Enter The Donjon

A practical laser attack on the go

Workshop 06 - Grehack 24

Agenda

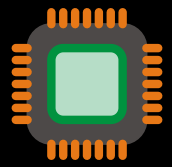
Fault injection principles

Attack of the OneKey Mini

Live execution

Workarounds and questions

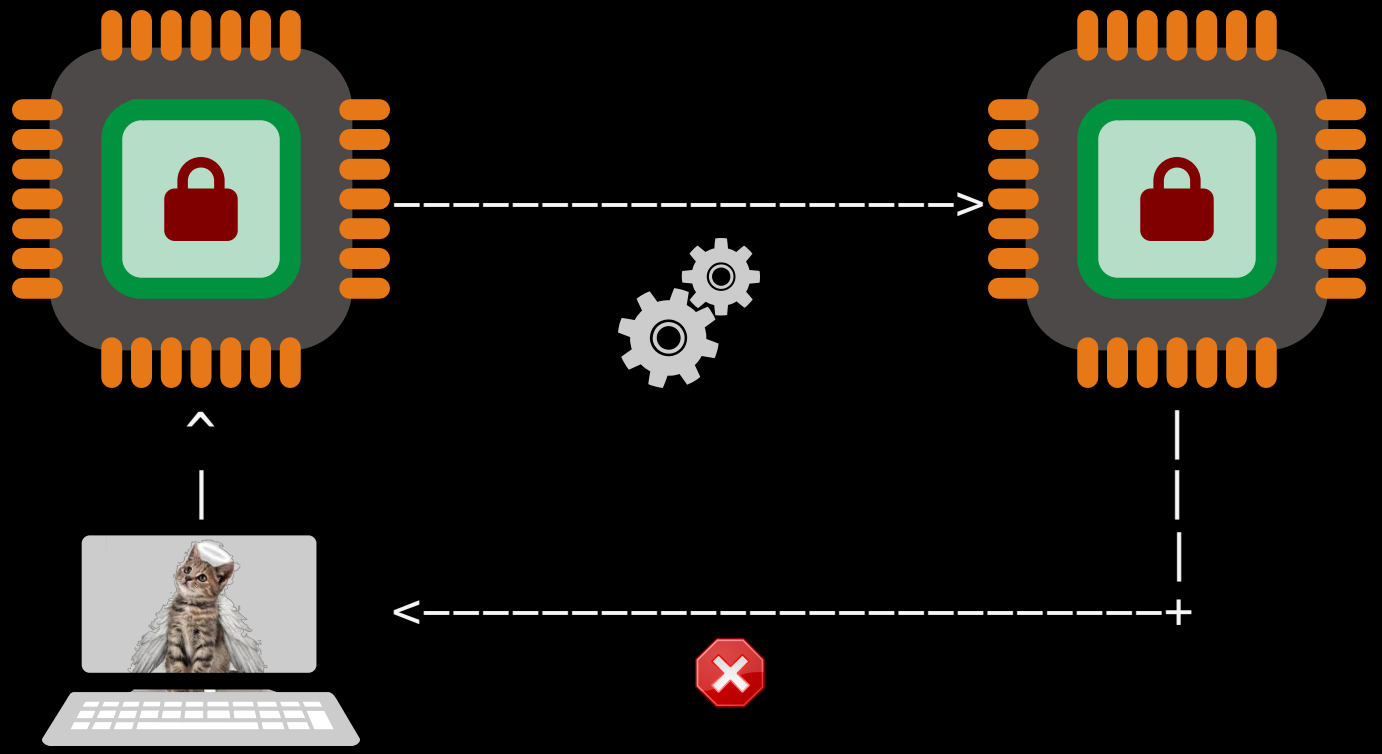
Fault Injection? What is it?


