Ledger

Keep it Cheap: Multiple Faults Attacks in Practice

Karim Abdellatif and Olivier Hériveaux

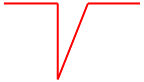
Karim.abdellatif,olivier.heriveaux@ledger.fr

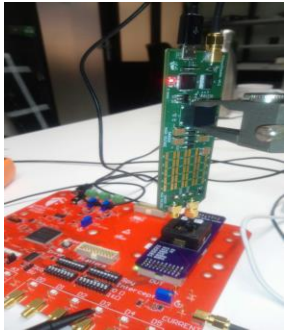
Goals

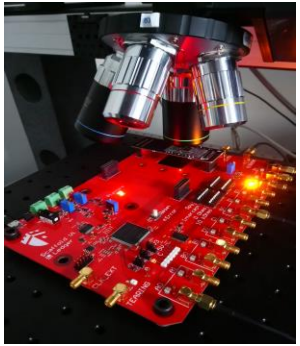
- Building homemade tools for injecting faults
- Considering low cost components
- Validation on IoT chips

Fault Injection in Donjon

- Clock Glitch
- Power Glitch
- Electromagnetic
- Laser







Agenda

- Why Multiple Fault Attacks?
- Low cost synchronization
- Power glitch setup
- EM setup
- Conclusion

Why Multiple Fault Attacks?

Practical example

- **An IoT chip has three different configuration modes**
  - **A**: No security feature is activated
  - **B**: Bootloader is enabled, but commands used to read and write memory are disabled
  - **C**: All the security features for IP protection are enabled
- **The goal is to convert the configuration from C to A to dump the firmware (memory)**

Plan

Algorithm 1: Attack sequence of C configuration

```
while True do
    Initialize-Fault(parameters);
    uart.transmit(X, trigger=1);
    if (uart.receive=ACCEPT) then
        Go to B configuration attack;
```

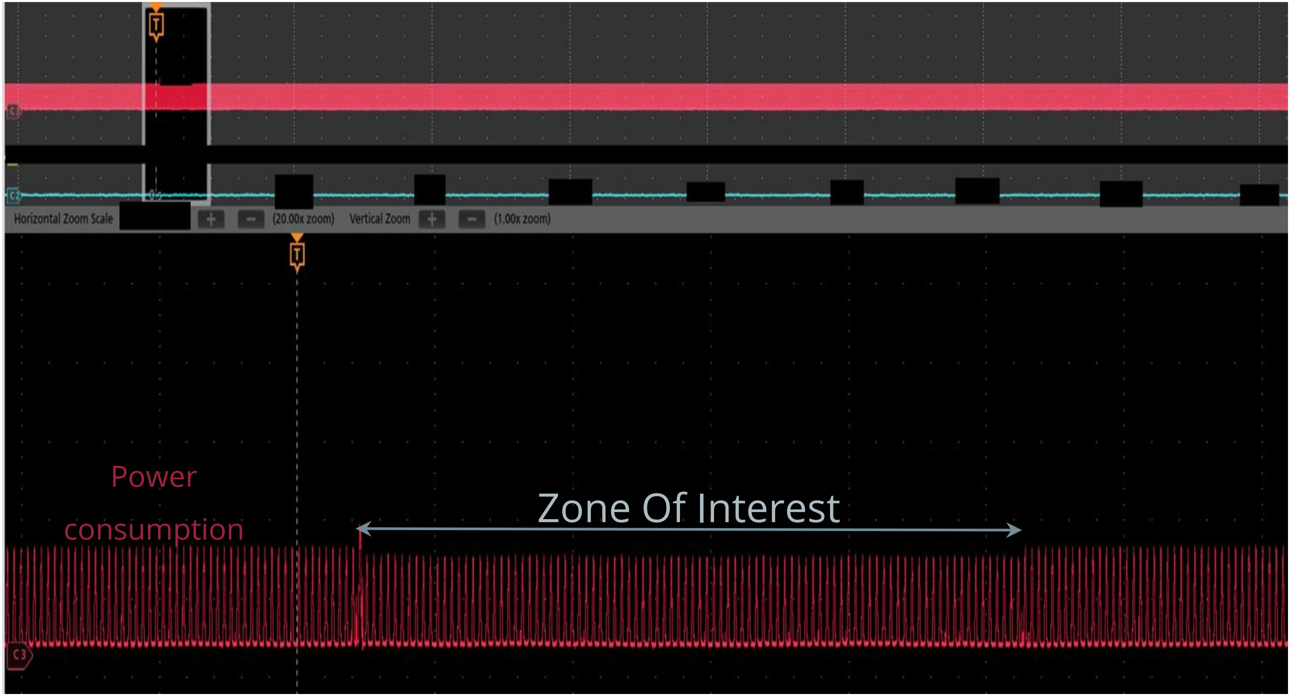
Algorithm 2: Attack sequence of B configuration

```
Initialize-Fault(parameters);
Read Memory Content (trigger=1, address, number of
  bytes);
if (uart.receive=ACCEPT) then
    Data=uart.receive(number of bytes);
else
    Data=None;
```

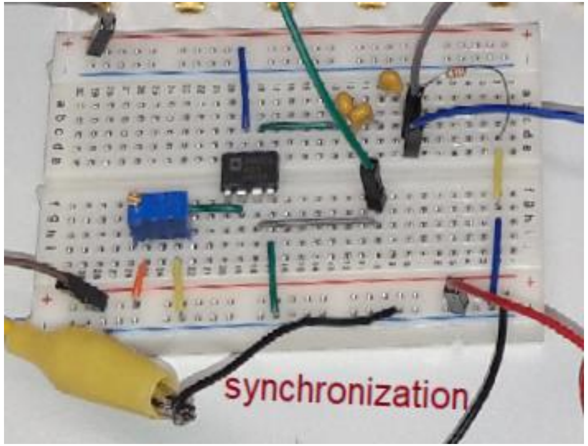
To dump the memory: Two fault attacks (or more) must be chained!

