brightsight®

your partner in security approval

Fault Injection, a fast moving target in evaluations

brightsight®

Outline

- Commonly used fault injection methods
- Not so commonly used fault injection methods
- Fault attacks in the real world
- Practical considerations
- Common practice for security labs
- Near future attack scenarios
- Rating tables
- What if this goes on?
- Sense and non-sense
- Conclusion

Security evaluation participants – DEVELOPER

- Is primarily interested in a certificate
- Is, at best, interested in vulnerabilities for future products
- Has a customer who is pushing the dead-line
- Is working on a future product because the TOE is already “finished”
- Performs most of the work
- Sponsor of the evaluation process
- Does 9 out of 10 times a very good job
- Raises the evaluation effort for commercial reasons (EAL6, EAL7+)

- THESE ARE NOT ACCUSATIONS, THIS IS HOW BUSINESS WORKS

- Task: develop products that are up for the job with sufficient security against reasonable costs

Security evaluation participants – LAB

- Is pushed for the dead-line by the developer
- Needs documentation and samples before the evaluation can start (delivery shifts, dead-line shifts not)
- Is always too expensive and too slow
- Needs to develop tools that support new technology (NFC, SWP, etc.)
- Needs to keep up with developments of attack techniques
- Evaluation outcome is unpredictable (broken for unclear reasons)

- THESE ARE NOT ACCUSATIONS, THIS IS HOW BUSINESS WORKS

- Task: Perform a security assessment with sufficient assurance within a reasonable amount of time and cost

Security evaluation participants – CERTIFICATION BODY

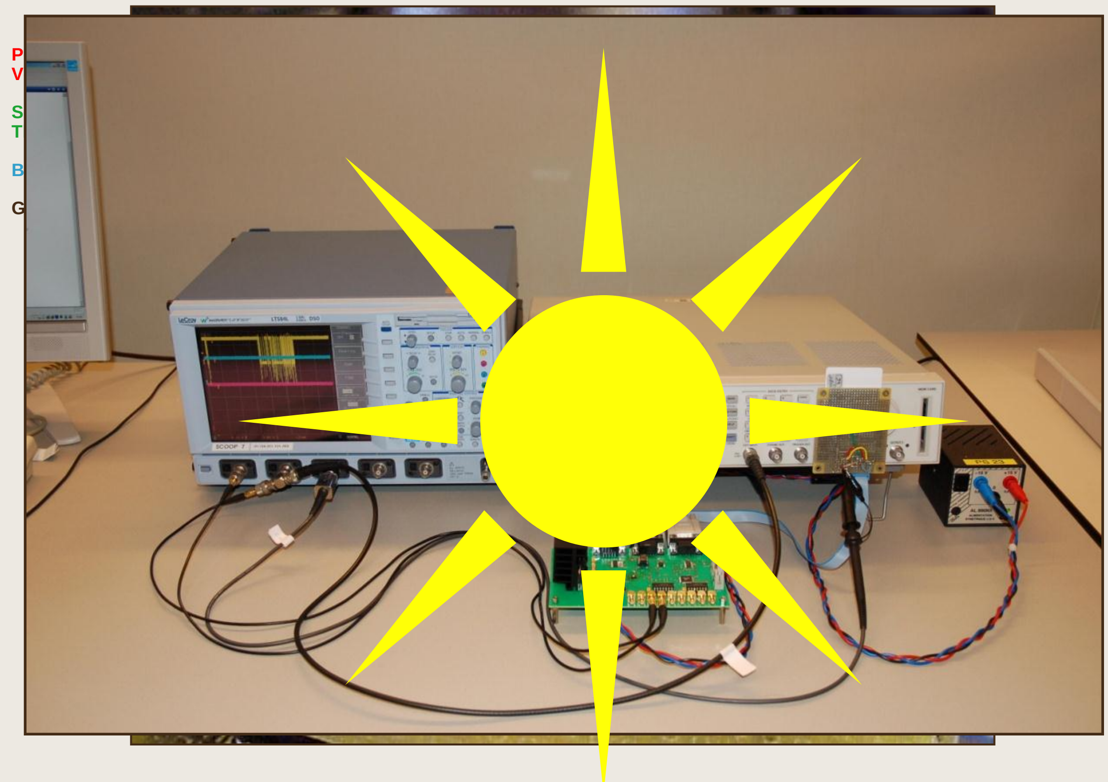
- Has no commercial interest
- Aims at optimal security to avoid liability
- Considers any possible attack scenario equally important

