Large Laser Spots and Fault Sensitivity Analysis

Falk Schellenberg, Markus Finkeldey, Nils Gerhardt, Martin Hofmann, Amir Moradi and Christof Paar
Ruhr-Universität Bochum

PhotonFX^2
FKZ 16KIS00-15/26/27

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

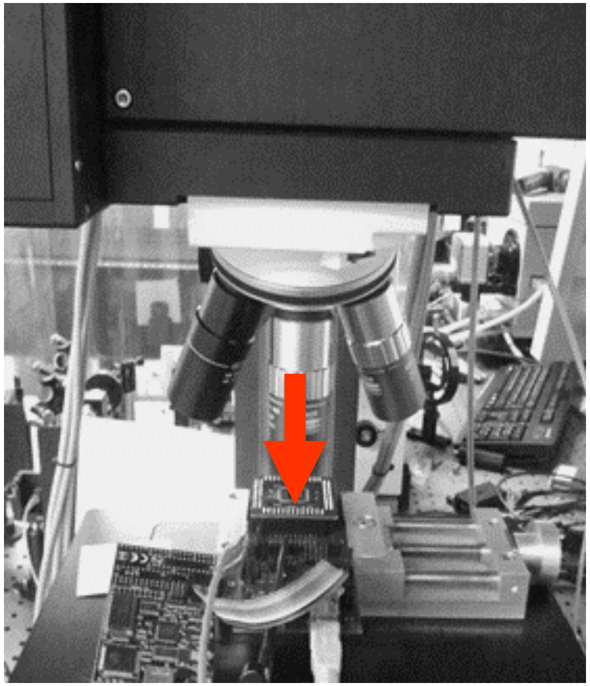
Fault Injection

Idea: Faulty computation might leak secret key!

Trivial Fault Attack

- Assume asymmetric key memory with respect to faults:
  - 0 → 1: possible using fault injection
  - 1 → 0: impossible
- Attack:
  - Send identical input repeatedly
  - Inject fault into key memory, bit-wise!
  - Ciphertext?
    - Changed → key bit was 0
    - Unchanged → key bit was already 1

Fault Injection



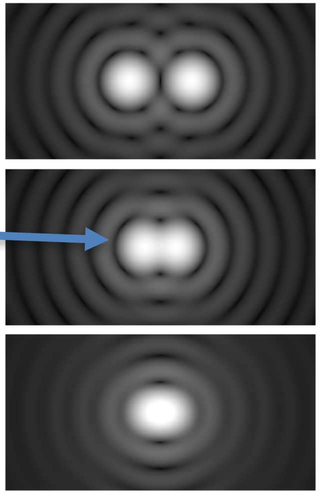
Physical Methods

- Clock glitches
- Voltage glitches
- EM pulses
- Light (flash lamps, **lasers**)

Laser Fault Injection

- Precise **spatial control** ("up to single transistors")
- Precise timing
- SRAM: Trivial fault attack possible!

Motivation



Future?

- Spot size is **physically** bounded!
- Diffraction limit (Rayleigh-Criterion): $\frac{1.22\,\lambda}{2\,\mathrm{NA}}$
- Example:
  - Typical numerical aperture (NA): 0.7
  - $\lambda = 975$nm
  - → 850 nm effective spot

Physical limit for laser fault injection reached?