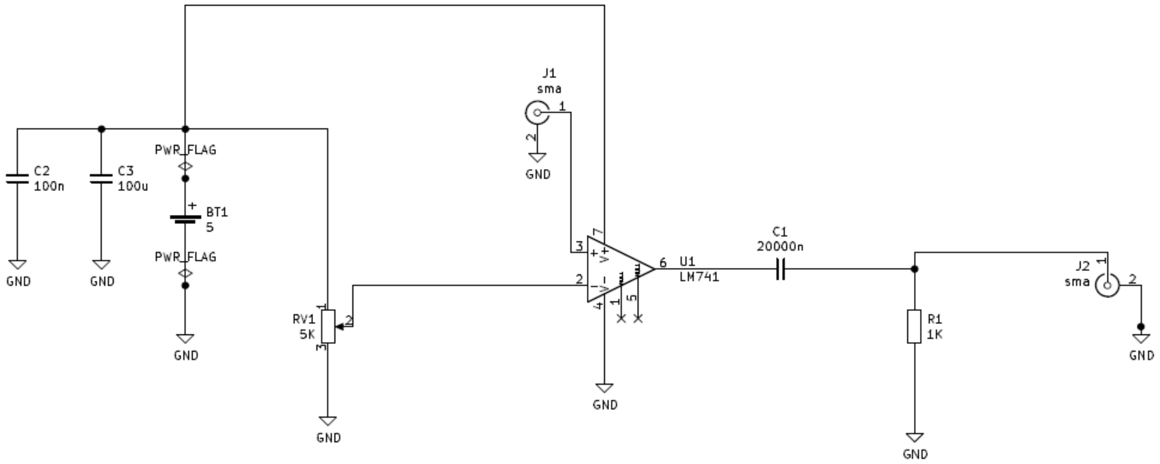
Low Cost Synchronization

Example: Configuration B

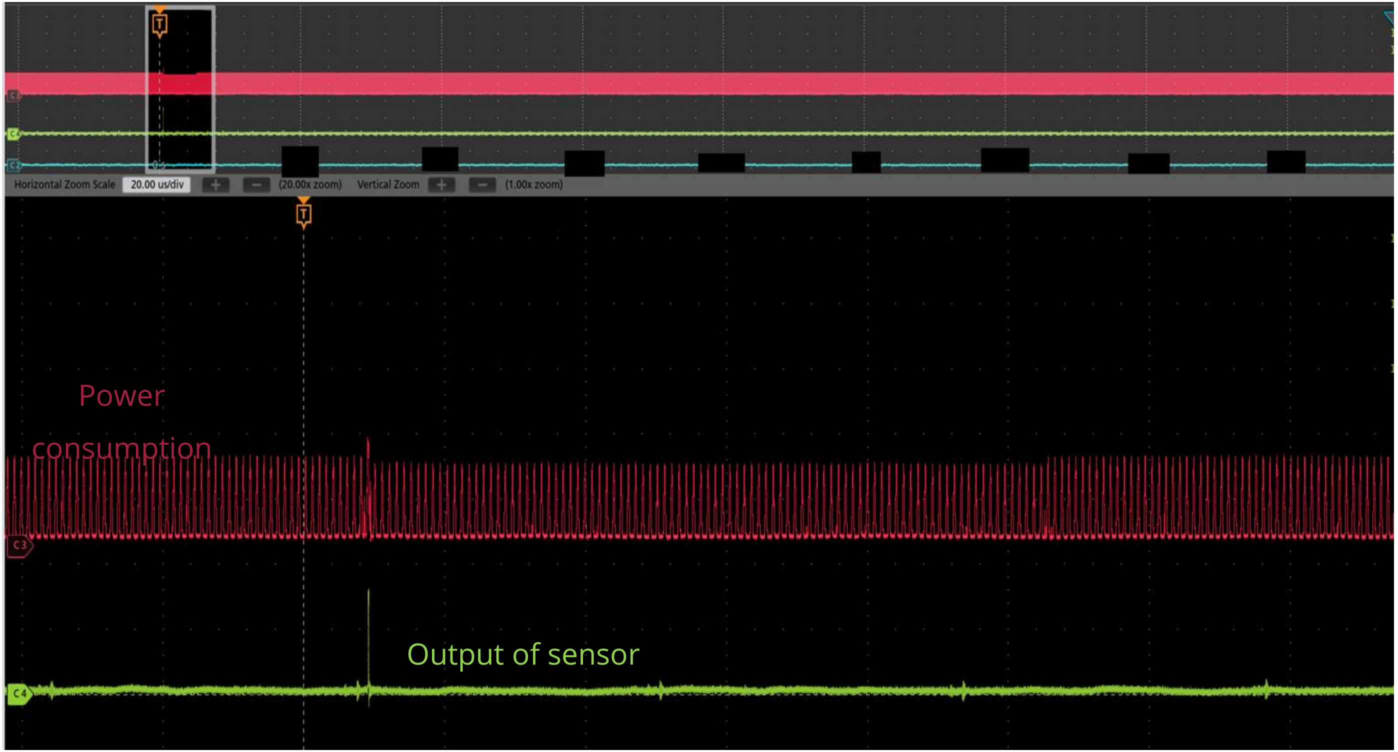


Analog sensor

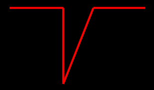




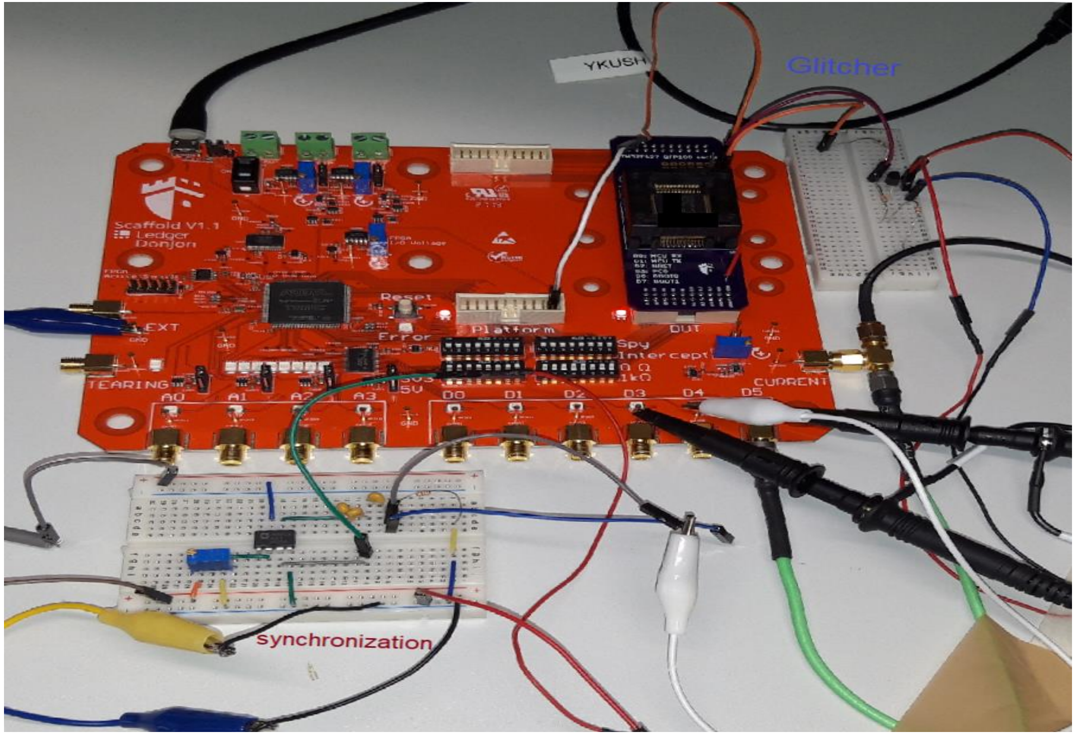
