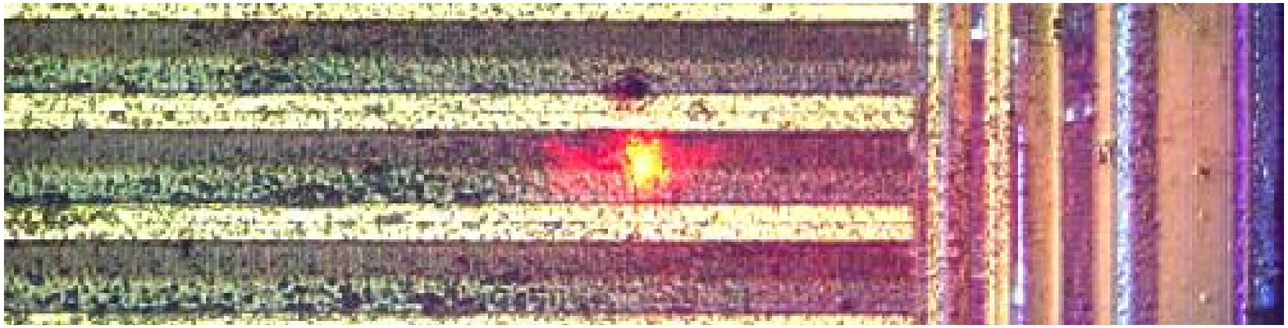
Practical optical fault injection on secure microcontrollers



Jasper G. J. van Woudenberg
Marc F. Witteman
Federico Menarini

FDTC2011, 28-9-2011

This talk

- About…
- Contribution: develop specialized hardware to overcome previous higher order optical fault injection limitations
  - High fault injection repetition rate
  - Trigger synchronization to process
- Experiment 1: stable double-fault attack
- Experiment 2: pattern-based trigger synchronization
- Future: triple fault attacks, multi-location attacks
- Conclusion

Riscure Profile

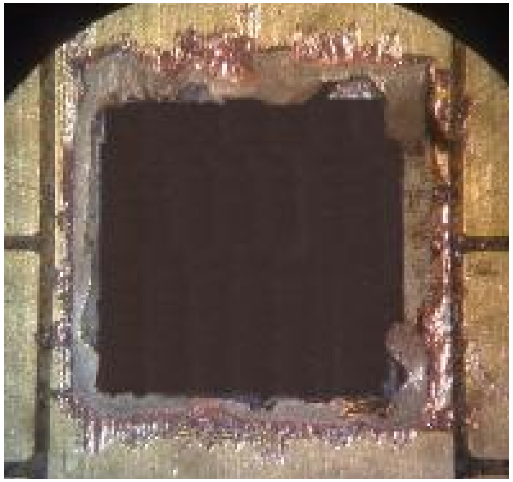
- Founded in 2001
- Based in Delft, the Netherlands and San Mateo, California
- Clients in North America, Europe and Asia
- **EMVco lab** accredited
  - Not a CC lab!
- Market leader in **side channel test tools**
- Pay TV, smart card, mobile payment, smart metering

Motivation

- Fault injection is the science (art?) of manipulating a device such that security mechanisms can be circumvented
- State-of-the-art smart cards come with FI Countermeasures
- Injecting faults multiple times can defeat those countermeasures
  - Mandatory requirement by EMVco and CC since 2011
  - Accurate control (timing, power) is very important
- Few publications of these attacks in practice using state-of-the-art tools

