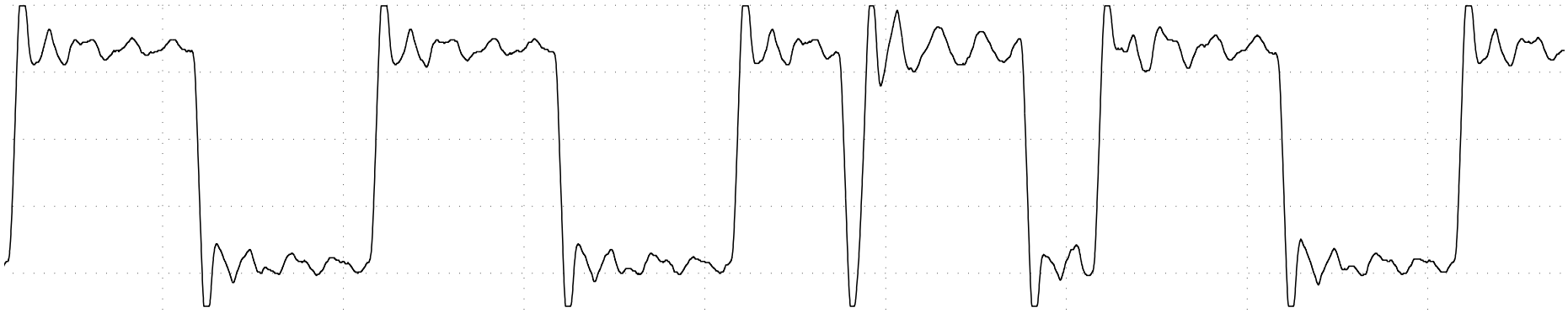
Fault Attacks and Countermeasures



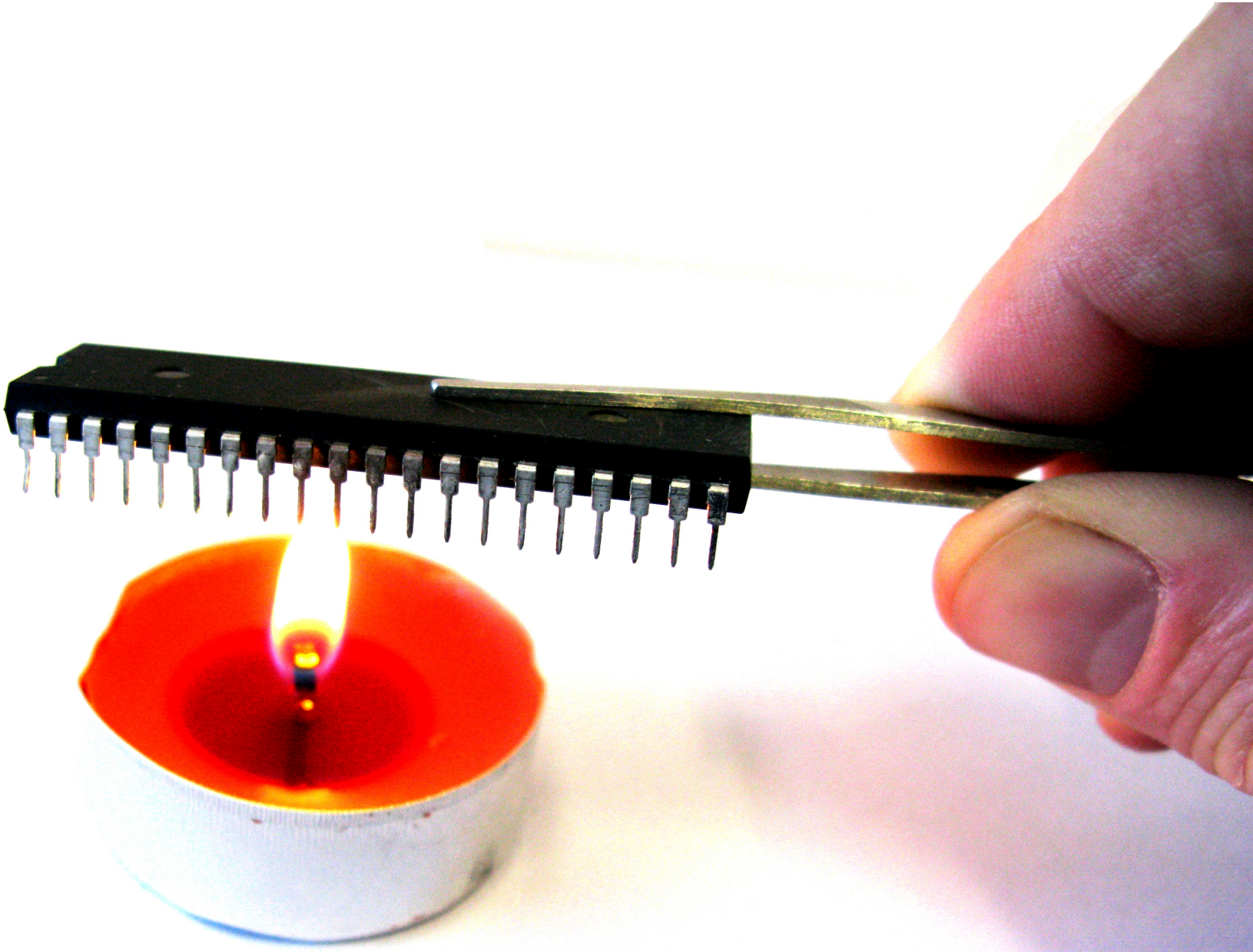
Michael Hutter

Summer School on Design and Security of Cryptographic Algorithms and Devices for Real-World Applications

Ŝibenik, Croatia, 1-6 June, 2014

Outline

What are Fault Attacks?



Fault Models

- Duration of faults
  - Transient
  - Permanent
  - Destructive
- Controllability (precise, loose, no) [15]
  - Fault location
  - Fault timing
- Fault precision
  - Single bit
  - Few bits
  - Byte/word

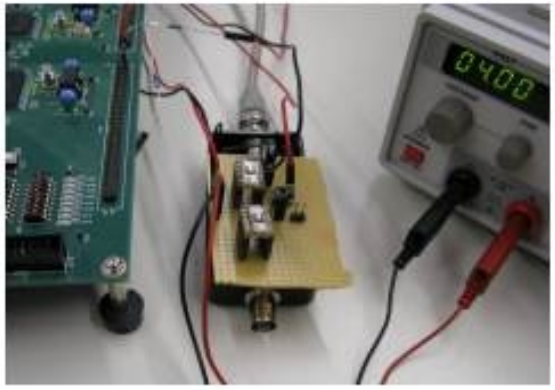
Fault Types

- Let $B = \{b_0, b_1, ..., b_{n-1}\}$ be an arbitrary set of bits in memory [15].
- **Stuck-at faults**
  - Bits of B get fixed to a value $\{0, 1\}$ and cannot be changed anymore
  - $b_i \rightsquigarrow b'_i \qquad \forall i \in [0, n-1]$
- **Bit-flip faults**
  - E.g., all bits of B get flipped
  - $b_i \rightsquigarrow b'_i = 1 - b_i \qquad \forall i \in [0, n-1]$
- **Random faults**
  - Bits of B are randomly set
  - $b_i \rightsquigarrow b'_i \in \{0, 1\} \qquad \forall i \in [0, n-1]$
- **Set/reset faults**
  - Bits of B are set to 1 or 0
  - $b_i \rightsquigarrow b'_i = c_i \qquad c_i \in \{0, 1\} \qquad \forall i \in [0, n-1]$

Adversaries and Threats

- Class I
  - Clever outsider
- Class II
  - Knowledgeable insider
- Class III
  - Company/university