Synchronization



Power Glitch

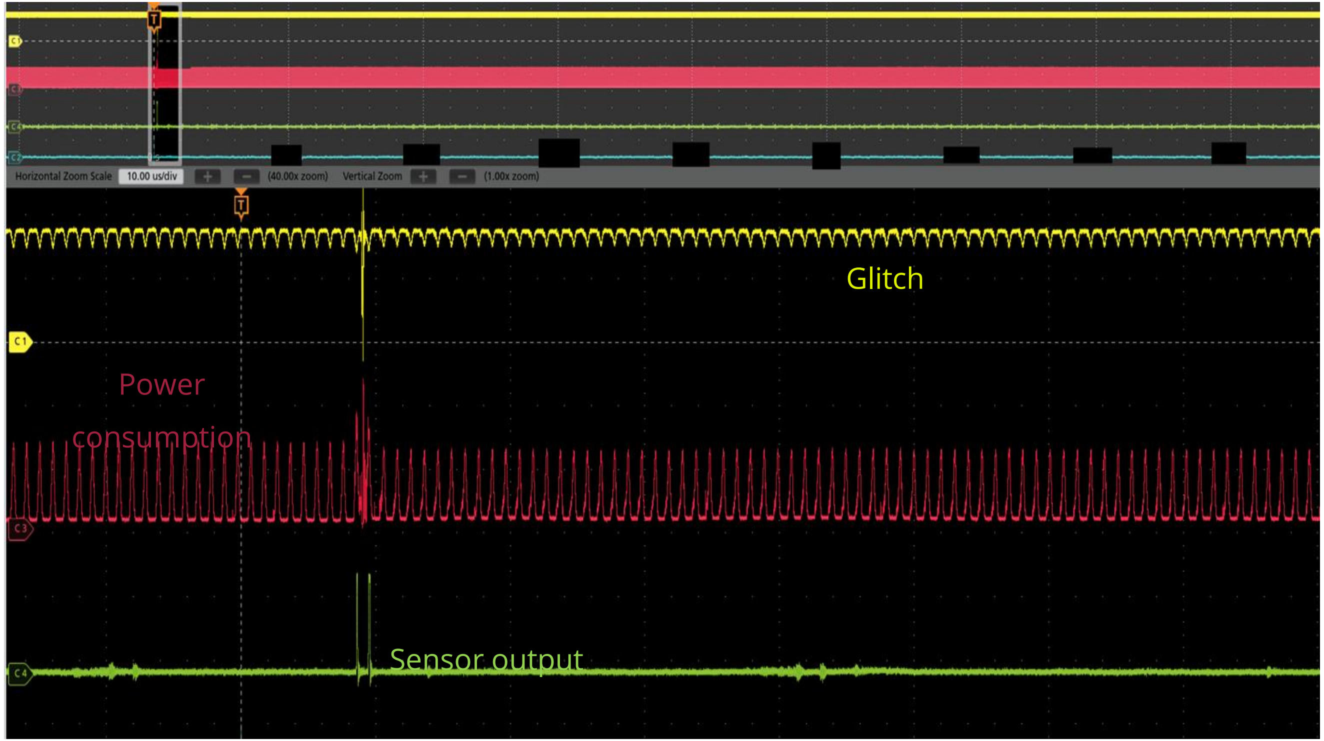


Setup

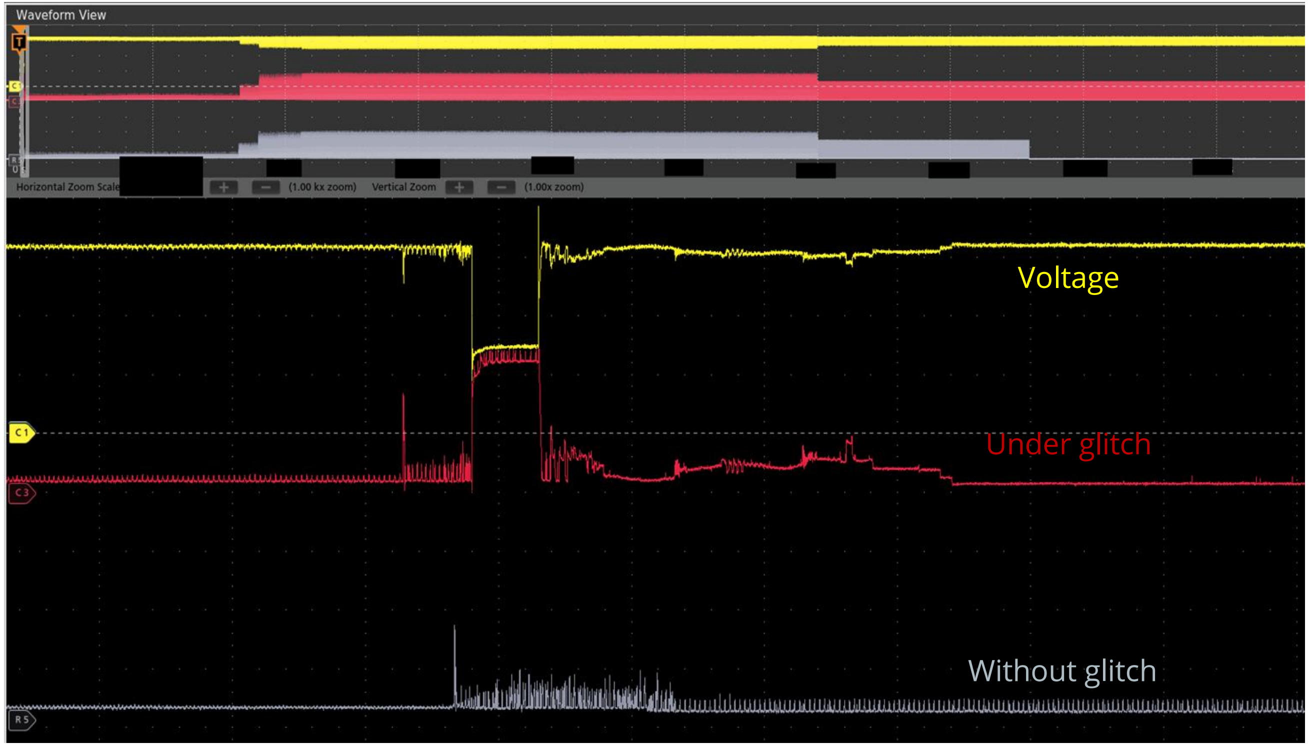


Scaffold: https://github.com/Ledger-Donjon/scaffold

B configuration (Successful attack)

