

## Продвинутые способы атаки: оптические возмущения высоких порядков

### Цели обучения в этом курсе

* Понимание того, как оптические возмущения работают у разных типов лазеров
* Be able to explain the motivation behind a dual laser attack
* Be able to define/configure a dual laser setup



## Physics of different laser types: when to use what

### Effect of Optical FI: Power and fault duration

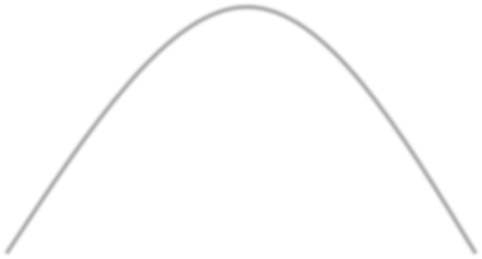
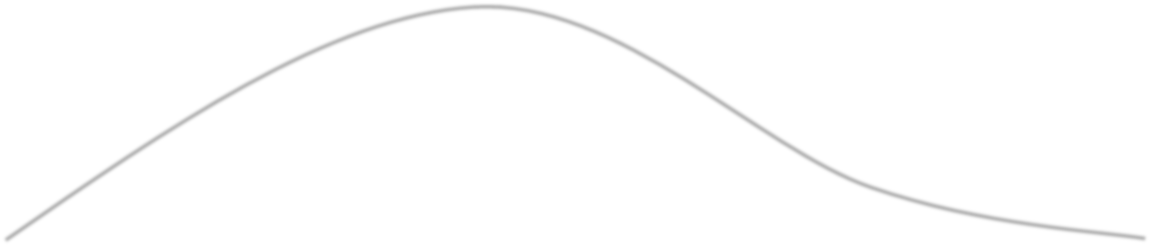
* 1. Build-up interval to reach logic toggle

▫ Generate excess of free electrons to reduce channel resistance

* + - **Duration depends on pulse intensity**
  1. Maintain interval to preserve new logic state

▫ Maintain excess of free electrons to keep channel resistance low

* + - **Duration depends on pulse duration**
  1. Recovery interval to toggle back to original state
     + **Duration depends on excess of free electron and charge**



fault

1

2

3

threshold band

public

laser pulse 4

### Хар-ки лазеров

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **Диодный лазер** | | |  | **Импульсный** | |
|  |  | |  | | |  | |
| цвет | ИК | КР | ИК | КР | ГОЛ | ИК | ЗЕЛ |
| мода | ом | | мм | | | | |
| Длина волны  [нм] | 1064 | 980 | 1064 | 808 | 445 | 1064 | 532 |
| Длительность | 2 нс - ∞ | | 20 нс - 100 мкс | | | ≤ 4 нс | |
| Скважность | 2 нс - ∞ | | 20 нс - ∞ | | | 1 мс - ∞ | |
| Задержка |  | | 50 нс | | | 1 мкс | |
| Импульс | 4.6 Вт\* | 5.2 Вт\* | 20 Вт | 14 Вт | 3 Вт | * 10 кВт | * 7.5 кВт |
| Диаметр, мкм | Ø 1\*\*\* | | 6 x 1.5\*\* | 6 x 1.5\*\* | 4 x 1.4\*\* | Ø 2\*\* | |
| Волокно | обязательно | | возможно | | | обязательно | |

* measured at 50 ns, lower for shorter pulses

\*\* measured with spot size reducer and 50x objective

\*\*\* measured with 100x objective 5

### Riscure laser specifications: what to remember

|  |  |  |  |
| --- | --- | --- | --- |
|  | **DIODE LASER** | | **PULSED LASER** |
|  |  |  |  |
| Mode | Single | Multi | |
| Pulse duration | Very short to  always on | Short to always on | Only very short |
| Time between  pulses | Really short | Short | Long (1ms) |
| Power | medium | High | Ultra high |
| Spot size [µm] | smallest | medium | small |

6

power



|  |  |  |
| --- | --- | --- |
| dpss | | |
|  | diode | |
|  |  |

time

DPSS power equals 1000x diode power

Short pulses influence high dynamic circuits and influence only one to a few clock cycles

7

Diode laser:

* + Laser beam exits diode directly following diode current dynamics

Diode Pumped Solid State Laser:

* + Light Emitting Diode charges optical energy in YAG crystal
  + Laser beam exits YAG after opening Q-switch in short and fixed intense pulse
  + Power regulated by LED power and attenuator

8

Imagine we have a DPSS and diode lasers of same color (λ=1064nm) and a flip-chip.

We want to inject a fault in a hardware AES128 crypto engine (f=166MHz) to perform AES DFA. Which laser would you use (and why)?

At 166MHz, a clock cycle lasts 6ns

Assuming we want to fault only round 9, we may need a very short pulse.

* + - DPSS laser pulse width is <4ns: viable option
    - Multimode laser pulse width >20ns: not viable, we will hit likely several rounds
    - Single mode laser pulse width >2ns: viable option depending on power delivery due to substrate thickness



transparenc

y silicon

public



optimal for thicker substrate

backside substrate < 75 μm

etal < 1 µm

wave length

y for faults

sufficient energ

aps in m

penetrate g

400

600

800

1000 1200 10

**445**

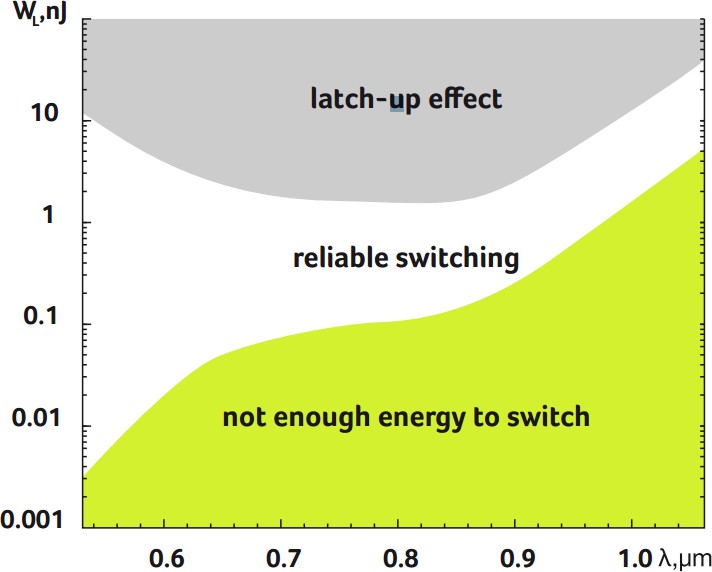
front side metal

back side silicon

**532**

**808**

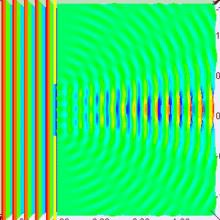
980 1064

optical power

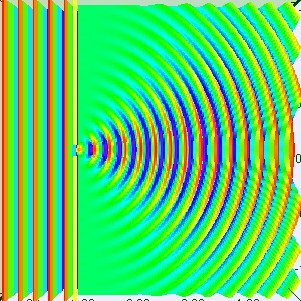
wavelength

For shorter wavelengths (808, 532 and 445 nm), reliable switching occurs at lower power level and

over wider power range 11



short wavelength compared to aperture



long wavelength compared to aperture

Light of short wavelength (445 nm) goes straight through small holes in metal shielding