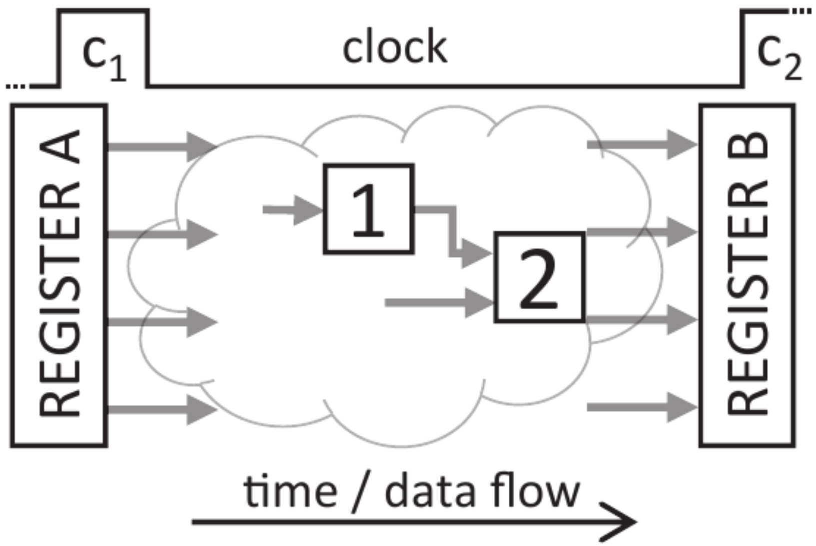
- SRAM: limit at 45nm? → **maybe***
- Latest technology inherently secure? **No!**

**Selmke et al.:* "Precise Laser Fault injections into 90nm and 45nm SRAM-cells", CARDIS'15

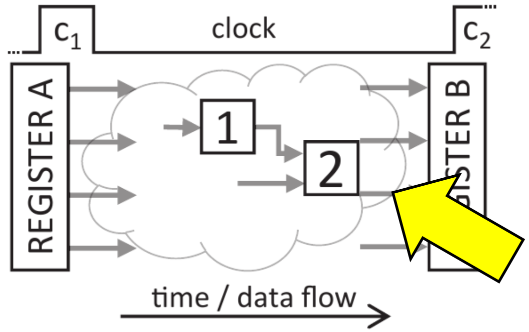
Large Laser Spots and Fault Sensitivity Analysis*

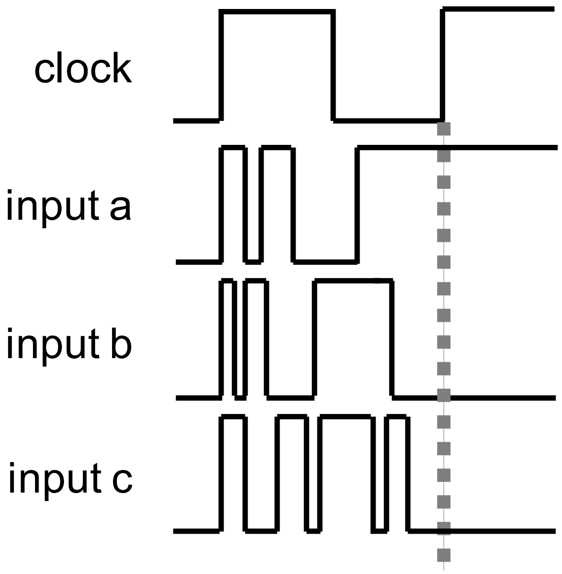
**Moradi et al.*: “On the Power of Fault Sensitivity Analysis and Collision Side-Channel Attacks in a Combined Setting”, CHES’11

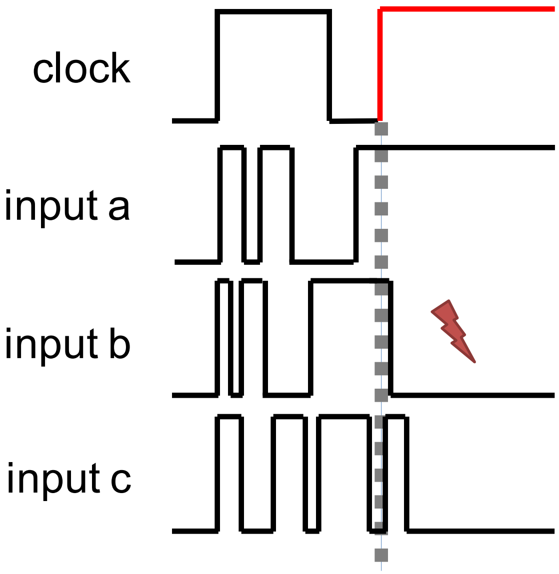
Combinatorial Circuits



Clock Glitches







Important observations:

- Critical delay depends on input

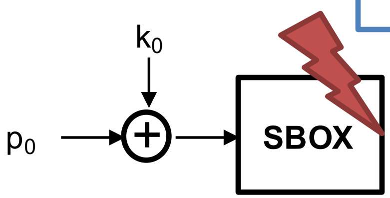
➔ *Identical* input means *identical* critical delay

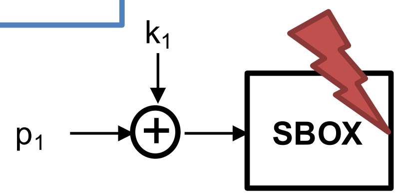
“Collision Correlation”-Enhanced Fault Sensitivity Analysis

How to exploit?

Example: glitch position fixed at 50% faulty outputs, 1000 random plaintexts

$$k_0 = k_1$$





p0	#faulty
0	6
1	0
2	20
3	4
4	1
255	5

high correlation

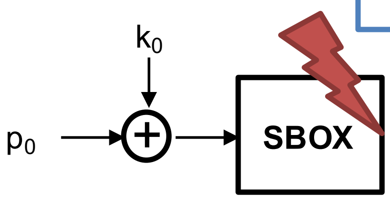
p1	#faulty
0	7
1	0
2	19
3	5
4	0
255	6

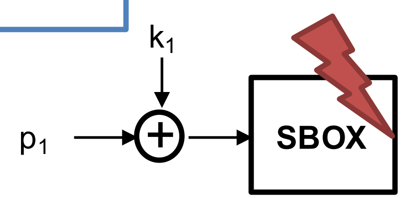
"Collision Correlation"-Enhanced Fault Sensitivity Analysis

How to exploit?

Example: glitch position fixed at 50% faulty outputs, send 1000 inputs

$$k_0 = k_1 \oplus \Delta$$





p0	#faulty
0	6
1	0
2	20
3	4
4	1
255	5

~~no correlation~~

high correlation

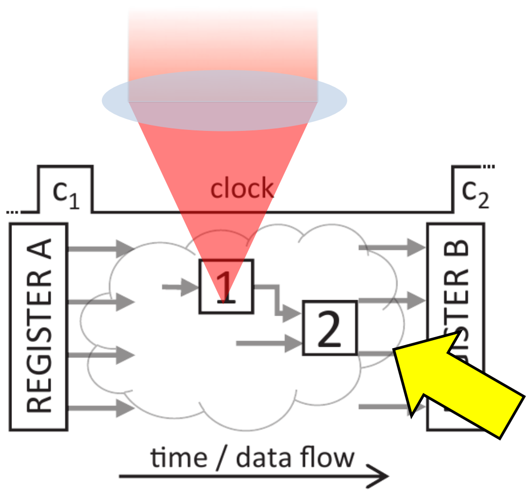
p1 / $\overline{p_1}$	#faulty
0	7 / 6
1	1 / 18
2	21 / 27
3	5 / 0
4	1 / 0
255	6 / 1