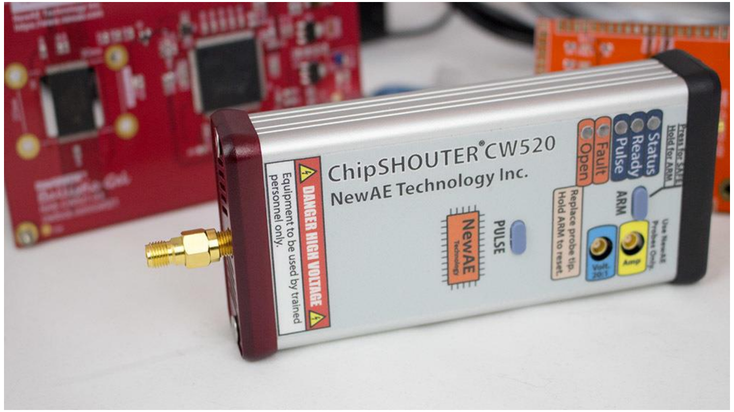


C configuration (Successful attack)



Low Cost EM Setup: SiliconToaster [FDTC-2020]

Commercial Tools



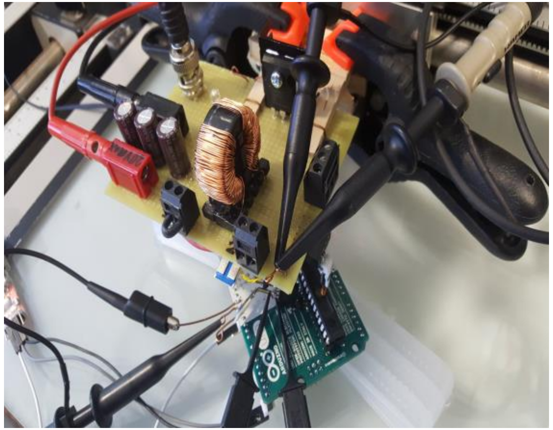
ChipSHOUTER, $3300 USD
(NewAe)

ChipSHOUTER: http://store.newae.com/chipshouter-kit/

Setups from Academia

Ordas et al. (FDTC 2015)

Cui et al. (USENIX 2017)



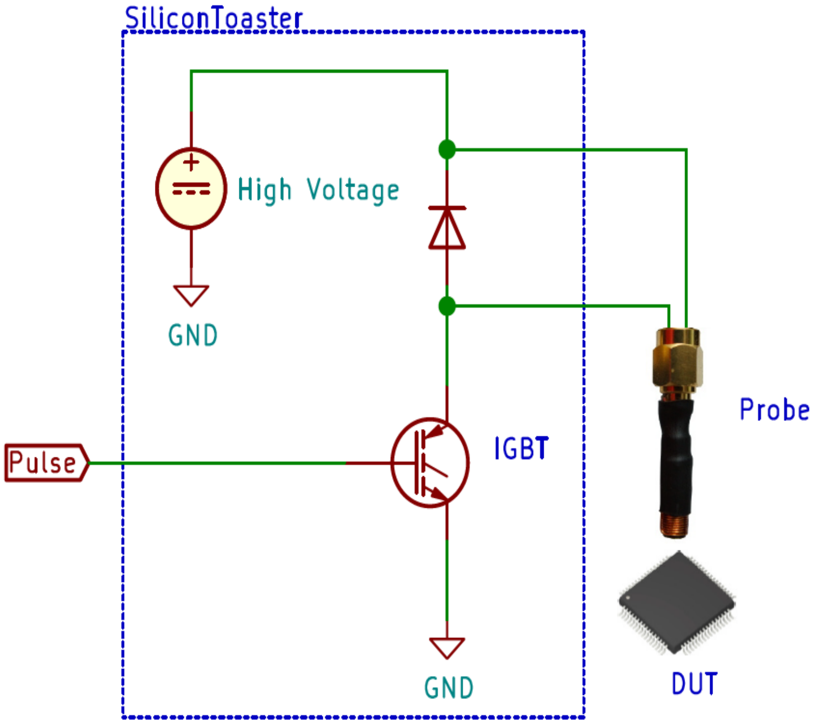
Balasch et al. (DCIS 2017)

- **Commercial** pulse generator

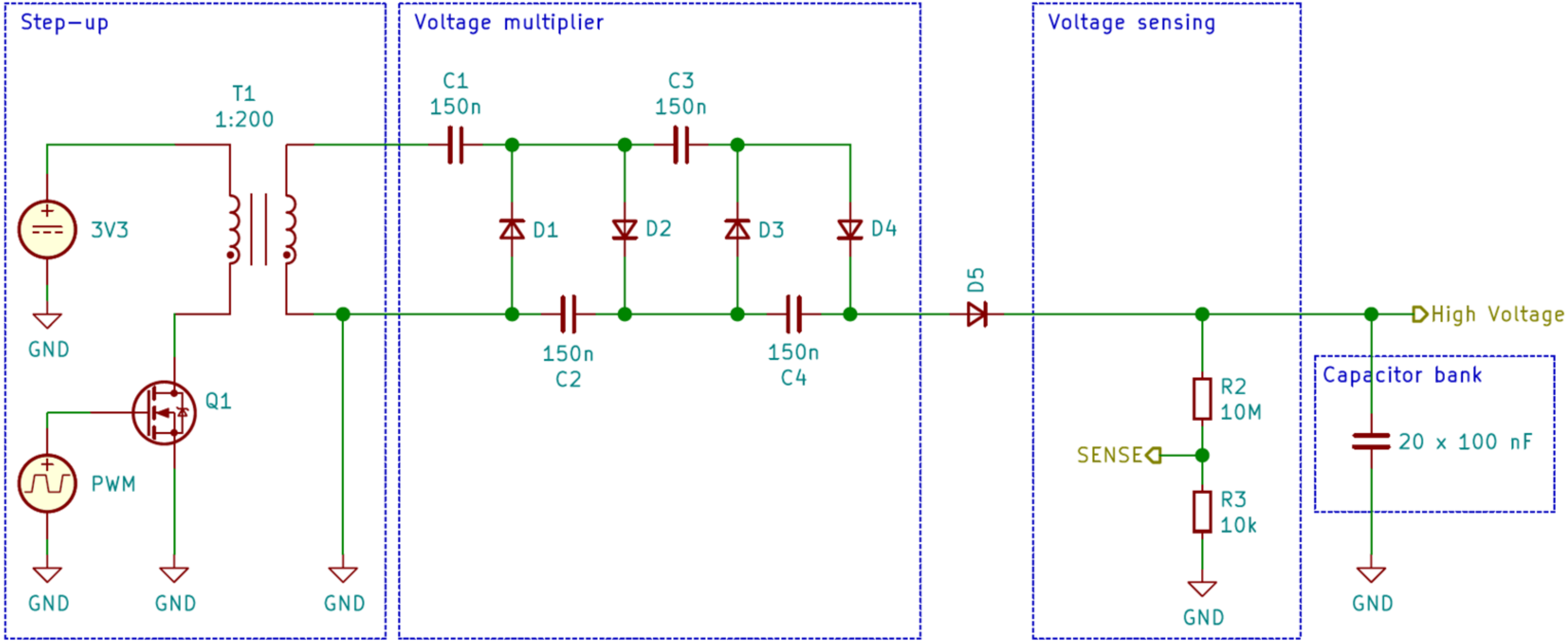
- Hand-made pulse generator with **fixed voltage**
- **External power** supply to feed the pulse generator

