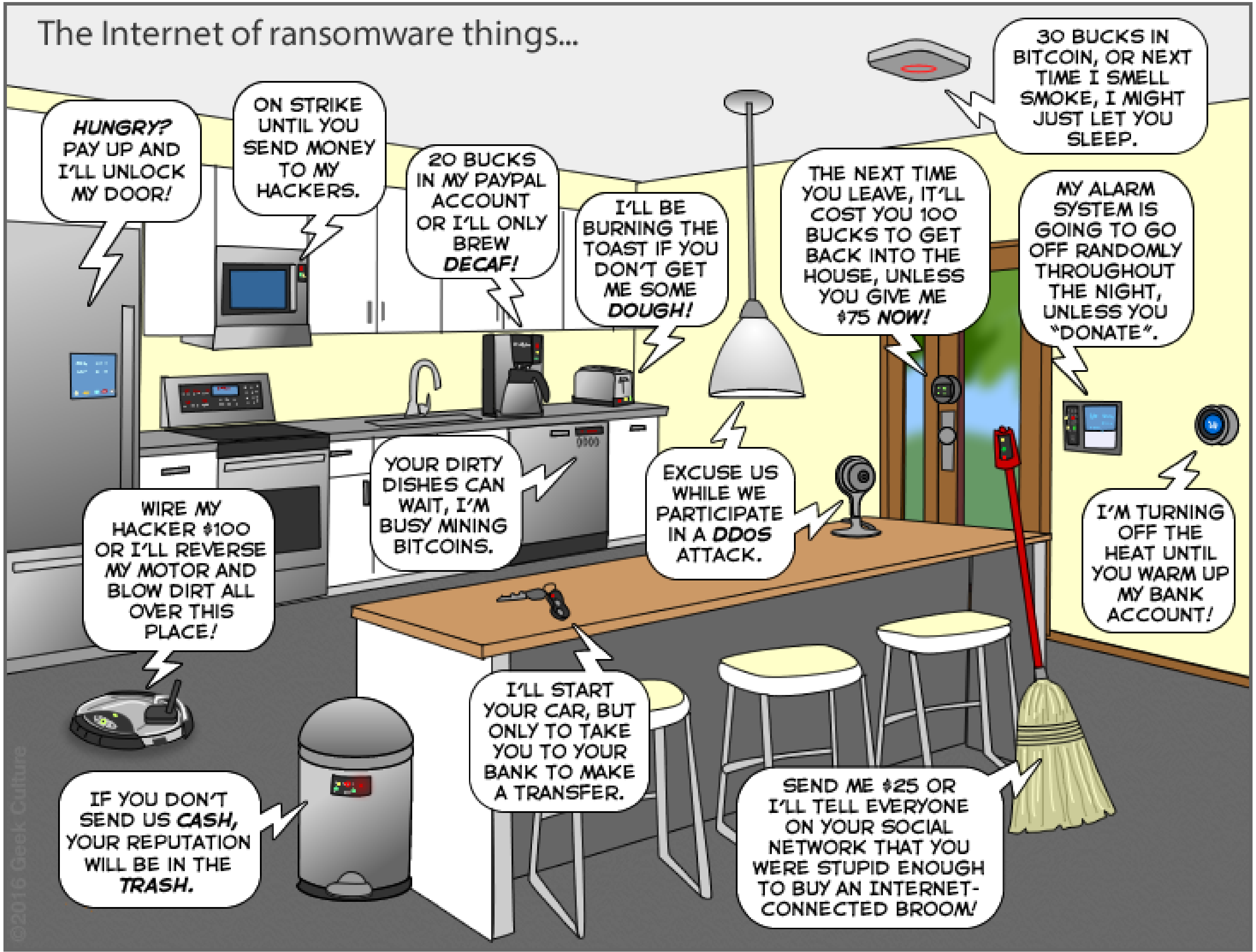
IoT Goes Nuclear: Creating a ZigBee Chain Reaction

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


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture

Typical IoT devices: Philips Hue Smart Lights

Typical IoT devices: Philips Hue Smart Lights

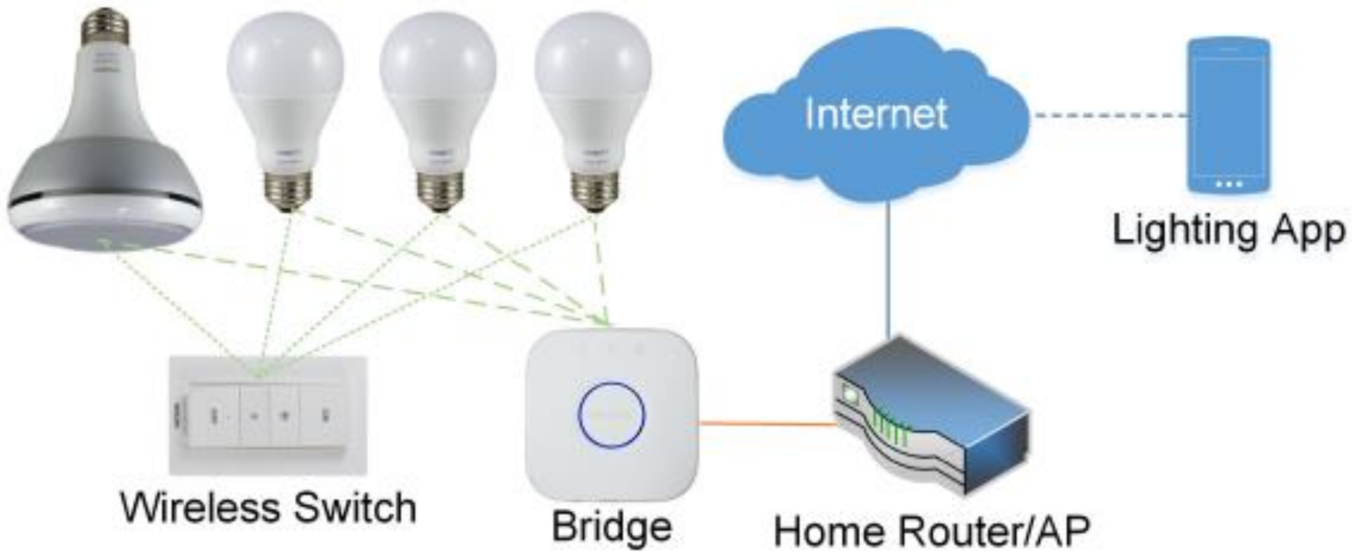
- Mature technology and standards, a relatively simple system

Typical IoT devices: Philips Hue Smart Lights

- Mature technology and standards, a relatively simple system

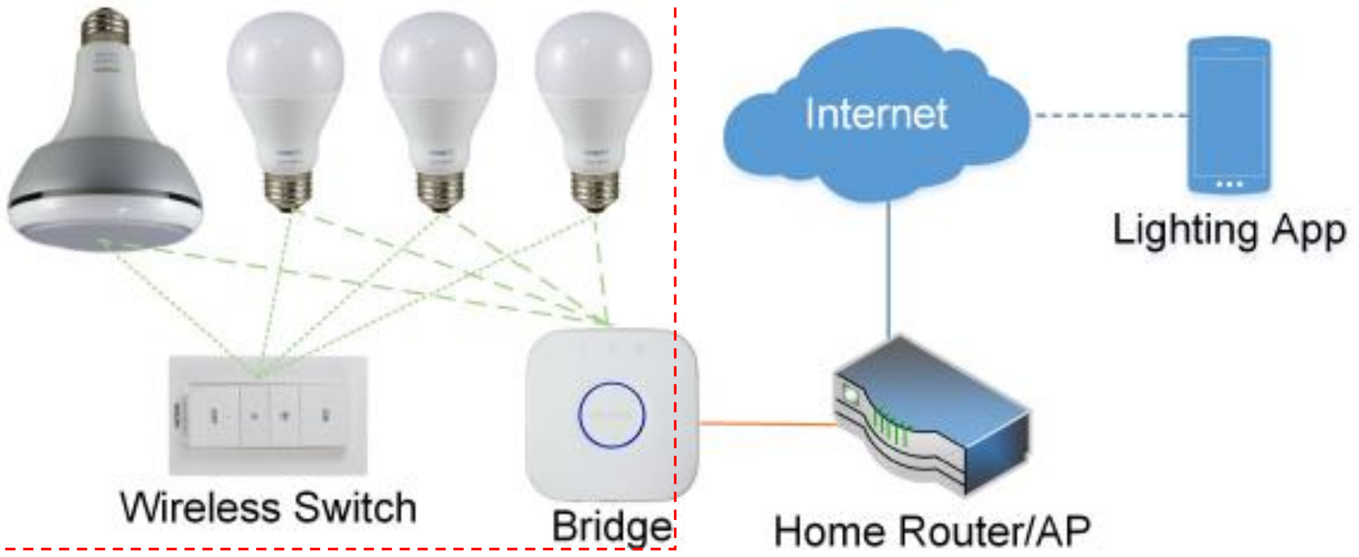
- A high end product with high end security, but…