- THESE ARE NOT ACCUSATIONS, THIS IS HOW BUSINESS WORKS

- Task: Overseer of the evaluation process

Commonly used fault injection methods

- Active probing
- Voltage glitching
- Light flashing



Not so commonly used fault injection methods

- Less practical
  - High voltage pulse
  - Magnetic pulse
  - Radio active sources

- Solved by common practice technology
  - Reset glitching
  - Clock glitching

Fault attacks in the real world

- Practical attacks performed by hackers, not security labs or university

- calling cards (public phone)
- pay TV cards
- micro controllers (lock bit)
- mass unblocking of chips in production line
  (>300,000 chips with 100% hit rate)

- All attacks performed using **Voltage Glitching**!

- All attacks have attack level **basic**!

Practical considerations

- What does the lab have what I (attacker) haven't got?

- Developer information
  - Design knowledge of the hardware
  - Design knowledge of the software (source code)
  - Timing indication or control about the timing

- Easy access to different attack technologies
  - Etching
  - Reverse engineering
  - Power consumption analysis tools
  - Lots of equipment and expertise (power supplies, function generators, oscilloscopes, high-end pulse generators, laser cutters, high power CW lasers, 35 fellow experts)

Common practice for security labs

- Voltage glitches
  - Multiple glitches
  - -20V < Vglitch < +20V
  - Tglitch > 8ns increasing in 1ns steps

- Light flashes
  - Tflash => nanoseconds (laser cutter)
  - Tflash >= nanoseconds and longer (solid state laser)
  - NIR, red, green
  - Multiple flash (slow)(20ms – laser cutter)
  - Multiple flash (fast)(nanoseconds – solid state laser)
  - Single location
  - Basic countermeasure detection

Multiple flash (slow) example

- The flashes must be at sufficient interval > 20ms
- Applicable on RSA calculation with DFA countermeasure double calculation.

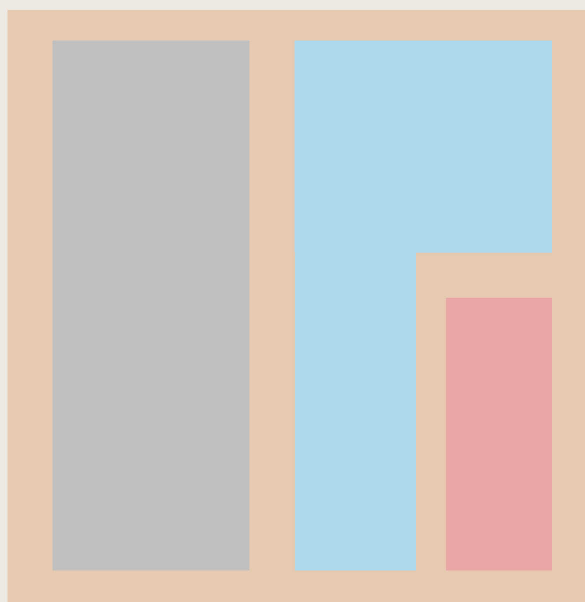
- Steps:
  - Execute a RSA calculation
  - Flash during the first RSA calculation
  - Flash at (approximately) the same instruction of the second RSA calculation
  - If both results are the same the DFA countermeasure will fail detection

- Only requires a low repetition rate laser

- Works because RSA is slow and the attacker can use Waiting Time extensions (WTX) to re-arm the laser