Hardware

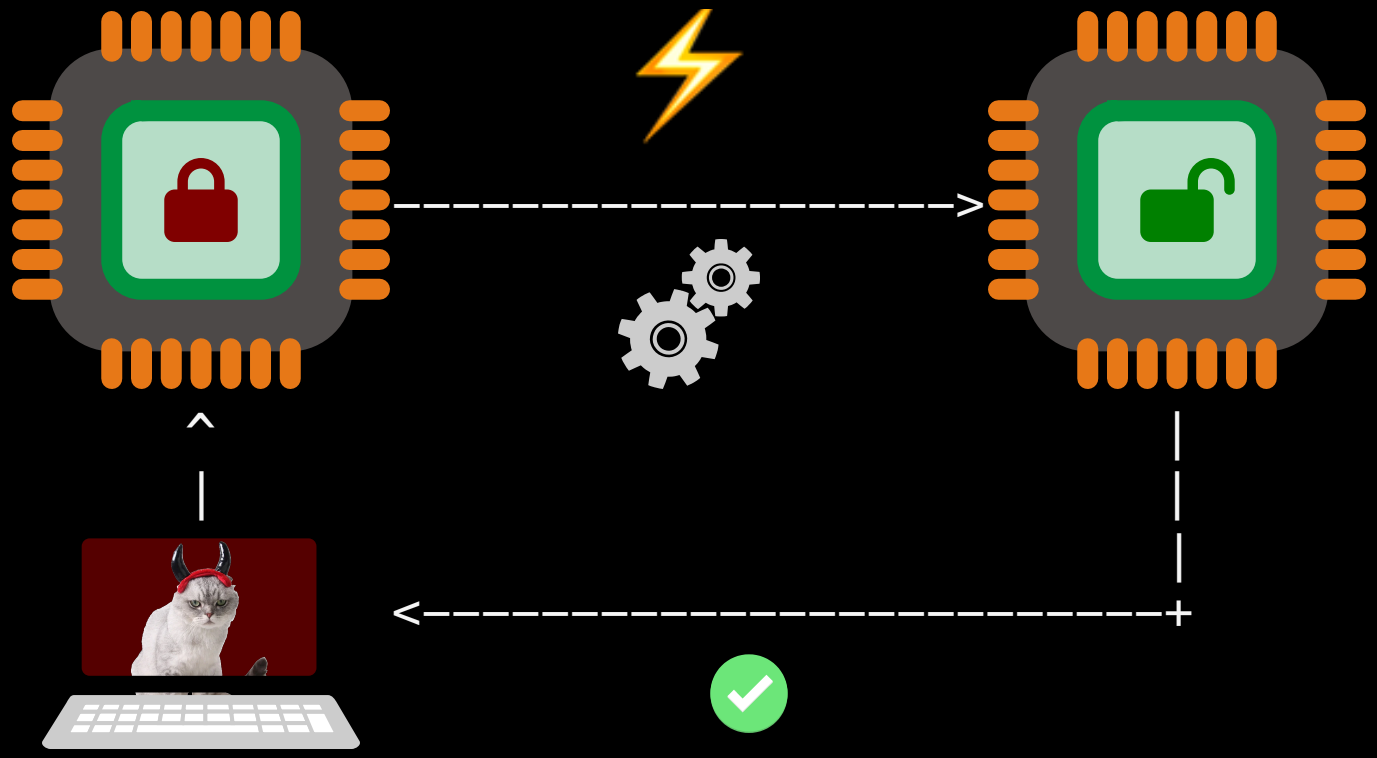

Physical perturbation


Process deflection

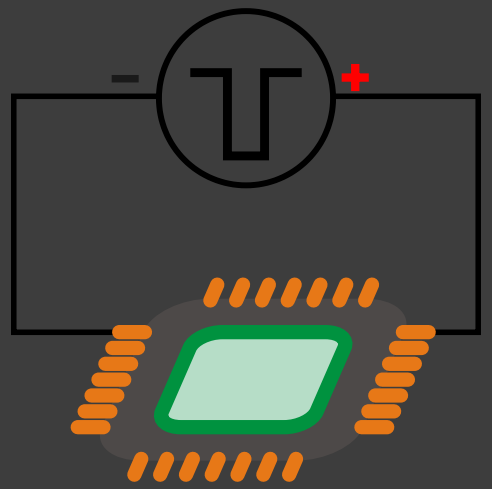
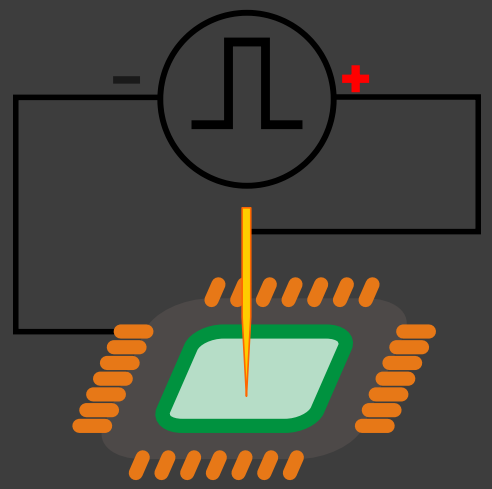
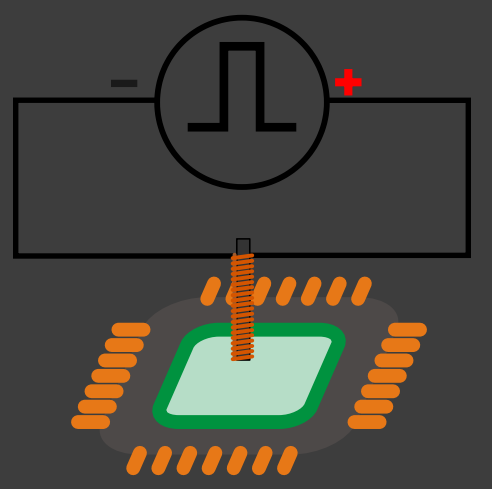
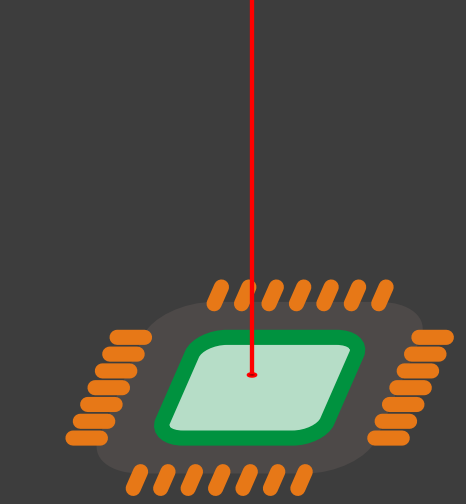
Unauthorized access