12

Transmission of light through sub wavelength apertures is given by

4

𝑟

𝜆0

𝑇 ∝

|  |  |  |
| --- | --- | --- |
| T | = | transmission coefficient |
| r | = | radius of aperture |
| λ0 | = | wavelength of incident light |

Light of short wavelength λ0 (445 nm) penetrates better through small apertures in metal shield

13

We have a SoC decapped from the front (metal side), and you see a lot of metal tracks on the chip.

We want to inject a fault in memory copy operation from external flash during the boot process.

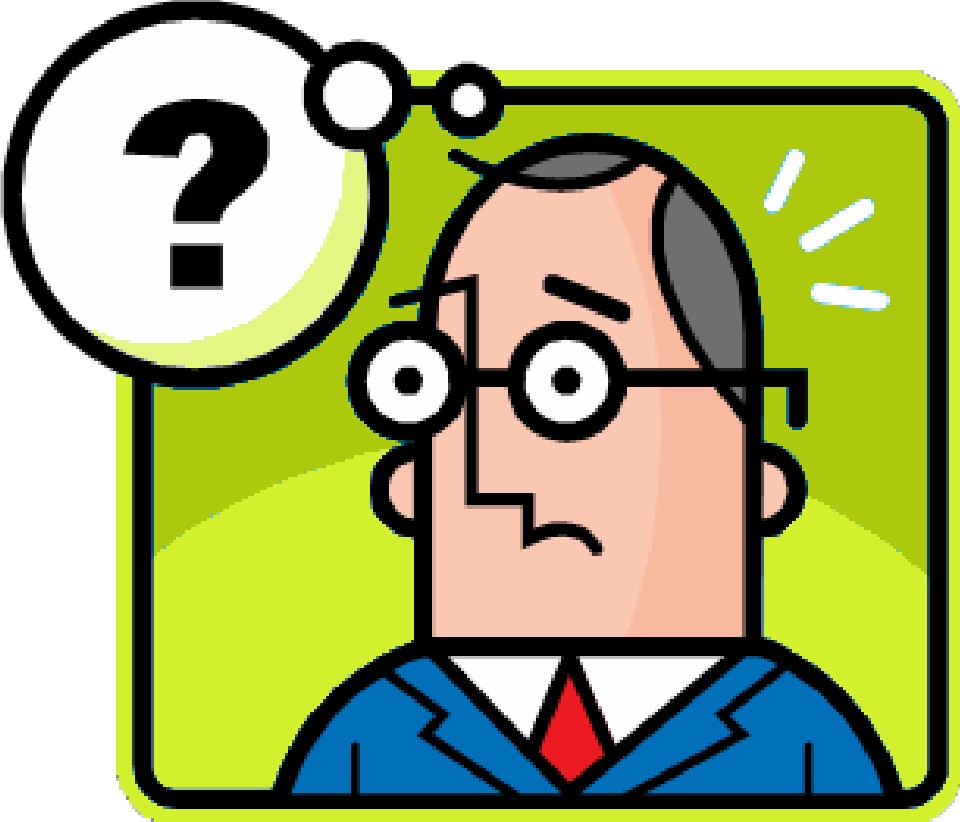
Which laser color would you use (and why)?

We will assume that the SoC frequency is high, but the memory accesses are typically slow  not so bound by laser pulse speed.

Shorter wavelength makes more sense (e.g. λ=445nm) if we want to shoot through the grid

…but we can shoot in other places with other laser colors!

Questions or remarks? ,1scura





## Dual laser attack

#### high-order optical FI

When we talk about dual laser attacks:

* + - * we refer to **several laser sources** shooting concurrently
      * we do not mean a single laser shooting multiple times

High-order optical fault injection (academic term) can refer to both

* + - * Verify what the paper means by this term
      * We will use dual laser attack to avoid confusion

Reason 1: mandatory test under several security testing schemes

…but why?

Hypothetical example of hardened crypto engine 1

* + - * DFA countermeasure: duplicated logic, integrity check

Input

How do you glitch this?

engine

Crypto

Compare?

AES

AES

Fault detected (no output)

Verified output

Hypothetical example of hardened crypto engine 2

* + - * Countermeasures: duplicated logic, integrity check, scattered crypto engine (components separated 10 μm away)

How do you glitch this

Input

AES

now?

AES

Fault detected (no output)

Compare?

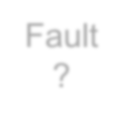
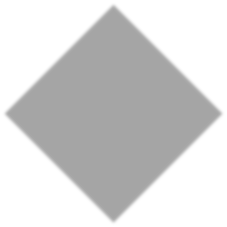
Verified output

Hypothetical example of hardened crypto engine 3

* + - * DFA countermeasure: light sensor

Input How do you glitch this?

General purpose CPU



Output if

no fault

Light sensor

AES

“unverified” output

Fault detected!

Fault

?

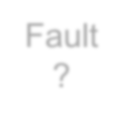
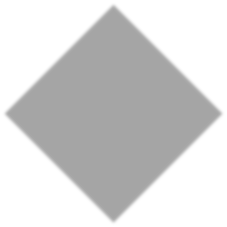
detected

Hypothetical example of hardened secure boot

* + - * DFA countermeasure: light sensor

Input How do you glitch this?