$$\overline{p_1} = p_1 \oplus \Delta$$

➔ **Test all possible $\Delta \in \{0, 1, 2, \ldots, 255\}$**

Large Laser Spots and Fault Sensitivity Analysis

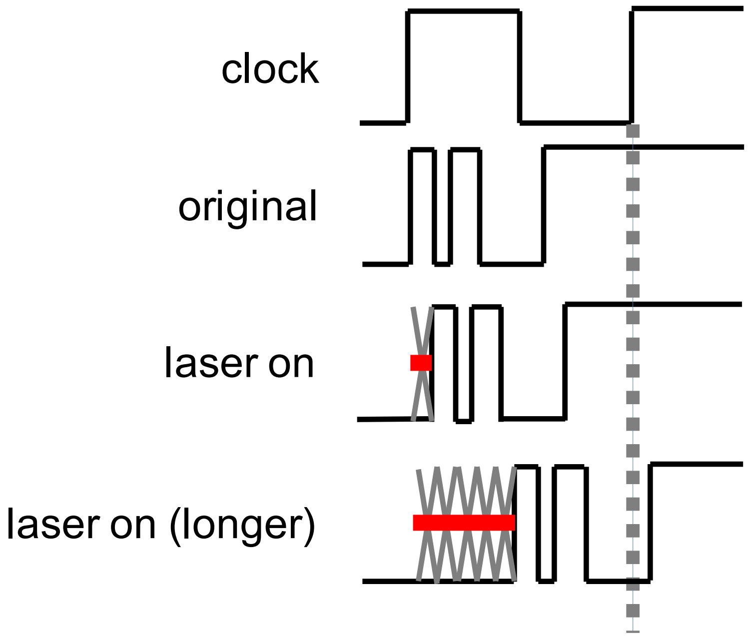
Timing Violations using Lasers



Laser Fault Injection in a nutshell:

- Set a signal to a false value
- For the **duration** of the pulse

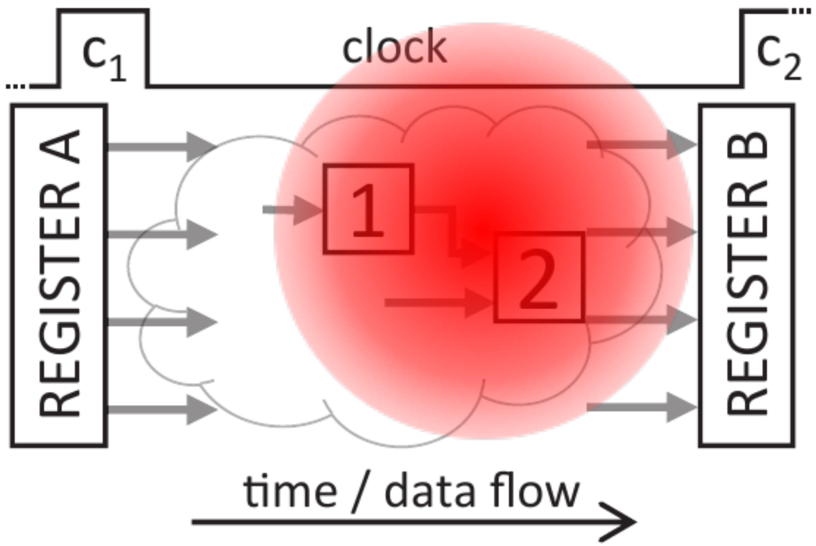
Timing Violations:



Identical input dependency as before!

RUB

Large Laser Spots?



