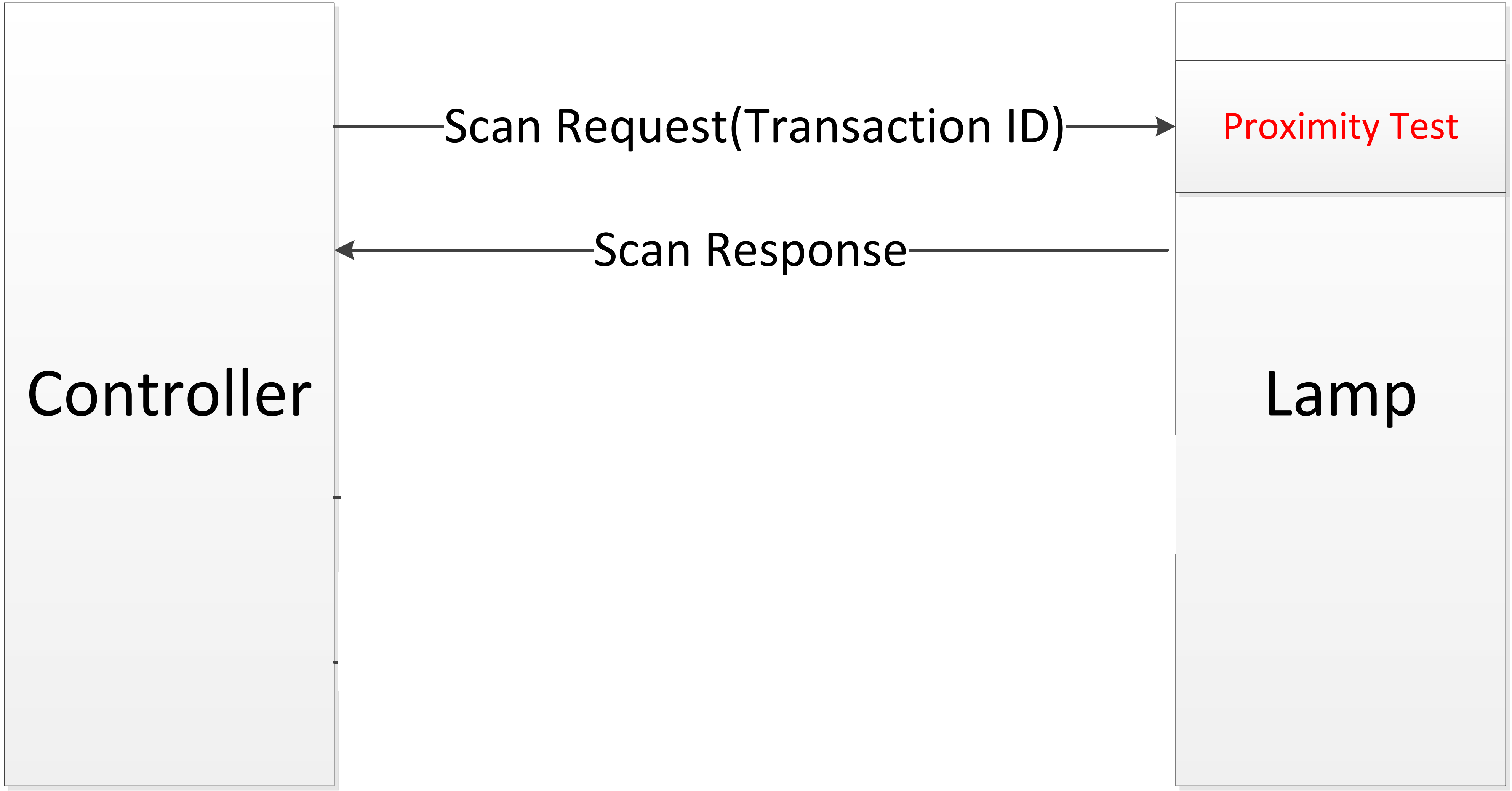
Challenges in taking over a preinstalled smart light

- ZigBee Light Link standard uses multiple cryptographic and security protocols to prevent misuse
- In particular, uses a proximity test to make sure that the only way to take control of an already installed Hue lamp is by operating it within 10-20 cm from its new controller

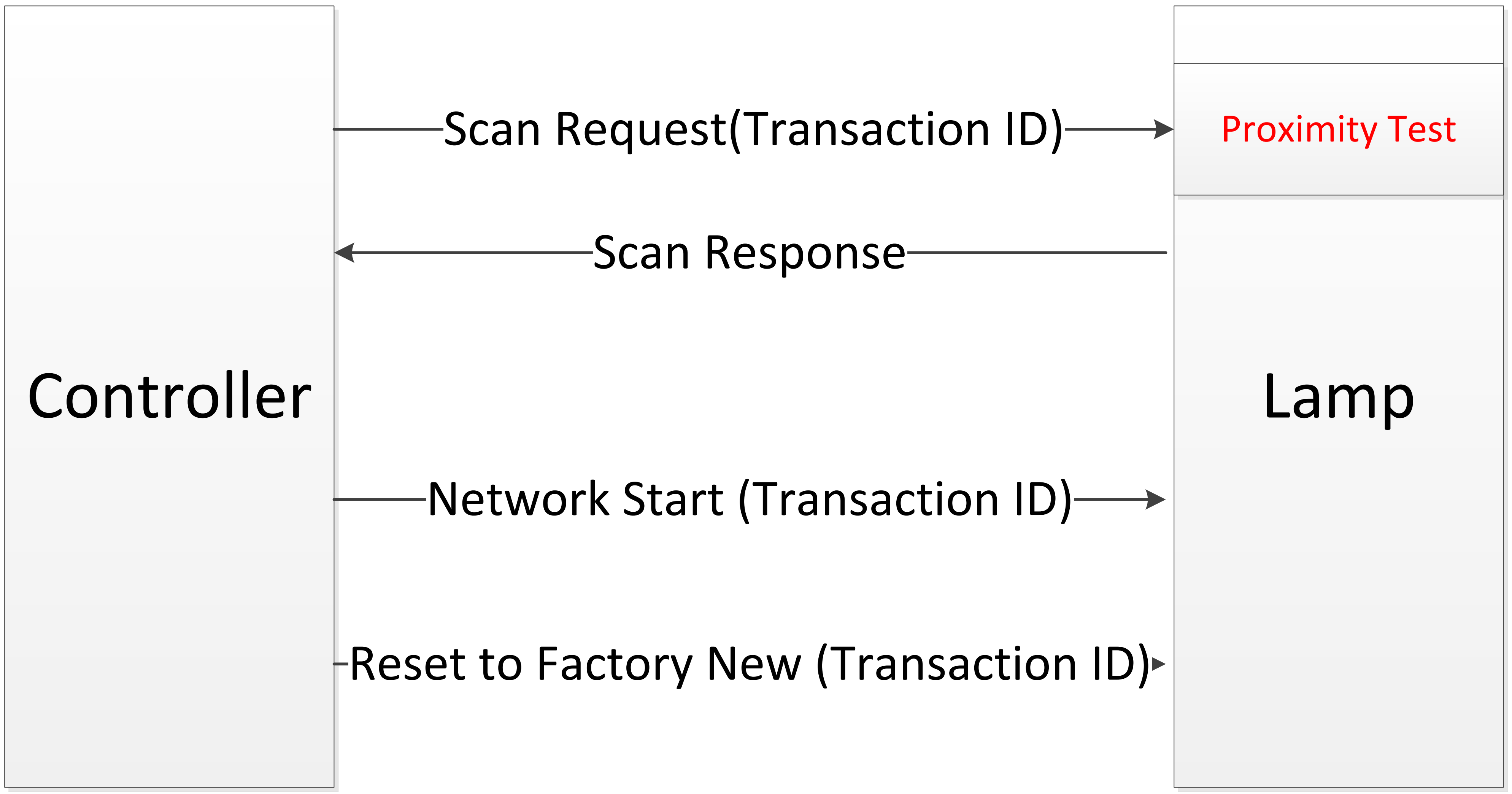
Protocol Session Outline



Protocol Session Outline



Protocol Session Outline



Protocol Implementation Bug

Protocol Implementation Bug

- We want to cause the light to Reset to Factory New

Protocol Implementation Bug

- We want to cause the light to Reset to Factory New

Field name	Data type	Octets
Inter-PAN transaction identifier	Unsigned 32-bit integer	4

Figure 37 – Format of the reset to factory new request command frame

7.1.2.2.4.1 Inter-PAN transaction identifier field

The *inter-PAN transaction identifier* field is 32-bits in length and specifies an identifier for the inter-PAN transaction. This field shall contain a non-zero 32-bit random number and is used to identify the current reset to factory new request.

Protocol Implementation Bug

- We want to cause the light to Reset to Factory New

Field name	Data type	Octets
Inter-PAN transaction identifier	Unsigned 32-bit integer	4

Figure 37 – Format of the reset to factory new request command frame

7.1.2.2.4.1 Inter-PAN transaction identifier field

The *inter-PAN transaction identifier* field is 32-bits in length and specifies an identifier for the inter-PAN transaction. This field shall contain a non-zero 32-bit random number and is used to identify the current reset to factory new request.

- Can't set a valid Transaction ID due to proximity test

Protocol Implementation Bug

- We want to cause the light to Reset to Factory New

Field name	Data type	Octets
Inter-PAN transaction identifier	Unsigned 32-bit integer	4

Figure 37 – Format of the reset to factory new request command frame

7.1.2.2.4.1 Inter-PAN transaction identifier field

The *inter-PAN transaction identifier* field is 32-bits in length and specifies an identifier for the inter-PAN transaction. This field shall contain a **Non-Zero** 32-bit random number and is used to identify the current reset to factory new request.

- Can’t set a valid Transaction ID due to proximity test

The case of ZERO (day)

The case of ZERO (day)

- How is the Session data is saved in memory?

The case of ZERO (day)

- How is the Session data is saved in memory?

```
typedef struct N_LinkTarget_ResponseParameters_t
{
  uint32_t   transactionId;
  uint32_t   responseId;
  uint8_t    zllInfo;
  uint8_t    zigBeeInfo;
} N_LinkTarget_ResponseParameters_t;
```

The case of ZERO (day)

- How is the Session data is saved in memory?

```
typedef struct N_LinkTarget_ResponseParameters_t
{
  uint32_t   transactionId;
  uint32_t   responseId;
  uint8_t    zllInfo;
  uint8_t    zigBeeInfo;
} N_LinkTarget_ResponseParameters_t;
```

- What is default values in the struct?