General purpose CPU



Light sensor

Security OTP

Security config

Fault detected

Fault

?

boot

Reason 1: mandatory test under several security testing schemes

because…

Reason 2: under some scenarios, a single laser will not do the trick

Examples:

* + - * Several physical locations
      * Replicated logic / double checks
      * Light sensors that cannot be avoided
      * Consecutive operations too close (faster than repetition rate of

e.g. the DPSS laser)

# Dual laser attacks are very powerful, but they are a p\*\*\* in the

“

a\*\* to perform in practice ”

Security Analyst

Parameters to configure for a ***single*** laser in Inspector:

* + - * Pulse power (0% to 100% max laser power)
      * Pulse length (~4ns to always on, minimum resolution 2 or 4ns)
      * Pulse time offset (4ns to infinite wait from trigger instant)
      * Pulse repetition (one or multiple shots in same location)
      * X and Y coordinates (step size <1μm)
      * Spot size (defined by 5x, 20x, 50x objectives + SSR)
      * Laser attenuation by filter (99.9%, 99%, 90% or no attenuation)

Total # parameters for a single pulse with one laser: 7

Total # parameters for n identical pulses with one laser: 8+n

Let’s set fixed parameters: 1 pulse, 5x lens + SSR, no filter

We still have 5 parameters

# FI attempts do we have with this single laser configuration?

* + - * 3mm x 3mm area, steps of 10μm
      * 1 pulse per spot
      * Random power between 5% and 50%
      * Random pulse length between 10 and 100ns
      * Random pulse time offset between 1000 and 1500ns

Solution:

* + - * 3mm==3000μm  3000/10=300 steps per axis
      * Each time we use a random value for power, length and time

▫ Total number of attempts = 90000

▫ In time (e.g. optimistic avg. time per shot 200ms)= **5hours**

Let’s add another laser shooting same pulse but 10ns later

# FI attempts do we have with a dual laser configuration?

* + - * 3mm x 3mm area, steps of 10μm
      * 1 pulse per spot for each laser
      * Random power between 5% and 50%
      * Random pulse length between 10 and 100ns
      * Random pulse time offset between 1000 and 1500ns

Solution:

* + - * For each position of laser 1, we have 300x300 shots of laser 2
      * (300x300) shots of laser1 \* (300x300) shots of laser2 =

**8,100,000,000 FI attempts**

▫ In time (e.g. optimistic avg. time per shot 200ms)= **51.37 YEARS**

**Issues of dual laser attacks**

#### Issue #1:

**It is not possible to search for every 2 laser configuration because…**

**Parameter explosion**

PARAMETERSSS

Issue #2

How does the physical setup for a dual laser attack look?

Requirements

* + - * Need to focus & position two laser beams
      * Need to configure the two laser pulses properties

Issue #2

How does the physical setup for a dual laser attack look?

Requirements

* + - * Need to focus & position two laser beams
      * Need to configure the two laser pulses properties

▫ Already solved: use Spider ***or*** VC glitcher + (Splitter or spider)

Two objectives with each one beam Two beams through one objective

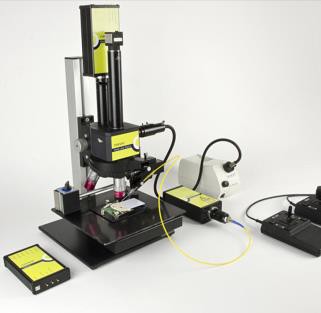
One objective with one beam and one fiber Two fibers

### Spot distance

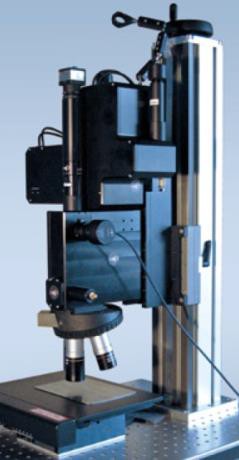
|  |  |  |
| --- | --- | --- |
| **Design** | **Minimal distance** | **Maximum distance** |
| 2 objectives | Objective diameter (~32 mm) | Die size |
| 1. objective, 2. beams | zero | Field of view of objective |
| 1 objective,  1 fiber | Half fiber diameter (~50 µm) | Die size |
| 2 fibers | Fiber diameter (~100 µm) | Die size |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

DLS 1.0: objective + fiber mounted on micro XYZ stage



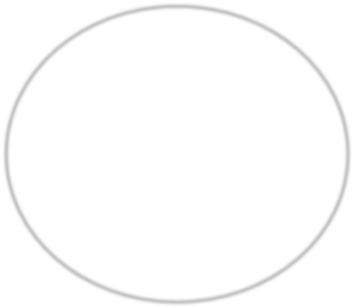
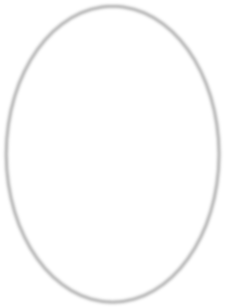
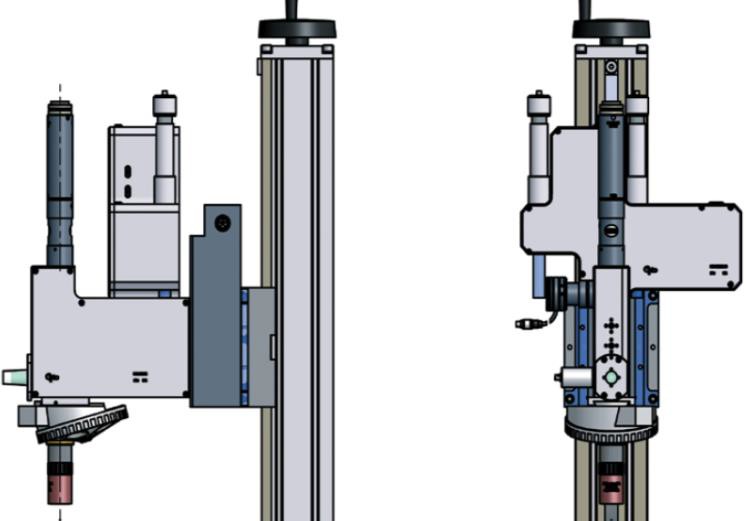
* + - * + Advantage: larger scan area
        + DISADVANTAGE: positioning & focusing laser fiber (don’t see the fiber)

Deprecated system due to difficult laser fiber positioning

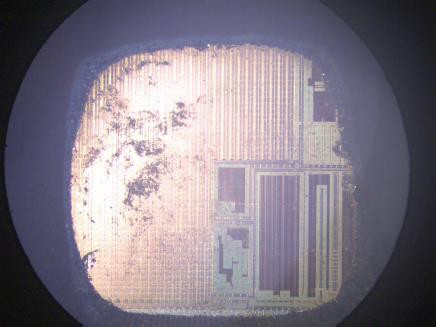
LS2: two beams in same objective

* + - * + Disadvantage: limited by field of view
        + ADVANTAGE: focusing & placement of laser beams is MUCH easier
        + Advantage: we can use also non-fiber- coupled lasers!