Setup

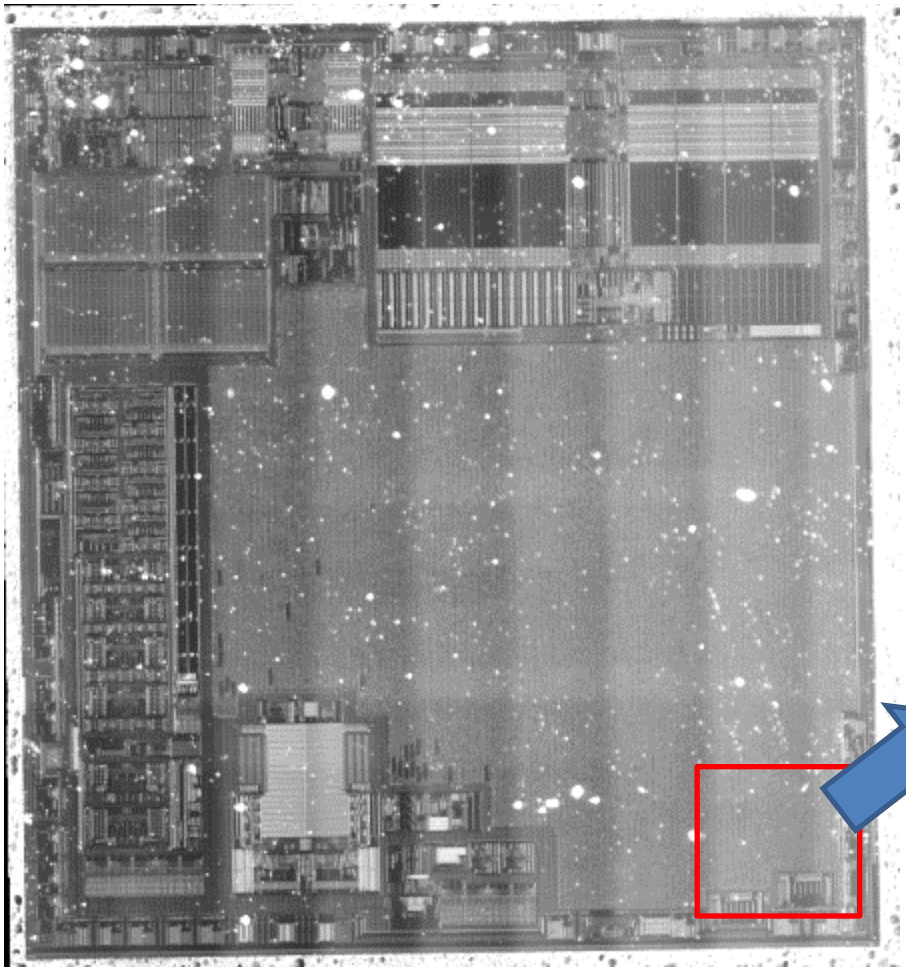
Device Under Test: Atmel ATXMega16A4U

- 250nm feature size
- Hardware AES
  - 375 clock cycles (serialized SubBytes)
  - Target: Combinatorial Sbox circuit

Optical Setup

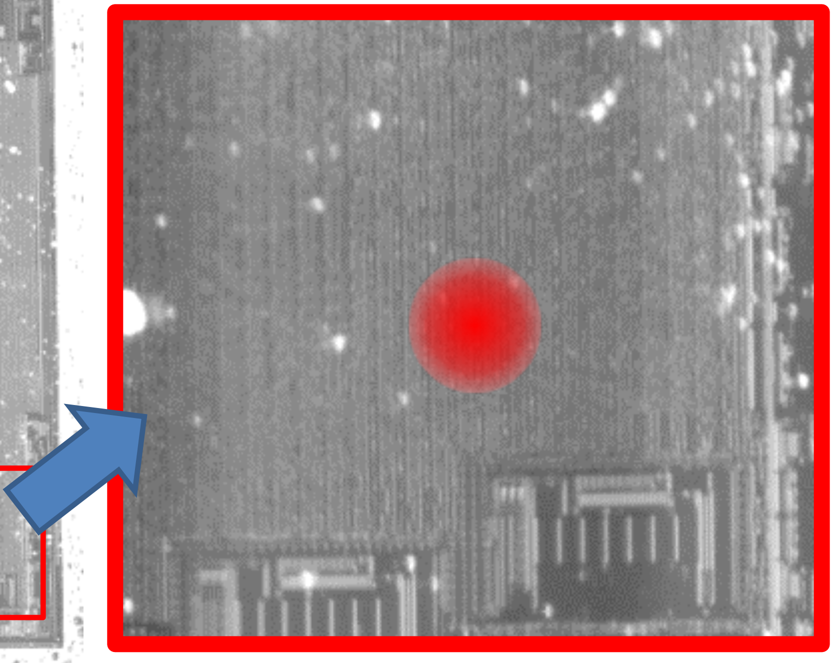
- Mitutoyo NIR 10x → 4.5 µm spot size @ 975nm
- 80 µm out-of-focus → **45 µm spot size**