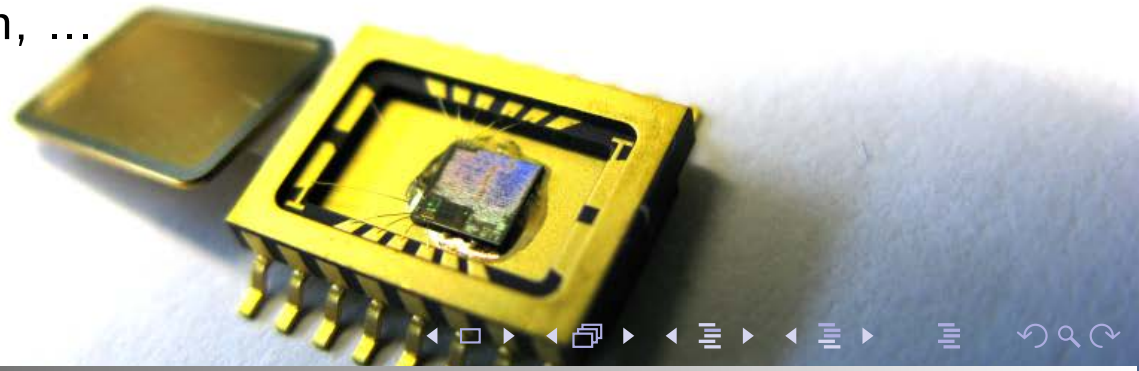
Adversaries Capability Range



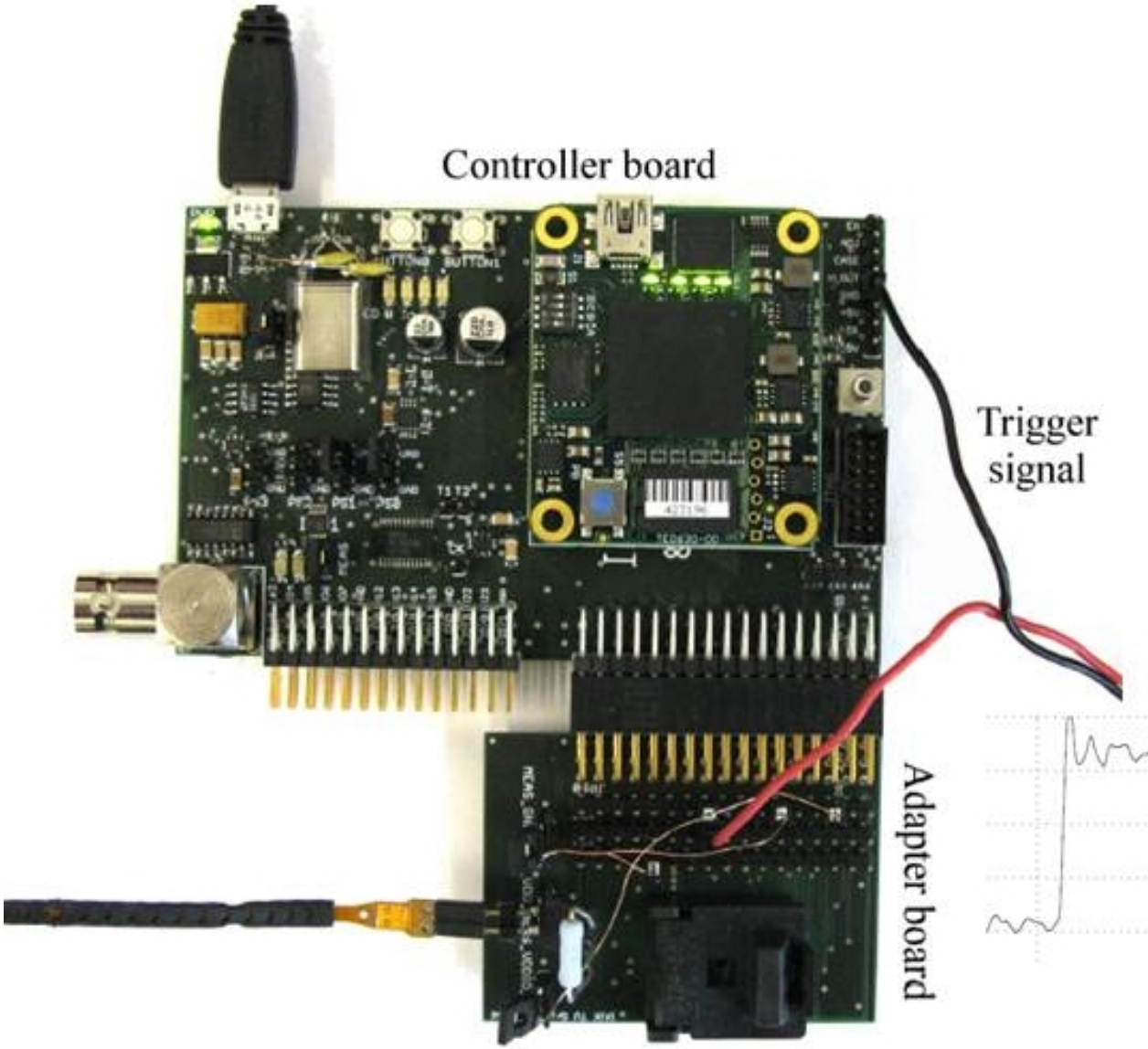



Fault-Injection Methods

- Non-invasive
  - Package left untouched
  - Modify working conditions
- Semi-invasive
  - De-capsulation, e.g., optical inductions
  - Allows direct contact to the chip die
- Invasive
  - Establish electrical contact to chip
  - Modification, destruction, ...

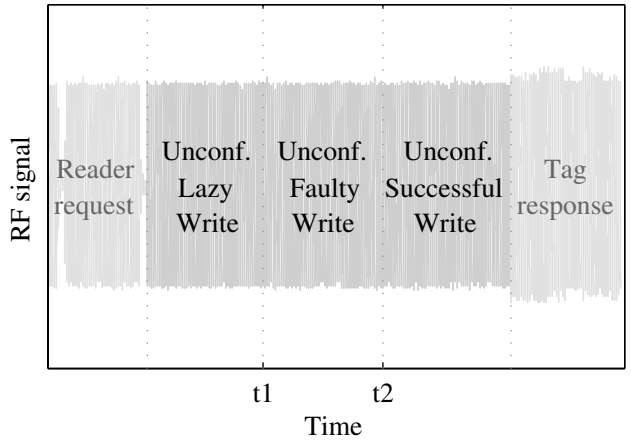


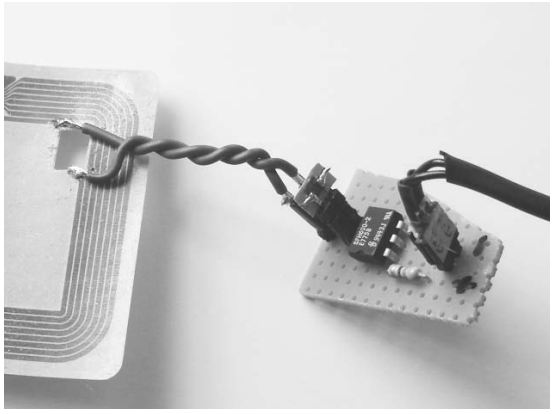
Non-Invasive Attack Setups - Spikes and Glitches

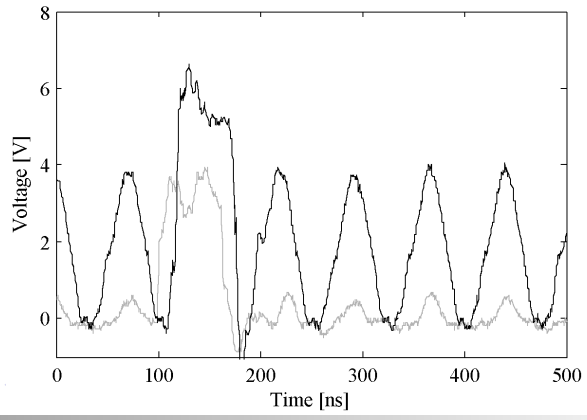


Spike/Glitch Attacks - Examples

- Under-voltage attacks (CHES 2008 [7])
  - RFID *antenna tearing* - cut-off power supply shortly
- Over-voltage spikes (ECCTD 2009 [8])
  - Transistor can switch to higher voltages ($>$ 5 Volts) for a short period of time
- Clock-glitch attacks
  - Mostly timing violations (setup/hold)
- Fault effects
  - Allow to change memory content
  - Change of program flow: skipping instructions, program-counter changes, tampering loop bounds, opcode changes, modifications of instruction and/or operand addresses, ...