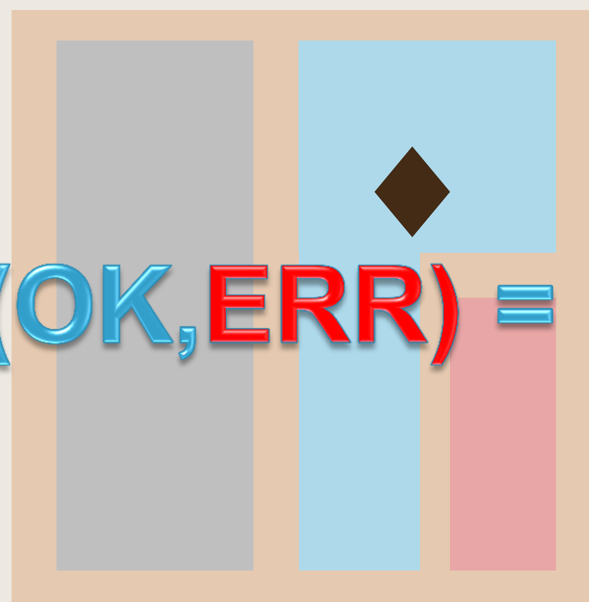
Normal execution

RSA = OK



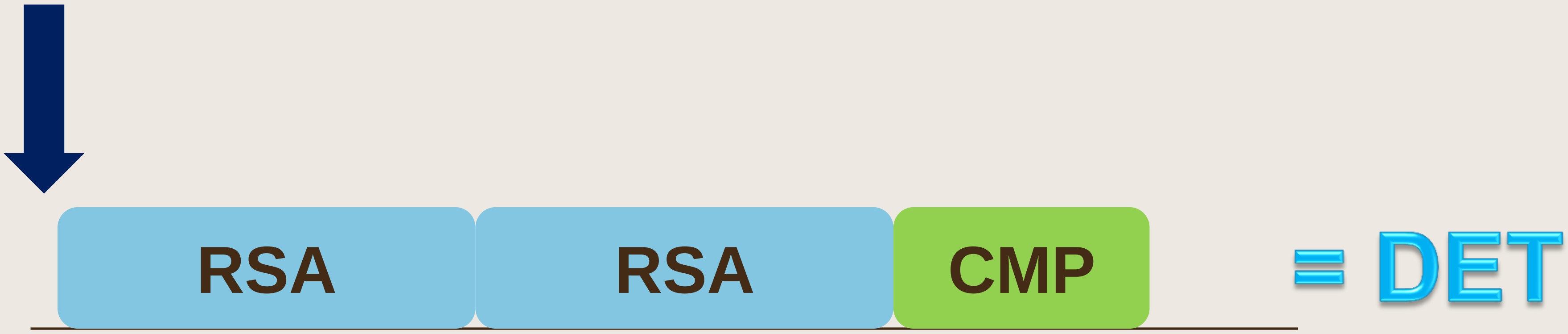
Single flash no countermeasure

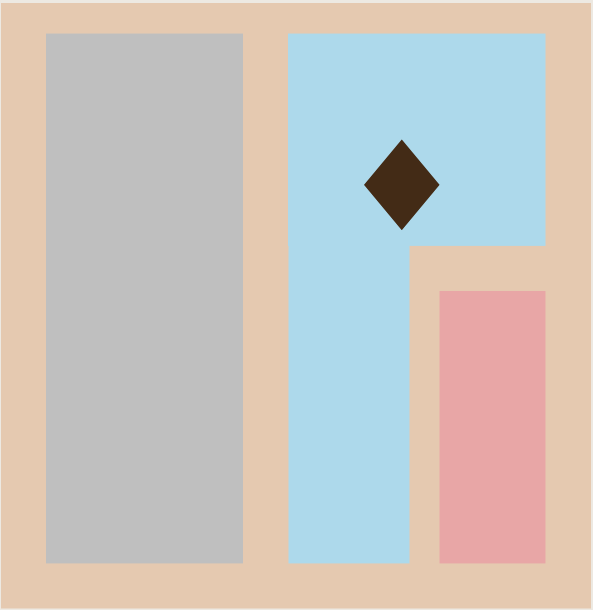
RSA = ERR



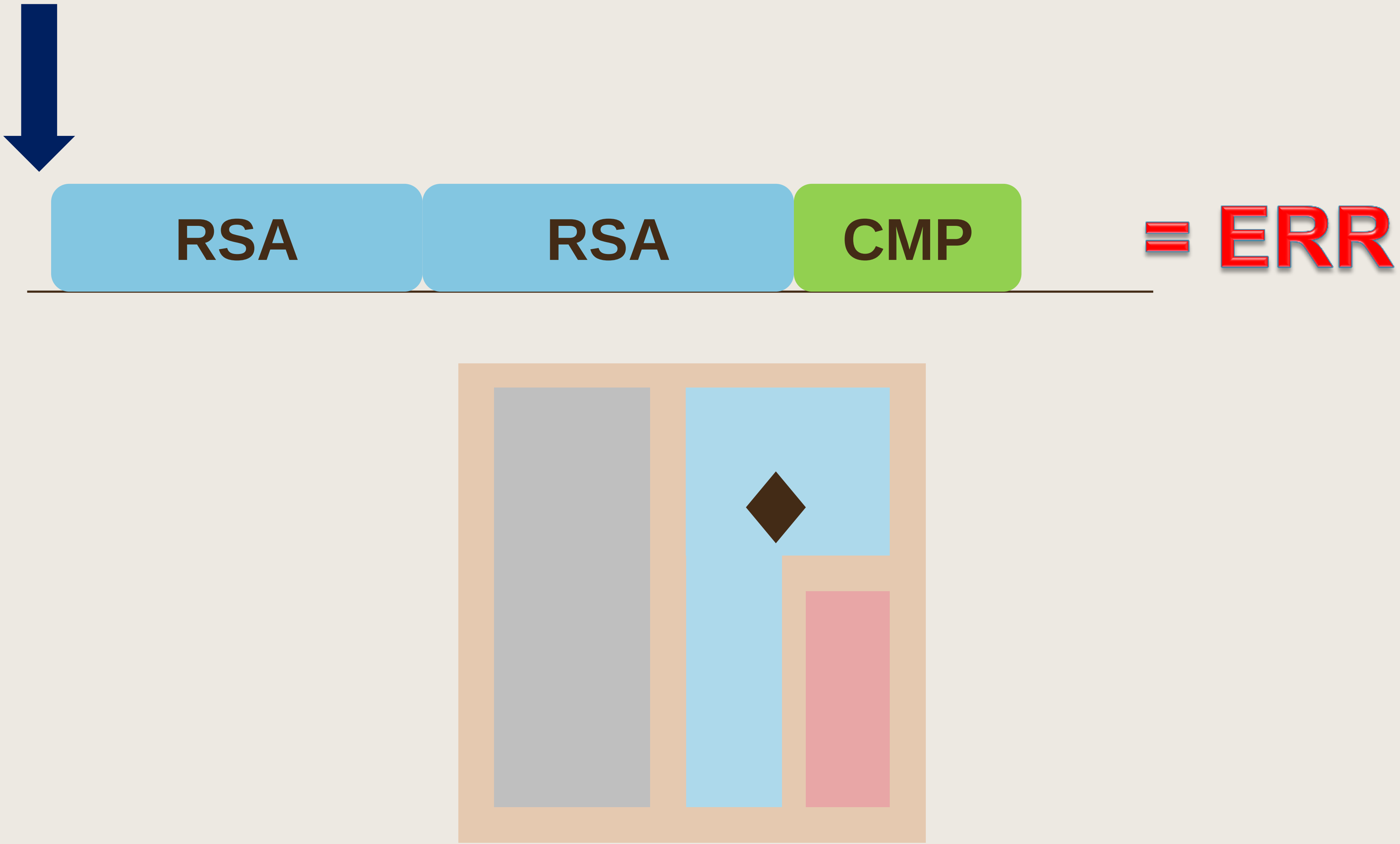
DFA(OK,ERR) = KEY

Single flash with countermeasure





Double flash



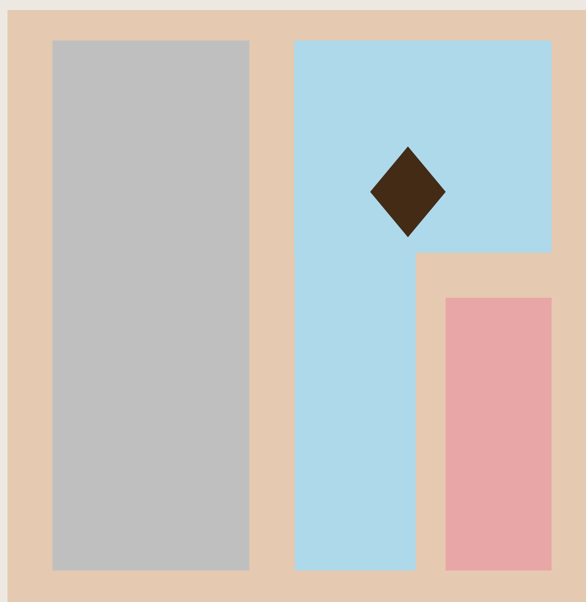
Multiple flash (fast) example