1. Two laser sources through one microscope objective



1. Each beam can be positioned and both lasers can be fired independently
2. Laser spots distance bound by field of view



restricted

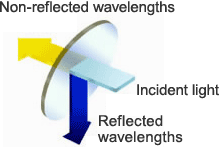
1. Closed loop control system

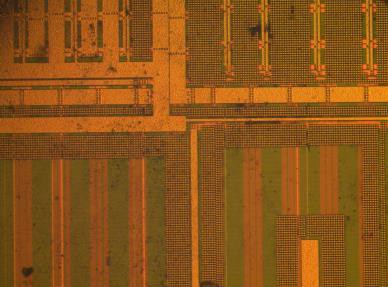
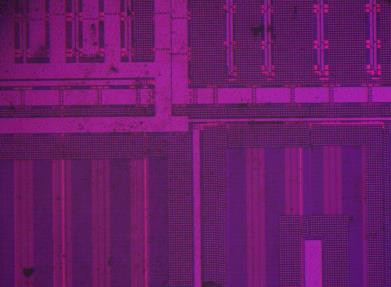
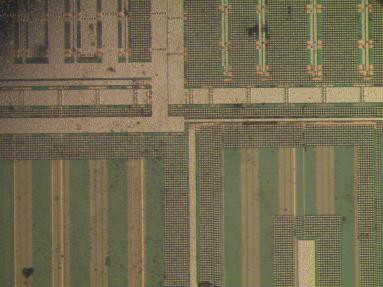
 5x objective, 1x zoom,  3.6 mm (piñata)

34

### LS2 laser colors:

**all optics in one solution**

1. Optimized optics provide maximum optical power, required for
   * Fast and flexible diodes
   * Effective backside illumination
   * When used for optical emission analysis
2. Full laser range requires two beam splitters
   * For navigational camera + working laser in one solution
   * User can insert / remove beam splitter
   * All wavelengths supported (445 nm, 532 nm, 808 nm, 1064 nm)



no beam splitter

restricted

808 & 1064 nm

445 & 532 nm

35

Issue #2

Dual laser setup is more complex than single laser setup Reason: we use more tools

* LS2
* *TwinScan*
* Laser source 1
* *Laser source 2*
* Spider or VCGlitcher*+(Spider/Splitter)*

Issue #3: cost of the setup

For a single laser setup, we need:

LS2 + TwinScan + laser source + Spider or VCGlitcher

For a dual laser setup, we need:

LS2 + TwinScan + laser source1 + laser source 2 + Spider or VCGlitcher+(Spider/Splitter)

Dual laser attack setup is quite more expensive

* Additional TwinScan module on LS2
* Additional laser source
* Additional Spider or Splitter if you use a VC glitcher for SC

Why is it interesting? (2 items)

* It is mandatory for some security testing schemes
* Can achieve successful attacks that a single laser cannot do under certain scenarios

Why is it a p\*\*\* in the a\*\*? (3 items)

* Parameter search explodes very quick
* Setup is more complex
* Setup is more expensive



**One more thing ...**

##### ,1scura

**One more thing…**

Imagine we have a fast CPU (f=1.5GHz) that computes software AES twice and then checks the results

We want to do DFA on it.

How many laser pulses we need?

* We need 2: one for the computation, another for the check

However, it is a very thick flip-chip…

* We want to use DPSS 1064nm laser
* Diode lasers cannot deliver lots of power in same time as the DPSS laser

How?

###### Dual laser setup with two DPSS 1064nm lasers

**Recap of dual laser attack**

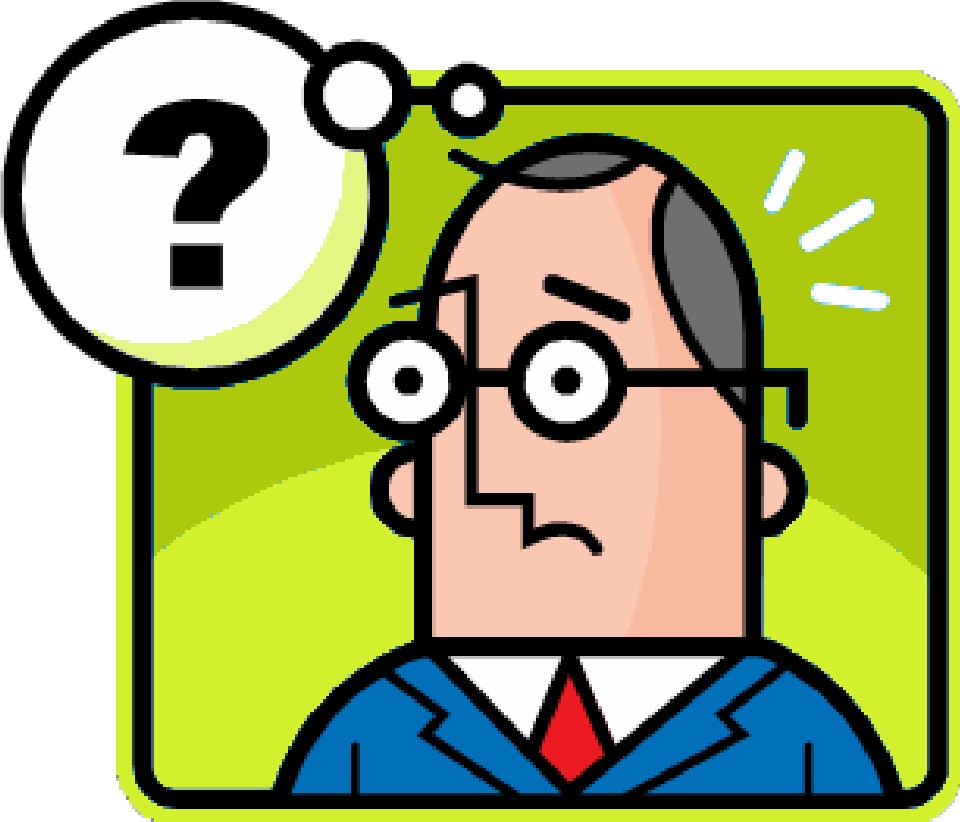
Why is it interesting?

* It is mandatory for some security testing schemes
* Can achieve successful attacks that a single laser cannot do under certain scenarios
* We can do multiple laser shots with high-power lasers that take time to recharge

What are the issues with the attack?

* Parameter search explodes very quick
* Setup is more complex
* Setup is more expensive