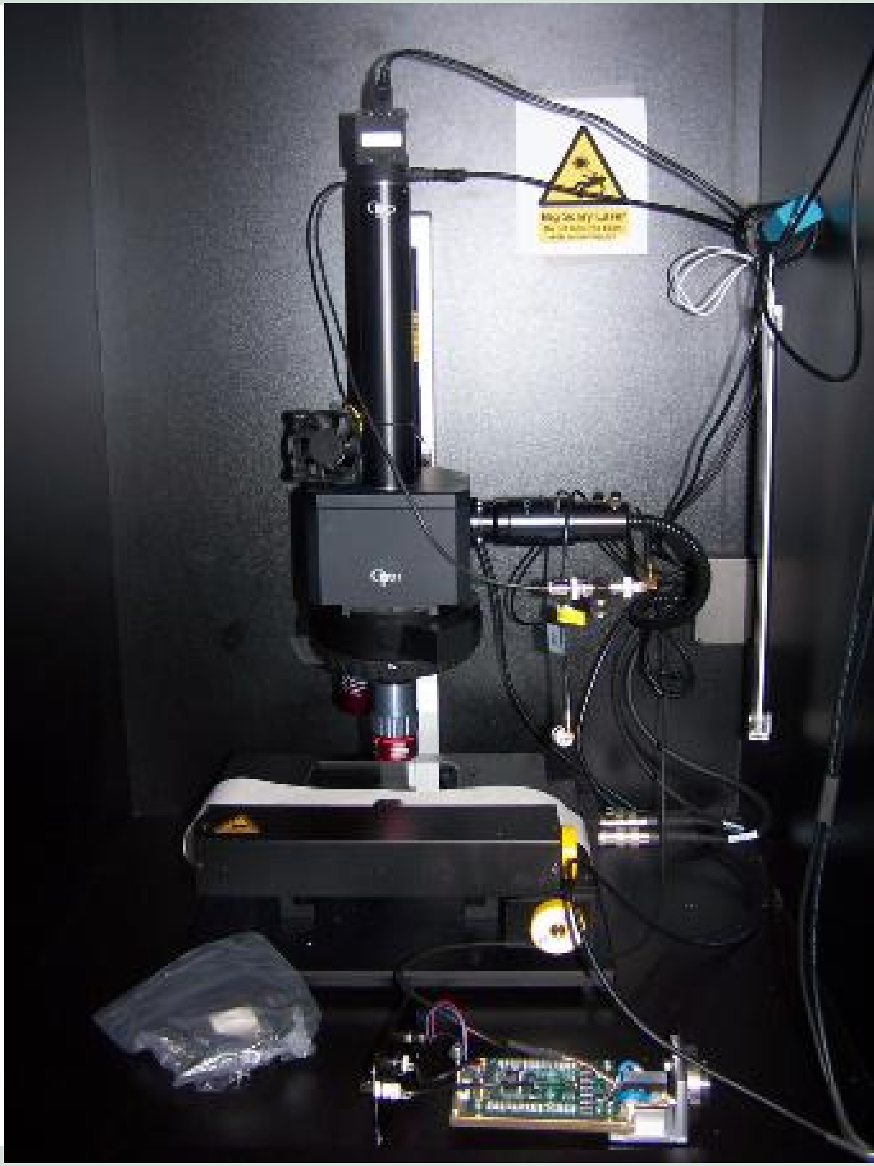
Experiments card 1

- Only main CPU, clocked externally at 1MHz
- Only countermeasure: double PIN verification
- Goal: skip both PIN verifications
- Approach:
  - Back side
  - Find sensitive location on chip
  - Find correct timing
- Show dual fault repeatability



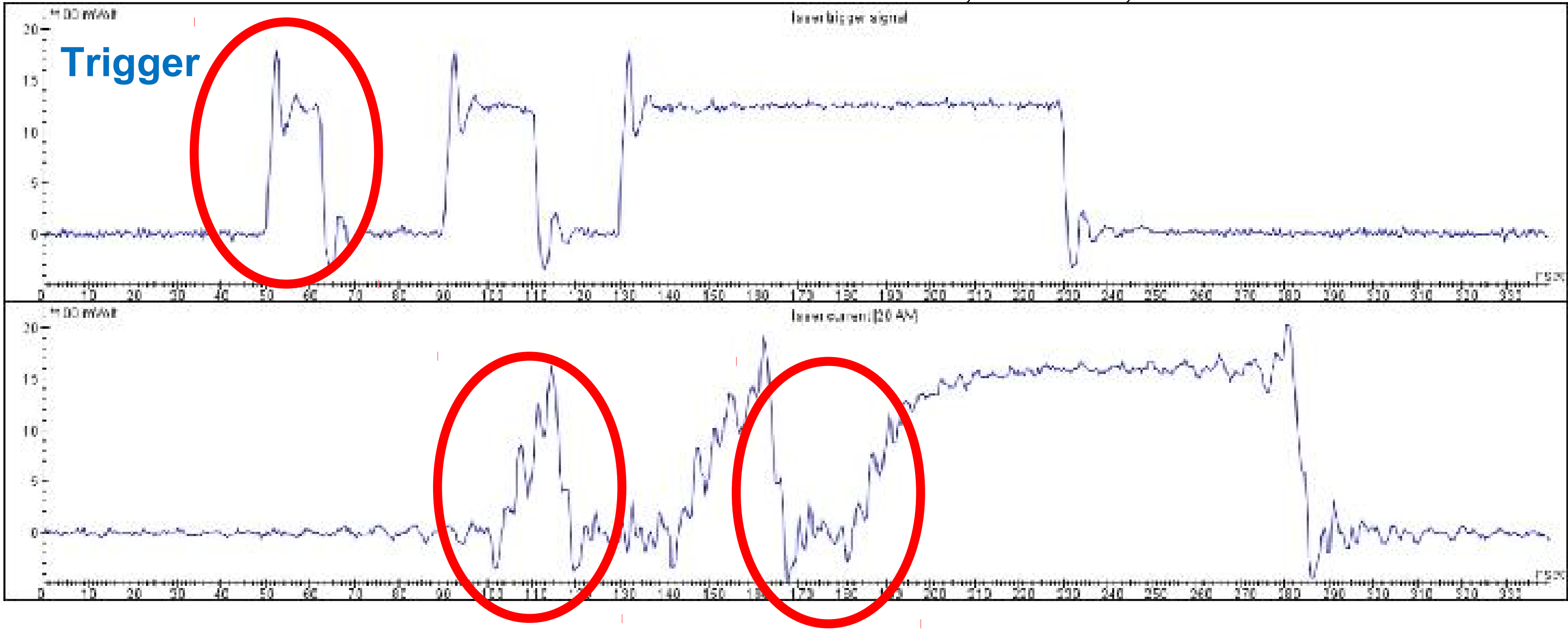
Optical setup used

- Multimode diode lasers
  - 808nm: 14W
  - 1064nm: 20W
  - Pulse freq: 25 MHz ~ 40ns
  - 50ns trigger delay
- XY stage
- FPGA-based target control & trigger with 2ns time resolution
- FPGA-based real-time pattern matcher
- Oscilloscope
- Control software (Inspector)