- The flashes will follow each other at very short intervals
- Applicable also on fast algorithms such as DES with DFA countermeasure double calculation.

- Steps:
  - Execute a DES calculation
  - Flash during the first DES calculation
  - Flash during the second DES computation
  - If both results are the same the DFA countermeasure will fail detection

- This requires
  - a fast re-triggerable laser
  - Accurate trigger source

Multiple flash



Near future attack scenarios

- Light flashes on two locations
- Light flashes on many locations

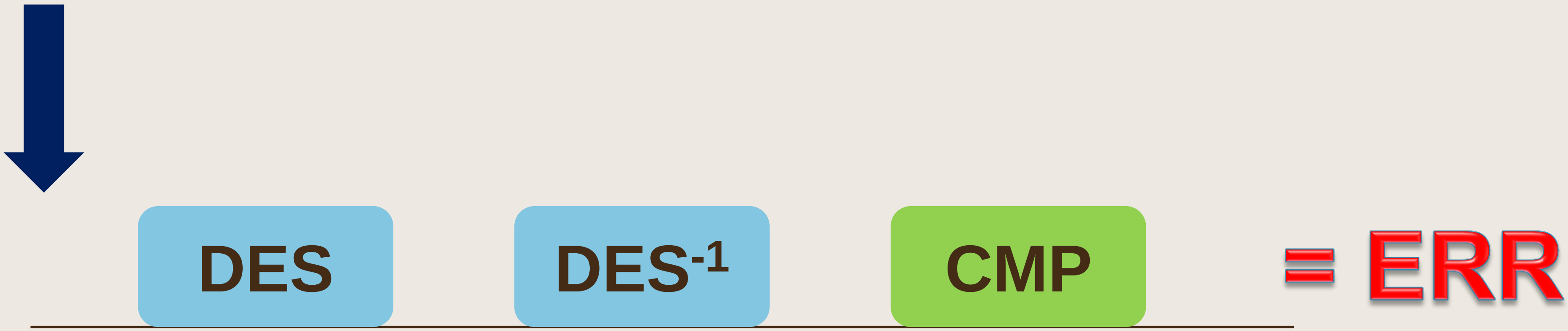
Two locations example

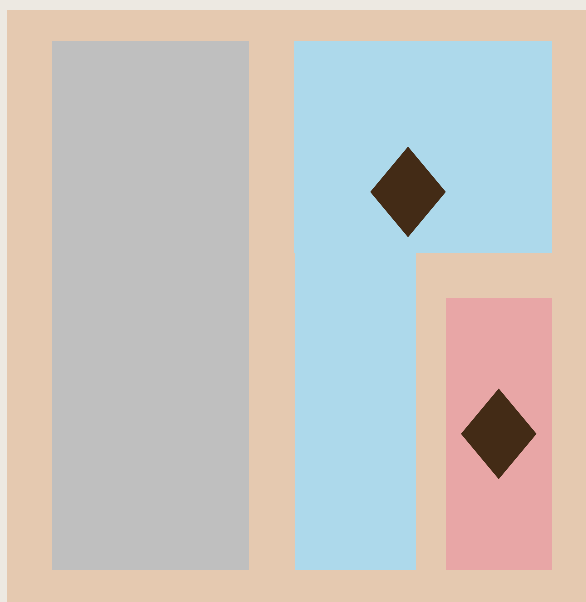
- The flashes will follow each other at very short intervals
- Applicable also on fast algorithms such as DES with DFA countermeasure reverse calculation.