SiliconToaster

- Programmable high voltage generation up to 1.2KV
- High voltage switching circuit
- Probe fabrication

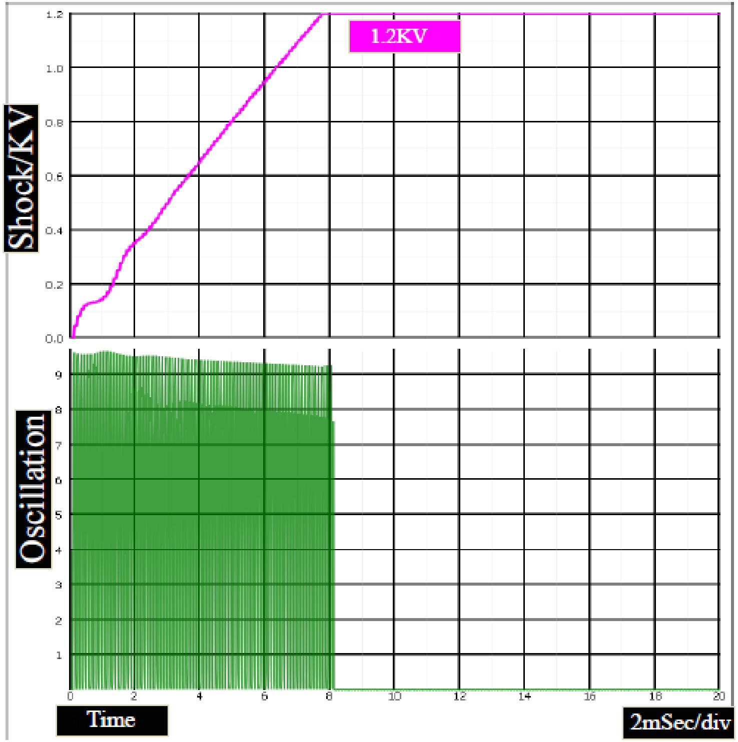


High Voltage Generator

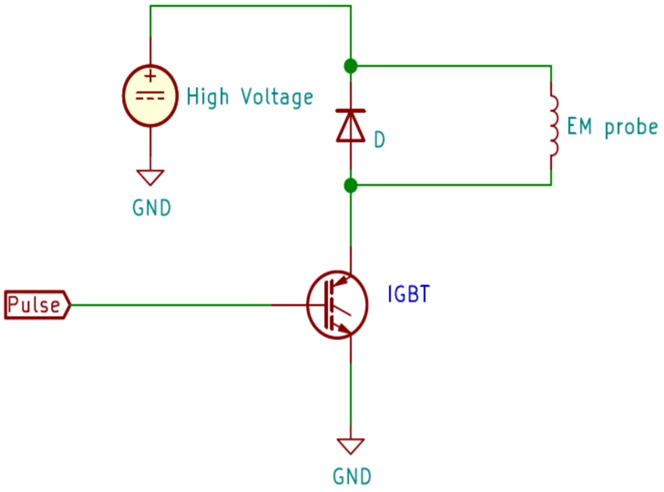


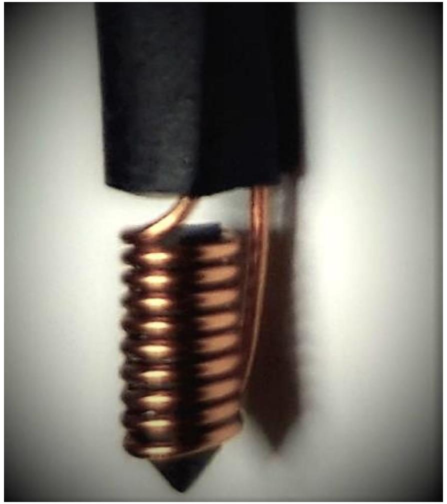
Programmable Voltage

- The generated high voltage depends on several parameters such as:
  - Number of pulses
  - Frequency of the input pulses
  - Pulse width
- With 8ms of pulses and frequency of 10KHZ, the output voltage is 1.2kV