The underlying ZLL protocol



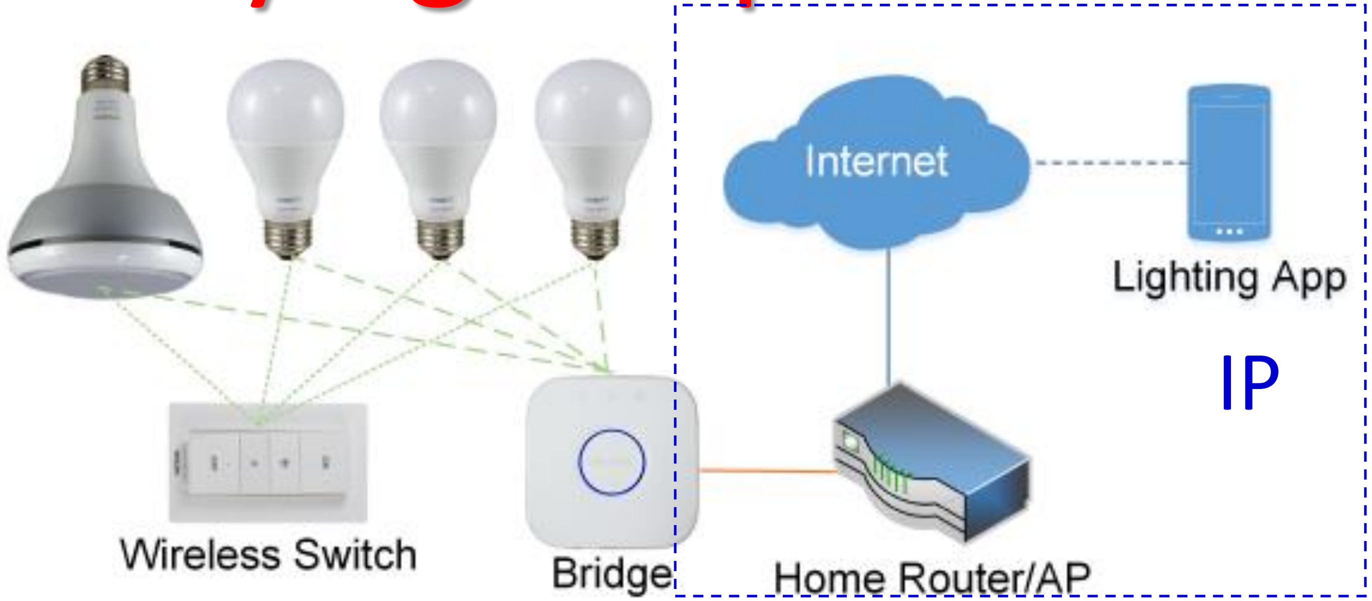
The underlying ZLL protocol

Zigbee
Personal
Area
Network



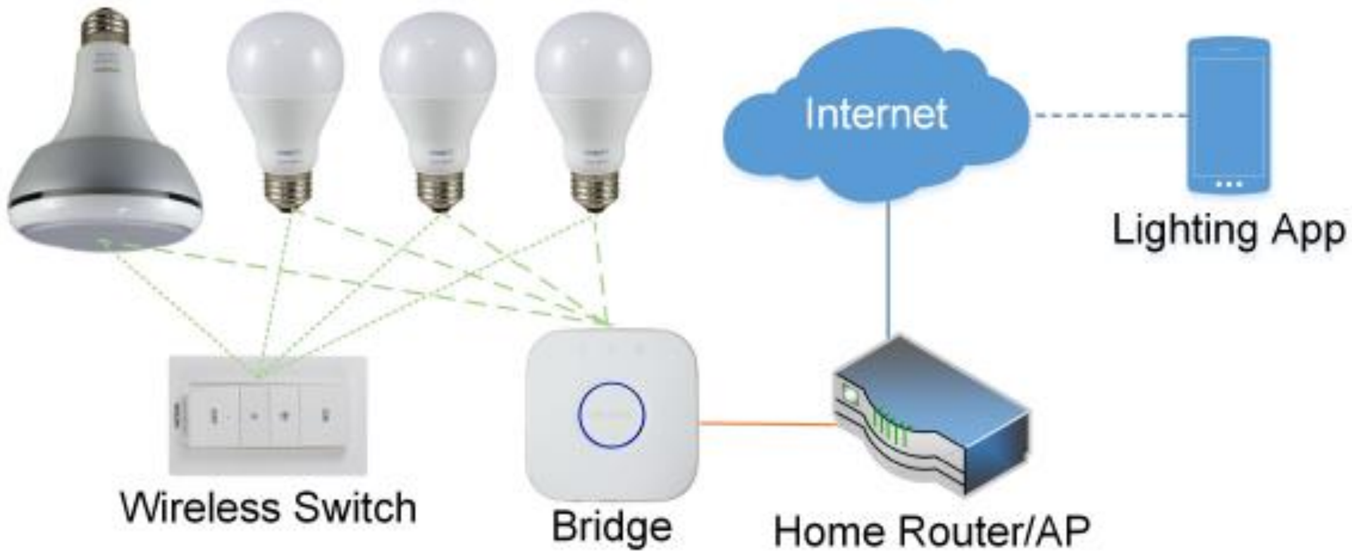
- Each installed light is connected to a central controller using the ZigBee Light Link (ZLL) wireless protocol in a Personal Area Network (PAN)

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

Creating a lightbulb worm

- A question: Can hackers create a worm which spreads using only the standard ZigBee wireless interface?

Creating a lightbulb worm

- A question: Can hackers create a worm which spreads using only the standard ZigBee wireless interface?
- Two main obstacles:

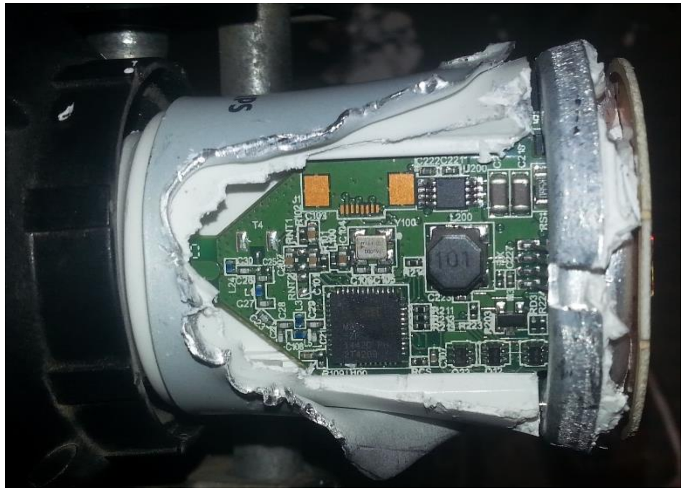
Creating a lightbulb worm

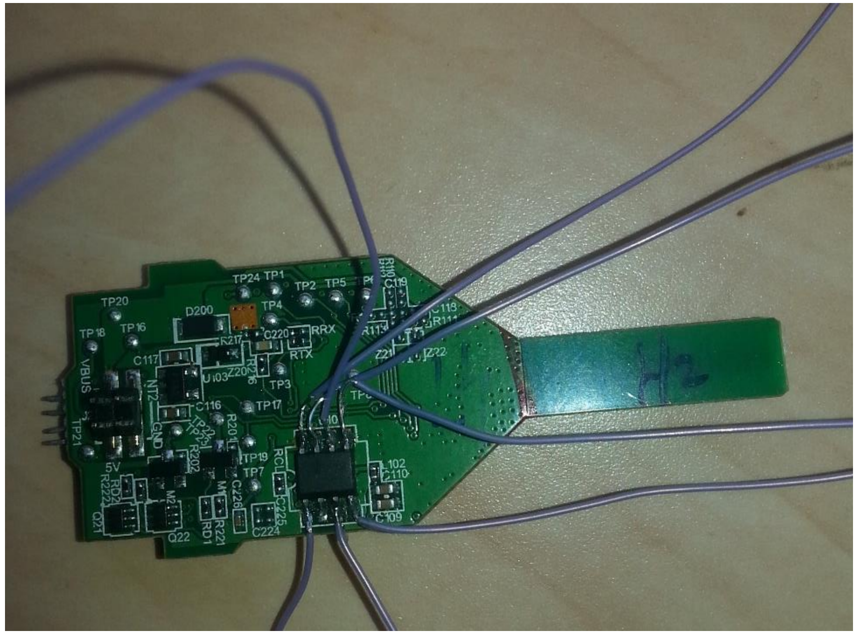
- A question: Can hackers create a worm which spreads using only the standard ZigBee wireless interface?
- Two main obstacles:
  - Taking over a preinstalled smart light

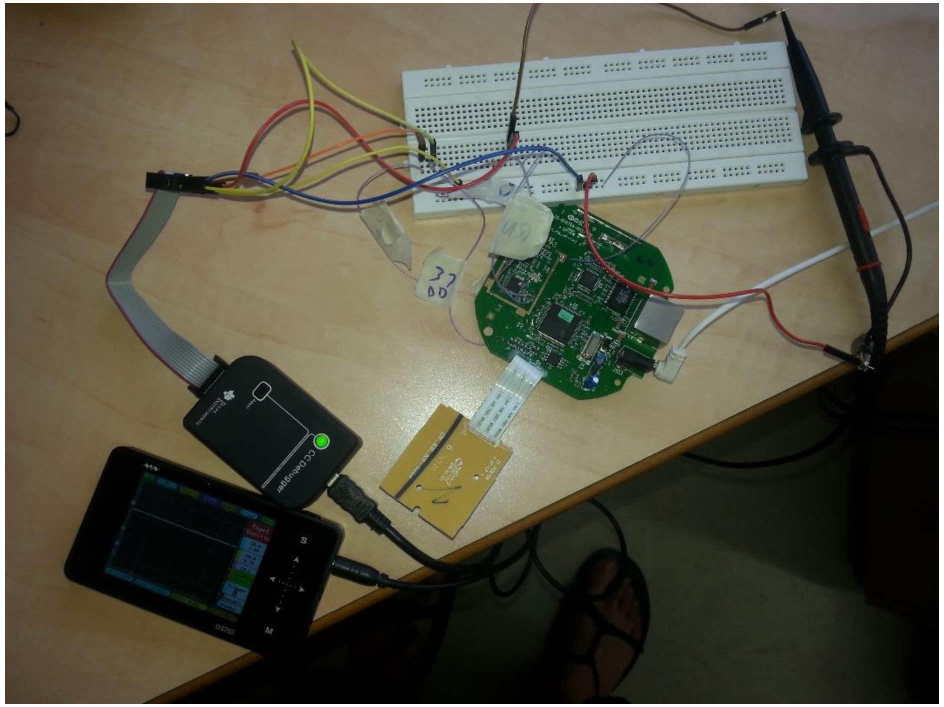
Creating a lightbulb worm

- A question: Can hackers create a worm which spreads using only the standard ZigBee wireless interface?
- Two main obstacles:
  - Taking over a preinstalled smart light
  - Spreading everywhere – finding a method for one smart light to infect nearby smart lights

3
vous propose.