- Steps:
  - Execute a DES calculation
  - Flash during the first DES calculation
  - Flash during the compare performed as DFA countermeasure so it will fail detection

- This requires
  - A laser set-up capable of flashing at two locations
  - Accurate trigger source

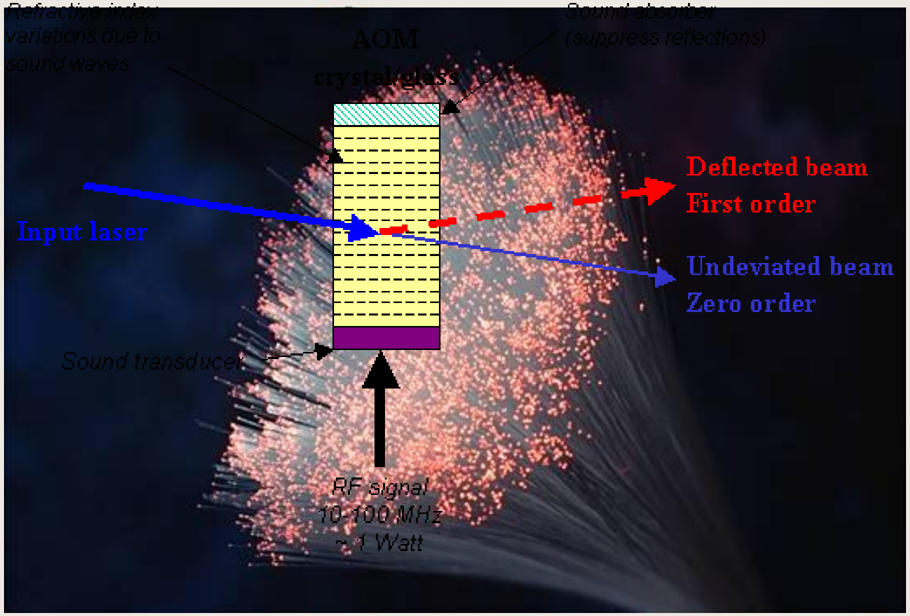
Two locations