The case of ZERO (day)

- How is the Session data is saved in memory?

```
typedef struct N_LinkTarget_ResponseParameters_t
{
  uint32_t   transactionId;
  uint32_t   responseId;
  uint8_t    zllInfo;
  uint8_t    zigBeeInfo;
} N_LinkTarget_ResponseParameters_t;
```

- What is default values in the struct?
- Well surely it is checked on access…

The case of ZERO (day)

- How is the Session data is saved in memory?

```
typedef struct N_LinkTarget_ResponseParameters_t
{
  uint32_t  transactionId;
  uint32_t  responseId;
  uint8_t   zllInfo;
  uint8_t   zigBeeInfo;
} N_LinkTarget_ResponseParameters_t;
```

- What is default values in the struct?
- Well surely it is checked on access…

```
/** Check if the transaction id is active.
\note The value zero is already rejected
      by N_InterPan.
*/
bool IsTransactionIdActive(uint32_t transactionId)
{
  if (GetFromResponseTable(transactionId) == NULL)
  {
    return FALSE;
  }
  return TRUE;
}
```

The case of ZERO (day)

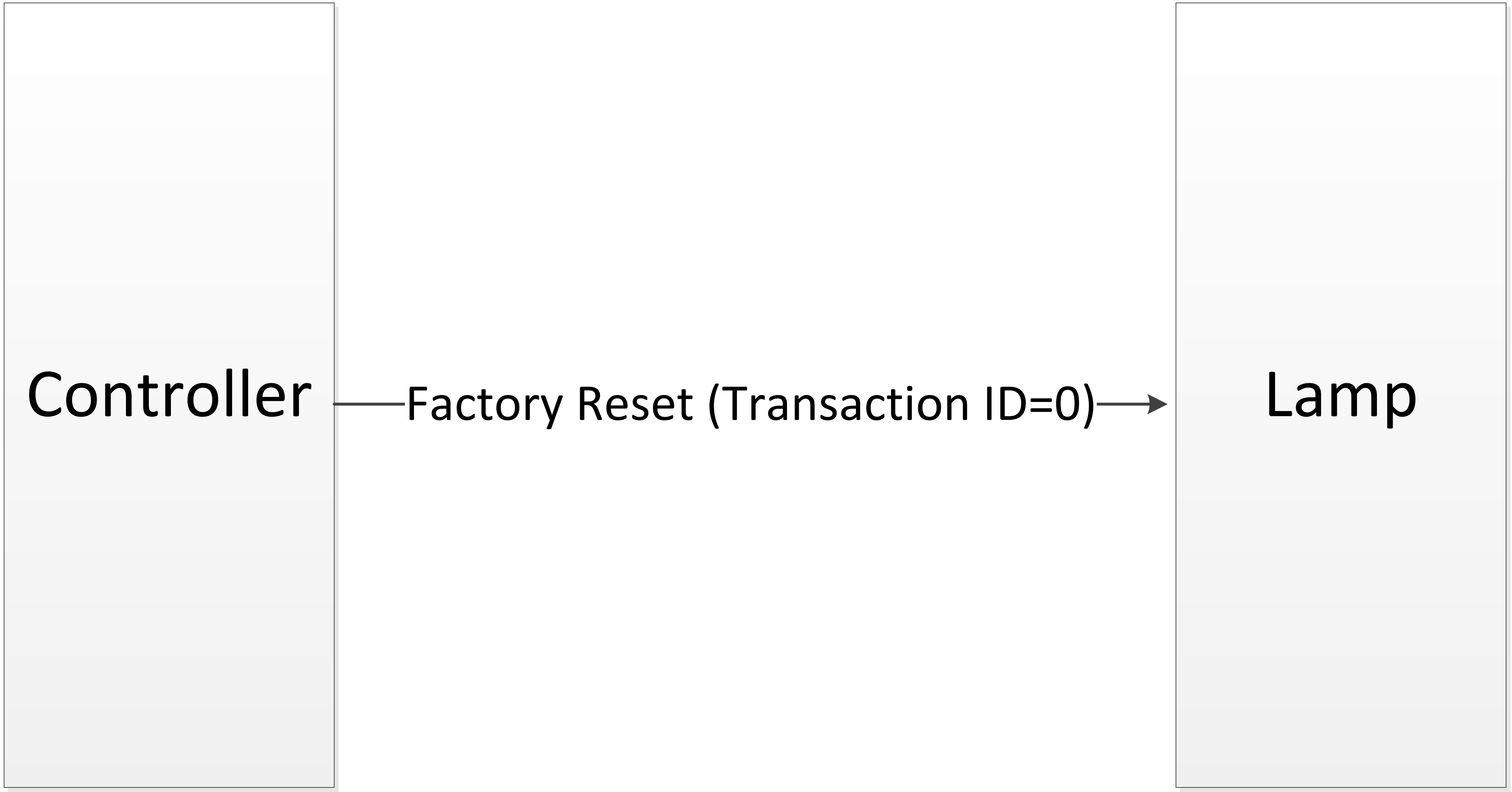
- How is the Session data is saved in memory?

```
typedef struct N_LinkTarget_ResponseParameters_t
{
  uint32_t   transactionId;
  uint32_t   responseId;
  uint8_t    zllInfo;
  uint8_t    zigBeeInfo;
} N_LinkTarget_ResponseParameters_t;
```

- What is default values in the struct?
- Well surely it is checked on access…
- Just on Scan Request message

```
/** Check if the transaction id is active.
\note The value zero is already rejected
      by N_InterPan.
*/
bool IsTransactionIdActive(uint32_t transactionId)
{
  if (GetFromResponseTable(transactionId) == NULL)
  {
    return FALSE;
  }
  return TRUE;
}
```

Protocol Attack Outline

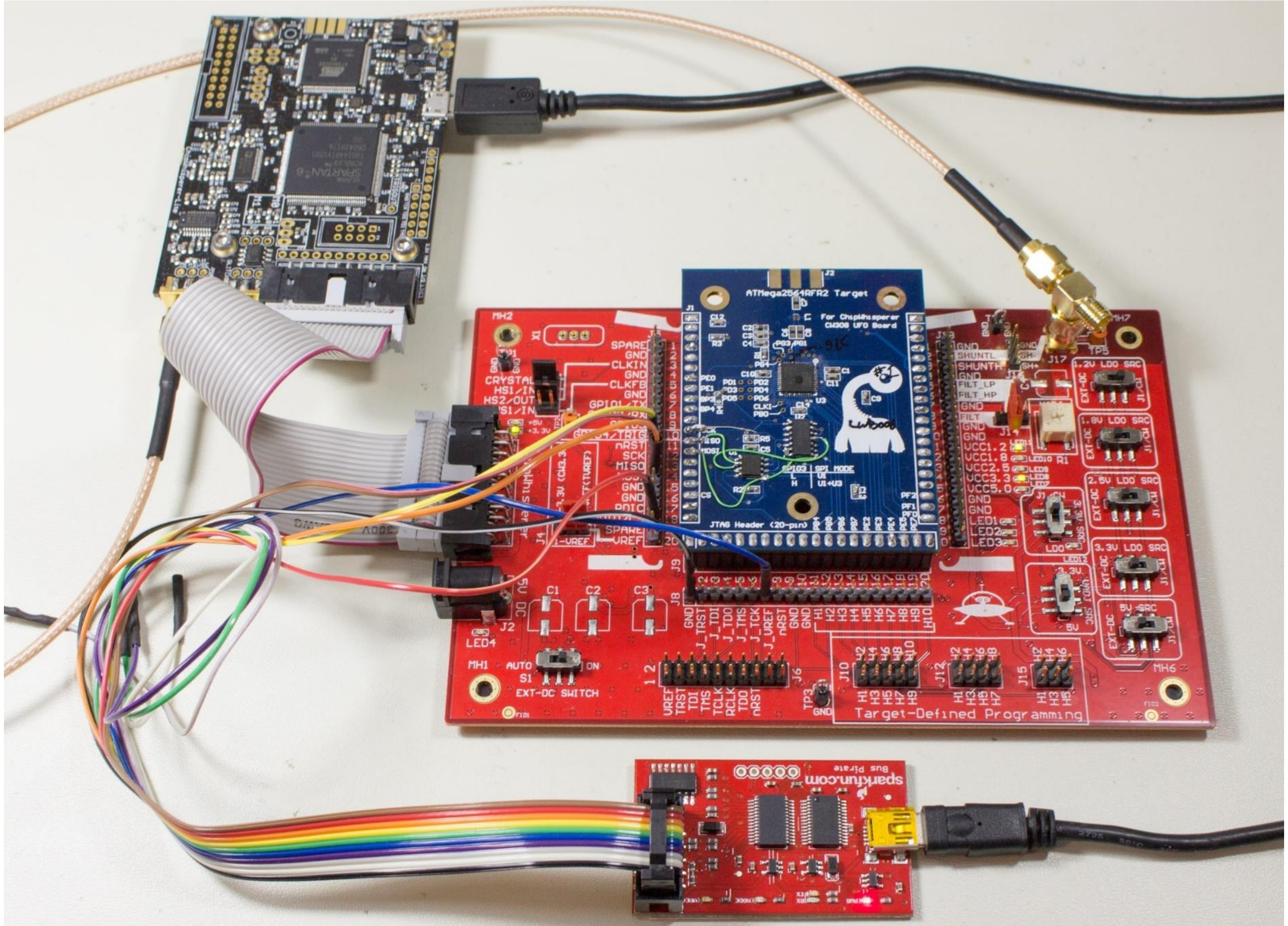


We bought a cheap and lightweight commercial Zigbee evaluation kit:

ZigBee WarFlying - Taking over a building's lights

By launching a drone carrying a fully automated attack equipment 400 meters away

Spreading everywhere



Getting software updates

- No software update for Atmel based lamps

Getting software updates

- No software update for Atmel based lamps
- So lets impersonate to an older model and version

Getting software updates

- No software update for Atmel based lamps
- So lets impersonate to an older model and version
- Looked for posting on upgrades on the Internet (mainly Reddit)

Getting software updates

- No software update for Atmel based lamps
- So lets impersonate to an older model and version
- Looked for posting on upgrades on the Internet (mainly Reddit)

Known upgrades (From Internet Posts)

66009663 -> 66013452

65003148 -> 66013452 (recorded with type 100)

66010820 -> 66012457 (recorded with type 104) (GU10)

65003148 -> 66012457 (recorded with type 104) (GU10)

65003148 -> 66013452 (recorded with type 103)

Light impersonating

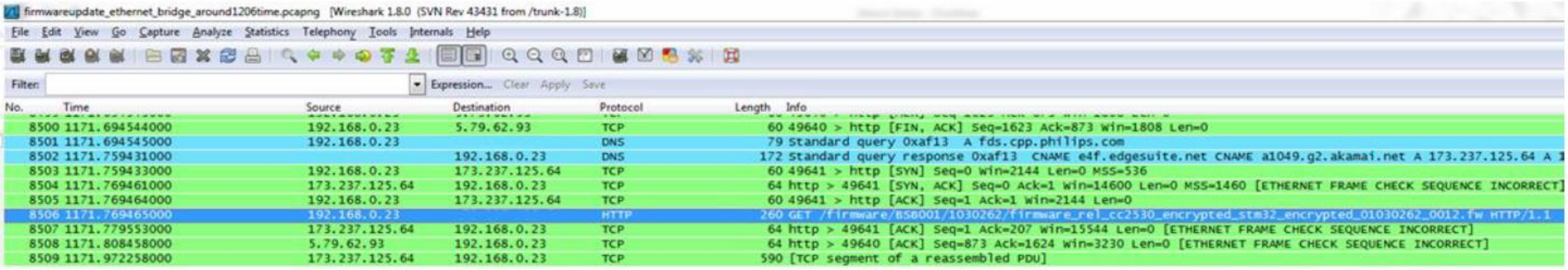
- Write impersonating code, to identify as old models

Light impersonating

- Write impersonating code, to identify as old models
- Sniff OTA updates on Zigbee and on bridge

Light impersonating

- Write impersonating code, to identify as old models
- Sniff OTA updates on Zigbee and on bridge

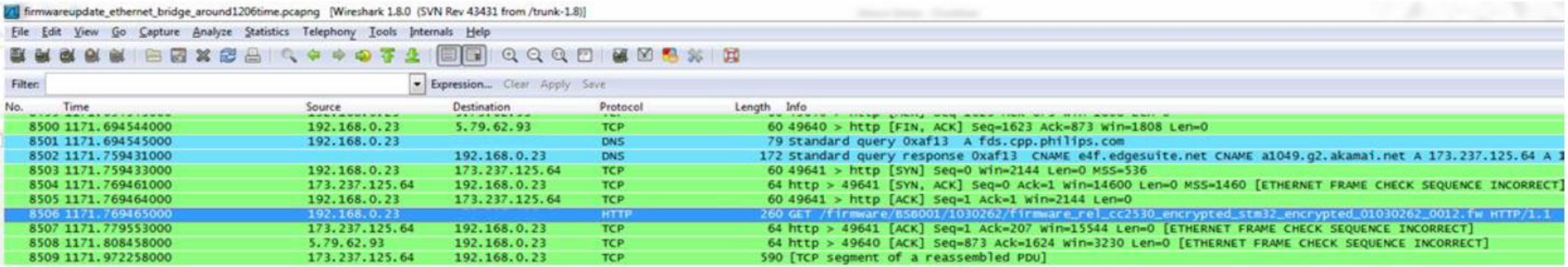


http://xxx/firmware/HUE0100/66013452/ConnectedLamp-Target_0012_13452_8D.sbl-ota

http://xxx/firmware/BSB001/1030262/firmware_rel_cc2530_encrypted_stm32_encrypted_01030262_0012.fw