101


TP24
TP1
TP2
TP5
TP20
D200
TP4
TP18
TP16
C220
RRX
RTX
C117
U103
TP3
TP17
VBUS
C116
TP21
TP19
TP7
C109
C110
H2


CCDebugger
S
M

Taking over a preinstalled smart light

Taking over a preinstalled smart light

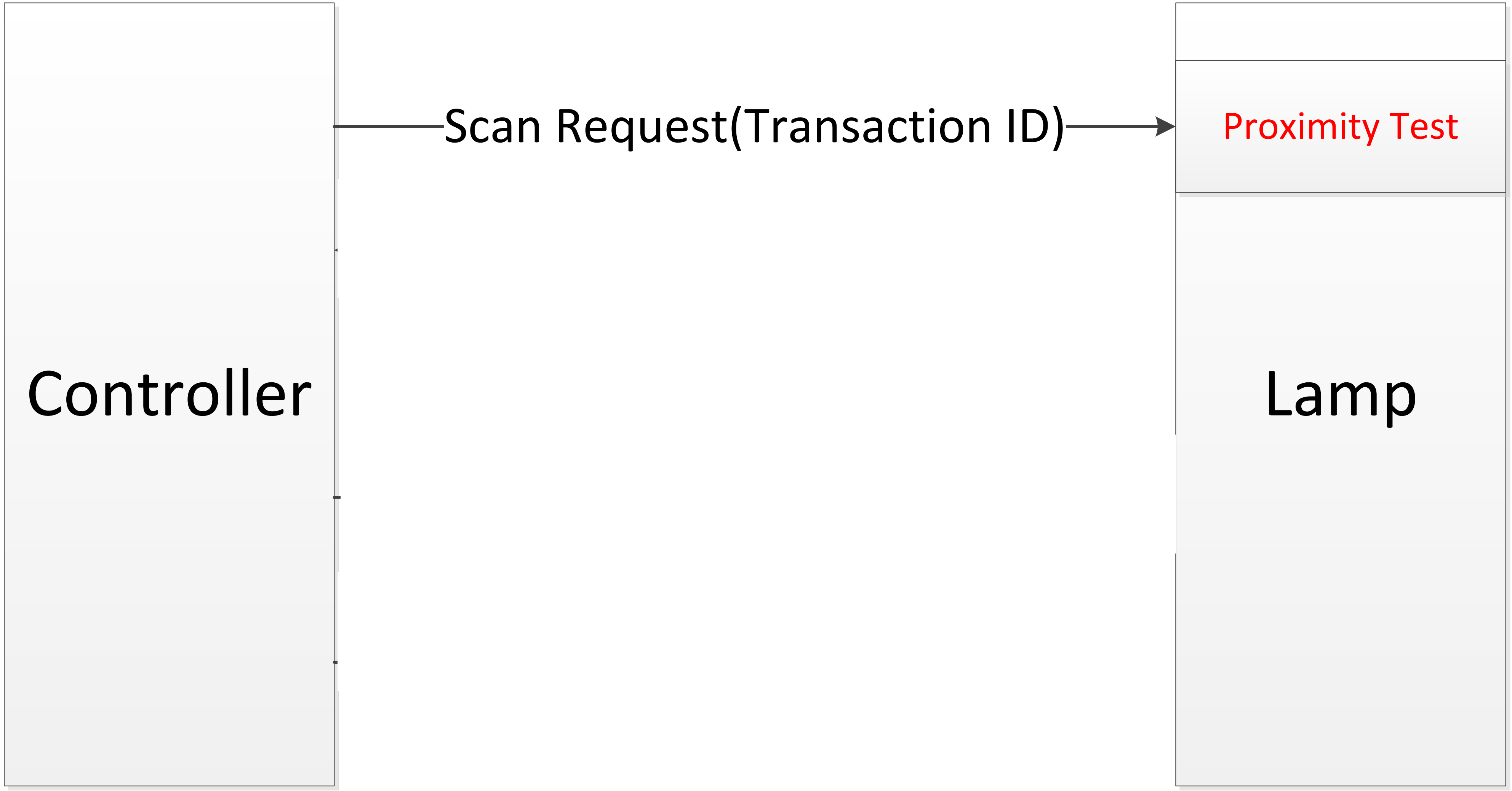
- ZigBee Light Link standard uses multiple cryptographic and security protocols to prevent misuse

Taking over a preinstalled smart light

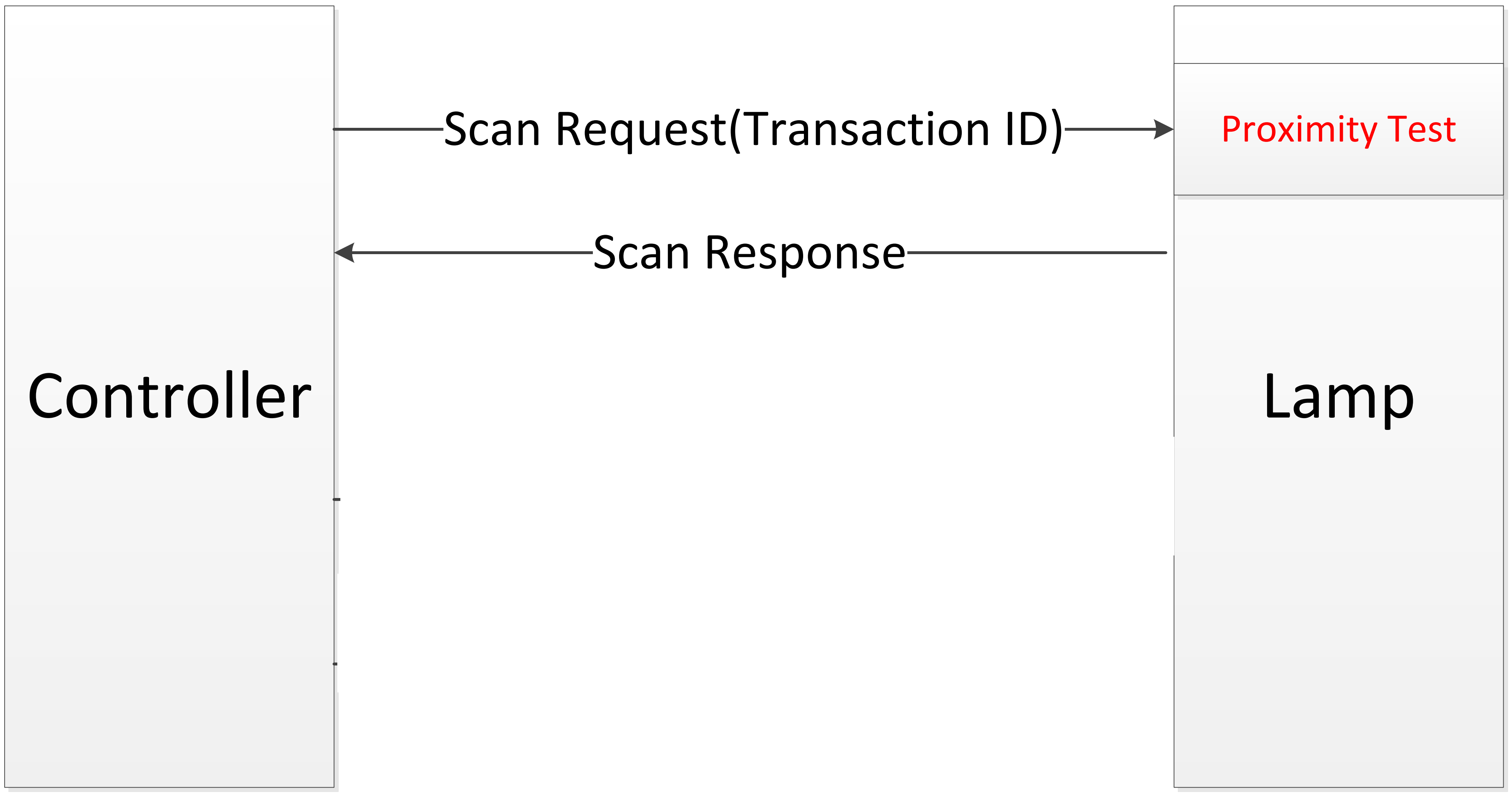
- ZigBee Light Link standard uses multiple cryptographic and security protocols to prevent misuse