Questions or remarks? ,1scura





## Exercise/demo:

**steps to do a dual laser attack**

### Steps to do a dual laser attack

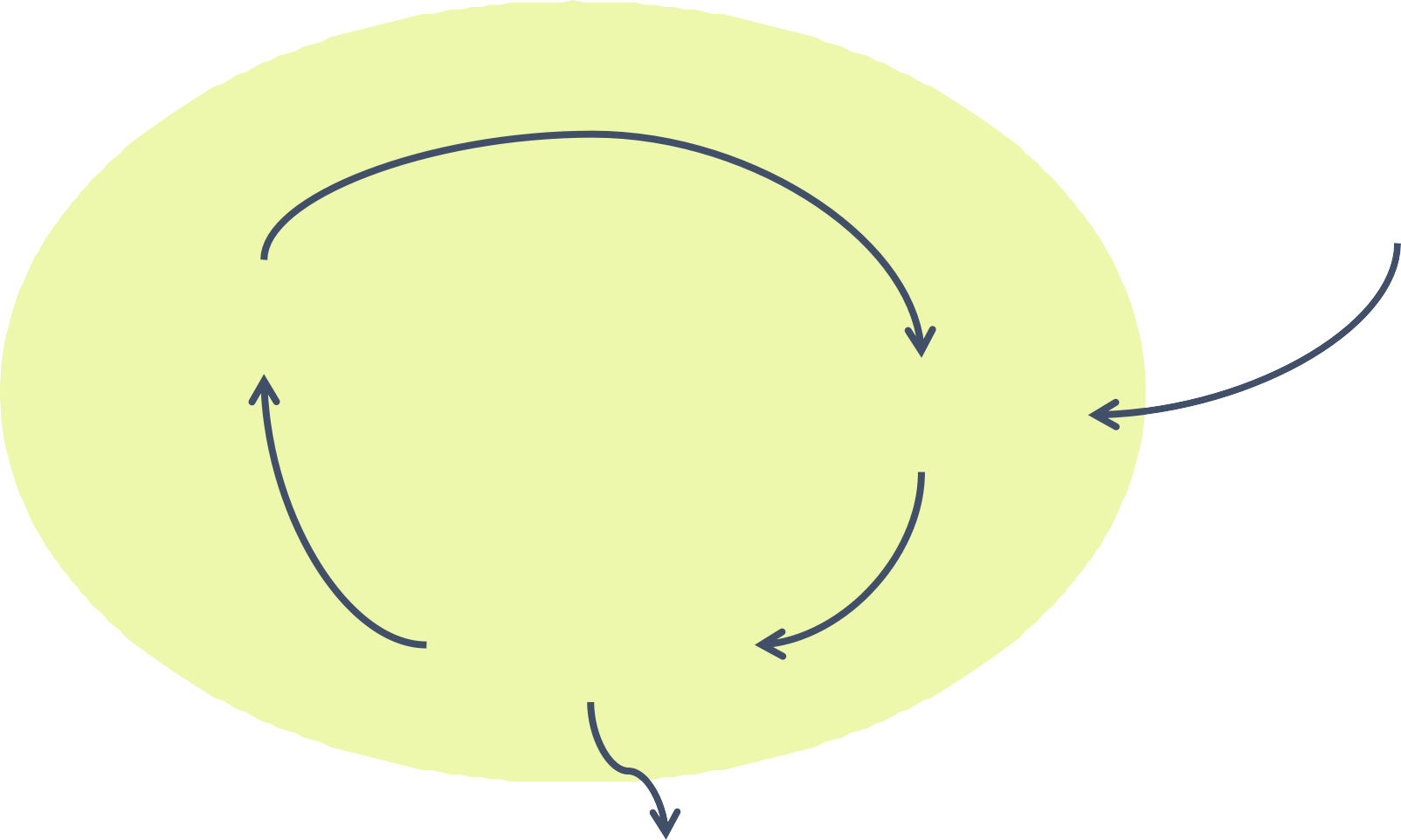
For a dual laser attack we have a hard prerequisite:

* We need to reduce our search as much as possible due to parameter explosion: learn as much as you can before attack!

Initial

analysis SCA profiling

FI profiling



Refinement

FI attack

Minimal test case?

Analysis

Conclusion

Proposed steps for a dual laser attack

1. Profile your target with SCA (if possible)
2. Profile your target with a single laser first:

Sensitive areas, parameter ranges, etc…

1. Minimal test case: think if a single laser attack is still feasible. If so, go for it instead.
2. If dual laser still looks like the only choice, build the setup and verify that it works before actual shooting
3. Start the dual laser search (try to narrow the parameter ranges as much as you can, remember parameter explosion!)

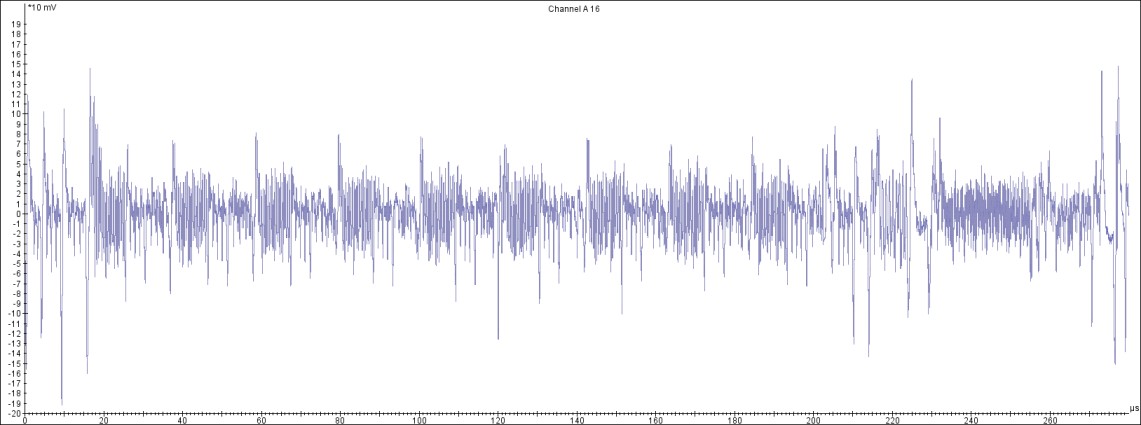
We are going to “build” a dual laser setup for doing DFA on the pinata board decapped back-side:

* Implementation does AES twice and then a check
* One laser will shoot at the memory to corrupt the computation
* One laser will shoot at the CPU to corrupt the crypto check

Step 1: profile your target with SCA

We know that this is an AES encryption, and the countermeasure is checking the result.

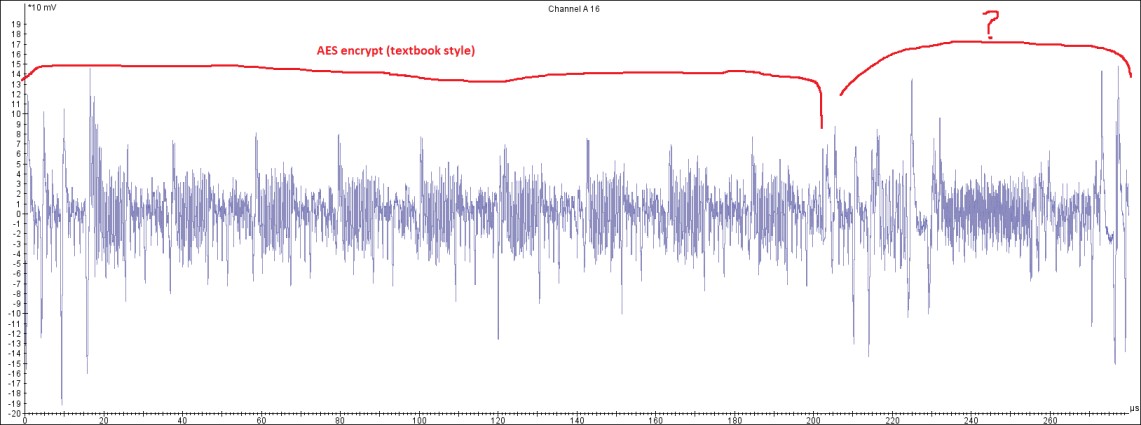
We made a SCA measurement. What is going on here?