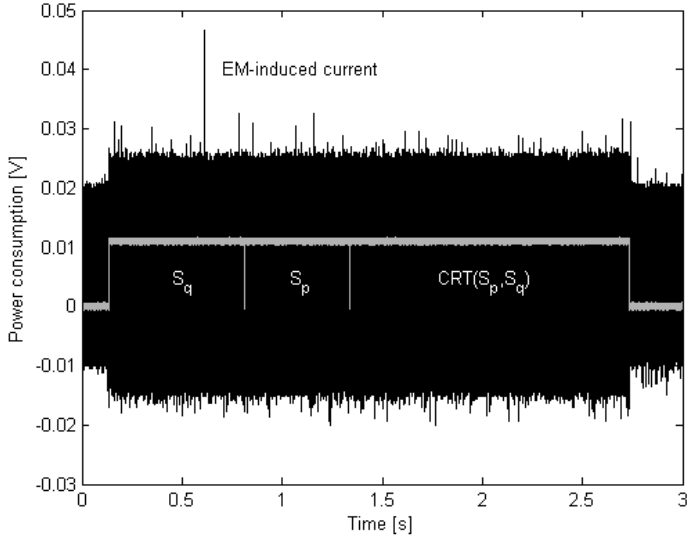




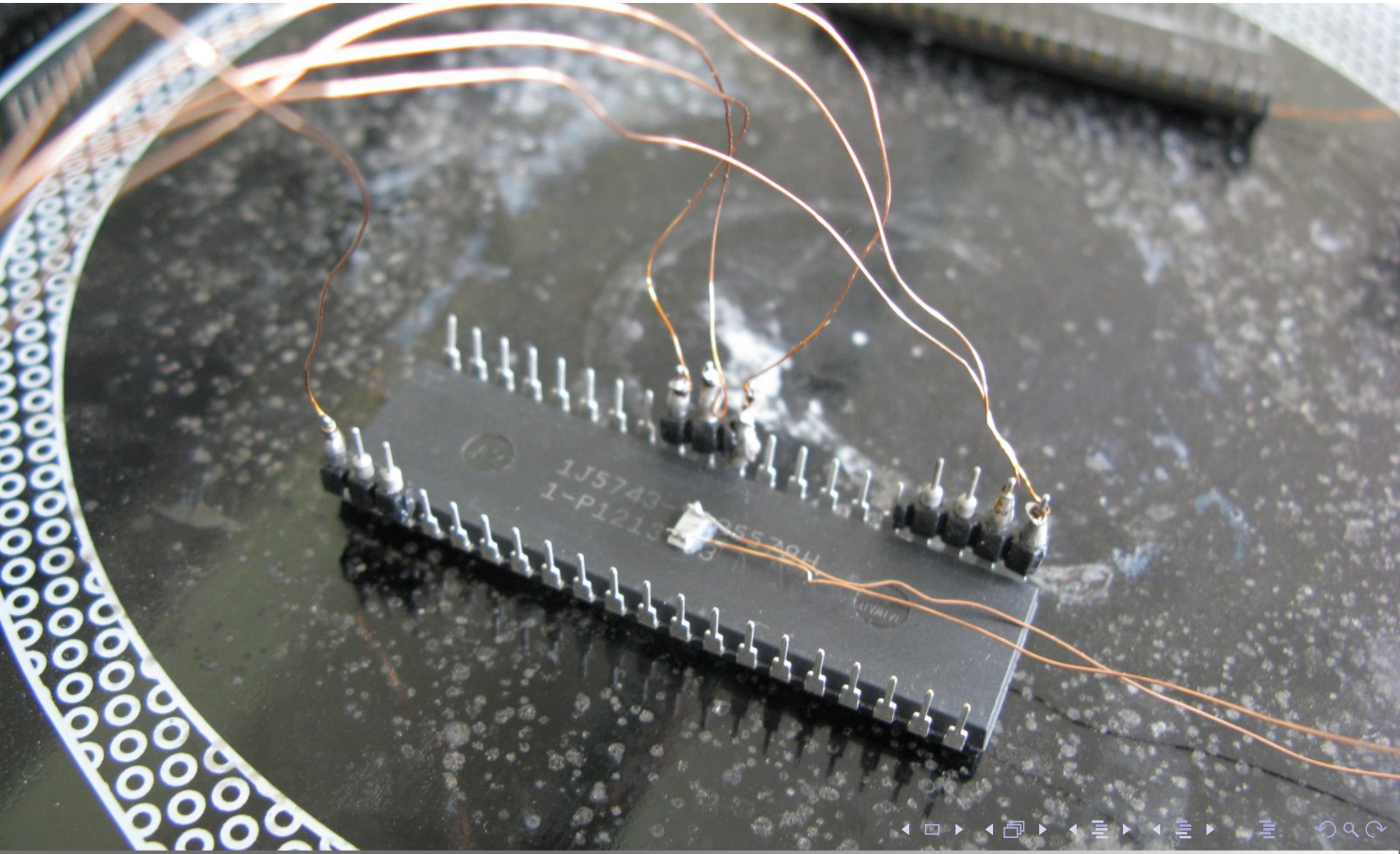
Non-Invasive Attack Setups - EM Pulses

EM Attack - Example

- EM pulses induce **Eddy currents** that cause transistors to switch
- Fault attack on a CRT-RSA signature generation [18, 2]
  - Let $n = pq$. Instead of calculating $S = m^d \bmod n$, you can split the computation into $S_1 = m^d \bmod p$ and $S_2 = m^d \bmod q$.