Light impersonating

- Write impersonating code, to identify as old models
- Sniff OTA updates on Zigbee and on bridge


firmwareupdate_ethernet_bridge_around1206time.pcapng [Wireshark 1.8.0 (SVN Rev 43431 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

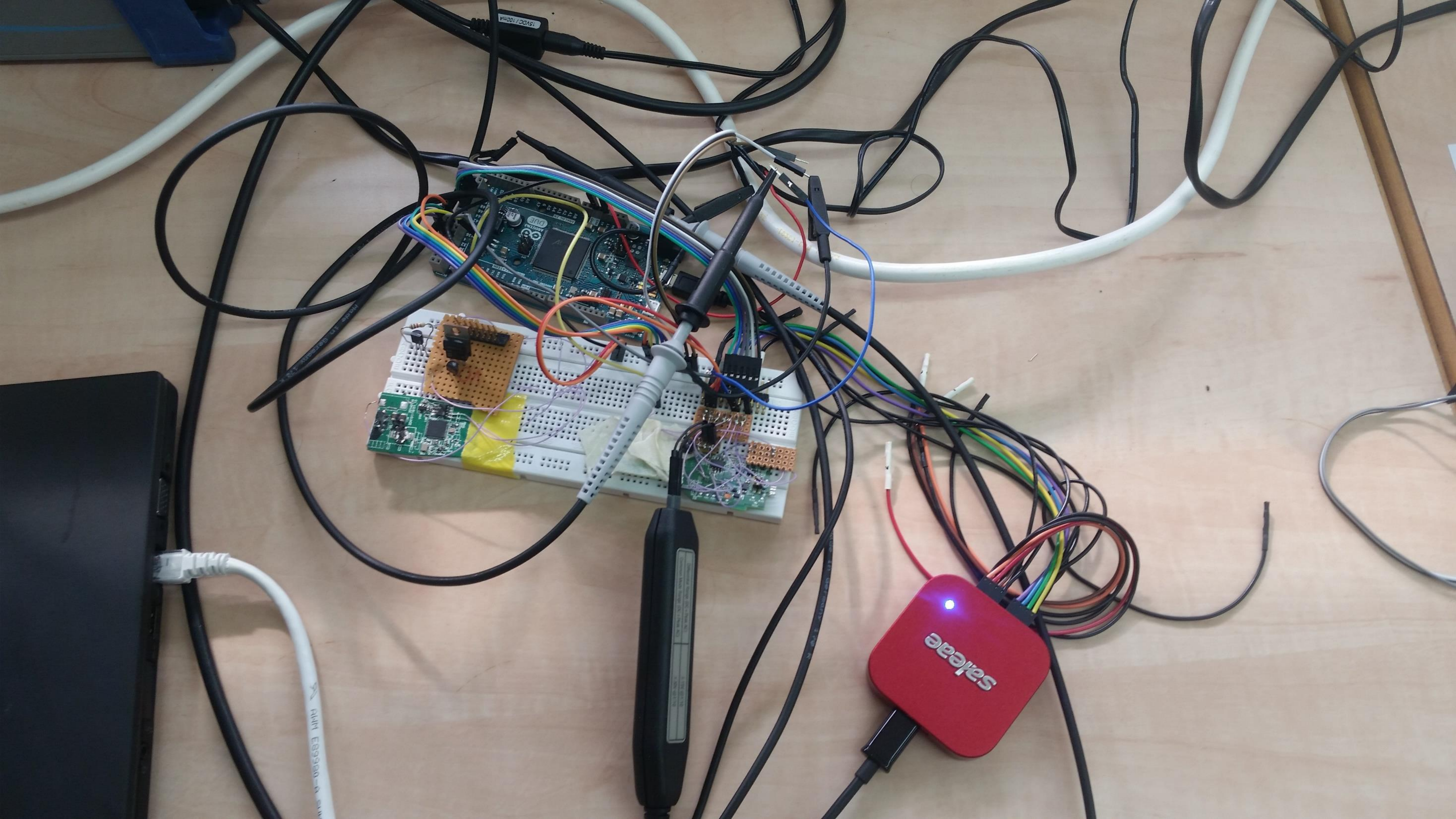
Filter: Expression... Clear Apply Save

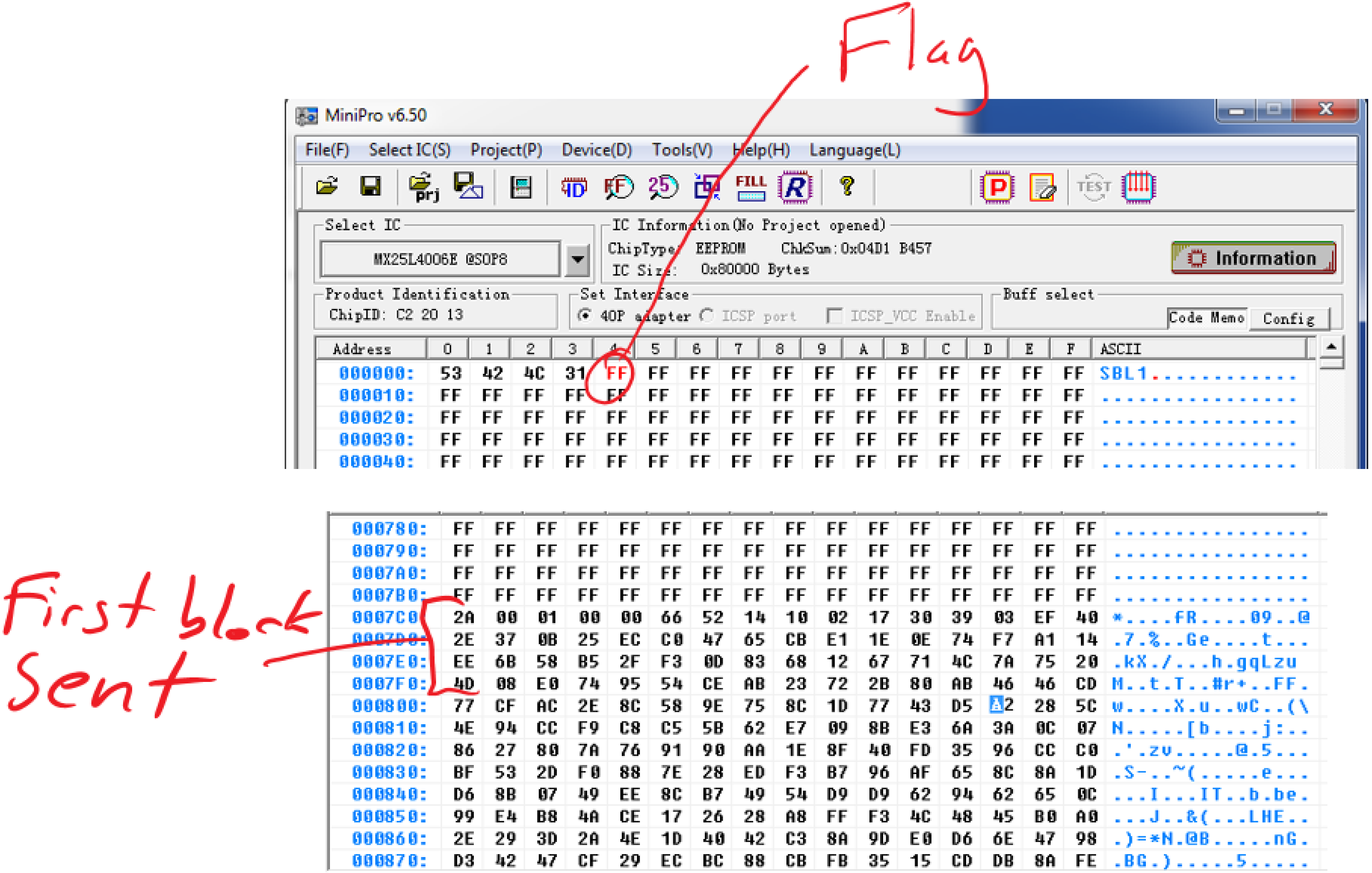
No.	Time	Source	Destination	Protocol	Length	Info
8500	1171.694544000	192.168.0.23	5.79.62.93	TCP	60	49640 > http [FIN, ACK] Seq=1623 Ack=873 Win=1808 Len=0
8501	1171.694545000	192.168.0.23		DNS	79	Standard query 0xaf13 A fds.cpp.philips.com
8502	1171.759431000		192.168.0.23	DNS	172	Standard query response 0xaf13 CNAME e4f.edgesuite.net CNAME a1049.g2.akamai.net A 173.237.125.64 A 1
8503	1171.759433000	192.168.0.23	173.237.125.64	TCP	60	49641 > http [SYN] Seq=0 Win=2144 Len=0 MSS=536
8504	1171.769461000	173.237.125.64	192.168.0.23	TCP	64	http > 49641 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
8505	1171.769464000	192.168.0.23	173.237.125.64	TCP	60	49641 > http [ACK] Seq=1 Ack=1 Win=2144 Len=0
8506	1171.769465000	192.168.0.23		HTTP	260	GET /firmware/BSB001/1030262/firmware_rel_cc2530_encrypted_stm32_encrypted_01030262_0012.fw HTTP/1.1
8507	1171.779553000	173.237.125.64	192.168.0.23	TCP	64	http > 49641 [ACK] Seq=1 Ack=207 Win=15544 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
8508	1171.808458000	5.79.62.93	192.168.0.23	TCP	64	http > 49640 [ACK] Seq=873 Ack=1624 Win=3230 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
8509	1171.972258000	173.237.125.64	192.168.0.23	TCP	590	[TCP segment of a reassembled PDU]

http://xxx/firmware/HUE0100/66013452/ConnectedLamp-Target_0012_13452_8D.sbl-ota

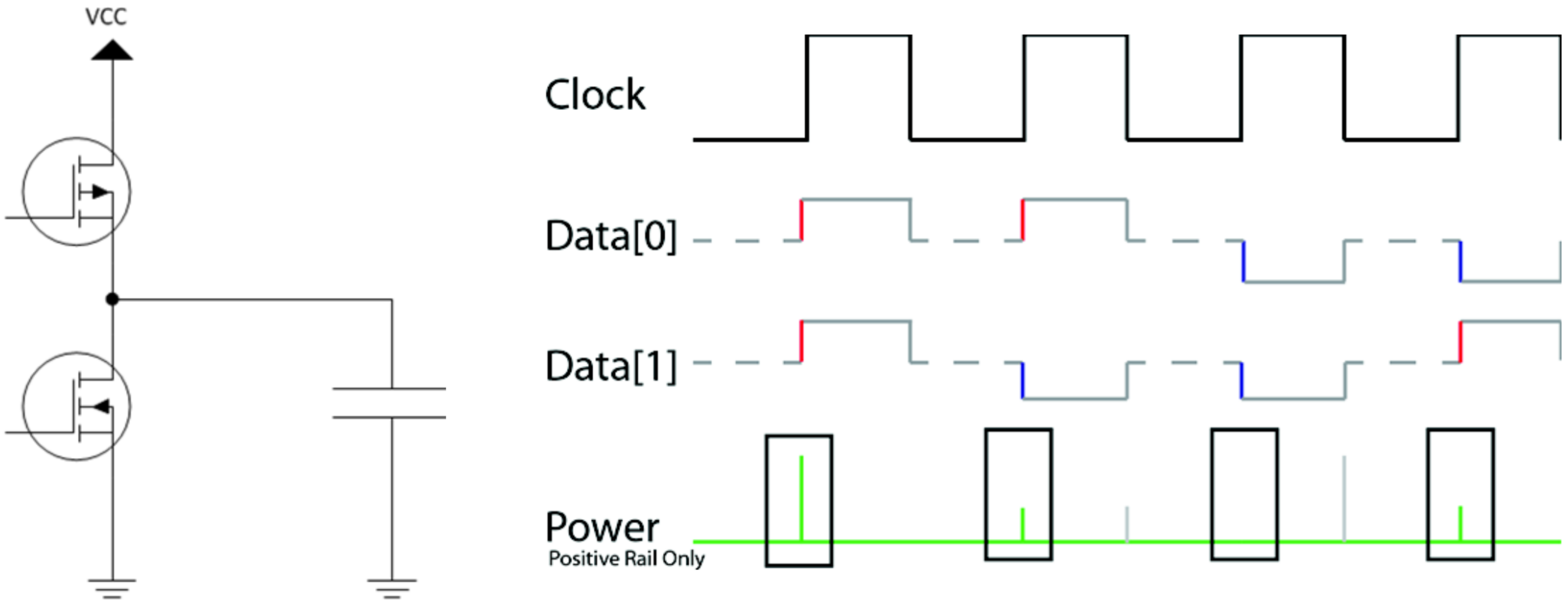
http://xxx/firmware/BSB001/1030262/firmware_rel_cc2530_encrypted_stm32_encrypted_01030262_0012.fw