Unauthorized access - Faulted



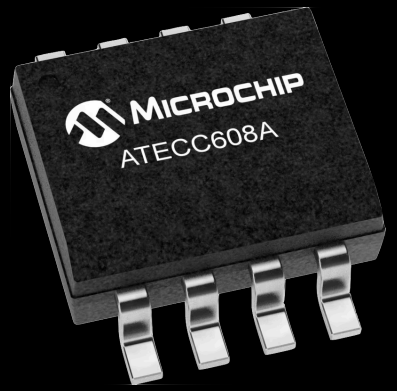
⚡ Physical perturbation types

Power glitch	FBBI	EMFI	Laser
Power cut	Voltage on the die	EM field	Illumination
			

Attack of the OneKey Mini

Laser on ATECC

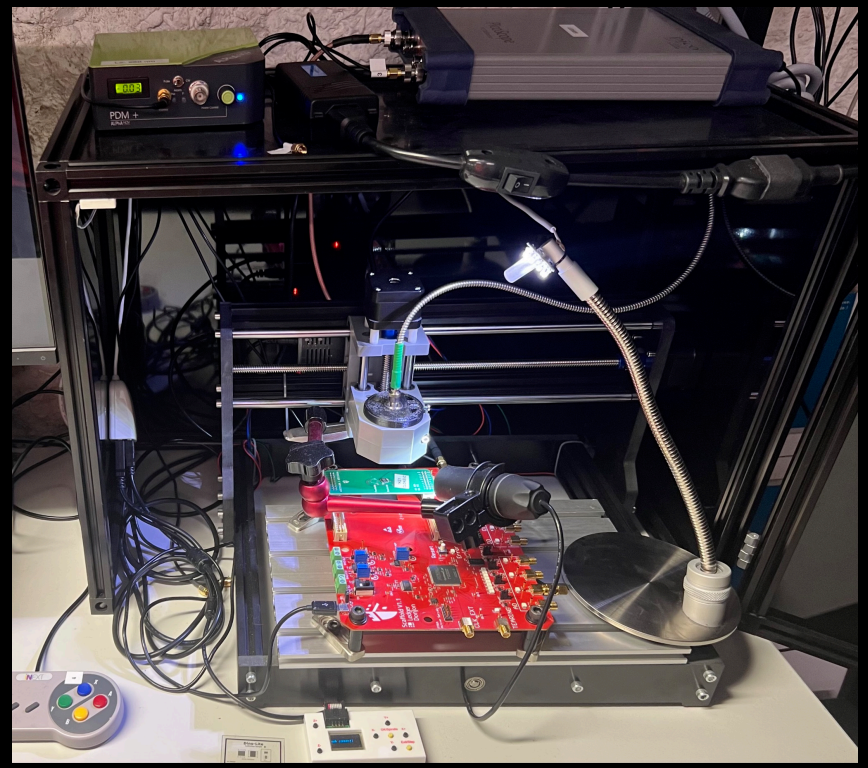
The Target Of Evaluation



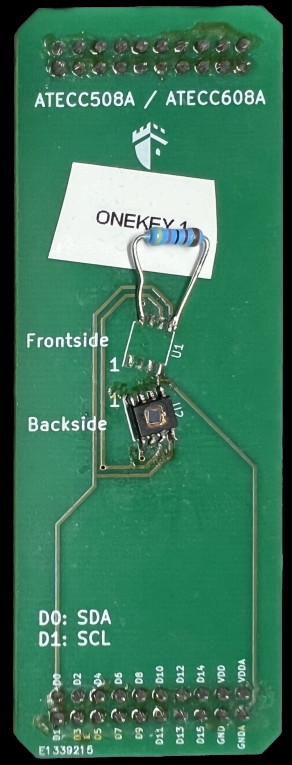
ATECC608A

One Key Mini

The Bench



Laser Bench



Daughter Board

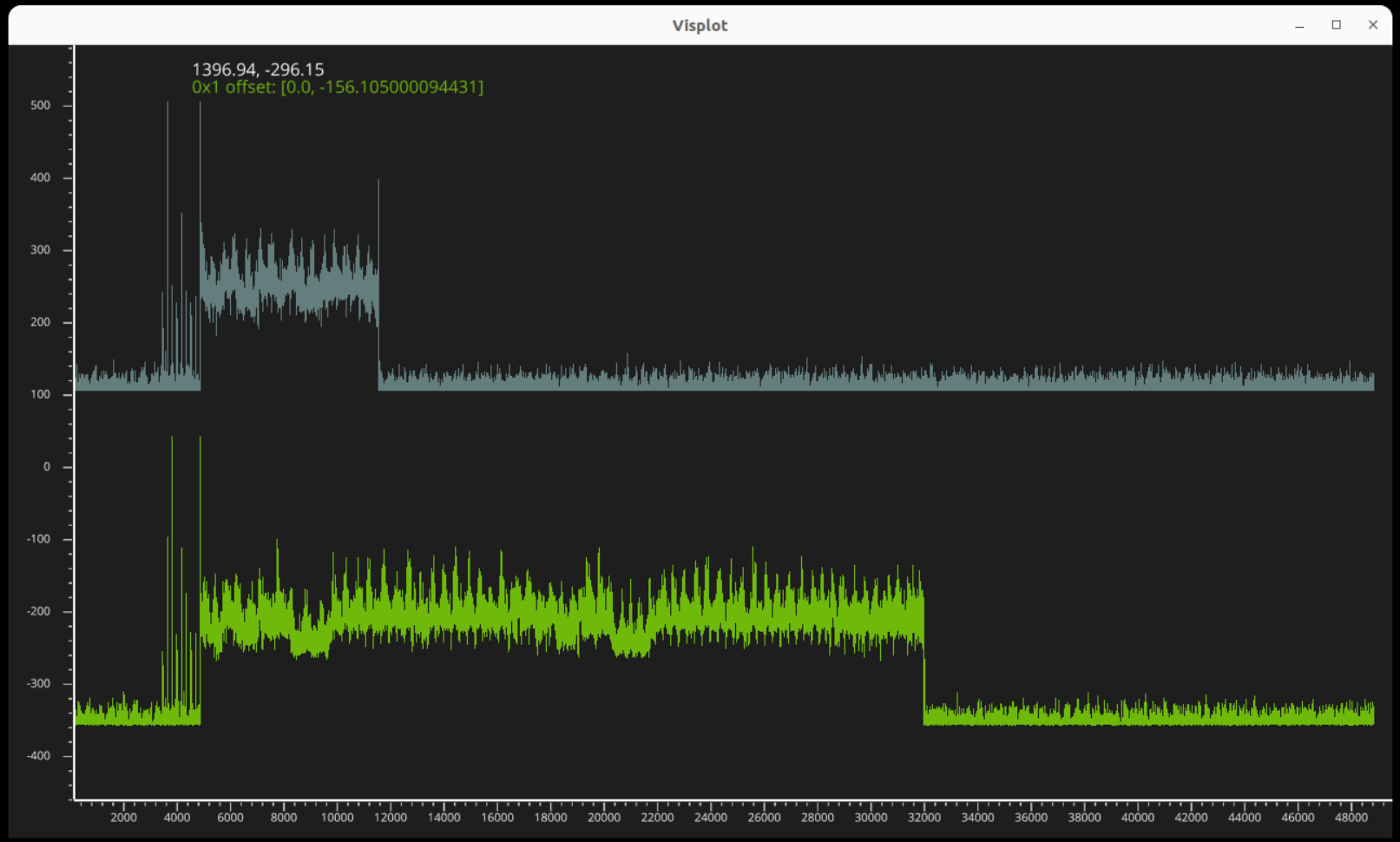
The Attack

```
# Authorized request
atecc.nonce()
atecc.gen_dig(1, atecc.KEY_SLOT1)
atecc.read(slot=6) ^ atecc.temp_key
# SUCCESS
```

```
# Unauthorized request
atecc.nonce()
atecc.gen_dig(14, atecc.KEY_SLOT14)
atecc.read(slot=6) ^ atecc.temp_key
# EXECUTION_ERROR
```

```
# Faulted request
atecc.nonce()
atecc.gen_dig(14, atecc.KEY_SLOT14)
atecc.read(slot=6, trigger=I2CTrigger.END.value) ^ atecc.temp_key
# EXECUTION_ERROR / TIMEOUT / SUCCESS / ...
```