High Voltage Switching circuit + Probe fabrication

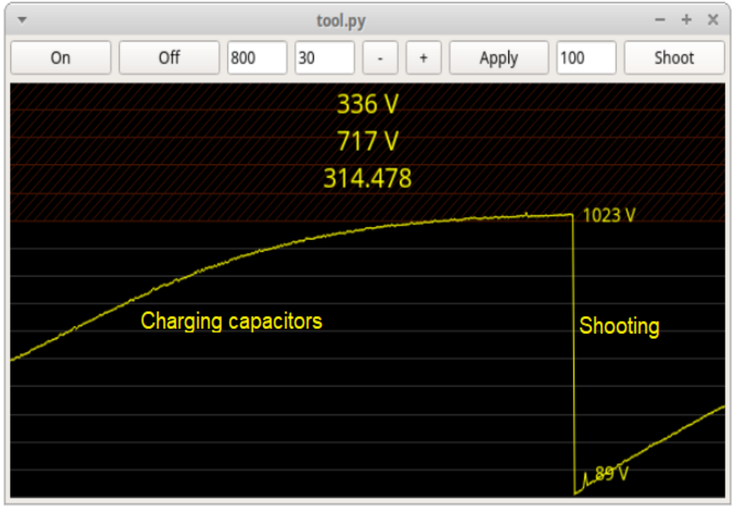


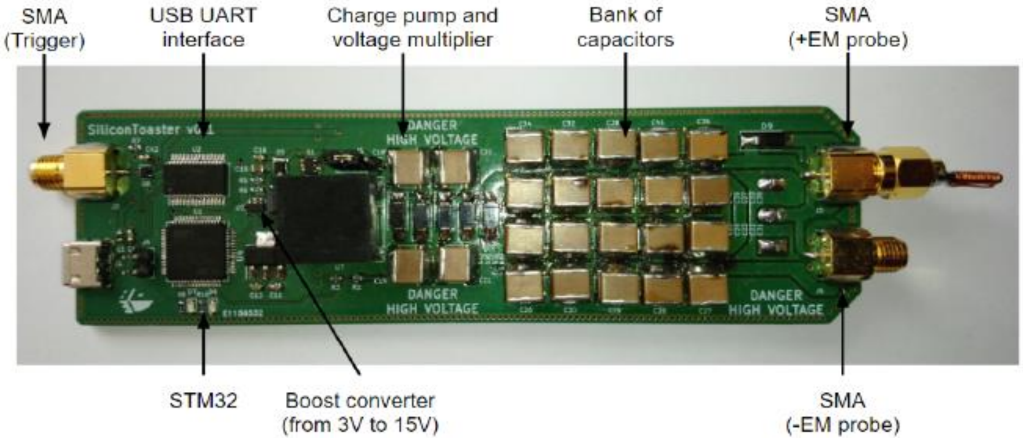


- IGBT: maximum ratings are 1.2kV collector-emitter voltage, 40A pulsed current and 20V gate-to-emitter voltage