- 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

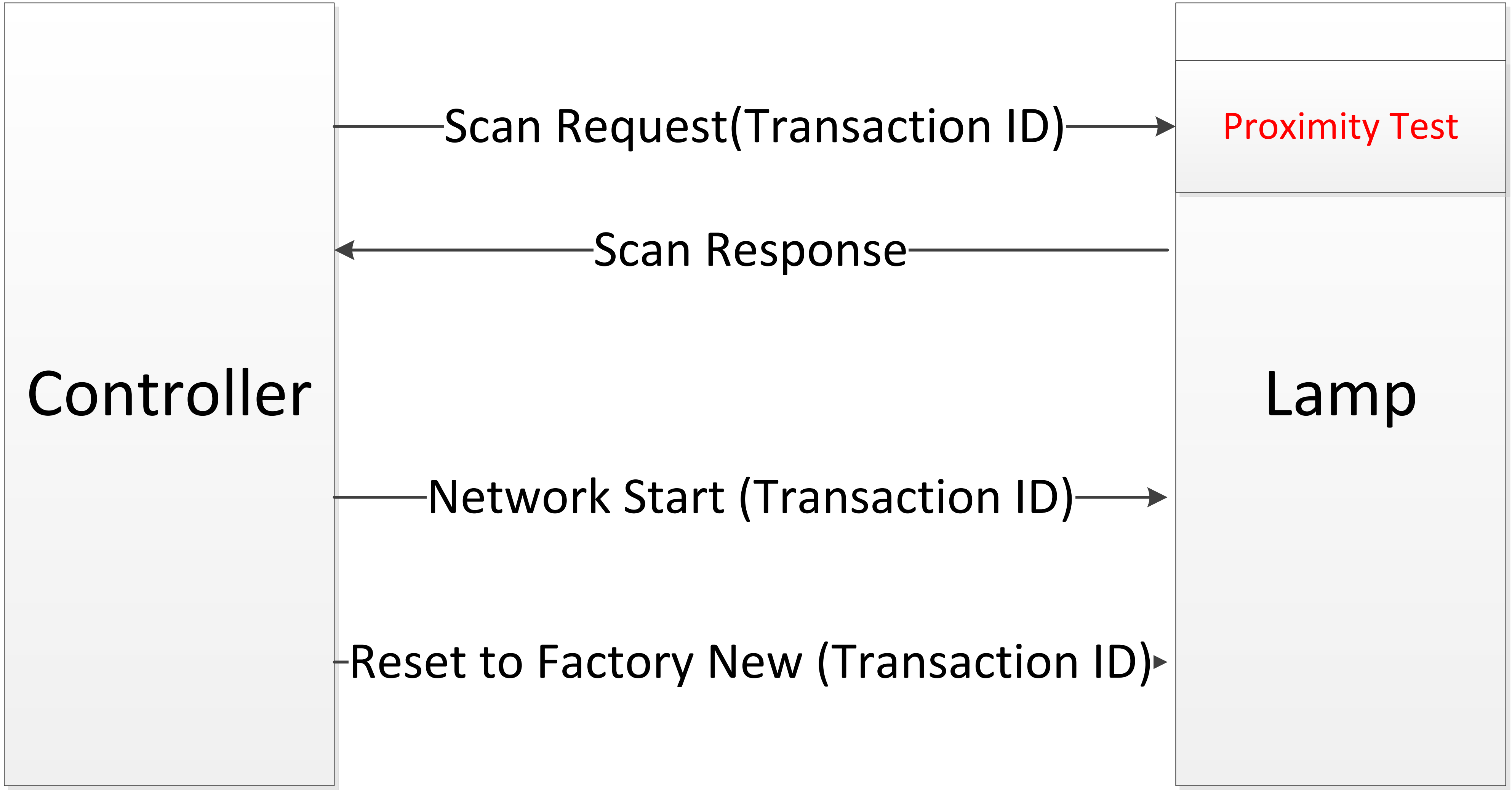
Protocol Outline



Protocol Outline



Protocol Outline



Controller
Scan Request(Transaction ID)
Proximity Test
Scan Response
Lamp
Network Start (Transaction ID)
Reset to Factory New (Transaction ID)

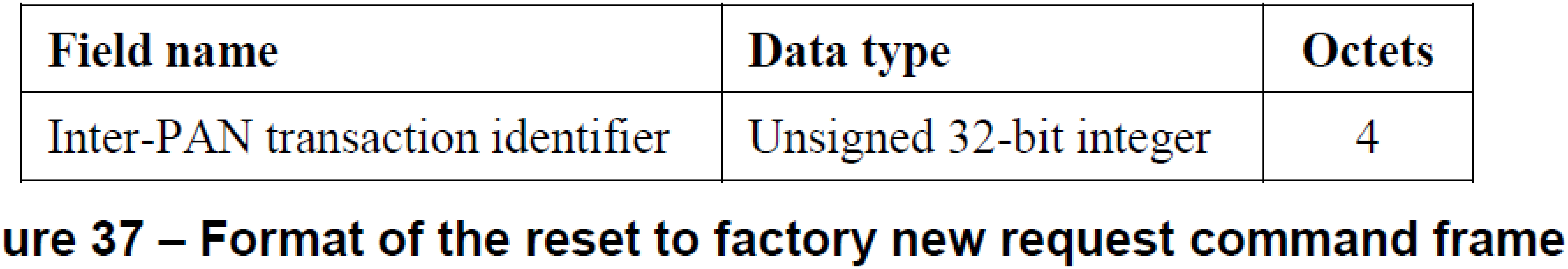
Protocol Implementation Bug

Protocol Implementation Bug

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

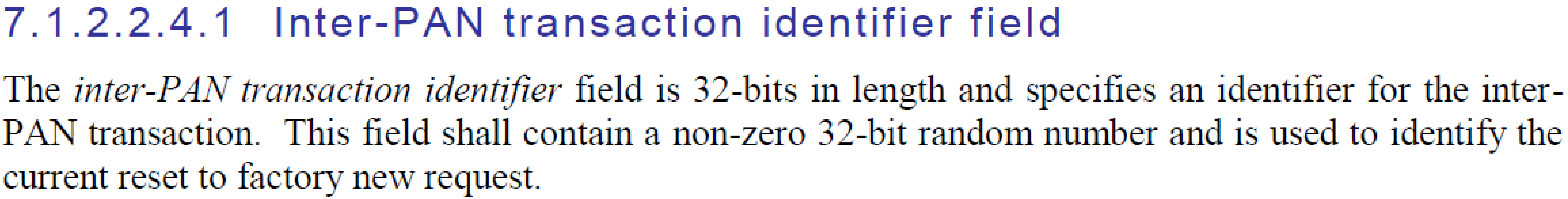
Protocol Implementation Bug

- 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

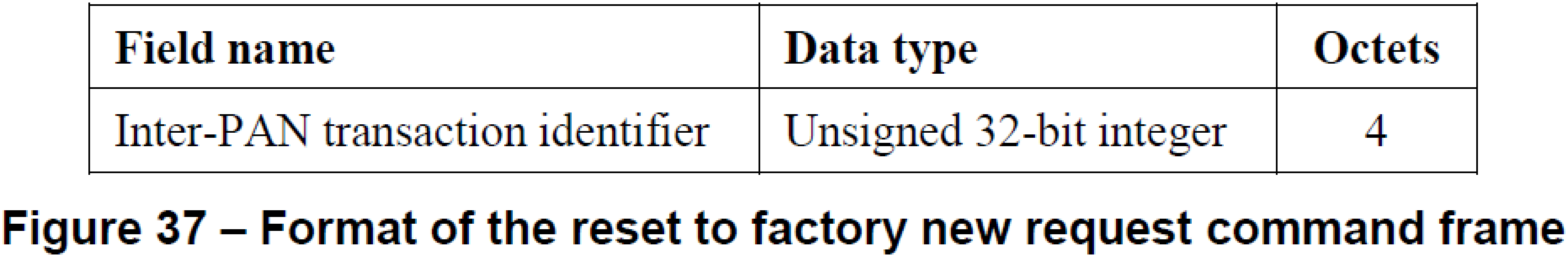


7.1.2.2.4.1 Inter-PAN transaction identifier field

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.

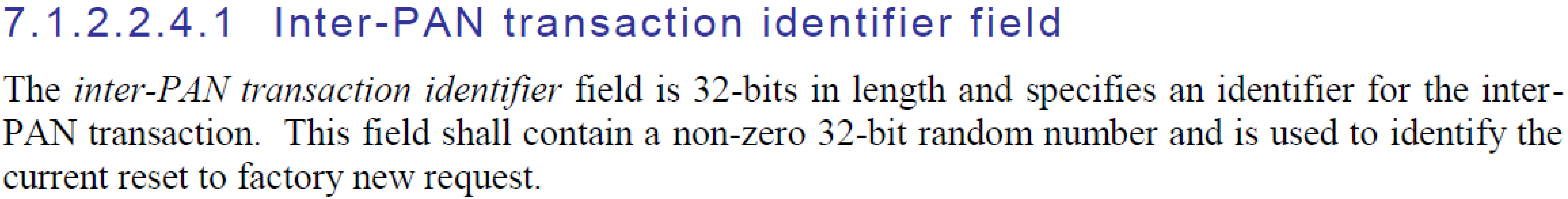
Protocol Implementation Bug

- 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



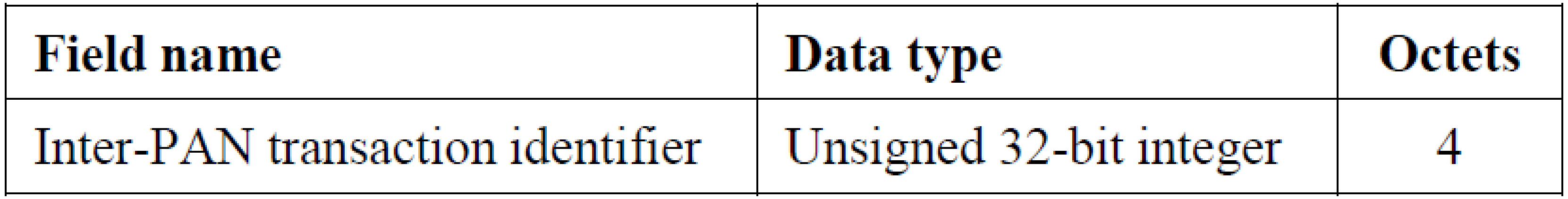
7.1.2.2.4.1 Inter-PAN transaction identifier field