- They are encrypted


saleae

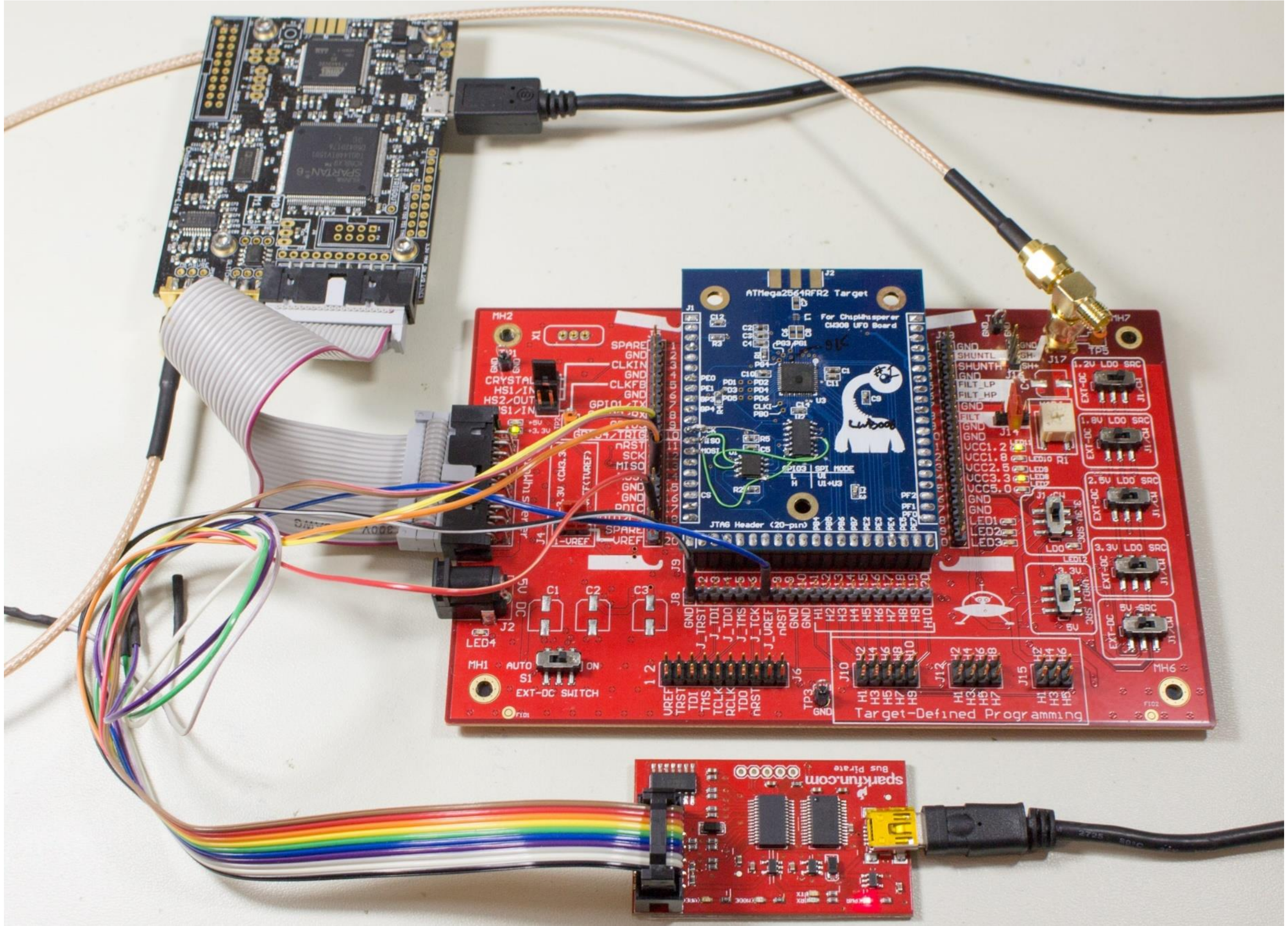

Flag
First block Sent
MiniPro v6.50
File(F) Select IC(S) Project(P) Device(D) Tools(V) Help(H) Language(L)
Select IC
MX25L4006E @SOP8
IC Information(No Project opened)
ChipType: EEPROM ChkSum:0x04D1 B457
IC Size: 0x80000 Bytes
Information
Product Identification
ChipID: C2 20 13
Set Interface
40P adapter ICSP port ICSP_VCC Enable
Buff select
Code Memo Config
Address 0 1 2 3 4 5 6 7 8 9 A B C D E F ASCII
000000: 53 42 4C 31 FF FF FF FF FF FF FF FF FF FF FF FF SBL1............
000010: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ....
000020: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ....
000030: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ....
000040: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ....
000780: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ....
000790: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ....
0007A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ....
0007B0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ....
0007C0: 2A 00 01 00 00 66 52 14 10 02 17 30 39 03 EF 40 *....fR....09..@
0007D0: 2E 37 0B 25 EC C0 47 65 CB E1 1E 0E 74 F7 A1 14 .7.%..Ge....t...
0007E0: EE 6B 58 B5 2F F3 0D 83 68 12 67 71 4C 7A 75 20 .kX./...h.gqLzu
0007F0: 4D 08 E0 74 95 54 CE AB 23 72 2B 80 AB 46 46 CD M..t.T..#r+..FF.
000800: 77 CF AC 2E 8C 58 9E 75 8C 1D 77 43 D5 A2 28 5C w....X.u..wC..(\
000810: 4E 94 CC F9 C8 C5 5B 62 E7 09 8B E3 6A 3A 0C 07 N.....[b....j:..
000820: 86 27 80 7A 76 91 90 AA 1E 8F 40 FD 35 96 CC C0 .'.zv.....@.5...
000830: BF 53 2D F0 88 7E 28 ED F3 B7 96 AF 65 8C 8A 1D .S-..~(.....e...
000840: D6 8B 07 49 EE 8C B7 49 54 D9 D9 62 94 62 65 0C ...I...IT..b.be.
000850: 99 E4 B8 4A CE 17 26 28 A8 FF F3 4C 48 45 B0 A0 ...J..&(...LHE..
000860: 2E 29 3D 2A 4E 1D 40 42 C3 8A 9D E0 D6 6E 47 98 .)=*N.@B.....nG.
000870: D3 42 47 CF 29 EC BC 88 CB FB 35 15 CD DB 8A FE .BG.).....5.....

Correlation power analysis

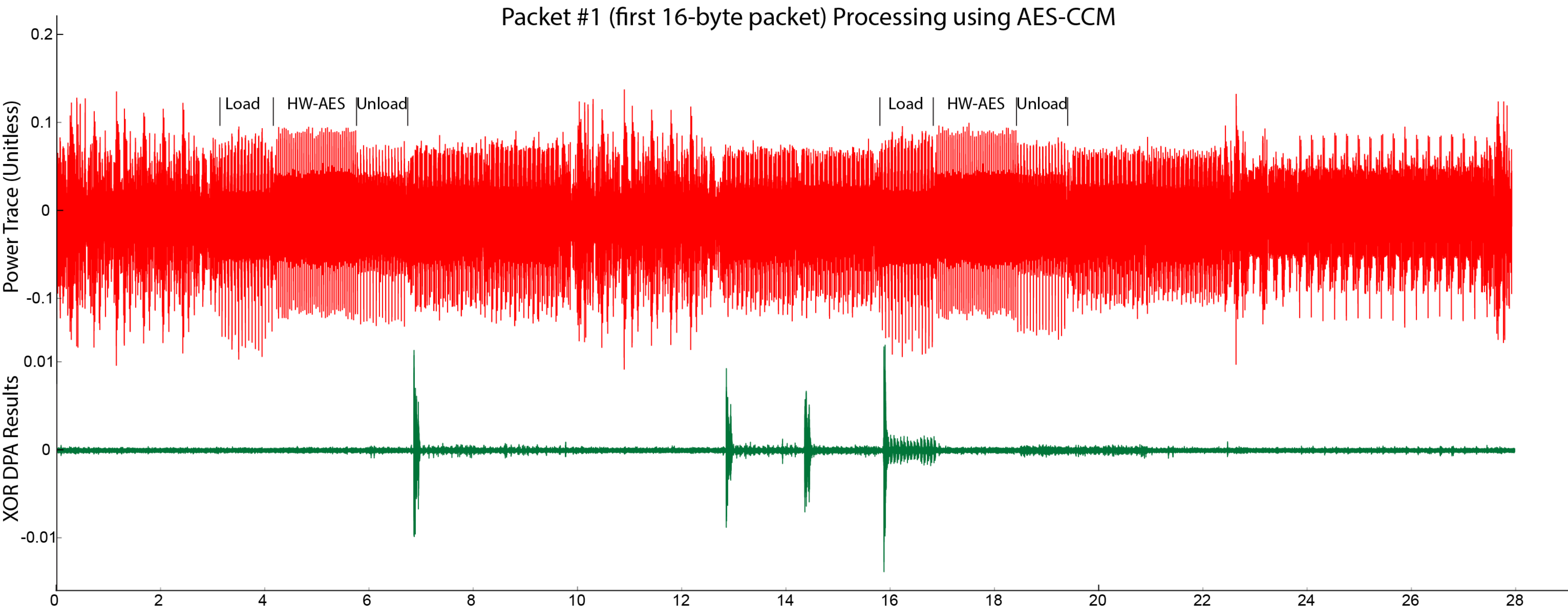


(a) (b)