The Attack



Unauthorized access

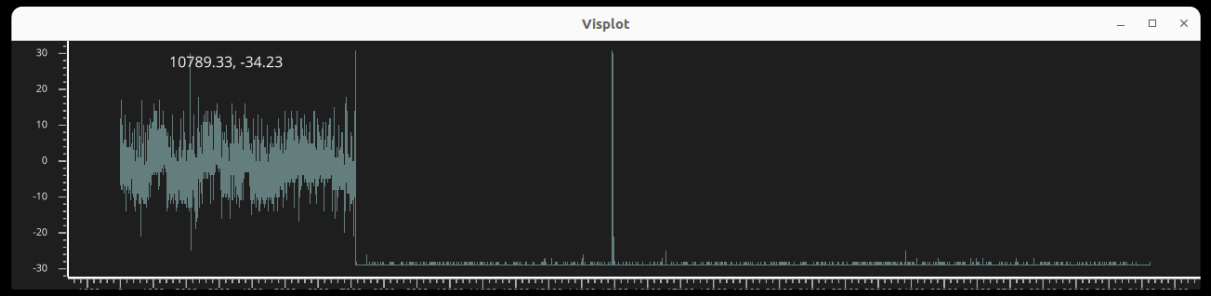
Authorized access

The Attack

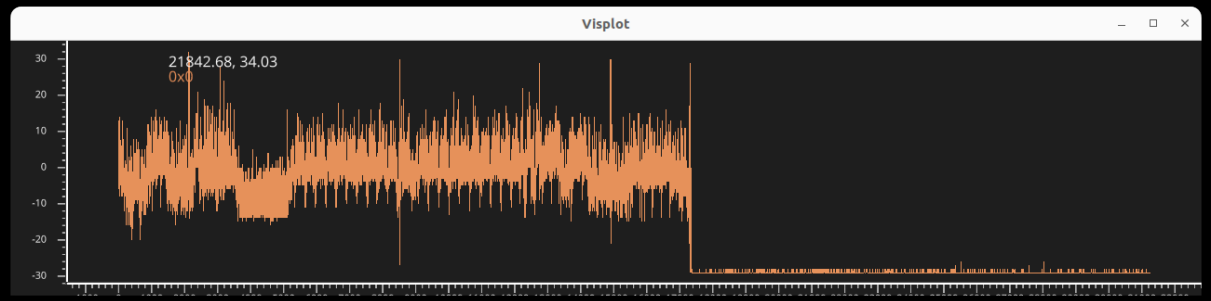
https://hardwear.io/archives/usa-2023/

Let's do it!