Laser trigger response

- Diode lasers: constant delay, high repetition rate, arbitrary pulse length and power modulation
  - YAG: 200ms to recharge fully (can be shortened for less power)
  - *Multi Fault Laser Attacks on Protected CRT-RSA, E Trichina, FDTC 2010*

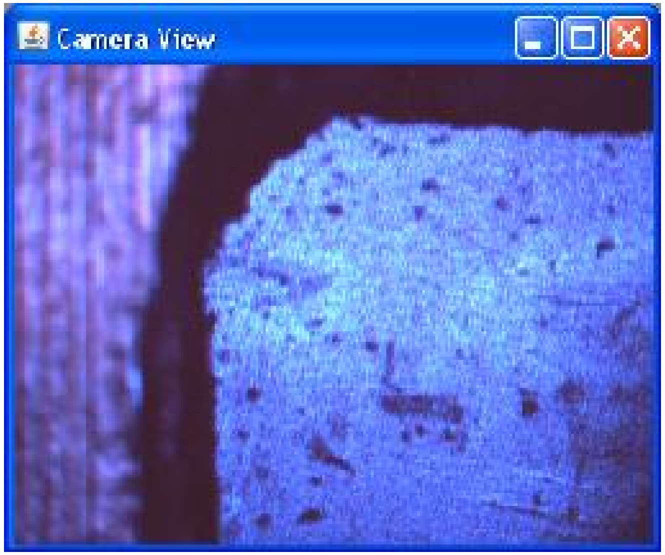


Laser response

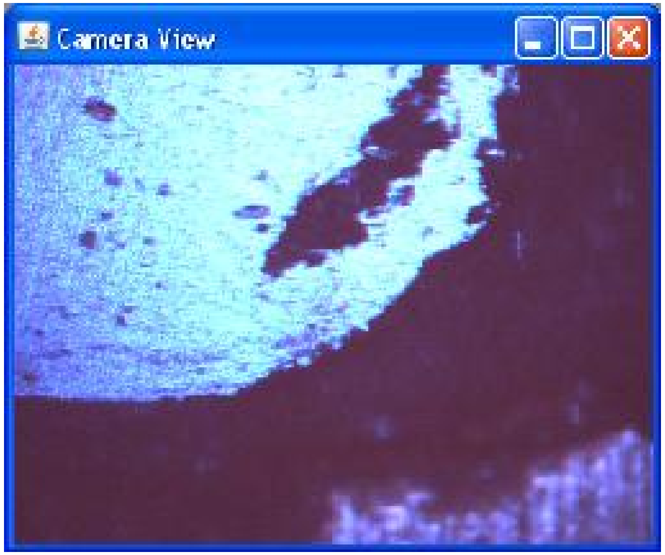
20 nsec interval

Find location

- Attempt to inject faults during ATR communication
  - Scan over surface
- ATR sent by CPU: faults indicate CPU location



A



B

Find timing

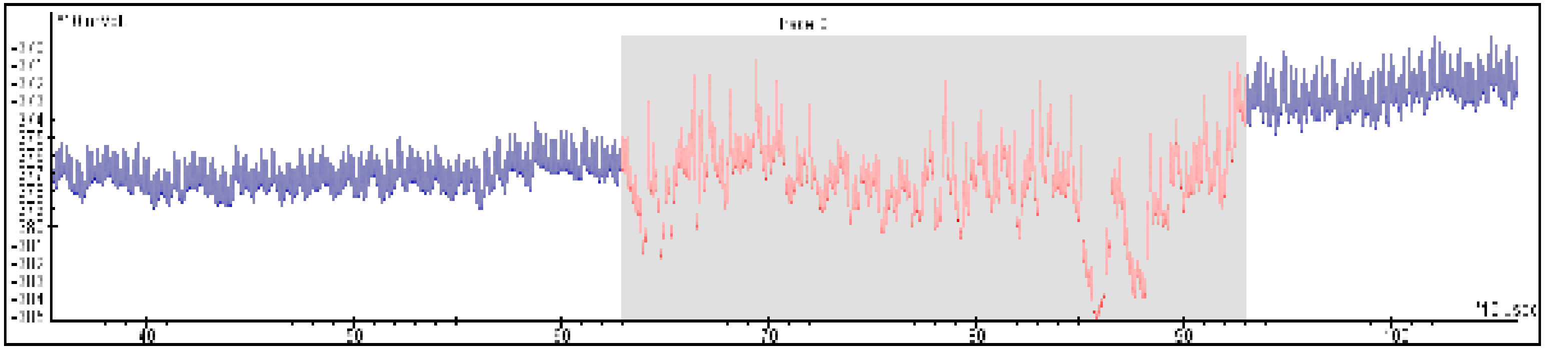
- Need to glitch two PIN verifications
- We cheat: card outputs which PIN verification succeeds
  - SW 6902: both fail
  - SW 6985: one succeeds, one fails
  - SW 9000: both succeed -> our goal
- Other feedback mechanisms used in ‘blackbox’ practice (e.g. power trace and/or timing)

Timing control

- Use FPGA to generate arbitrary triggers
  - At 2ns resolution
- Program in FPGA:
  - Send command
  - Wait x us (x s/w controlled)
  - Fire the laser
  - Wait y us (y s/w controlled)
  - Fire the laser
  - Receive answer