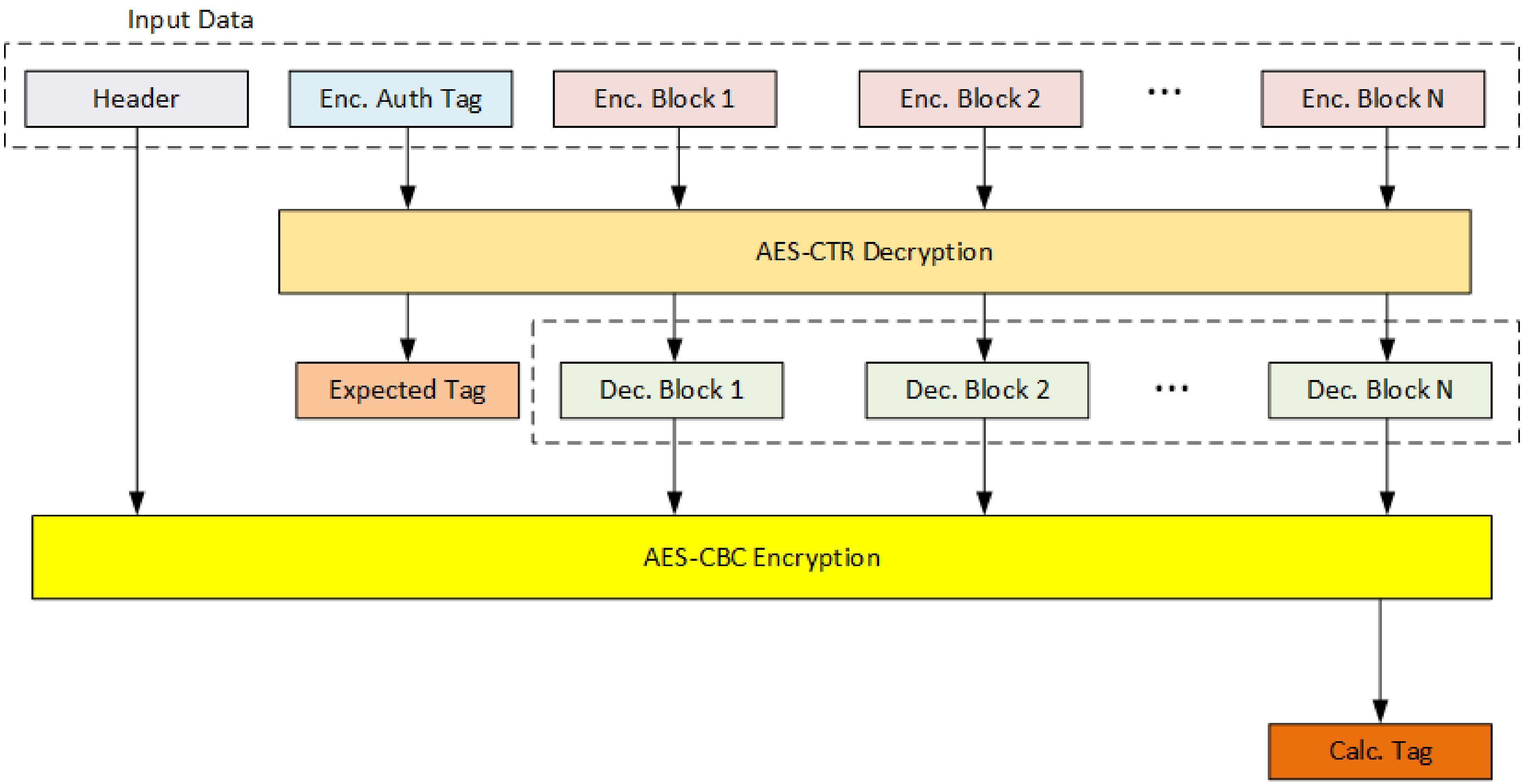
Power Analysis Example Setup



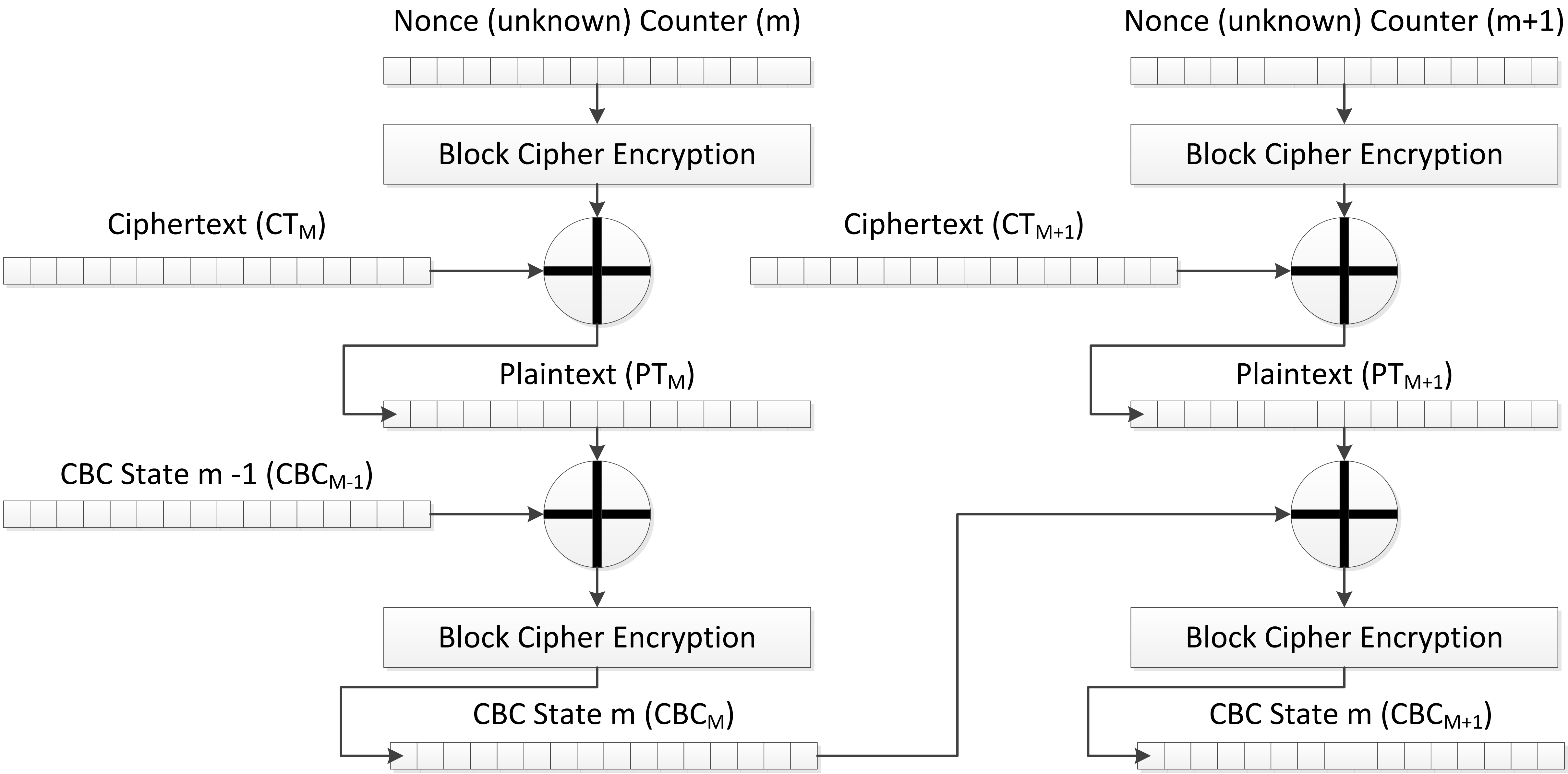
CPA for RE


Packet #1 (first 16-byte packet) Processing using AES-CCM
Power Trace (Unitless)
XOR DPA Results
Load
HW-AES
Unload
Load
HW-AES
Unload
0.2
0.1
0
-0.1
0.01
0
-0.01
0
2
4
6
8
10
12
14
16
18
20
22
24
26
28

CCM


Input Data
Header
Enc. Auth Tag
Enc. Block 1
Enc. Block 2
...
Enc. Block N
AES-CTR Decryption
Expected Tag
Dec. Block 1
Dec. Block 2
...
Dec. Block N
AES-CBC Encryption
Calc. Tag