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

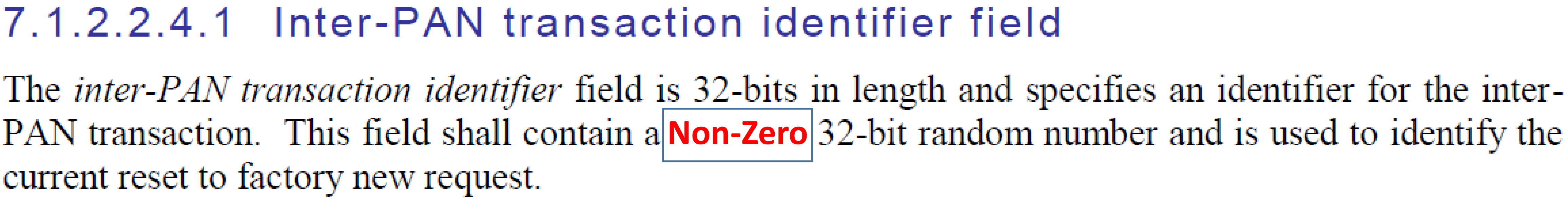
Protocol Implementation Bug

- 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

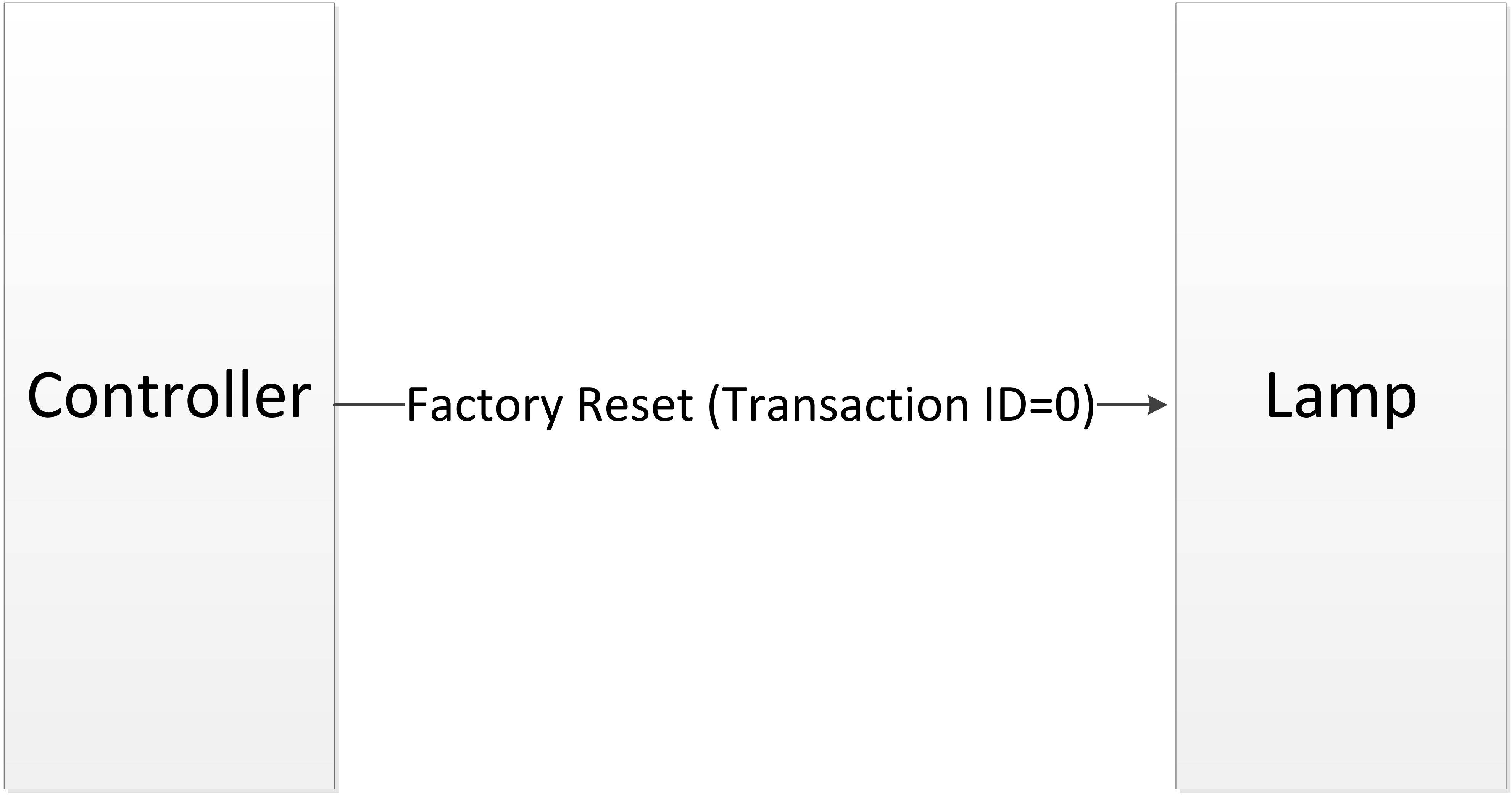


7.1.2.2.4.1 Inter-PAN transaction identifier field

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

Protocol Attack Outline



Controller

Factory Reset (Transaction ID=0)

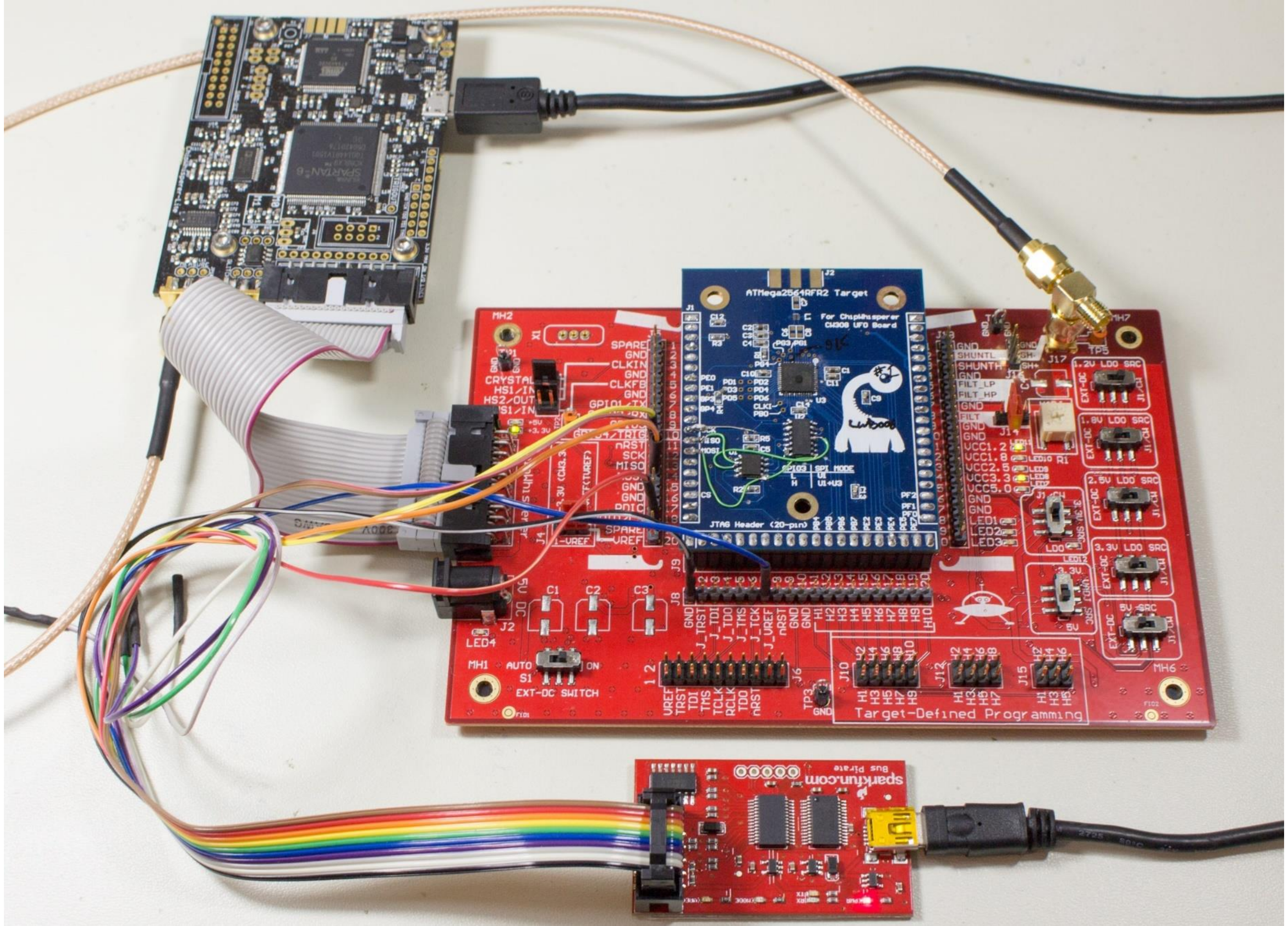
Lamp

We bought a cheap and lightweight commercial Zigbee evaluation kit:

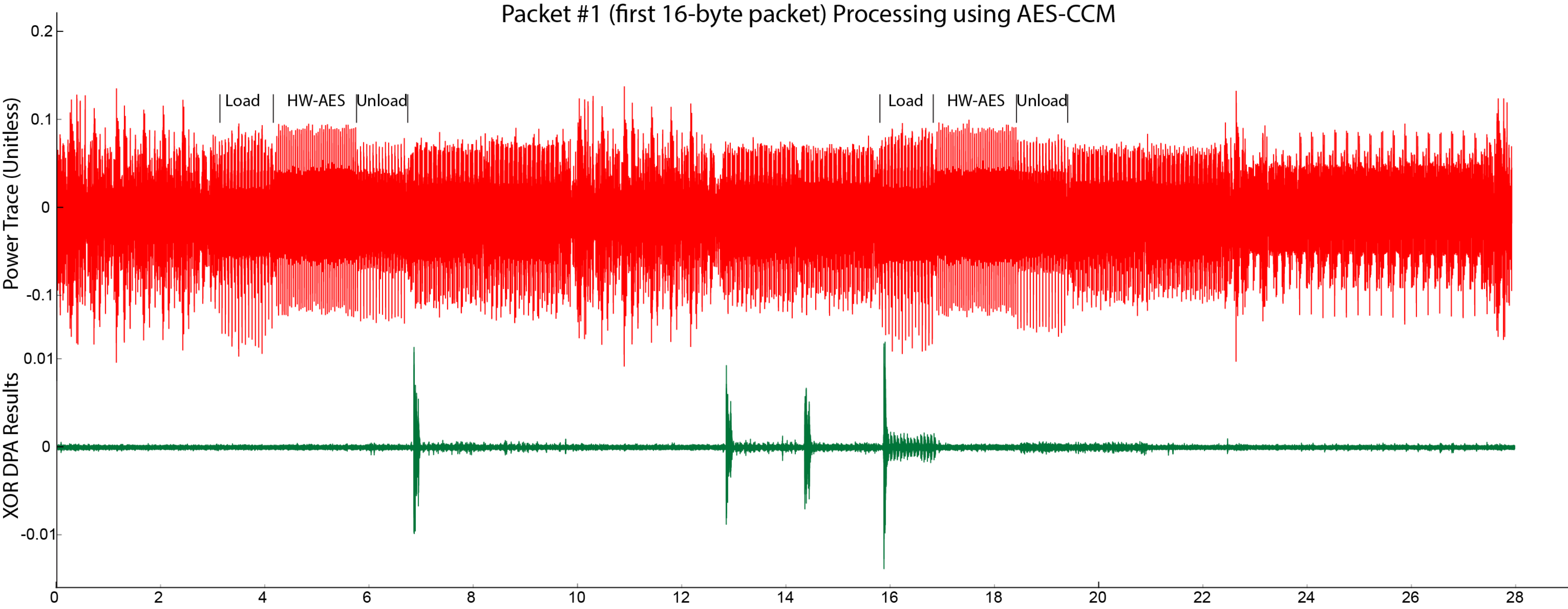
We then decided to take full control of all the smart lights in the same office building we attacked before