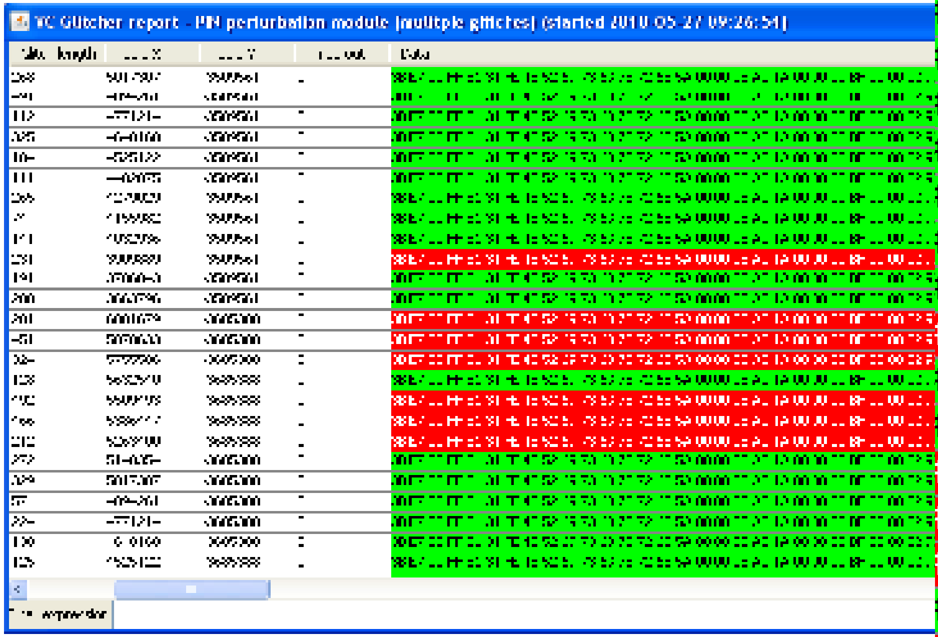
Timing 1

- Power trace to determine approximate timing
- Use one pulse between 630us and 930us
  - 1us increases: hit every instruction