Step 1: profile your target with SCA

We know that this is an AES encryption, and the countermeasure is checking the result.

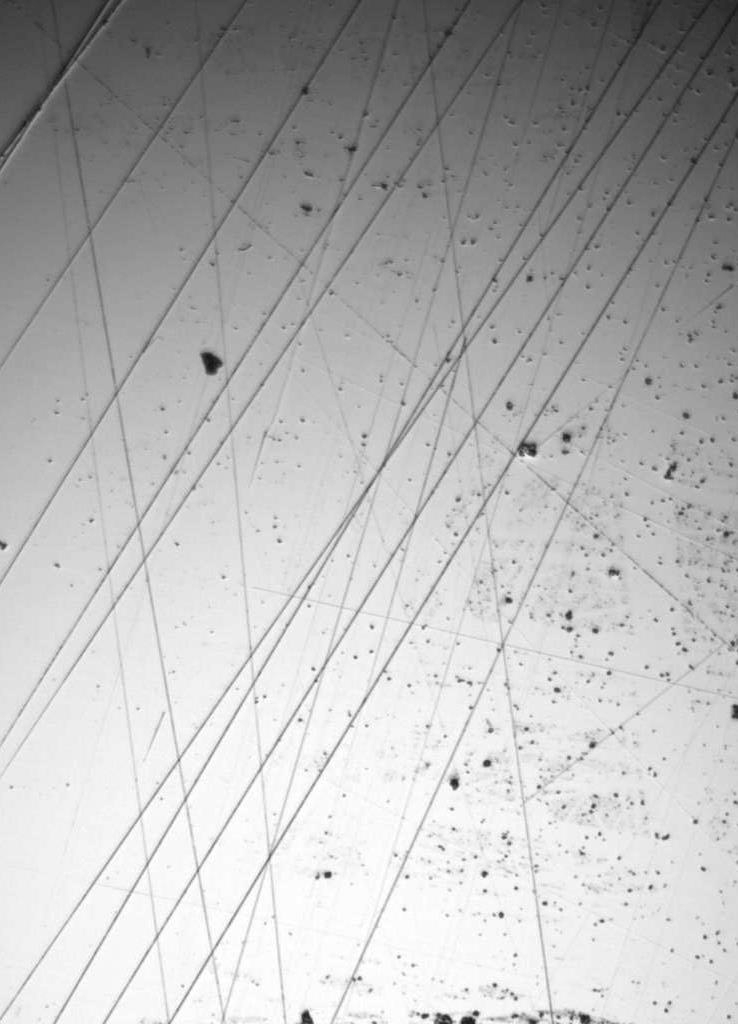
We made a SCA measurement. What is going on here?



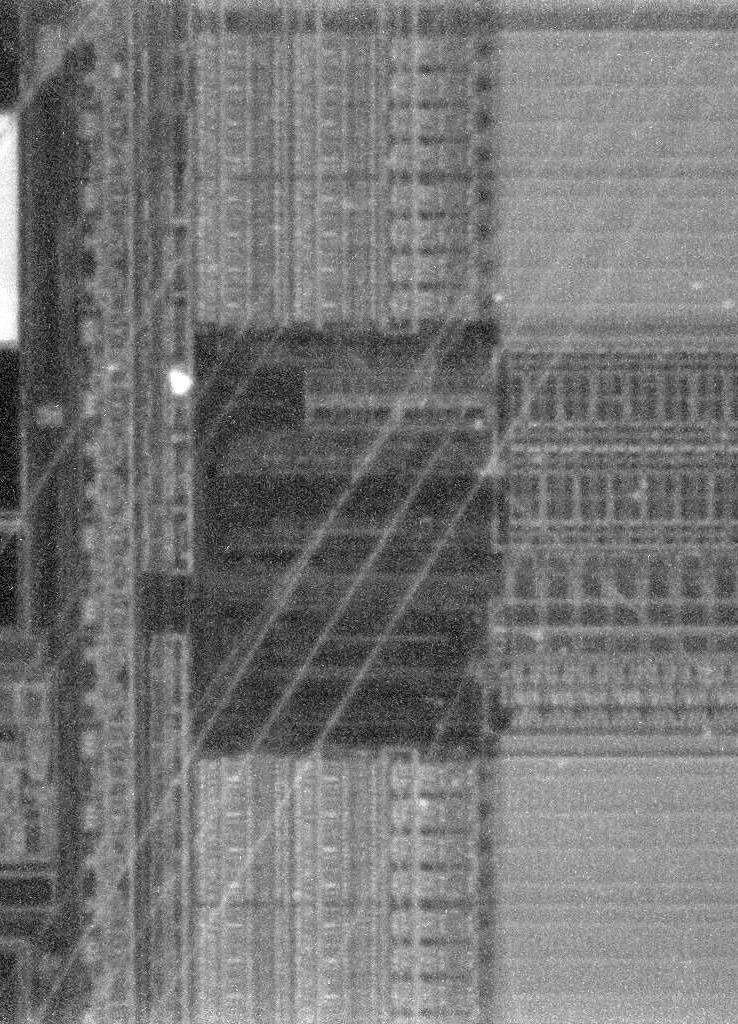
Step 2: profile your target with FI Intermezzo: NIR camera

Silicon is transparent for wavelengths >1200nm

We can shine this light and see the reflection on metal with a NIR camera



visible



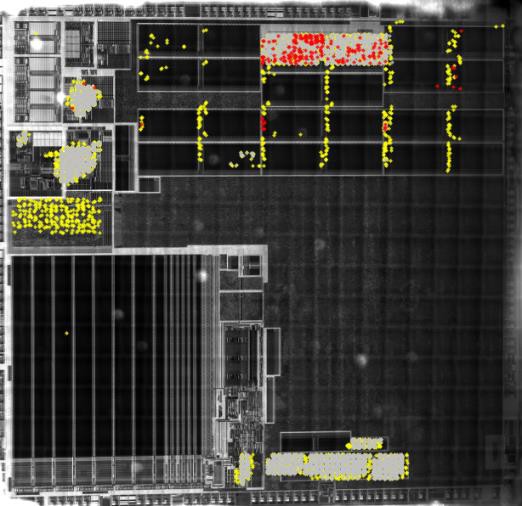
NIR



Step 2: profile your target with FI

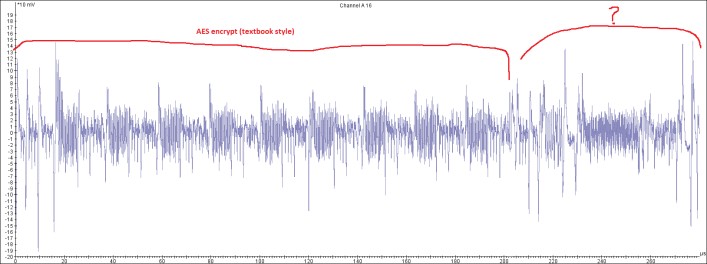
We want to know “where to shoot” in the chip

 Take a picture of the chip with the NIR camera upgrade

 Use a single laser and shoot at the device

Results plot overlapped on die picture (we will learn later how to do this)

Step 3: still makes sense to go for dual laser?