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

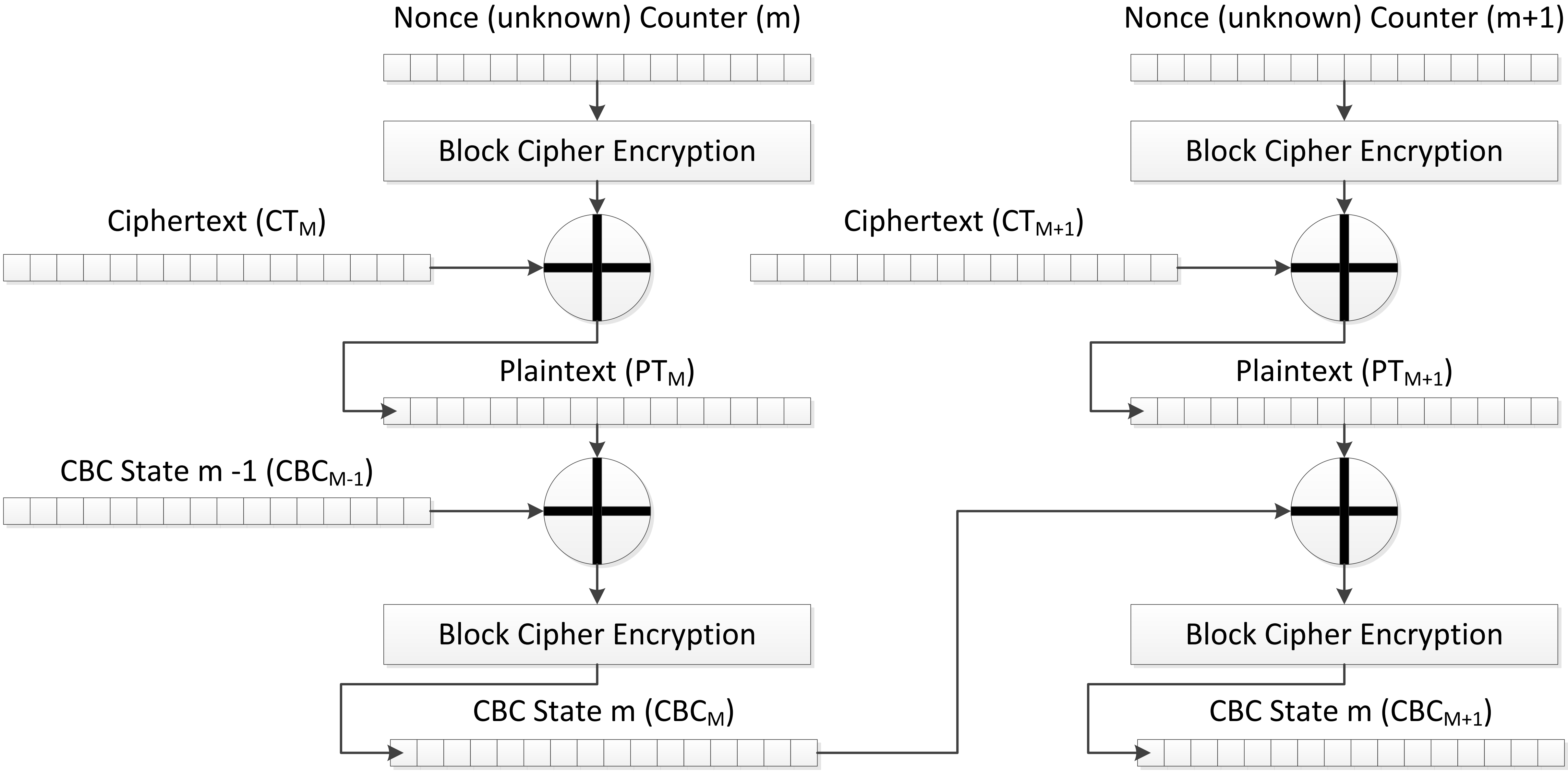
Spreading everywhere



CPA for RE


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

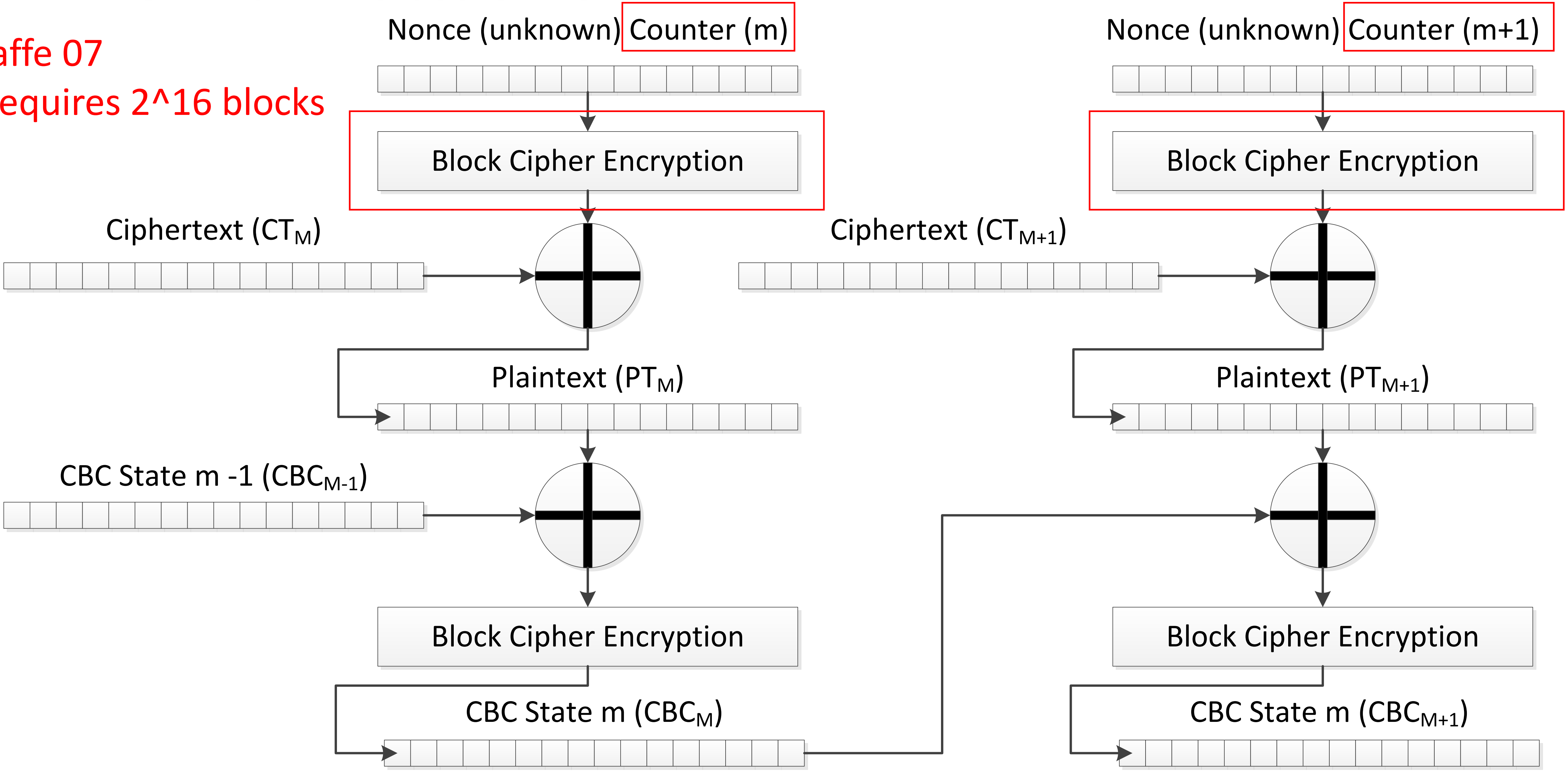
New CPA attack on CCM



New CPA attack on CCM

Jaffe 07

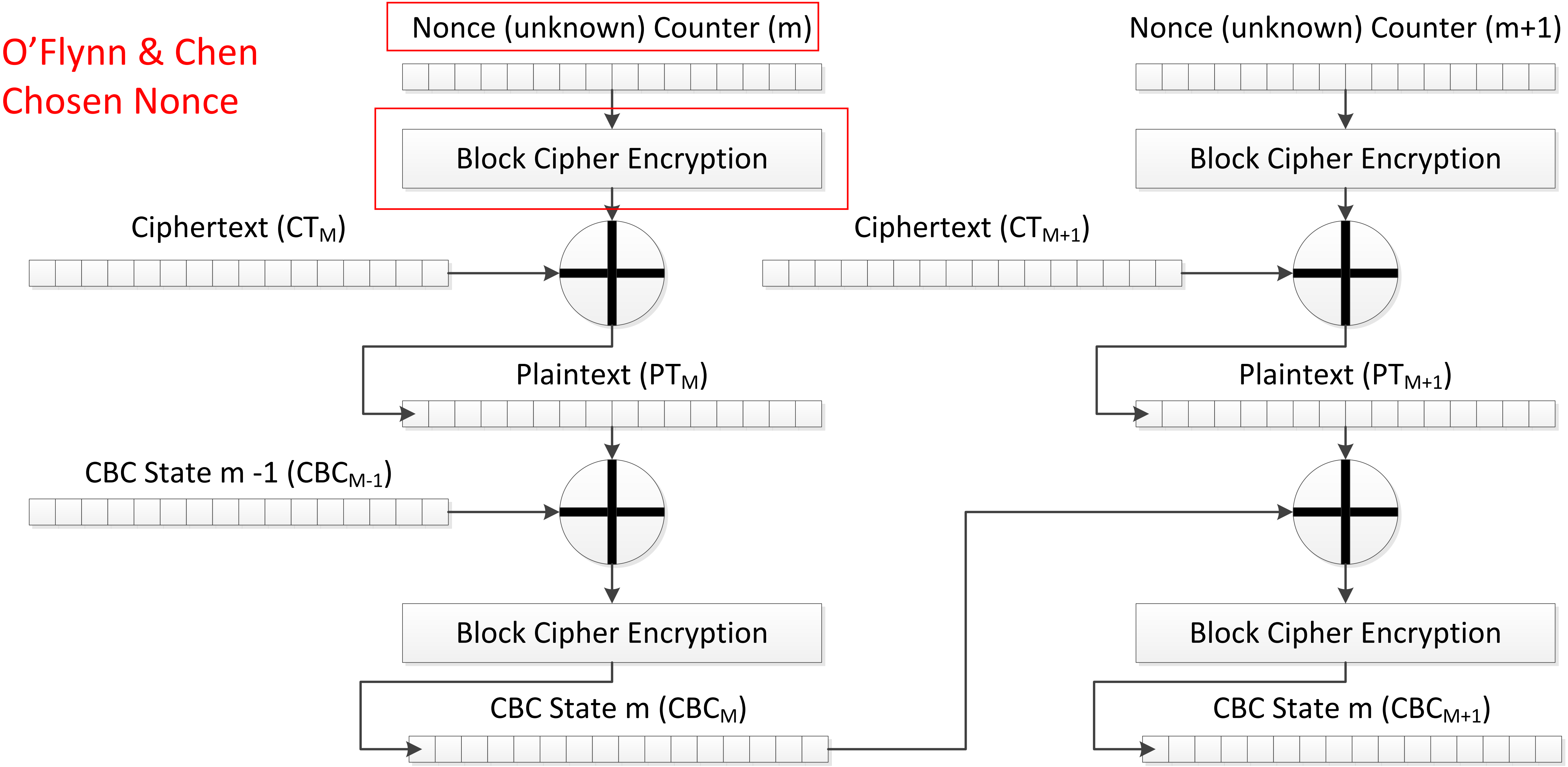
Requires 2^16 blocks



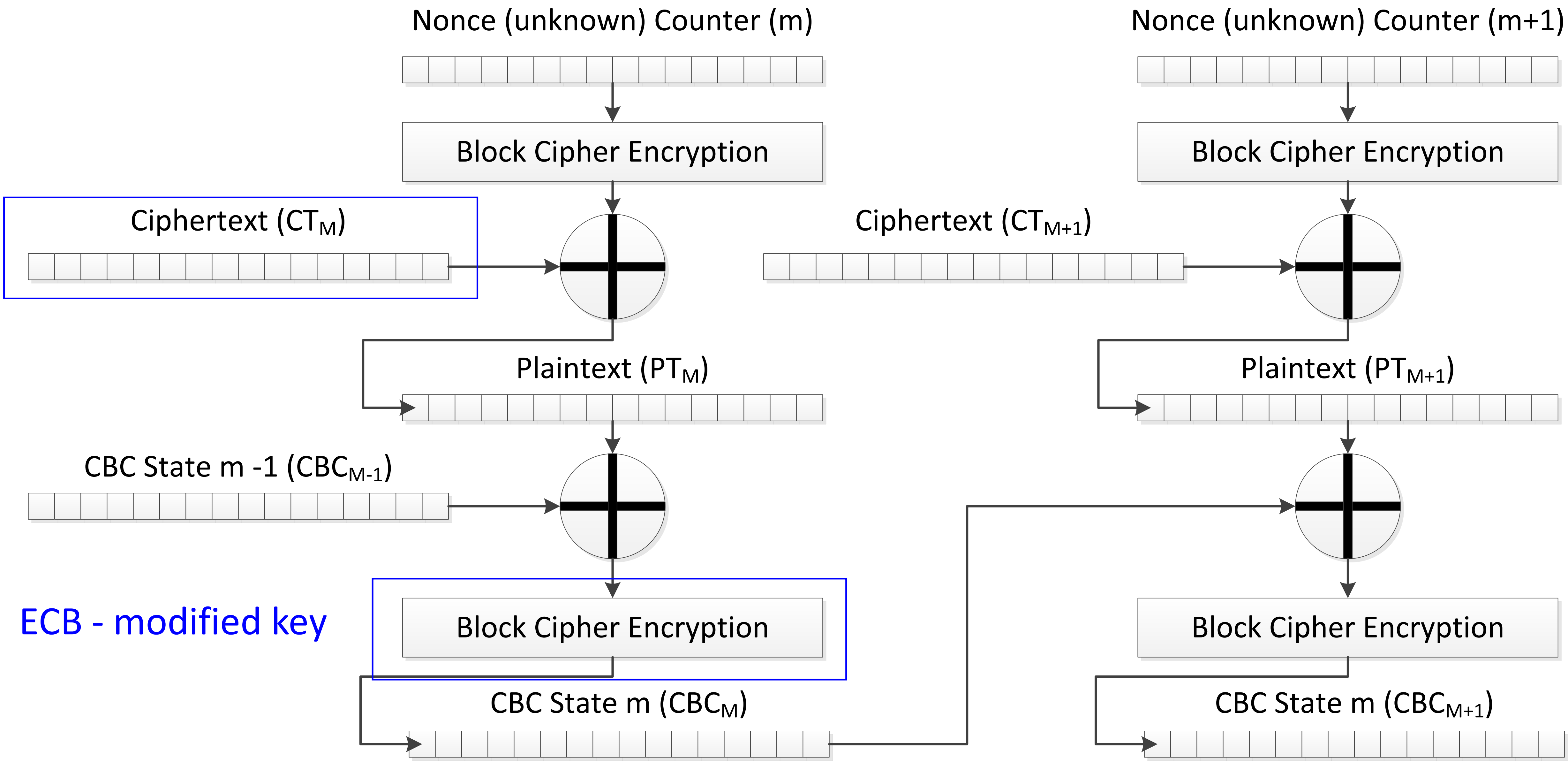