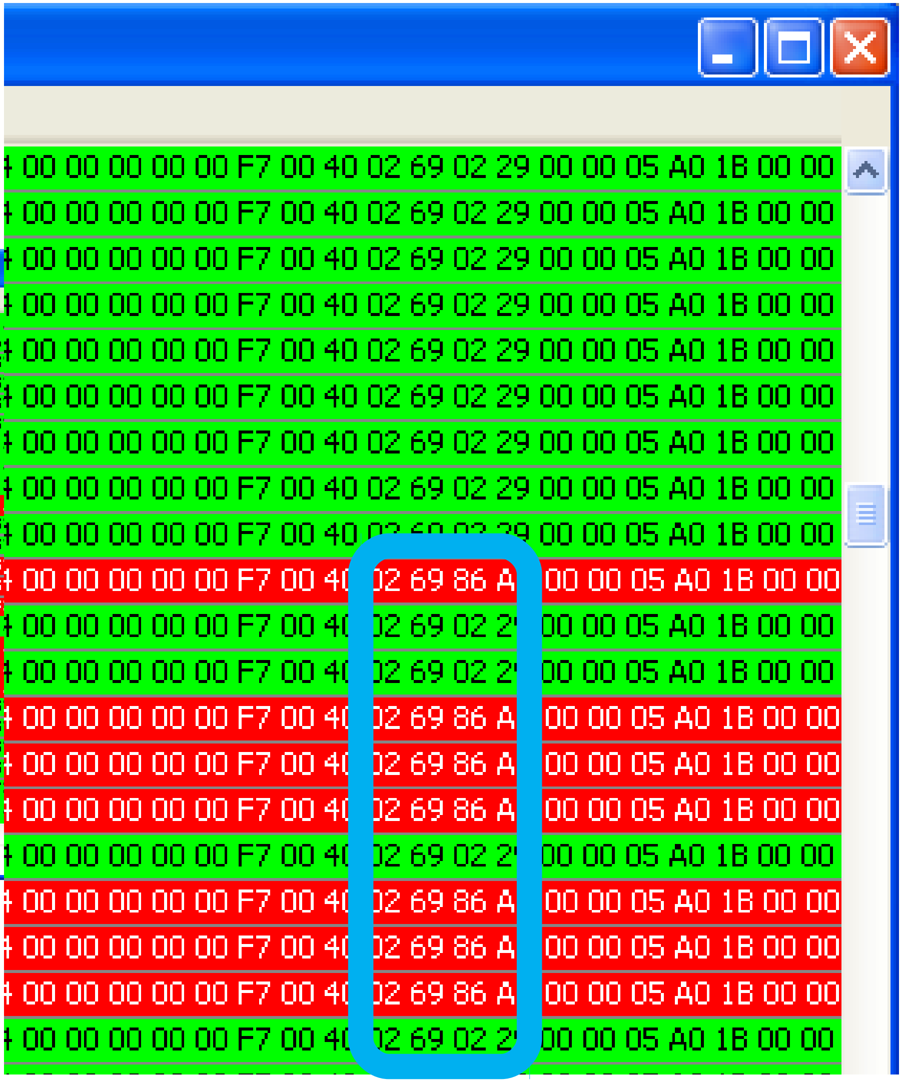


Timing 1

- Check output of card to find candidates for first timing



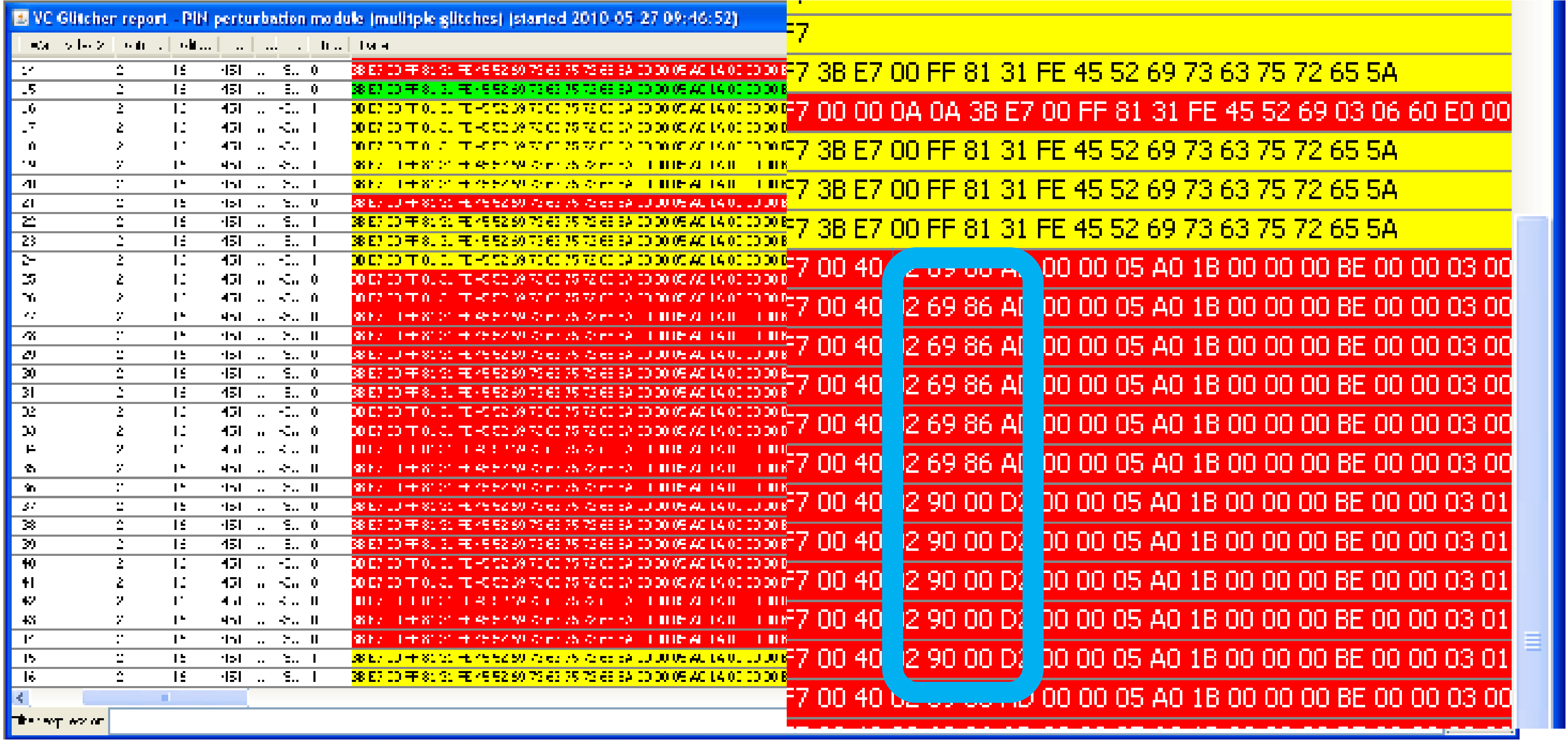
VC Glitcher report - PIN perturbation module (multiple glitches) (started 2010-05-27 09:26:54)



```
00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 86 A  00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 2  00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 2  00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 86 A  00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 86 A  00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 86 A  00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 2  00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 86 A  00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 86 A  00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 86 A  00 00 05 A0 1B 00 00
00 00 00 00 00 F7 00 40 02 69 02 2  00 00 05 A0 1B 00 00
```