- Fabricated from a flat coil of 6.6 mm diameter with 9 turns

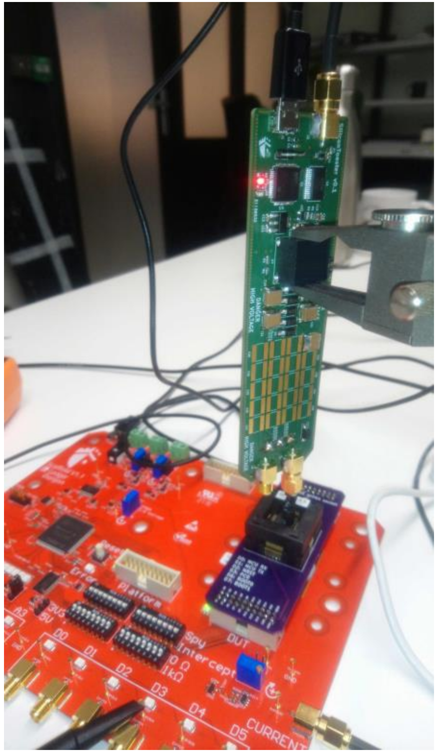
Final Model + GUI



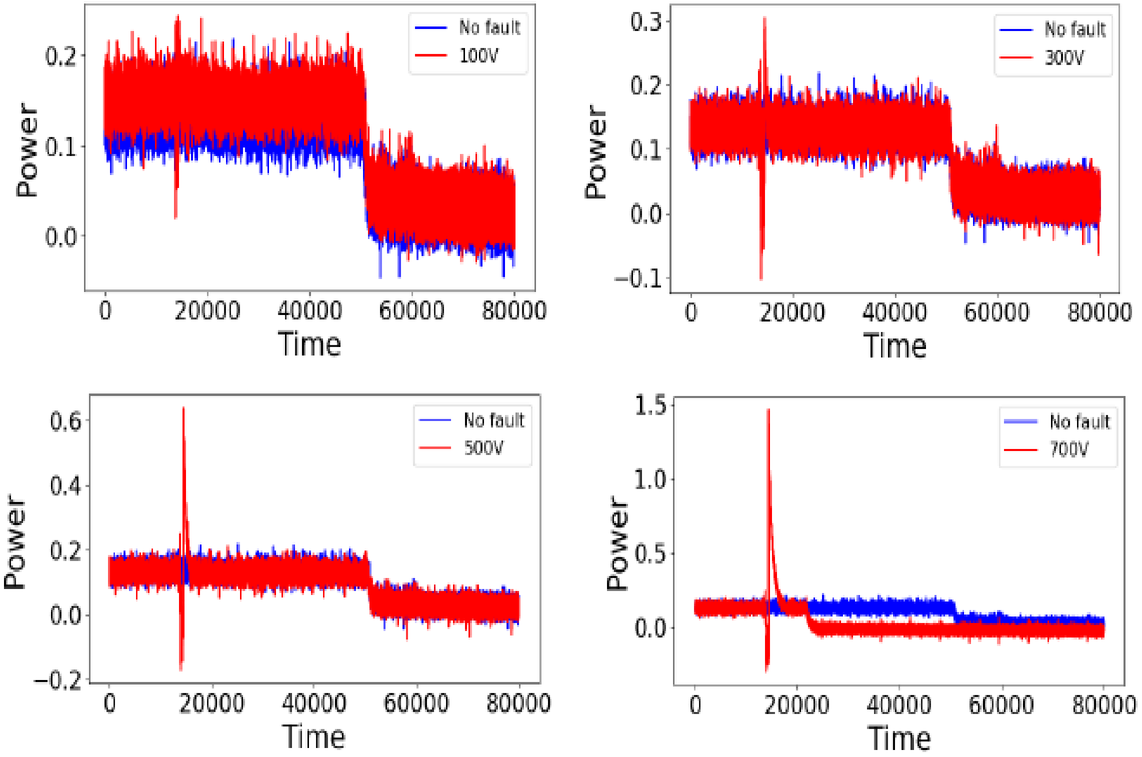


Setup

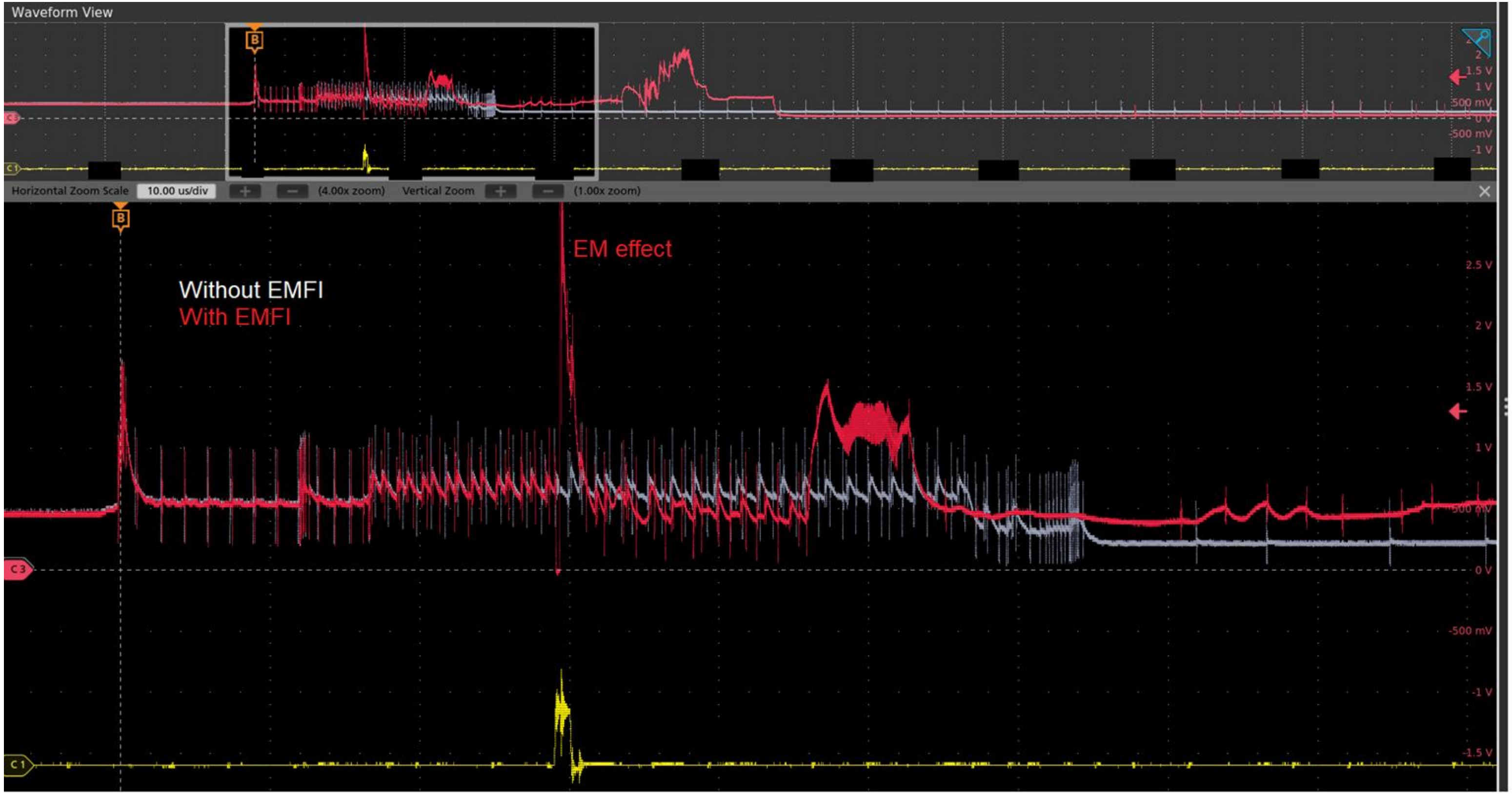
- The DUT was placed in a custom board socket
- **SiliconToaster** is used for injecting EM pulses to bypass the security configuration modes
- **Scaffold** board is also used to communicate with the DUT