ATXmega16A4U AES



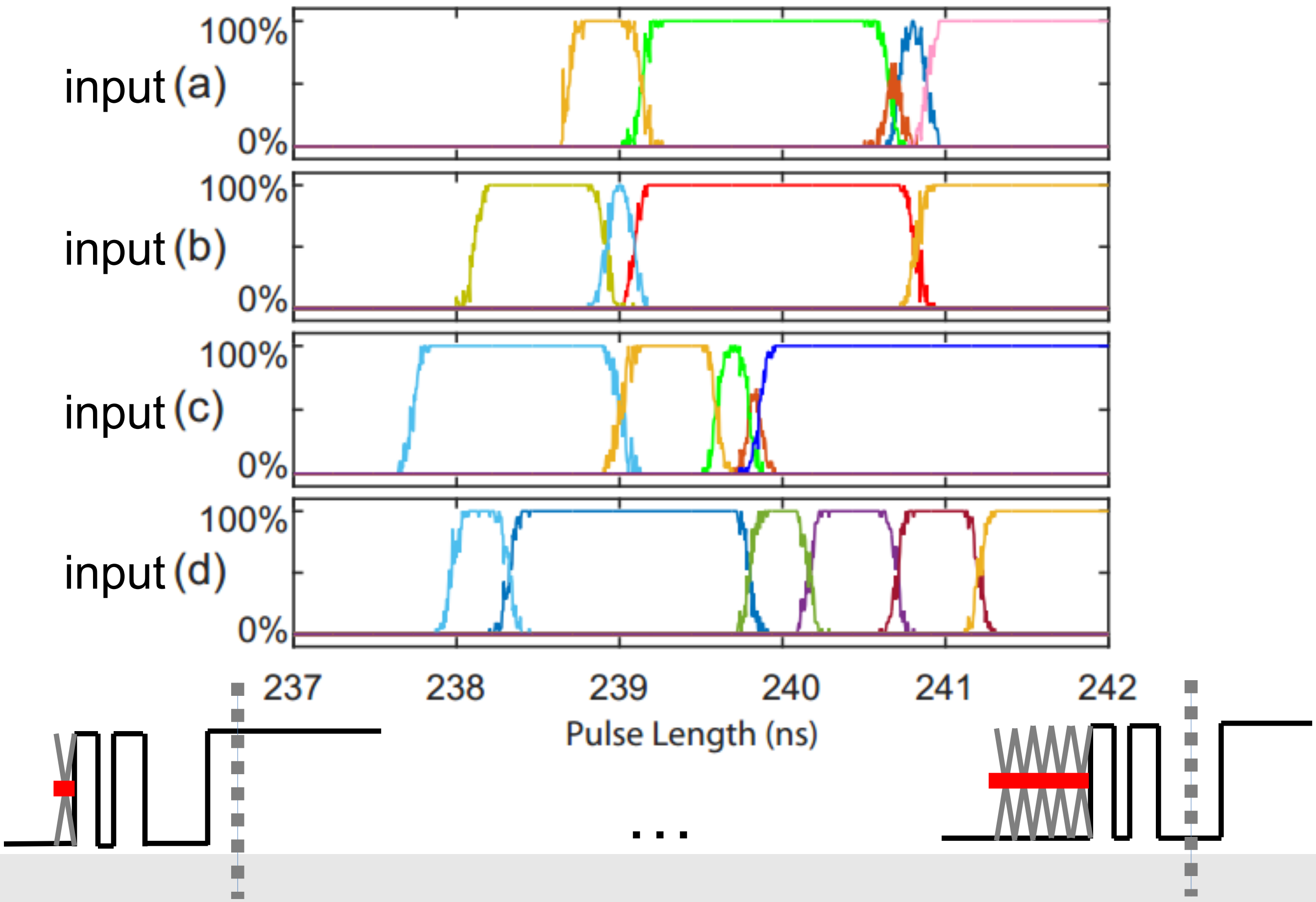
backside NIR

Arbitrary location within combinatorial Sbox

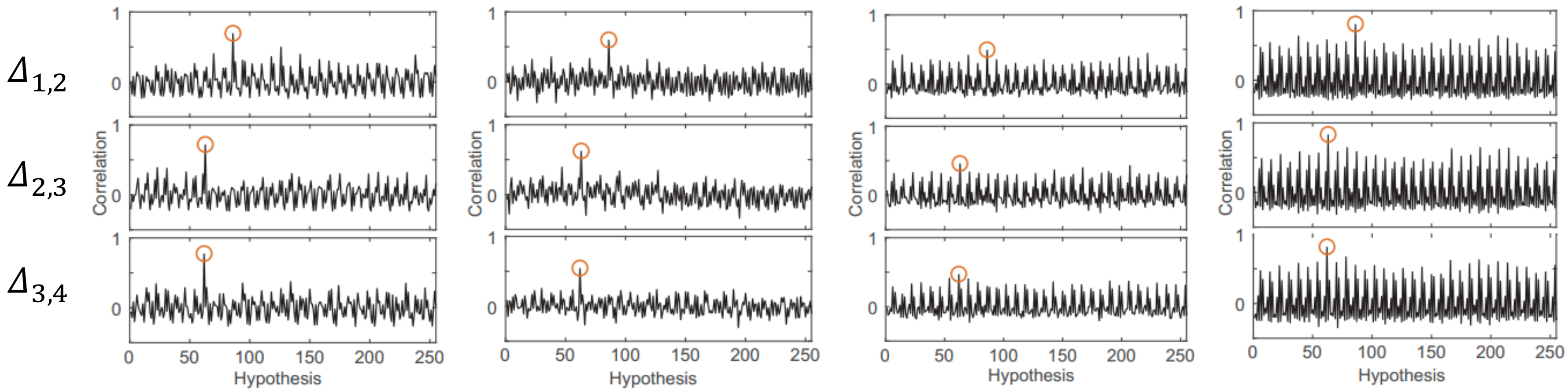


Characterization: Input vs Pulse Length

Four different fixed inputs, increasing laser pulse width (steps of 5ps)
Colors: different faulty output values



Results



(a) 20%, $N = 1000$ (b) 50%, $N = 1000$ (c) 80%, $N = 1000$ (d) 80%, $N = 5000$

Correlation for each delta hypothesis

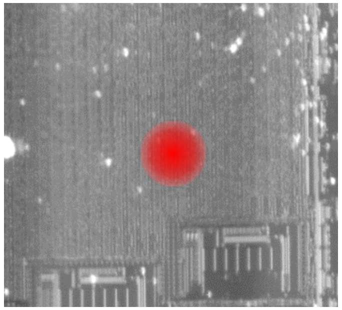
- Varying fault probability: {20%, 50%, 80%}
- N – Number of Measurements
- Example 20%, N=1000 → 200 out of 1000 shots faulty

→ Correct hypothesis shows highest correlation

Outlook

ATXmega (250nm min. feature size)

- Sbox: ~ 230 µm x 310 µm
- 45 µm spot



Scaling to 11nm?

- Sbox: ~ 10 µm x 13µm
- **~ 2 µm spot > diffraction limit**

Trade-Off: Spatial accuracy vs timing resolution

- ps / fs lasers with very low jitter available

Conclusion

- Considered timing violations using lasers
- Laser + FSA: very relaxed fault model
  - No ciphertext/faultytext
  - Only information whether fault occurred or not
  - Random (known) plaintext
  - **Large spot size OK**
  - Should work down to latest technology
- Countermeasures at smallest feature sizes **still required**

Future Work:

- Replacing very high speed clock glitches by laser fault injection?

Thanks!
Questions?