Timing 2

- Fix parameters for pulse 1
- Perform a second time interval scan for pulse 2



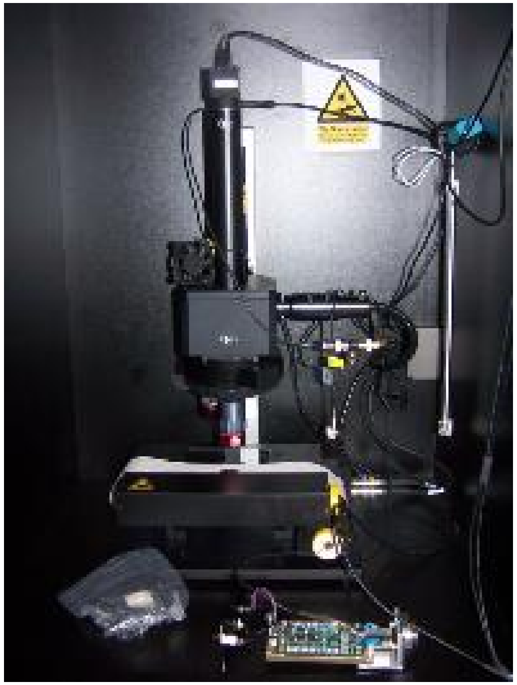
VC Glitcher report - PIN perturbation module (multiple glitches) (started 2010-05-27 09:46:52)

```
F7
F7 3B E7 00 FF 81 31 FE 45 52 69 73 63 75 72 65 5A
F7 00 00 0A 0A 3B E7 00 FF 81 31 FE 45 52 69 03 06 60 E0 00
F7 3B E7 00 FF 81 31 FE 45 52 69 73 63 75 72 65 5A
F7 3B E7 00 FF 81 31 FE 45 52 69 73 63 75 72 65 5A
F7 3B E7 00 FF 81 31 FE 45 52 69 73 63 75 72 65 5A
F7 00 40 [illegible] 00 00 05 A0 1B 00 00 00 BE 00 00 03 00
F7 00 40 2 69 86 AD 00 00 05 A0 1B 00 00 00 BE 00 00 03 00
F7 00 40 2 69 86 AD 00 00 05 A0 1B 00 00 00 BE 00 00 03 00
F7 00 40 2 69 86 AD 00 00 05 A0 1B 00 00 00 BE 00 00 03 00
F7 00 40 2 69 86 AD 00 00 05 A0 1B 00 00 00 BE 00 00 03 00
F7 00 40 2 69 86 AD 00 00 05 A0 1B 00 00 00 BE 00 00 03 00
F7 00 40 2 90 00 D2 00 00 05 A0 1B 00 00 00 BE 00 00 03 01
F7 00 40 2 90 00 D2 00 00 05 A0 1B 00 00 00 BE 00 00 03 01
F7 00 40 2 90 00 D2 00 00 05 A0 1B 00 00 00 BE 00 00 03 01
F7 00 40 2 90 00 D2 00 00 05 A0 1B 00 00 00 BE 00 00 03 01
F7 00 40 2 90 00 D2 00 00 05 A0 1B 00 00 00 BE 00 00 03 01
F7 00 40 [illegible] 00 00 05 A0 1B 00 00 00 BE 00 00 03 00
```

Conclusions card 1

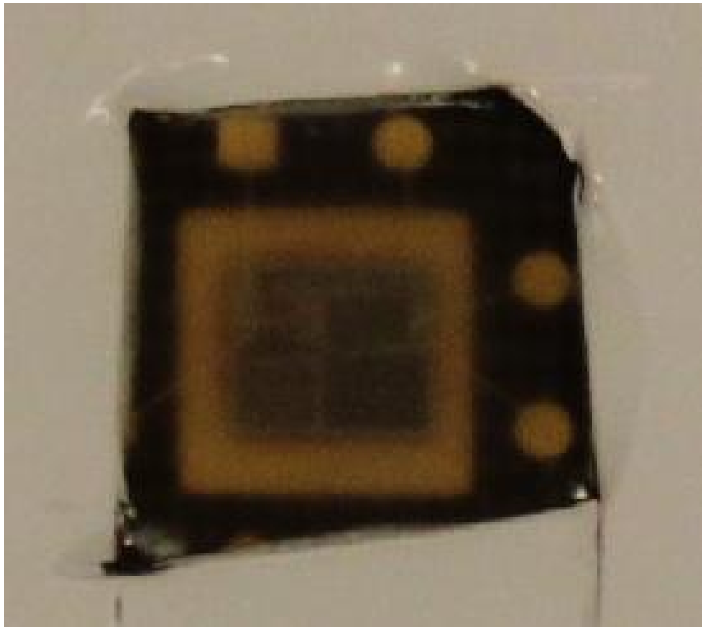
- 1000/1000 injections successful
- Delay between pulse 1 and 2 is 33us
- Changing timing by 1us changes outcome
- 808nm laser does not work, 1064nm laser does

- Repeatability requires fast and jitterfree system
- Diode lasers + fast control fit for this purpose