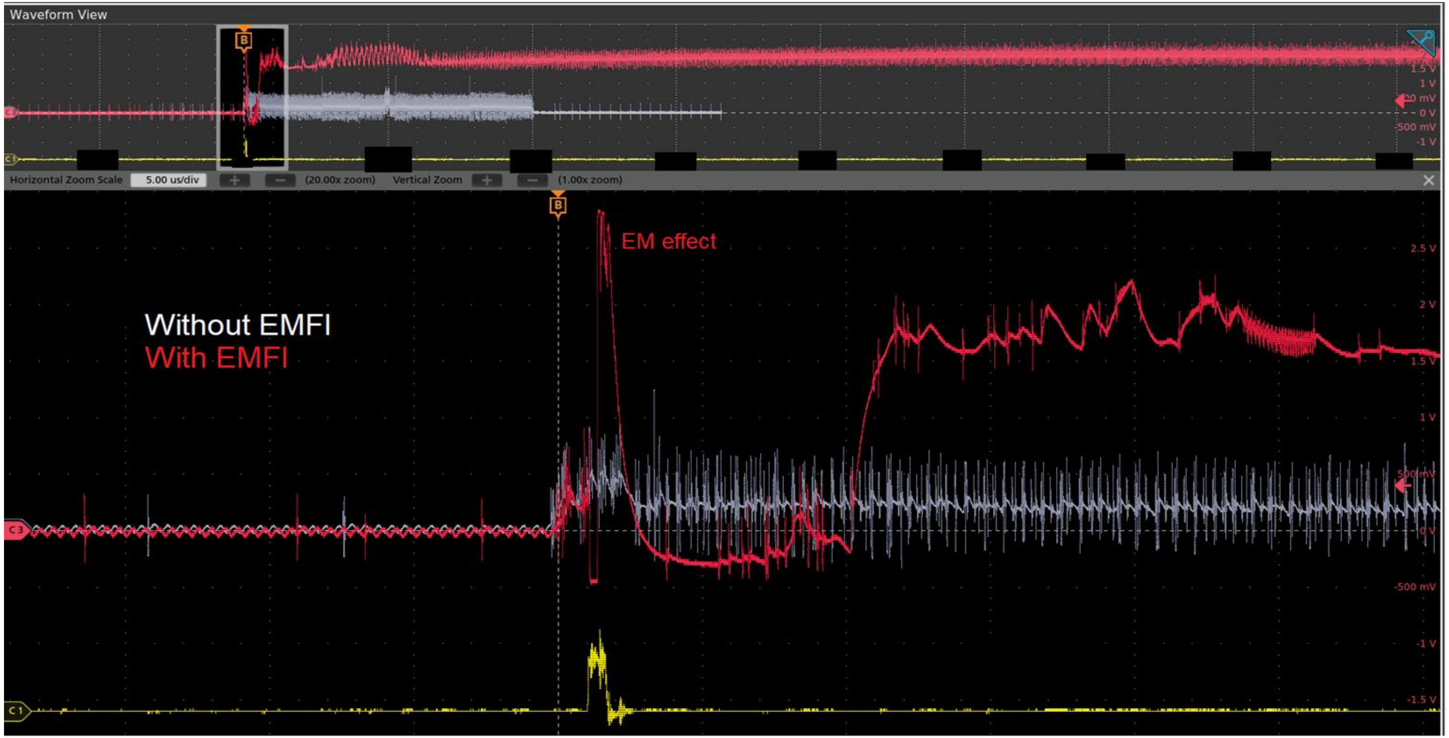
Programmable EM Pulse



C Configuration Attack: 400V + Success= 60%

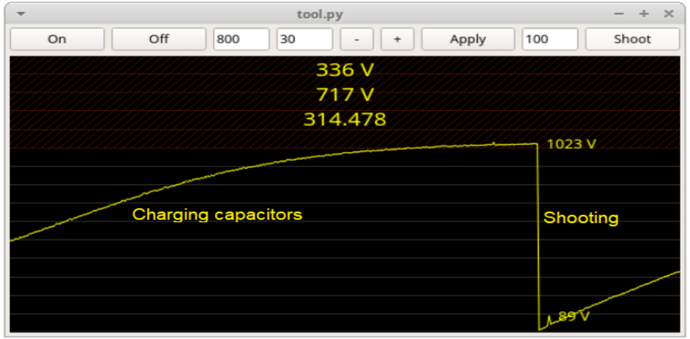


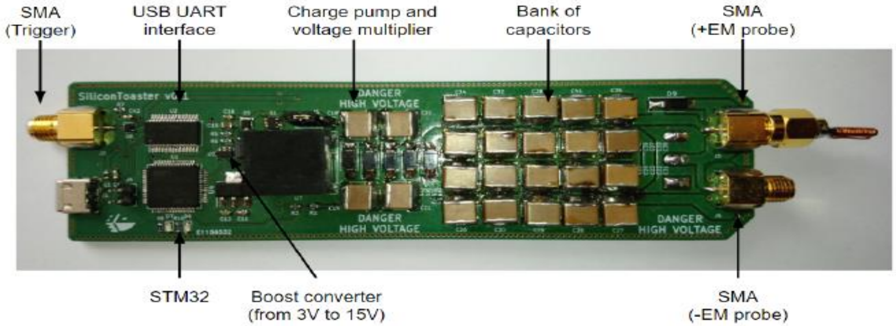
B configuration Attack: 400V + Success= 30%



Comparison with previous work

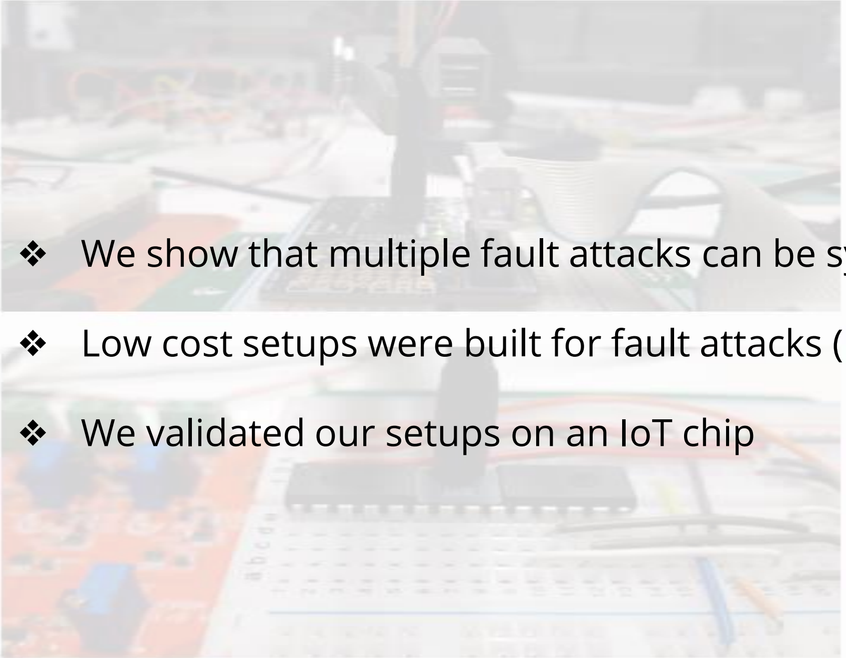
Design	EM voltage	Power supply	Visibility	Polarity
SiliconToaster	Programmable	USB-powered	GUI	Two SMA
USENIX 2017 + DCIS 2017	Fixed	External power supply	No	Another probe needed

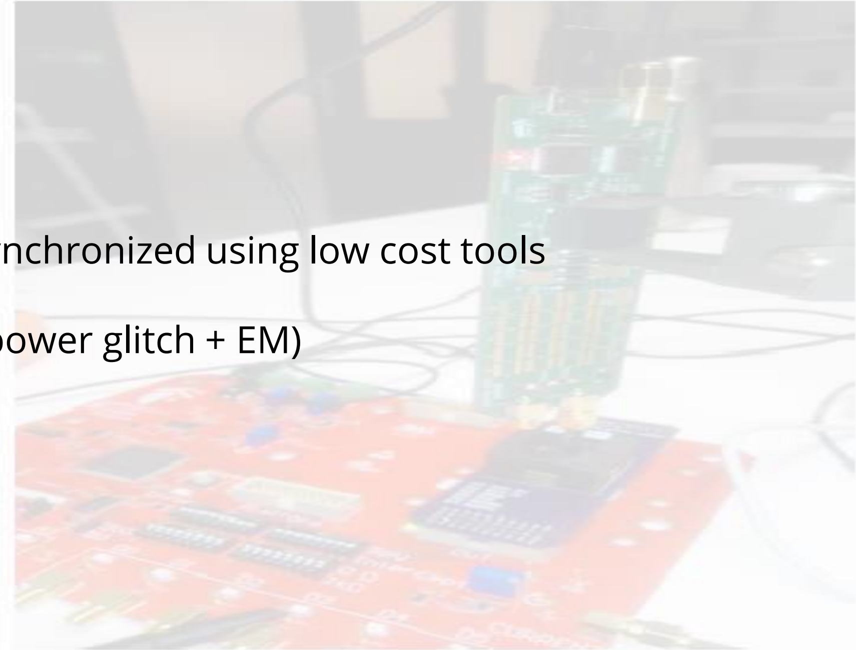




Conclusion

Conclusion





- ❖ We show that multiple fault attacks can be synchronized using low cost tools
- ❖ Low cost setups were built for fault attacks (power glitch + EM)
- ❖ We validated our setups on an IoT chip

Questions?