Two locations – possible solutions

- Acousto-optic modulator
- Dual lasers
- Fibers on chip surface



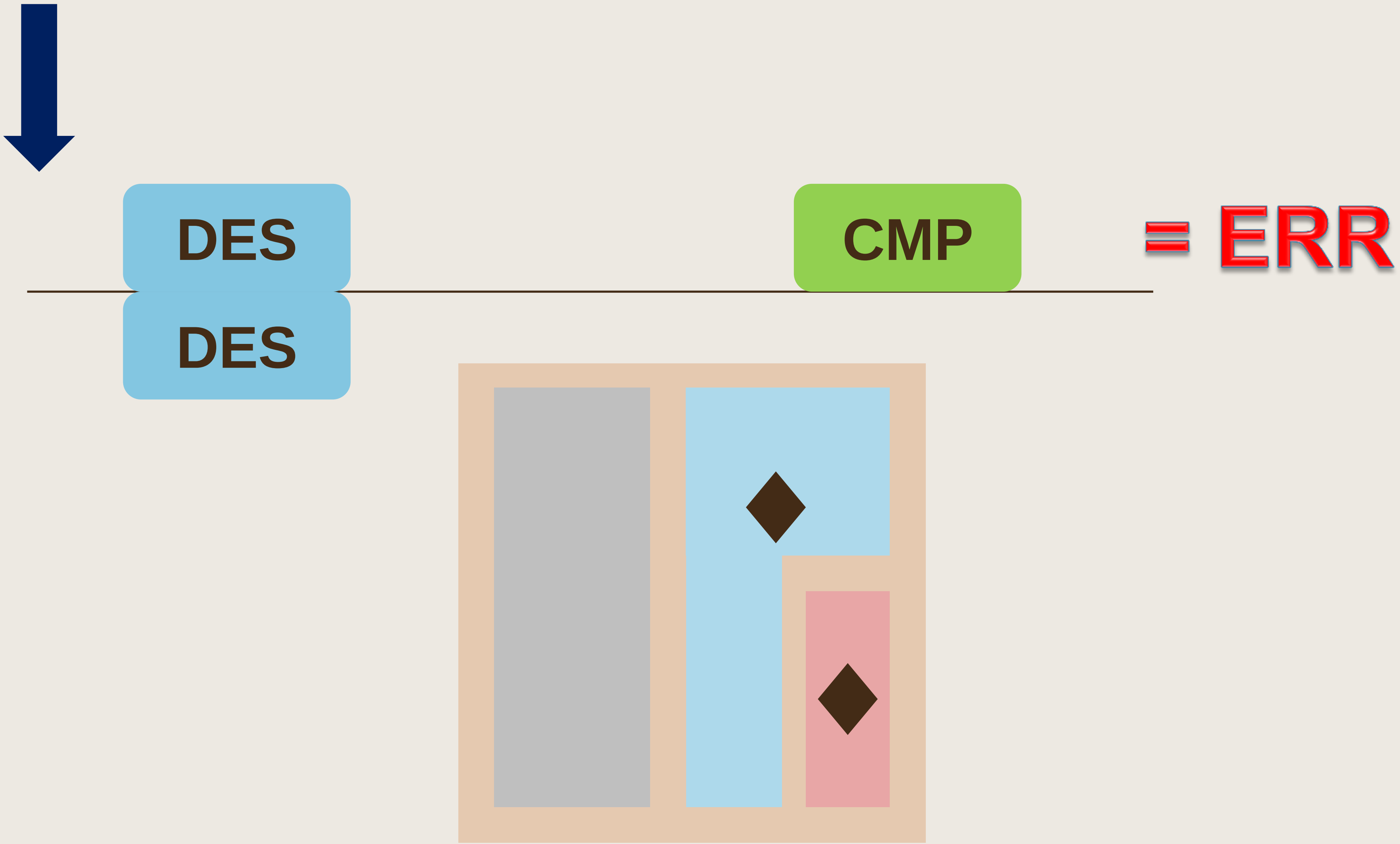
Light flashes on many locations example

- The flashes will occur at the same time
- Applicable also on fast algorithms such as DES with DFA countermeasure that implements two separate crypto processors.