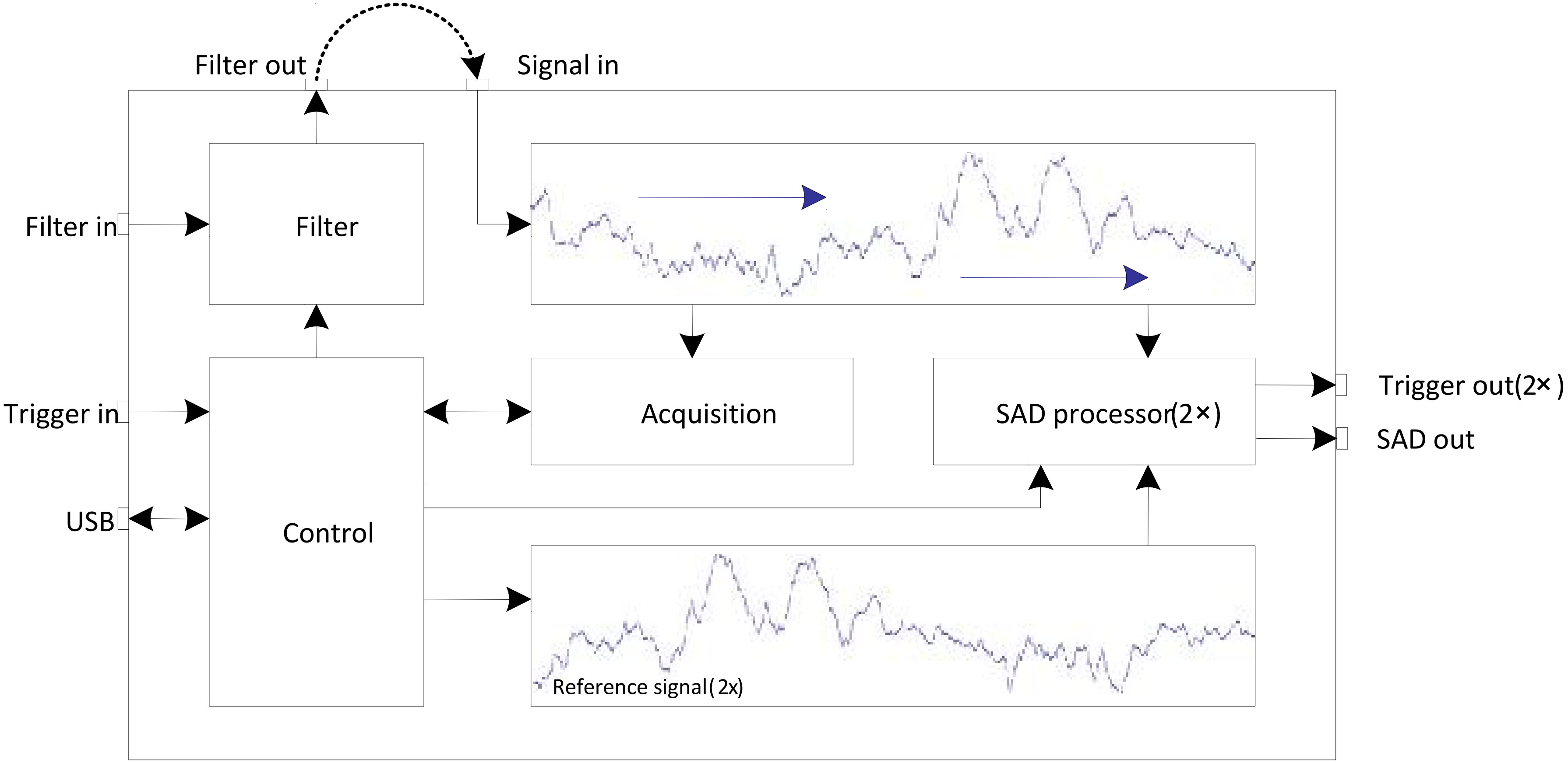
Experiments card 2

- Main CPU + crypto accelerator, clocked internally ~30MHz
- Countermeasure: unstable clock, FI detection & card termination
- Goal: corrupt DES output, keep card alive
- Approach:
  - Front side (through epoxy!)
  - Create synchronized trigger
  - Find sensitive location on chip
- Show synchronization
- Show termination prevention



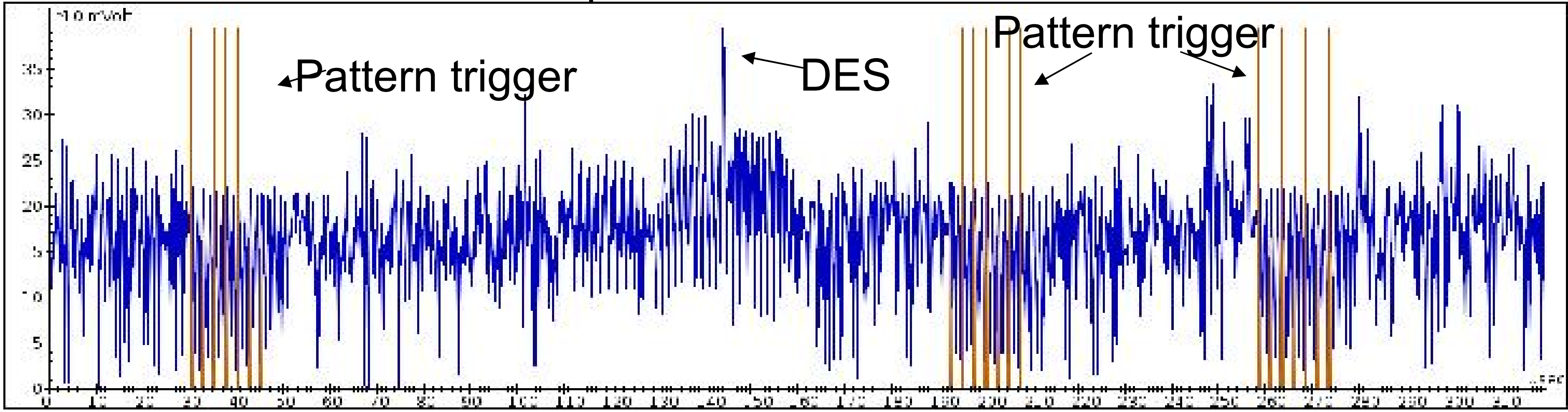
Create synchronized trigger

- Use real-time (filtered) pattern matching
- FPGA based, A/D running at 100MHz



FI control (FPGA)

- Send command
- Wait for external trigger
- Wait x us (x software controlled)
- Fire the laser
- If no external trigger within 100us: power off card
- Otherwise: read response