New CPA attack on CCM

O’Flynn & Chen

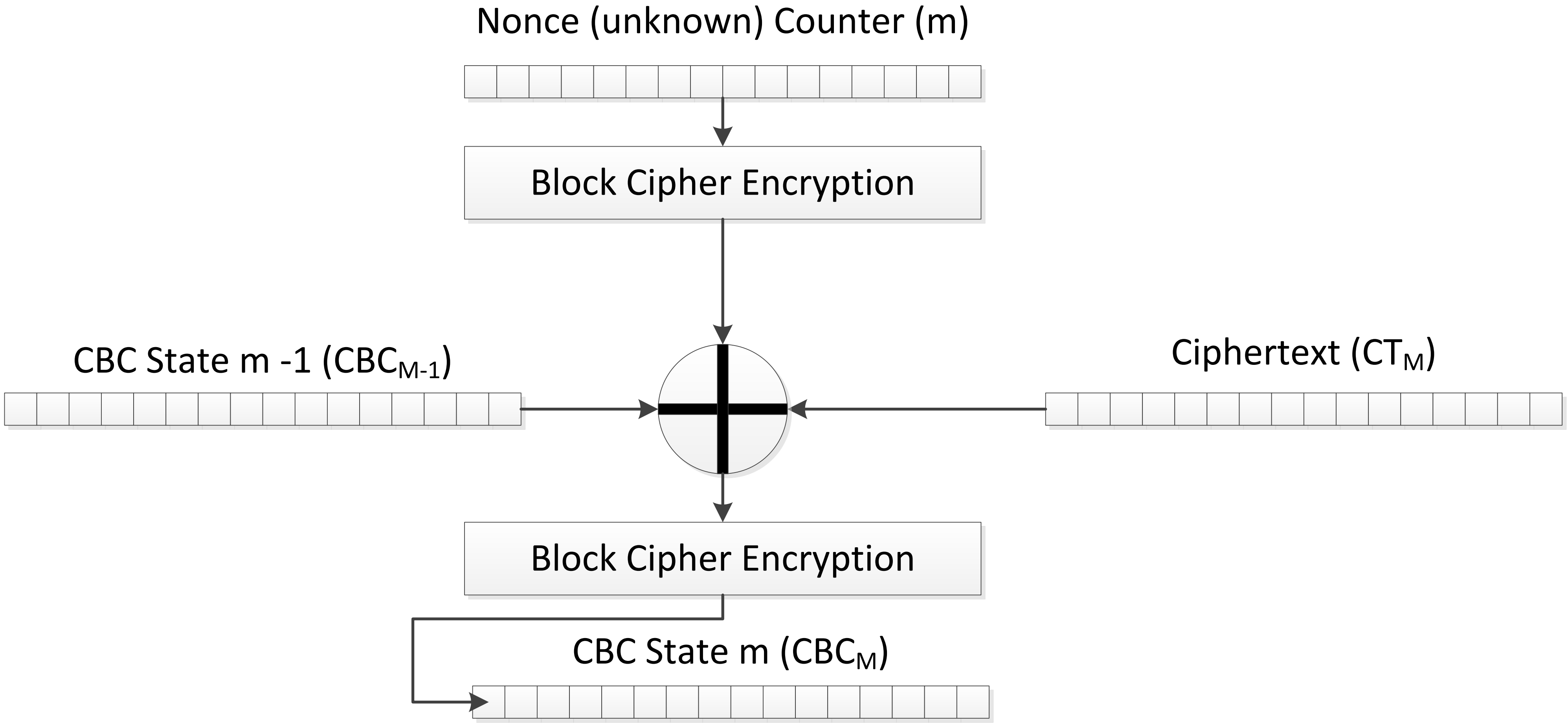
Chosen Nonce



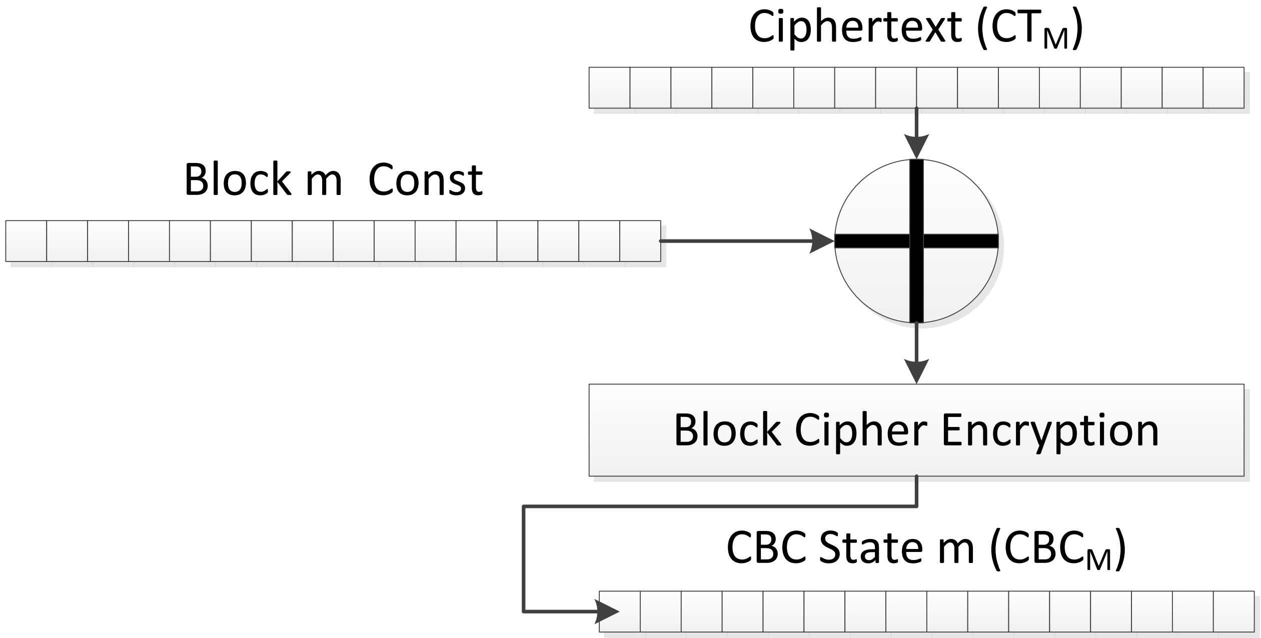
New CPA attack on CCM



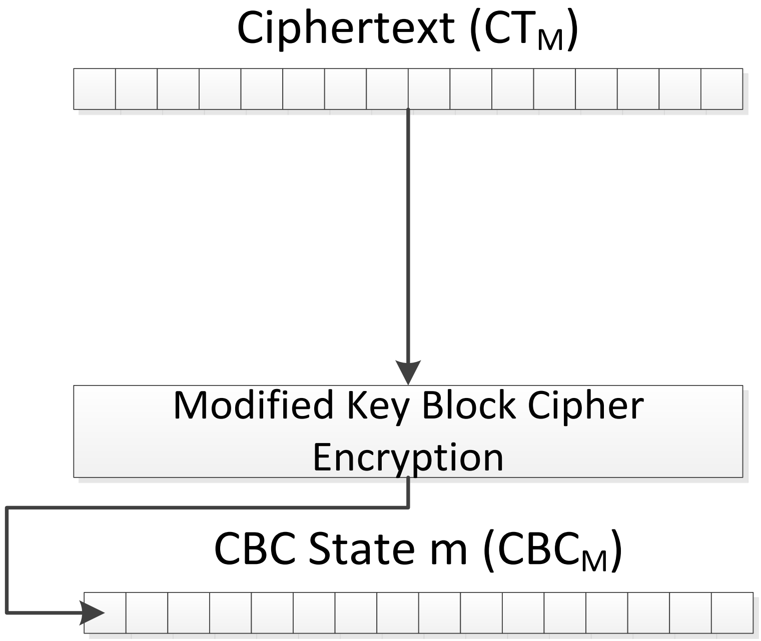
New CPA attack on CCM



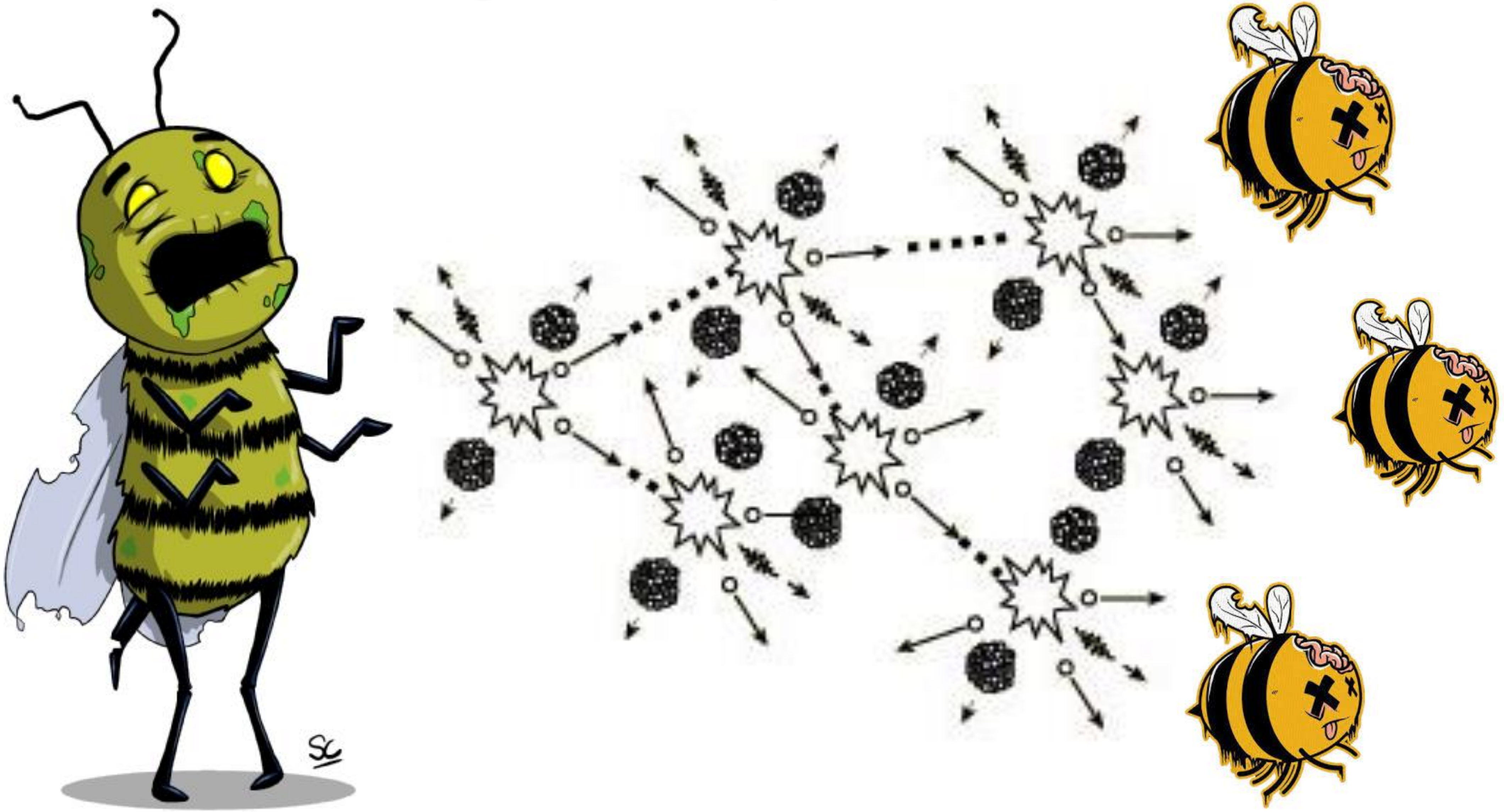
New CPA attack on CCM



New CPA attack on CCM



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