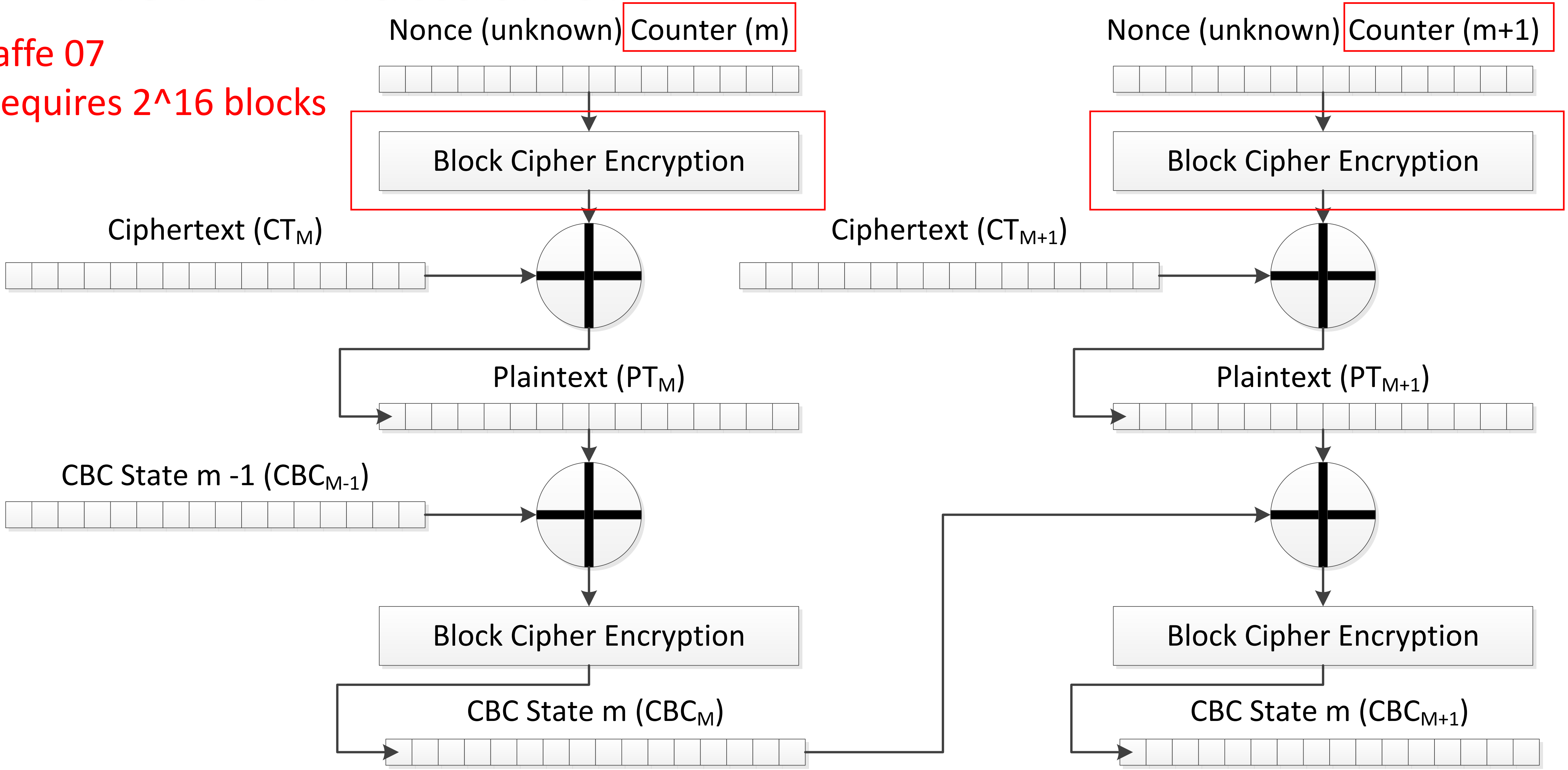
New CPA attack on CCM



New CPA attack on CCM

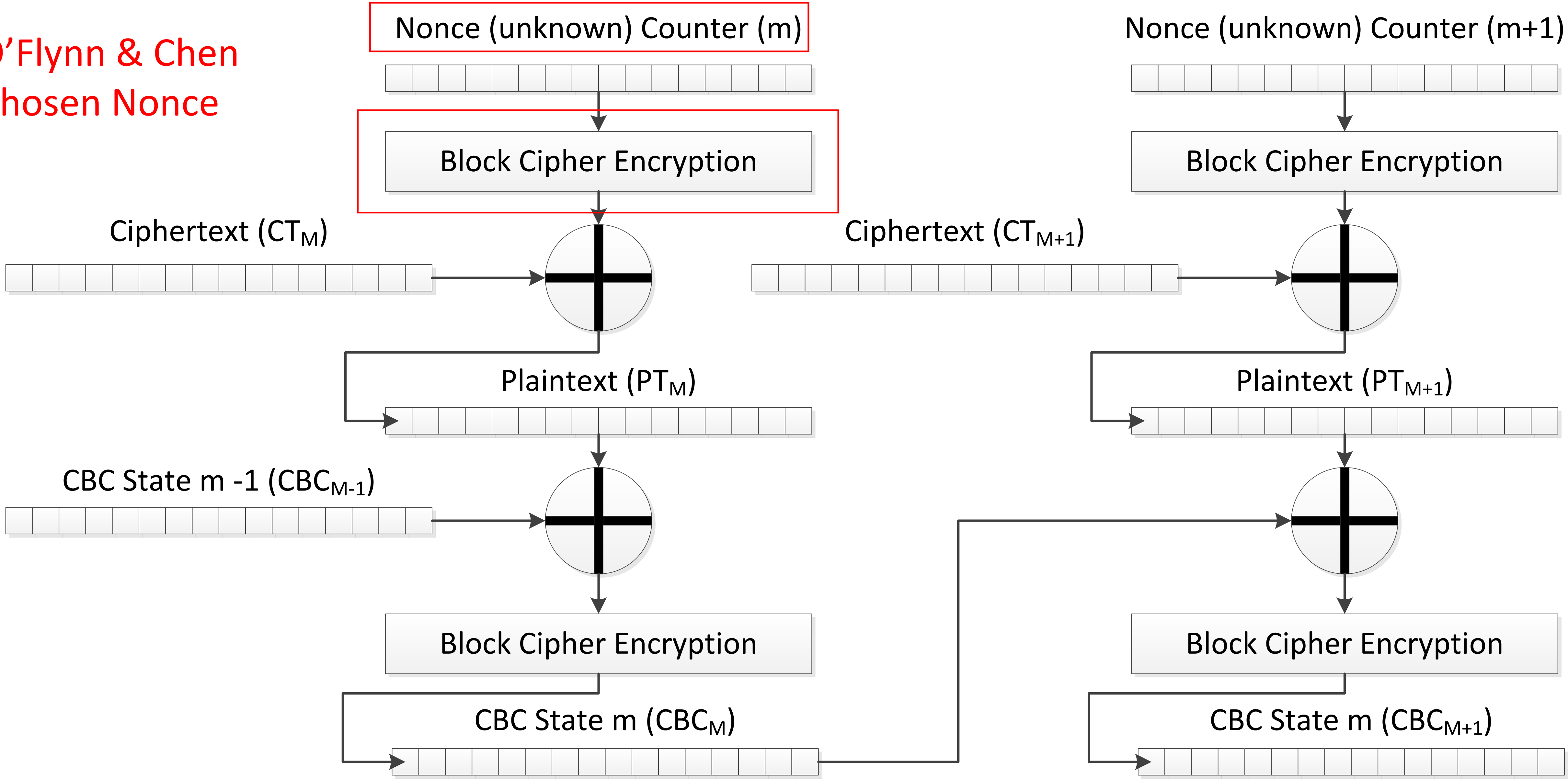
Jaffe 07

Requires 2^16 blocks

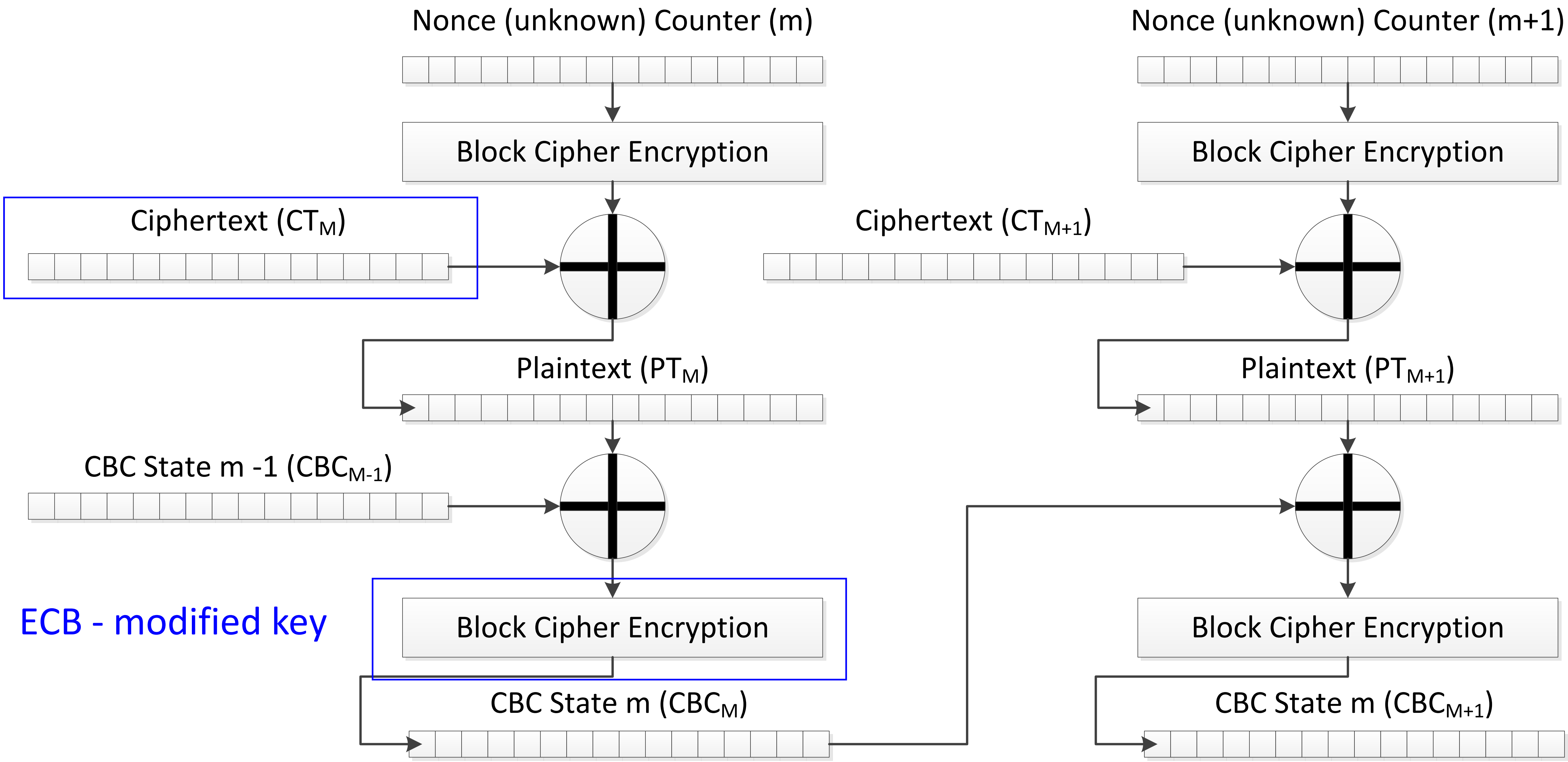


New CPA attack on CCM

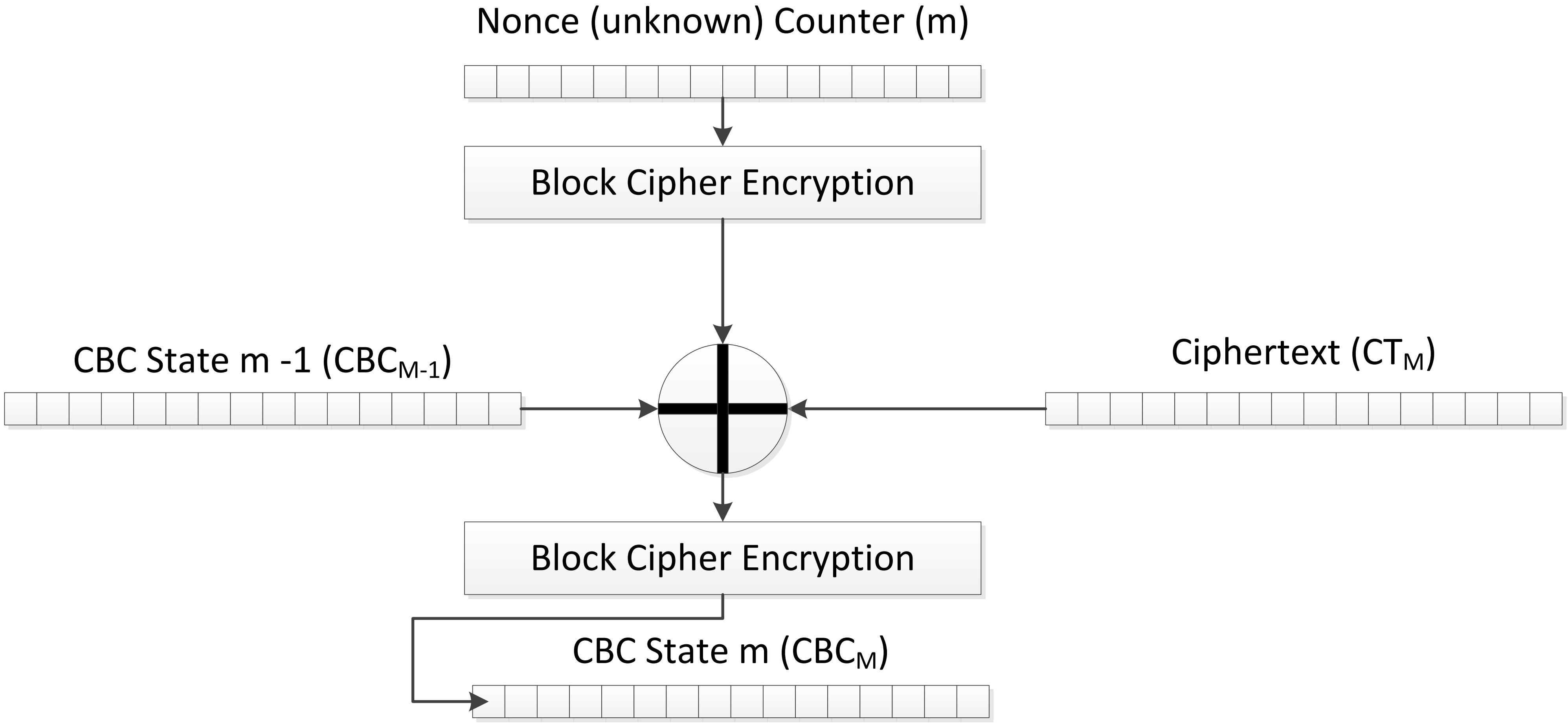
O'Flynn & Chen
Chosen Nonce



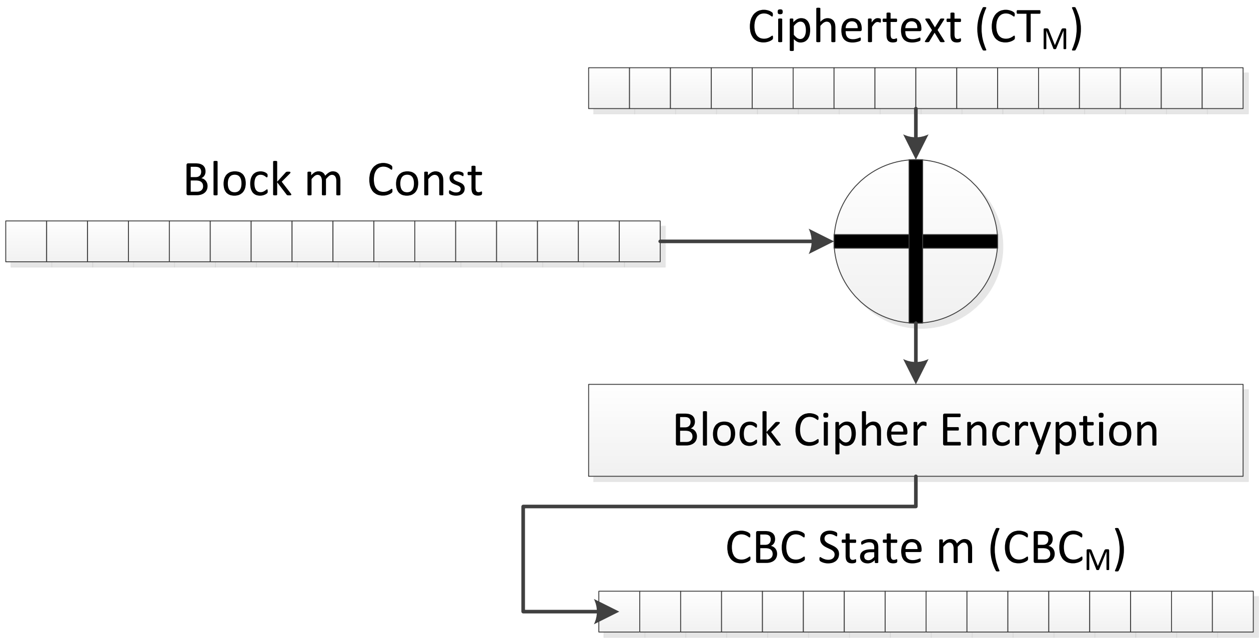
New CPA attack on CCM



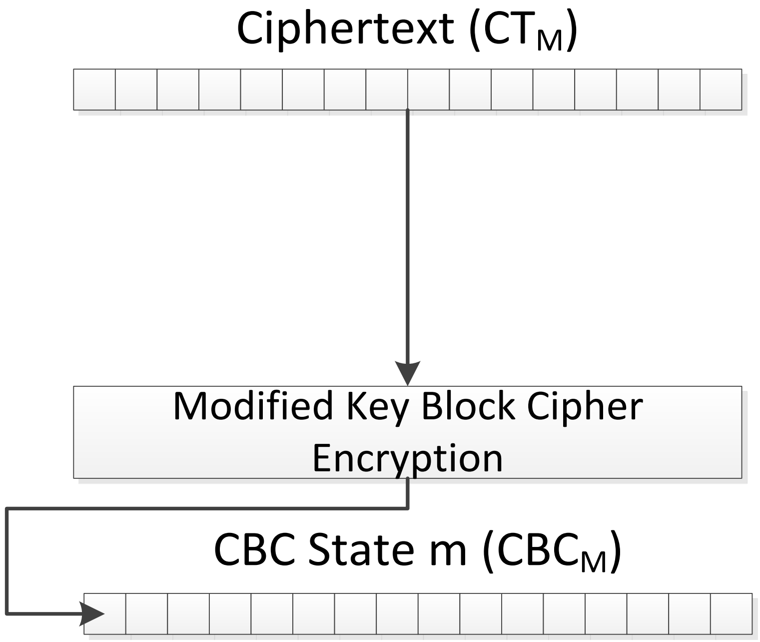
New CPA attack on CCM

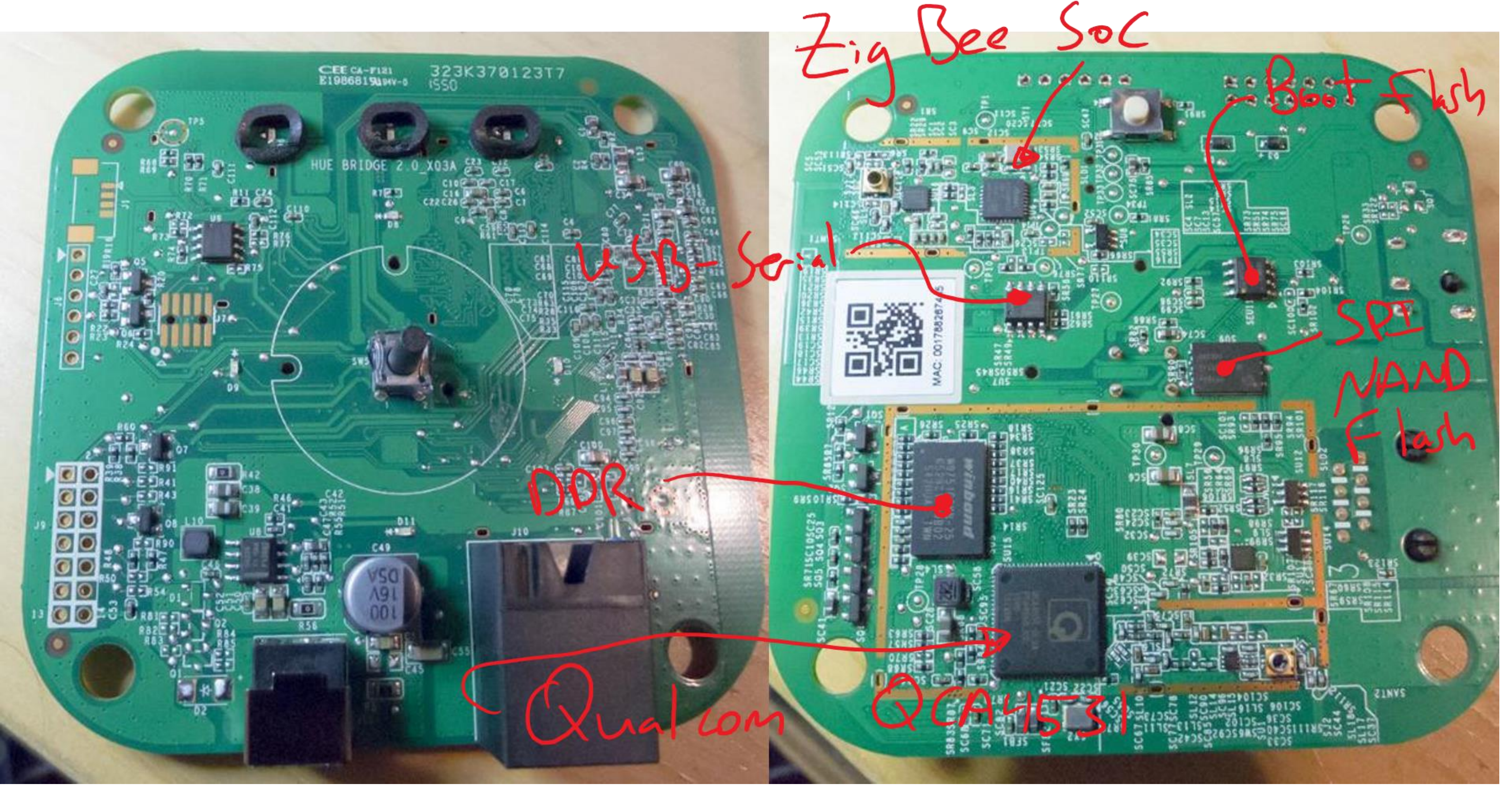


New CPA attack on CCM

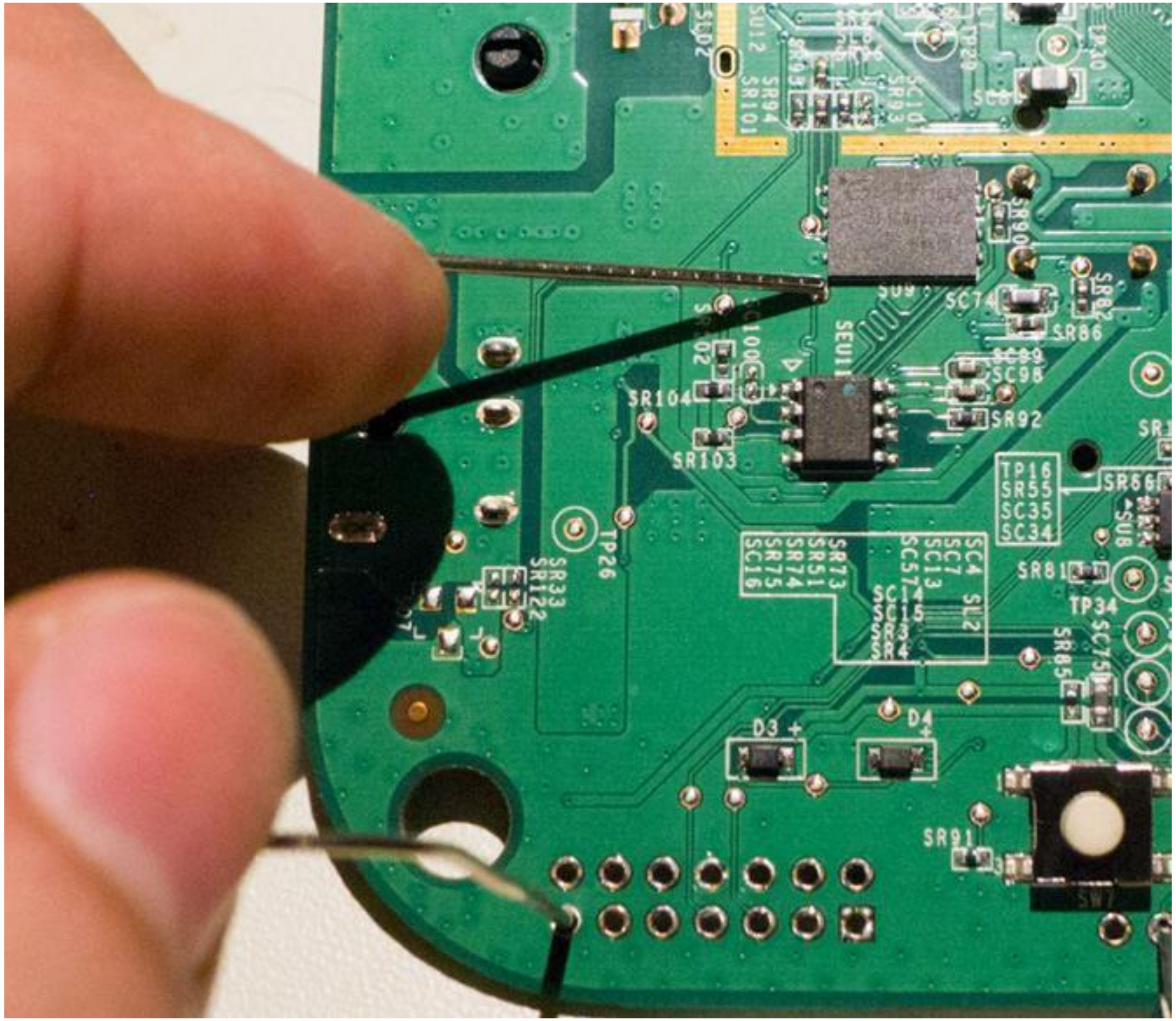


New CPA attack on CCM



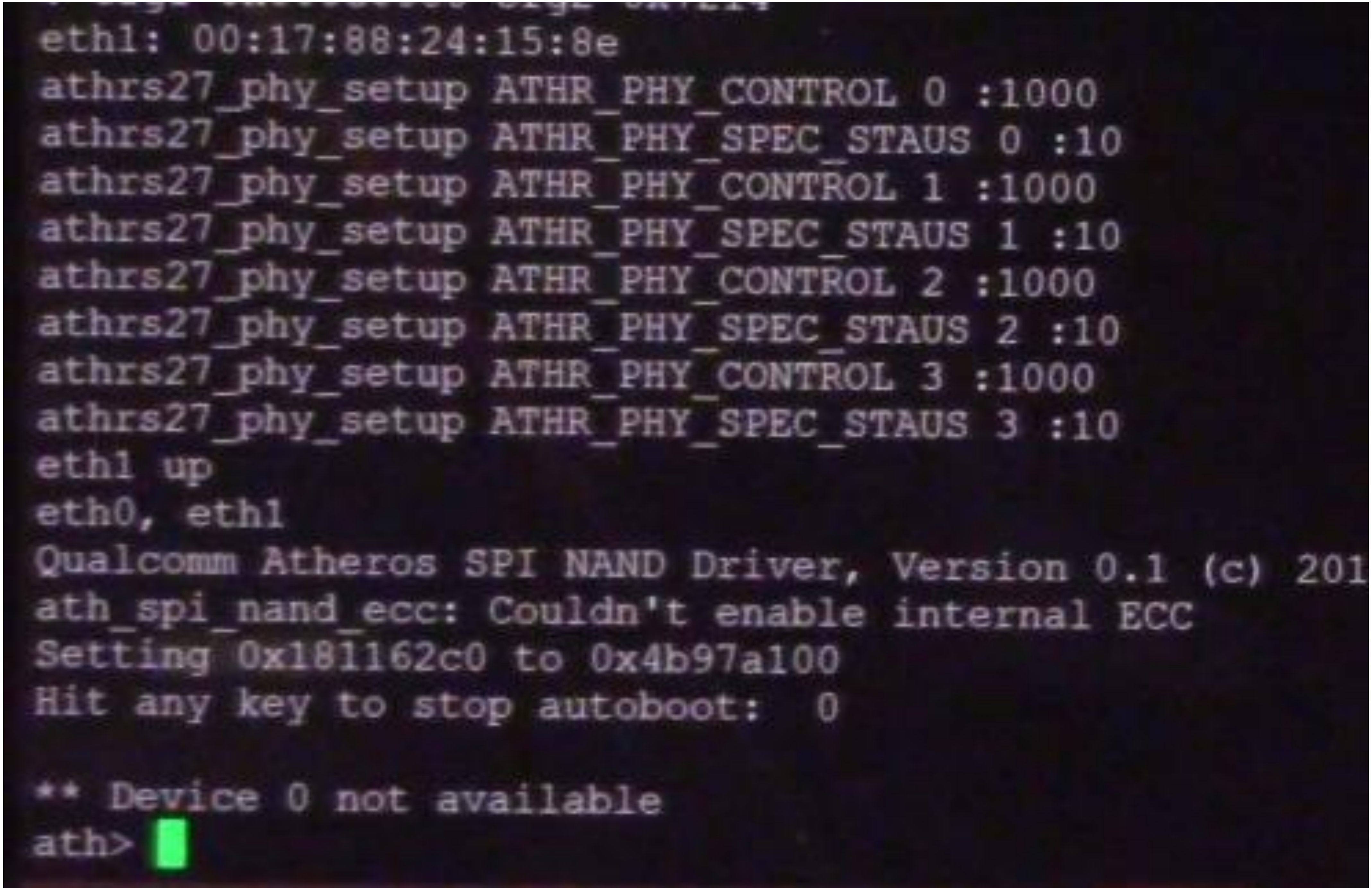

ZigBee SoC
Boot Flash
USB-Serial
SPI NAND Flash
DDR
Qualcomm QCA4531
HUE BRIDGE 2.0_X03A
323K370123T7

HACKING TOOLS

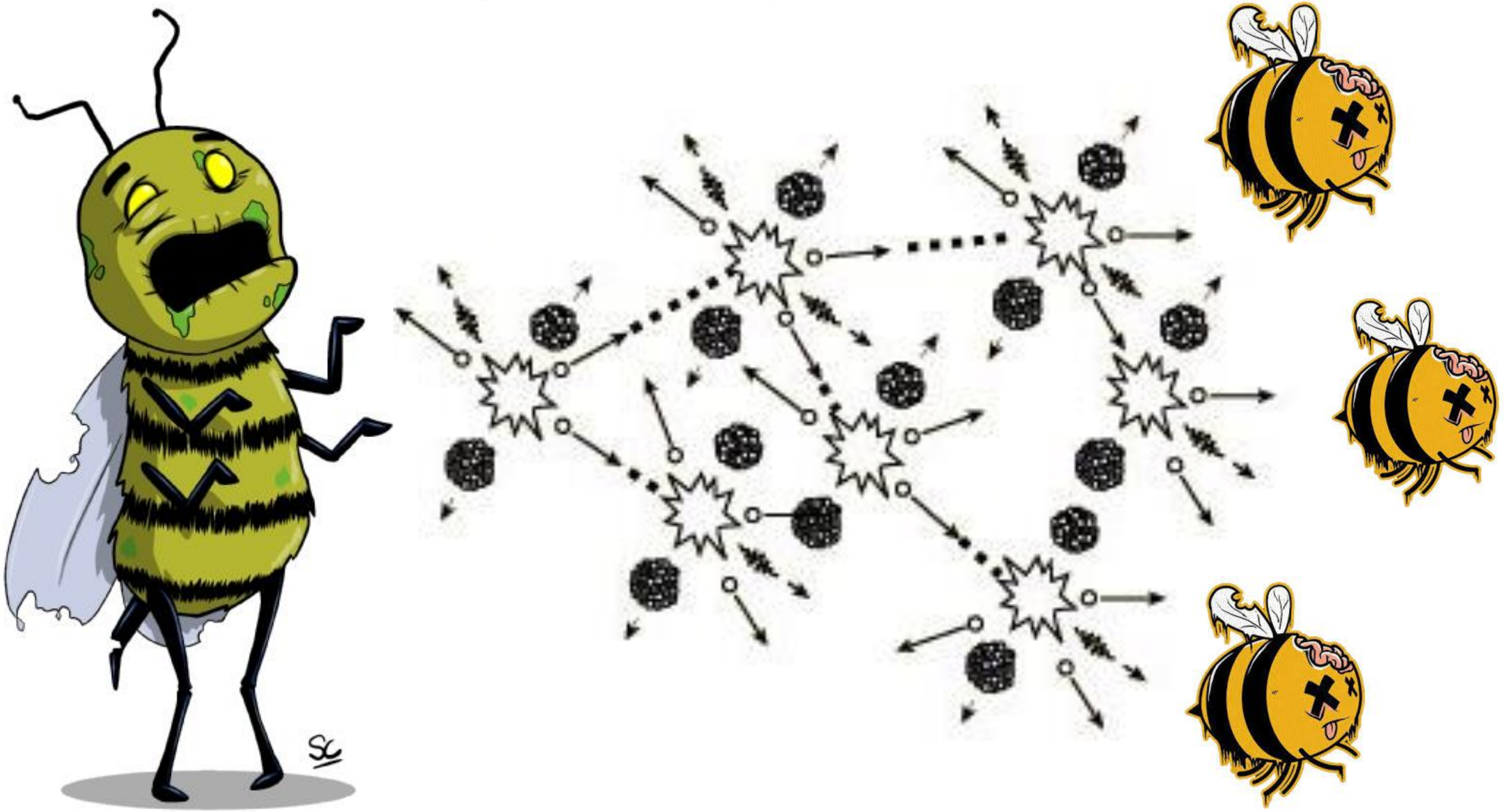


https://www.youtube.com/watch?v=hi2D2MnwiGM

Or: http://www.oflynn.com


eth1: 00:17:88:24:15:8e
athrs27_phy_setup ATHR_PHY_CONTROL 0 :1000
athrs27_phy_setup ATHR_PHY_SPEC_STAUS 0 :10
athrs27_phy_setup ATHR_PHY_CONTROL 1 :1000
athrs27_phy_setup ATHR_PHY_SPEC_STAUS 1 :10
athrs27_phy_setup ATHR_PHY_CONTROL 2 :1000
athrs27_phy_setup ATHR_PHY_SPEC_STAUS 2 :10
athrs27_phy_setup ATHR_PHY_CONTROL 3 :1000
athrs27_phy_setup ATHR_PHY_SPEC_STAUS 3 :10
eth1 up
eth0, eth1
Qualcomm Atheros SPI NAND Driver, Version 0.1 (c) 201
ath_spi_nand_ecc: Couldn't enable internal ECC
Setting 0x181162c0 to 0x4b97a100
Hit any key to stop autoboot: 0
** Device 0 not available
ath>

Creating An Explosive Infection:



A New Type of Attack:

A New Type of Attack:

- A hacker can infect all the smart lights in the whole city, provided that the density of smart lights is above a certain critical mass, which can be calculated with percolation theory techniques

A New Type of Attack:

- A hacker can infect all the smart lights in the whole city, provided that the density of smart lights is above a certain critical mass, which can be calculated with percolation theory techniques

- For a city such as Paris whose area is 105 square km, the critical mass is about 15,000 randomly located smart lights, which is surprisingly low

A New Type of Attack:

- The attacker can start the attack by just plugging in a single infected lightbulb anywhere in the city

A New Type of Attack:

- The attacker can start the attack by just plugging in a single infected lightbulb anywhere in the city
- The attack proceeds entirely via the ZigBee radio frequencies and protocols, which are not currently monitored, so its hard to locate the infection source

A New Type of Attack:

- The attacker can start the attack by just plugging in a single infected lightbulb anywhere in the city
- The attack proceeds entirely via the ZigBee radio frequencies and protocols, which are not currently monitored, so its hard to locate the infection source
- It does not use any TCP/IP packets, and thus cannot be stopped by standard internet security tools

What the Attacker Can Actually Achieve:

What the Attacker Can Actually Achieve:

- Widespread Blackout

What the Attacker Can Actually Achieve:

- Widespread Blackout
- The attacker can permanently brick all the smart lights

What the Attacker Can Actually Achieve:

- Widespread Blackout
- The attacker can permanently brick all the smart lights
- The attack can simultaneously turn all the city's smart lights on or off, possibly affecting the electricity grid

What the Attacker Can Actually Achieve:

- Widespread Blackout
- The attacker can permanently brick all the smart lights
- The attack can simultaneously turn all the city's smart lights on or off, possibly affecting the electricity grid
- Cause epileptic seizures in photosensitive people

What the Attacker Can Actually Achieve:

- Widespread Blackout
- The attacker can permanently brick all the smart lights
- The attack can simultaneously turn all the city's smart lights on or off, possibly affecting the electricity grid
- Cause epileptic seizures in photosensitive people
- The attacker can disrupt WiFi communication since WiFi and ZigBee share the same frequencies

Responsible disclousre

Responsible disclousre

- We contacted Philips and disclosed the vulnerabilities prior to publication

Responsible disclousre

- We contacted Philips and disclosed the vulnerabilities prior to publication