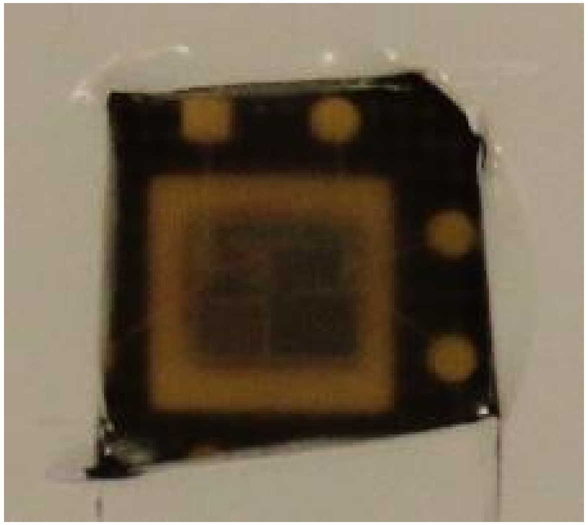
Finding the location

- Countercountermeasure in place: safe to scan surface
- Found timing where DES accelerator was producing faulty outputs
- Repeatly fire here (>50% success rate)

Conclusions card 2

- Before: wildly varying results, card termination <1000 injections
- After:
  - often DES output == DES input (break protocols)
  - card still happy at 60000 injections

- Timing jitter can be countered by:
  - pattern based triggering
  - a stable and fast laser response
- Card termination can be countered by:
  - pattern based triggering
  - control response <100us

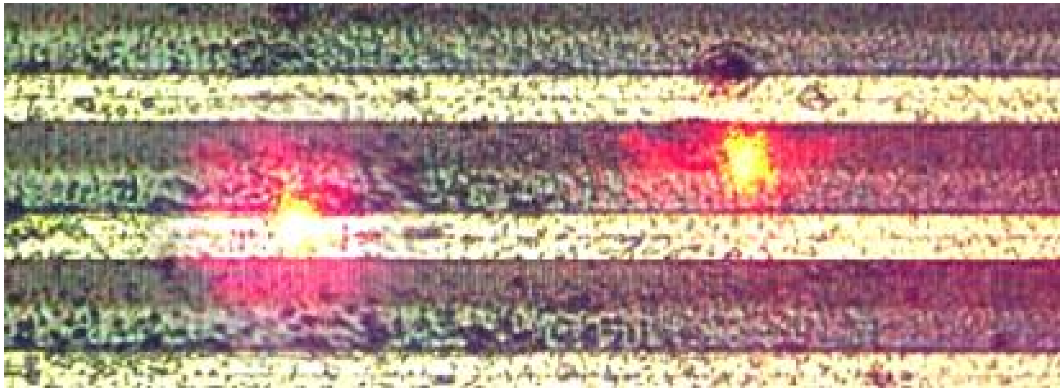


Latest development: triple glitch

- Performed successful triple glitching
  - RSA-CRT: glitch CRT + double verification
  - Latest smart card technology
  - 1% success rate (of obtaining full private key)
  - Lab condition: able to control countermeasures; no card termination

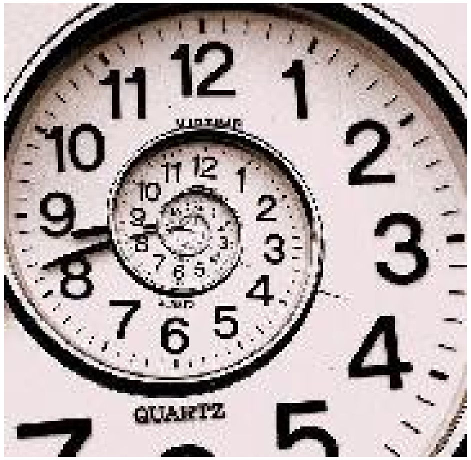
Latest development: multi location

- Add fiber-guided laser to setup
- Add second XY manipulator
- Double laser trigger
- Challenge: finding the (right location/time/etc)^2…



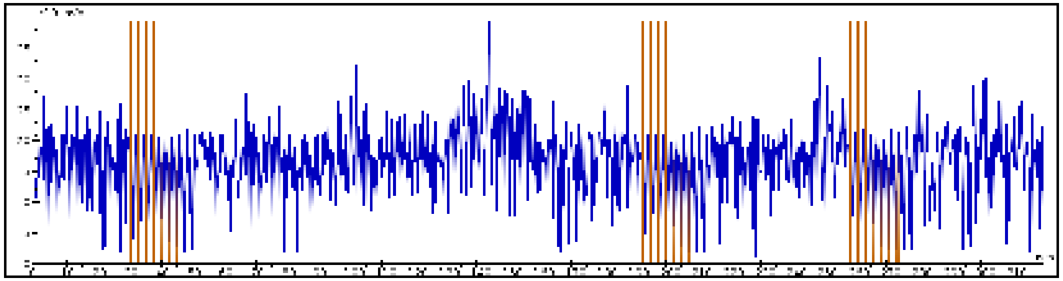
Summary

- State-of-the-art optical fault injection equipment allows much more control
  - Overcome limitations imposed by non-diode lasers (YAG,DPSS)
  - Overcome fixed-delay trigger limitations
- Precisely inject arbitrary number of faults
  - Experimentally: success with up to three



Conclusion

- EMVco and CC moved to multi-time and will likely move to multi-location FI
- Countermeasures need to be improved
  - Double verification not sufficient anymore
  - Side channel patterns (also after filtering!) should be minimized



Discussion

Jasper van Woudenberg

Senior Security Analyst

vanwoudenberg@riscure.com

Riscure B.V.
Frontier Building
Delftechpark 49
2628 XJ Delft
The Netherlands

Phone: +31 (0)15 251 4090
www.riscure.com

Shameful plug: WE ARE HIRING!