* For this attack, we could hit the CPU twice with a laser, since encryption and output check are both performed in the CPU
* AES round takes around 20μs, so it is feasible to shoot a laser twice. In theory, a double shot of single laser could work

▫ FYI in practice it works

* But for the sake of explanation, let’s imagine that our only option is a dual laser attack (single attack did not work / meaningless)

Step 4: “build” the setup

* Start up Inspector
* Compile and load the Sequence “SpiderLaserTwinScan.java”
* In Inspector, open the module and you will see to which ports we will connect the lasers in Spider

▫ Next session we will learn how to use Spider



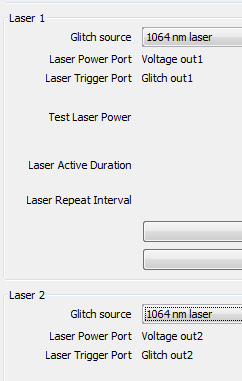
* “Build” the complete setup

▫ Lasers: multi-mode diode lasers. Which wavelength?

▫ TwinScan has a controller connected to the computer via a USB cable

▫ TwinScan mounts on top of the LS2 system

Step 4: “build” the setup

Equipment list:

* Pinata board (I/O: serial)
* Spider (usb)
* Laser1: 1064nm multimode diode
* Laser2: 1064nm multimode diode
* 2x SSR
* TwinScan (usb)
* Laser Station 2
* XYZ Tango controller (usb)
* NIR camera + ring light
* Safety box
* Cables, power supplies, …
* (optional) oscilloscope

55

Trigger out

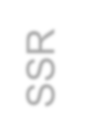
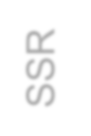
GND

VCC

Reset

Target

Embedded I/O



Pulse Amplitude

Digital glitch

Laser out

Diode Laser 1 (λ=1064nm)

SSR

SSR

Diode current

Step 4: “build” the setup

Diode Laser 2 (λ=1064nm)

Pulse Amplitude

+12V

Devices block diagrams

**Spider**

Glitch out 1

Glitch out 2

Voltage out 1

Voltage out 2

Voltage out 3

Voltage out 4

Voltage out 5

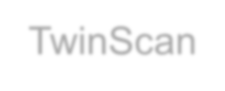
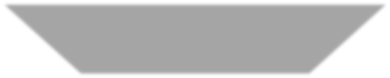
Voltage out 6

GPIOs core 1

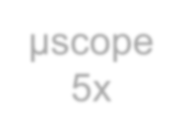
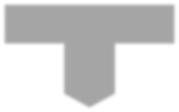
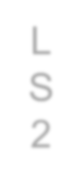
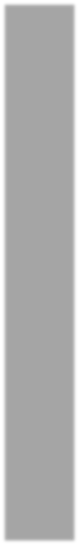
GPIOs core 2

usb

15V



TwinScan



L

S 2

cam

μscope

5x

USB

XYZ

Diode current

+12V

Digital glitch

Laser out



NIR light

Step 4: “build” the setup – setup proposal (PSUs not connected)

**Spider**

Diode Laser 1 (λ=1064nm)

Pulse Amplitude

Digital glitch

Diode current

Diode Laser 2 (λ=1064nm)

Pulse Amplitude

Digital glitch

Diode current

Glitch out 1

Glitch out 2

Voltage out 1

Voltage out 2

Voltage out 3

Laser out

Laser out

Voltage out 4

+12V

+12V

Voltage out 5

Safety Box

Voltage out 6

GPIOs core 1

SSR

SSR

cam

TwinScan μscope

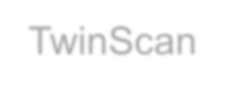
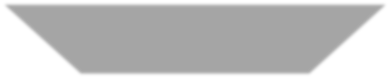
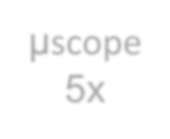
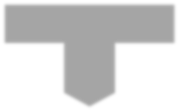
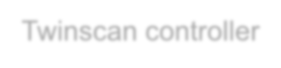
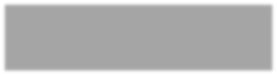
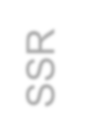
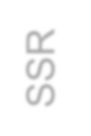
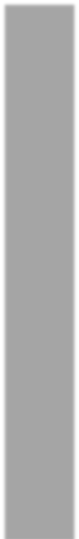
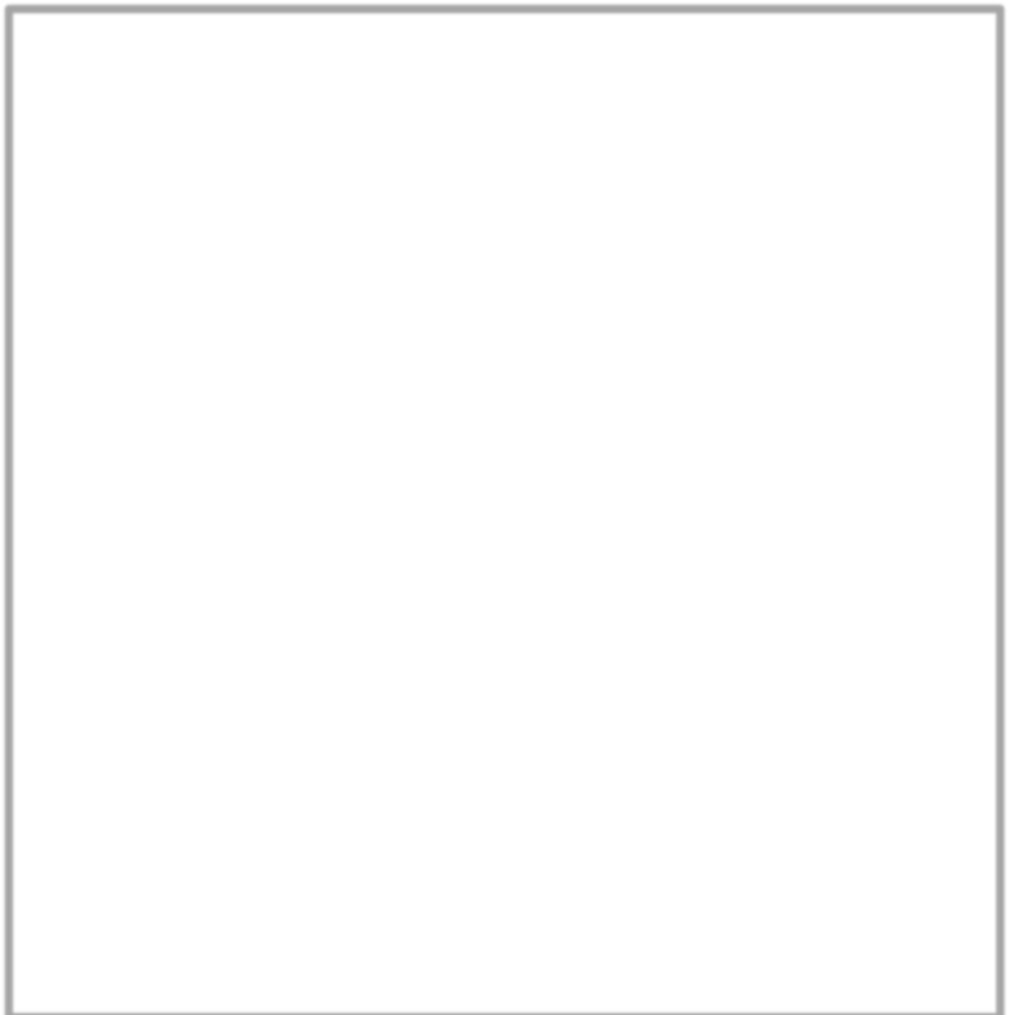
5x