  - The protocol implantation bug was fixed and an update was rolled out

Responsible disclousre

- We contacted Philips and disclosed the vulnerabilities prior to publication
  - The protocol implantation bug was fixed and an update was rolled out
  - The software update process remains vulnerable

What went wrong?

What went wrong?

- Without really thinking about it, we are going to populate our homes, offices and neighborhoods with billions of tiny transmitters/receivers

What went wrong?

- Without really thinking about it, we are going to populate our homes, offices and neighborhoods with billions of tiny transmitters/receivers

- These new IoT devices have ad-hoc networking capabilities built in, which has the potential to create a new communication medium, in addition to the traditional mediums of telephony and the internet

More information and videos

Paper site - iotworm.eyalro.net

Eyal Ronen - eyalro.net
Colin O'Flynn - colinoflynn.com

Hiroshi Fujiwara
Cyber Security
Research Center

EUROCRYPT2018

SAVE THE DATE | **APRIL 29 - MAY 3, 2018** | TEL-AVIV, ISRAEL

Eurocrypt 2018 is the leading European conference on all aspects of cryptography including Theoretical foundations, Deployment of cryptographic schemes, Cryptanalysis of widely used standards, Cryptographic protocols (such as voting), Quantum Cryptography, and Cryptographic currencies (such as bitcoin).

Organized as one of the three flagship conferences of the International Association for Cryptologic Research (IACR), this is the 37th edition of the conference. For the first time in Israel, leading professionals coming from academia, insdustry, and government agencies, from all over the world, will meet together to discuss the cutting edge of cryptographic research.

Program Chairs: Jesper Buus Nielsen (Aarhus Universitet, Denmark)
Vincent Rijmen (University of Leuven, Belgium)

General Chair: Orr Dunkelman (University of Haifa)

Local Organizers: Technion Hiroshi Fujiwara Cyber Security Research Center, headed by Eli Biham

Eurocrypt 2018

Warning! View in Real Life May be Better!