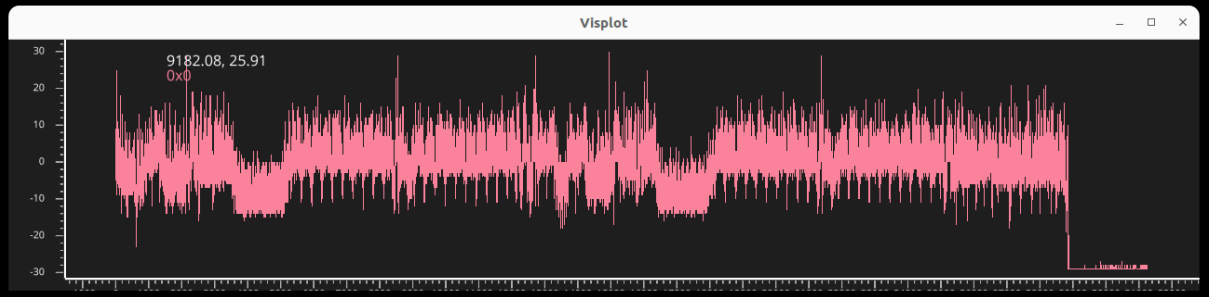
Perturbed executions



No perturbation



One perturbation



Two perturbations

Scan Result ~1 day execution

No effect: Transparent

SUCCESS

I2C Nack

Timeout

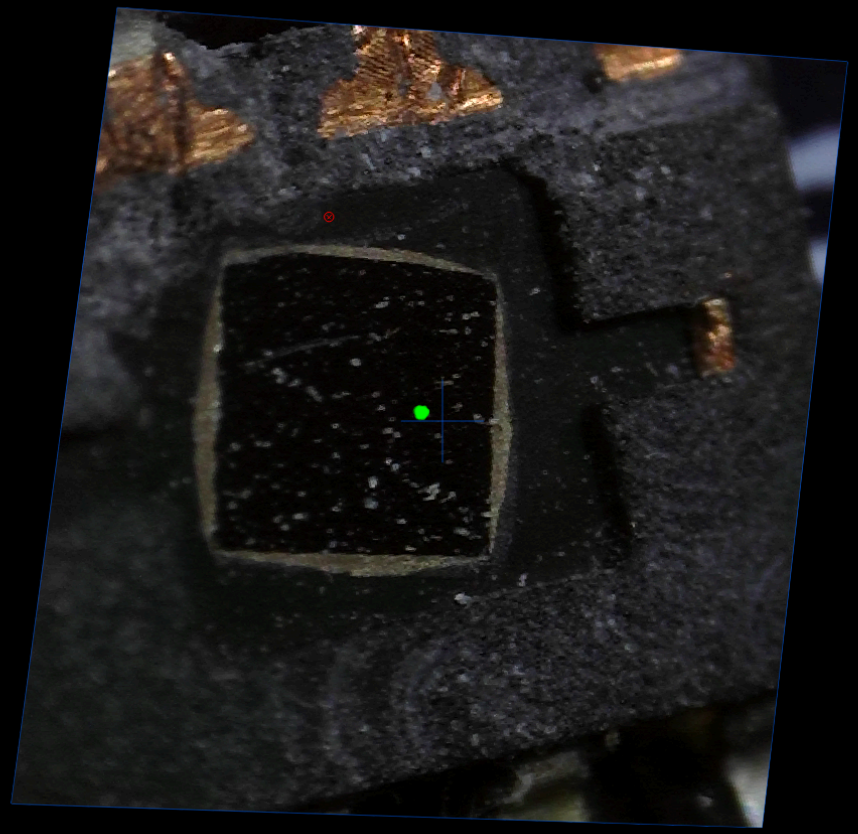
ECC_FAULT

AFTER_WAKE

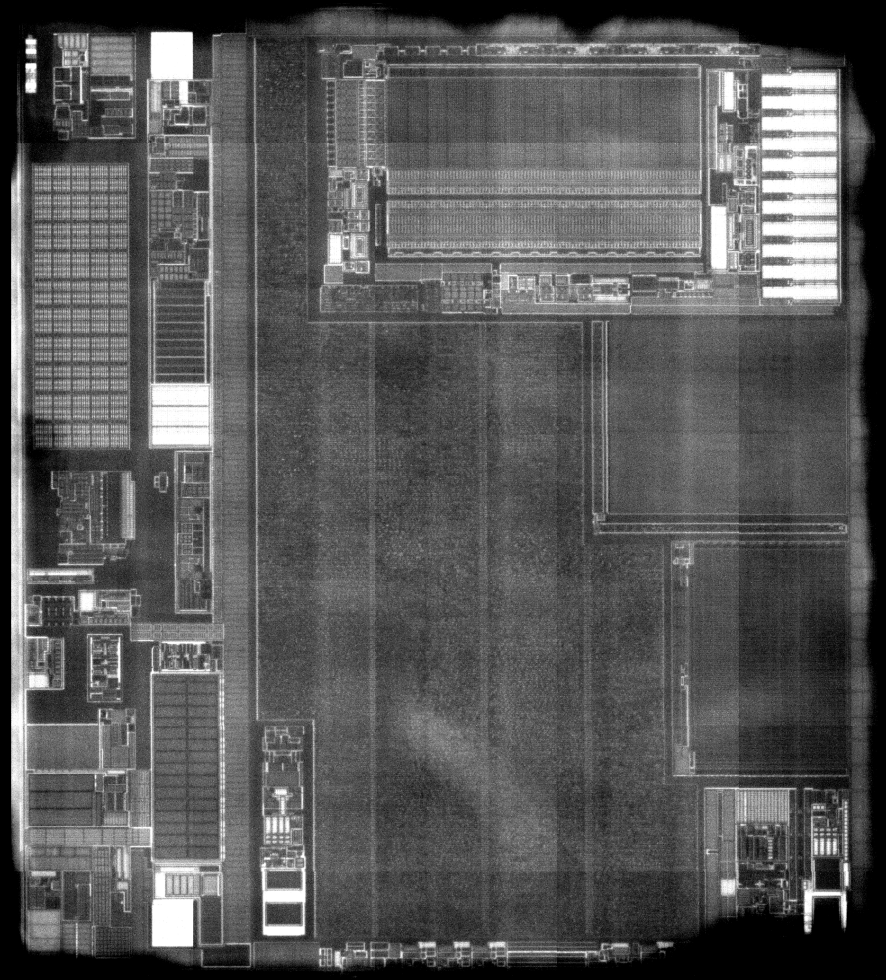
HEALTH_TEST_ERROR

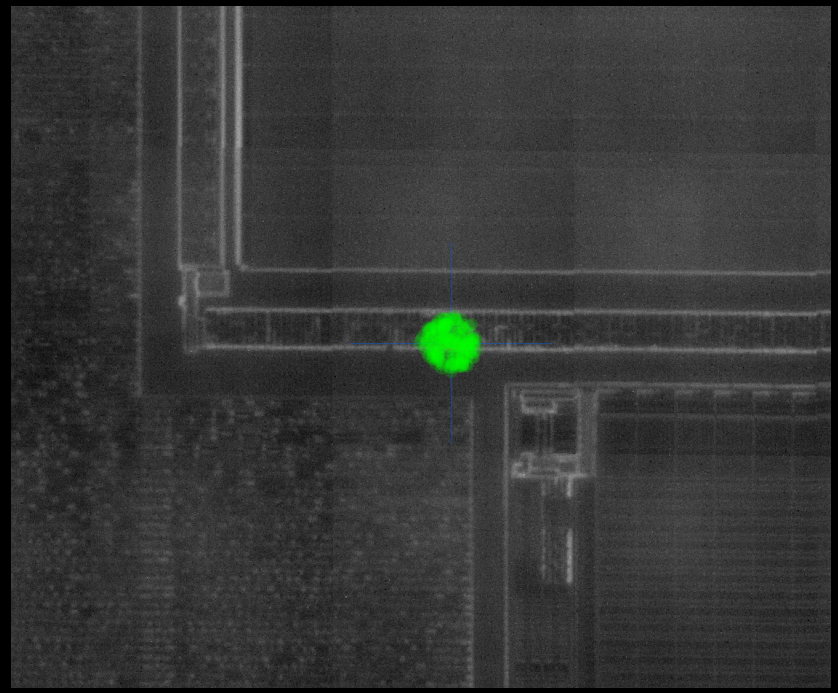
PARSE_ERROR

Scan Result ATECC608B / AES



Scan Result ATECC508A





Corrections and countermeasures

From the chip provider

Physical countermeasures

- Jitter
- Laser detectors
- Fault counting...

From the constructor

Implement a good configuration

- Lock all unecessary slots
- Use convenient features

Thank you for your attention

Questions?

https://donjon.ledger.com/enter-the-donjon-grehack24