NIR light

GPIOs core 2

usb 15V

Twinscan controller



PC

Embedded I/O

USB

VCC

Reset

Target

USB

USB

USB

USB USB USB USB

USB

XYZ

Trigger out

GND

Step 5: dual laser attack

Configure the settings for sequence for dual laser Configure the laser positions with your device off

* + Useful: blink the laser every now and then with minimum power

TwinScan mirror system enumerates in Inspector as a XYZ device

**WARNING: be careful with the amount of steps in the laser scans**

Get some coffee and wait for results after some hours…

Demo / video (if setup not available)

Q – We get no faults, what should we do?

* + Check the setup, this is one of the most complex setups and most likely something is wrong (cables, PSUs, Inspector code, …)

Q – We get too many faults, what should we do?

* + Tweak your parameters (especially laser power), as different components behave differently with the same laser pulse

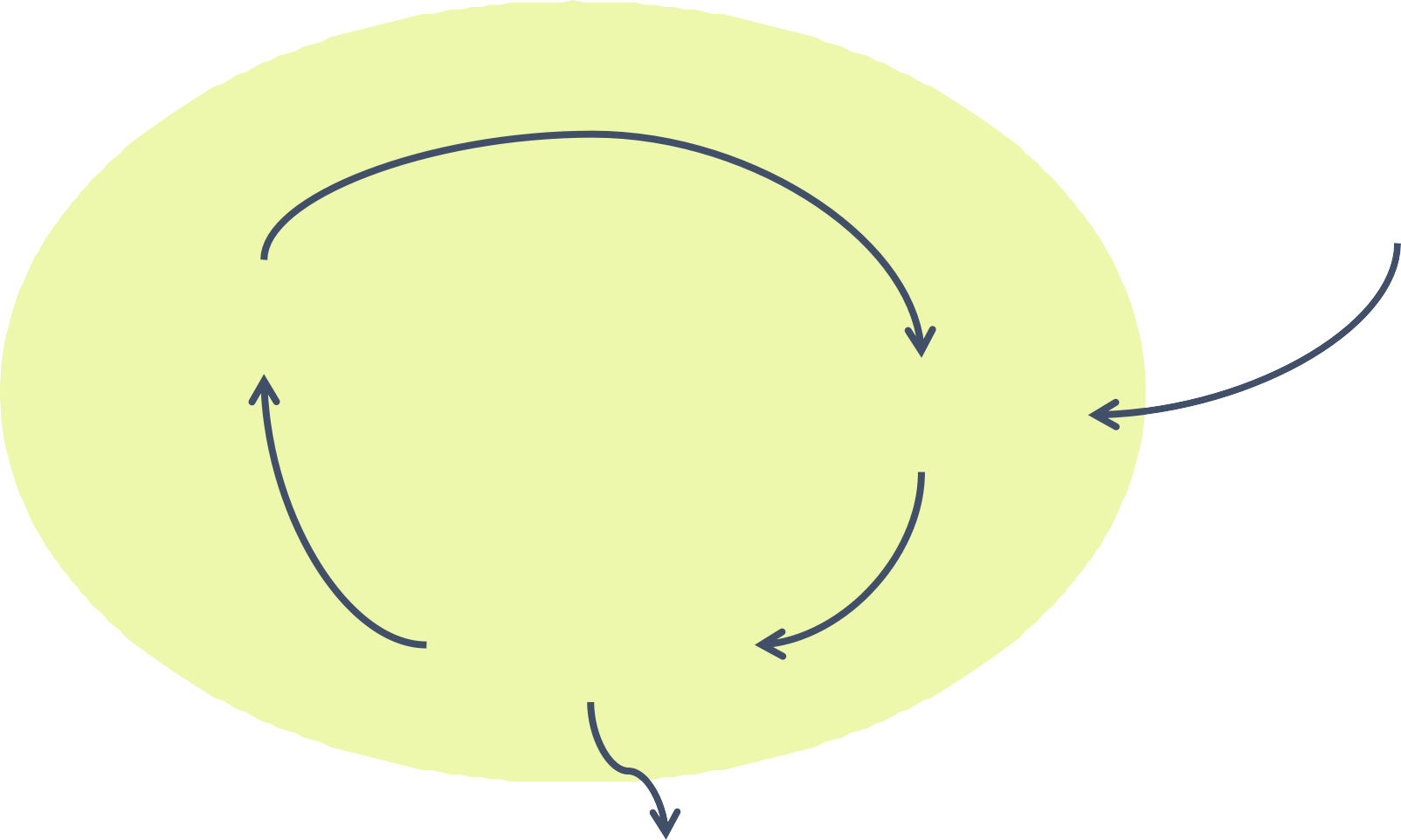
Q – Is this attack realistic?

* + If you have the floorplan of the chip (eg. evil maid scenario) and a high value asset (eg. root key of a CA), definitely

Initial

analysis SCA profiling

FI profiling



Refinement

FI attack

Minimal test case?



Analysis

Conclusion