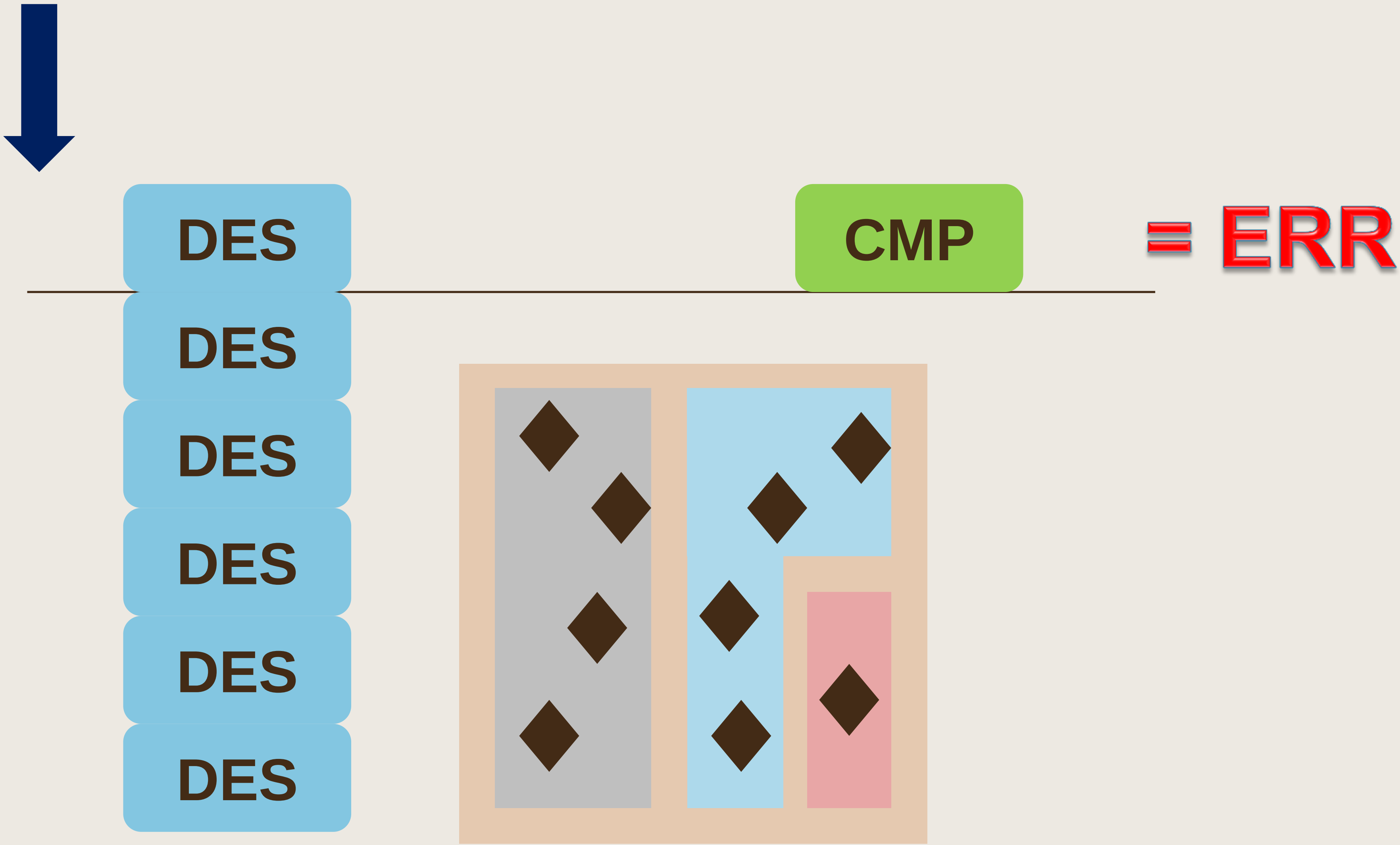
- Steps:
  - Execute a DES calculation
  - Flash during the DES calculation at both coprocessors
  - The compare performed as DFA countermeasure will fail detection

- This requires
  - a many locations capable laser set-up
  - Accurate trigger source

Multiple locations at the same time



Many many locations



Rating factors

- Time
- Expertise
- Knowledge of TOE
- Access to TOE
- Equipment
- Open samples

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Rating table example

Factor	Identification	Exploitation
Time	< 1 week (2)	1 day (3)
Expertise	Expert (5)	Proficient (2)
Knowledge	Restricted (2)	Public (0)
Access	< 10 (0)	< 10 (0)
Equipment	Specialized (3)	Specialized (4)
Open Samples	None (0)	NA (0)
Points Sub Total	**12**	**9**
Total	**21**	

Rating

- Equipment

Equipment	identification	exploitation	
None	0	0	points
Standard	1	2	points
Specialized	3	4	points
Bespoke	5	6	points
Multiple bespoke	7	8	points

- Laser cutter without any supporting equipment: **specialized**
- with supporting equipment: **specialized**
- with advanced trigger device: **specialized**
- with dual laser beam: **specialized**

What if this goes on?

- Increasing requirements for test set-up capabilities
  - Triple or quadruple laser beams
  - Highly advanced countermeasure detection systems
  - Multiple side-channel combinations (SPA, EMA)

- Hugh number of knob positions results in long testing times
  - Laser intensity flash 1, Laser intensity flash 2
  - Wavelength 1, wavelength 2
  - Position 1, Position 2
  - Timing 1, Timing 2
  - Silicon side, metal side

- A practical approach is required to keep testing feasible!

Sense and non-sense

- Breaking of a system shall be hard enough to make it unattractive/unprofitable
- Experiments that have been published were often applicable on a particular implementation which are not always state-of-the-art or open samples
- Every published attack IS important but should be evaluated for practical applicability and relevance for the product or type of products
- There is a limitation on the time spent on testing.

Conclusion

- Fault injection attacks have special attention from the certification bodies
- Some developments are really powerful
- The complexity of the considered attacks is increasing rapidly
- There is a risk that complicated attacks distract the attention from simpler and more threatening attacks (unjust assurance)
- Testing costs will increase over time