  - Use the Chinese Remainder Theorem (CRT) to combine them such that $S = aS_1 + bS_2 \bmod n = \mathrm{CRT}(S_1, S_2) \bmod n$
  - A faulty computation, e.g., in S_1, leads to $gcd(S - \tilde{S}, n) = gcd(a(S_1 - \tilde{S}_1), n) = q$

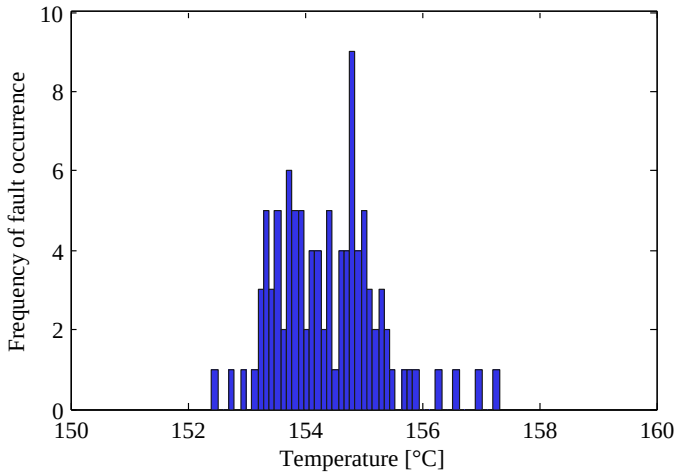


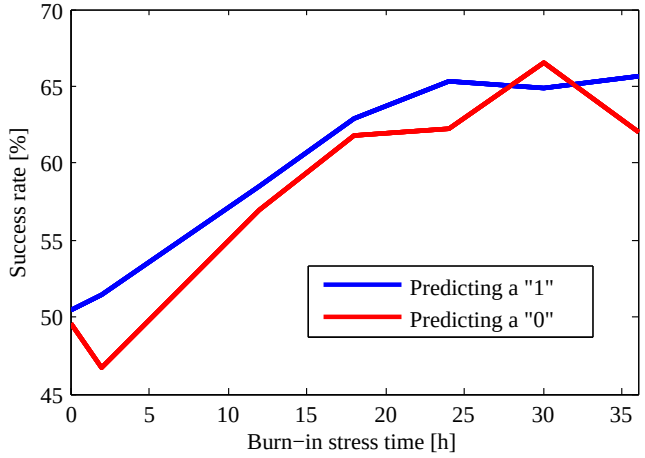
Non-Invasive Attack Setups - Temperature



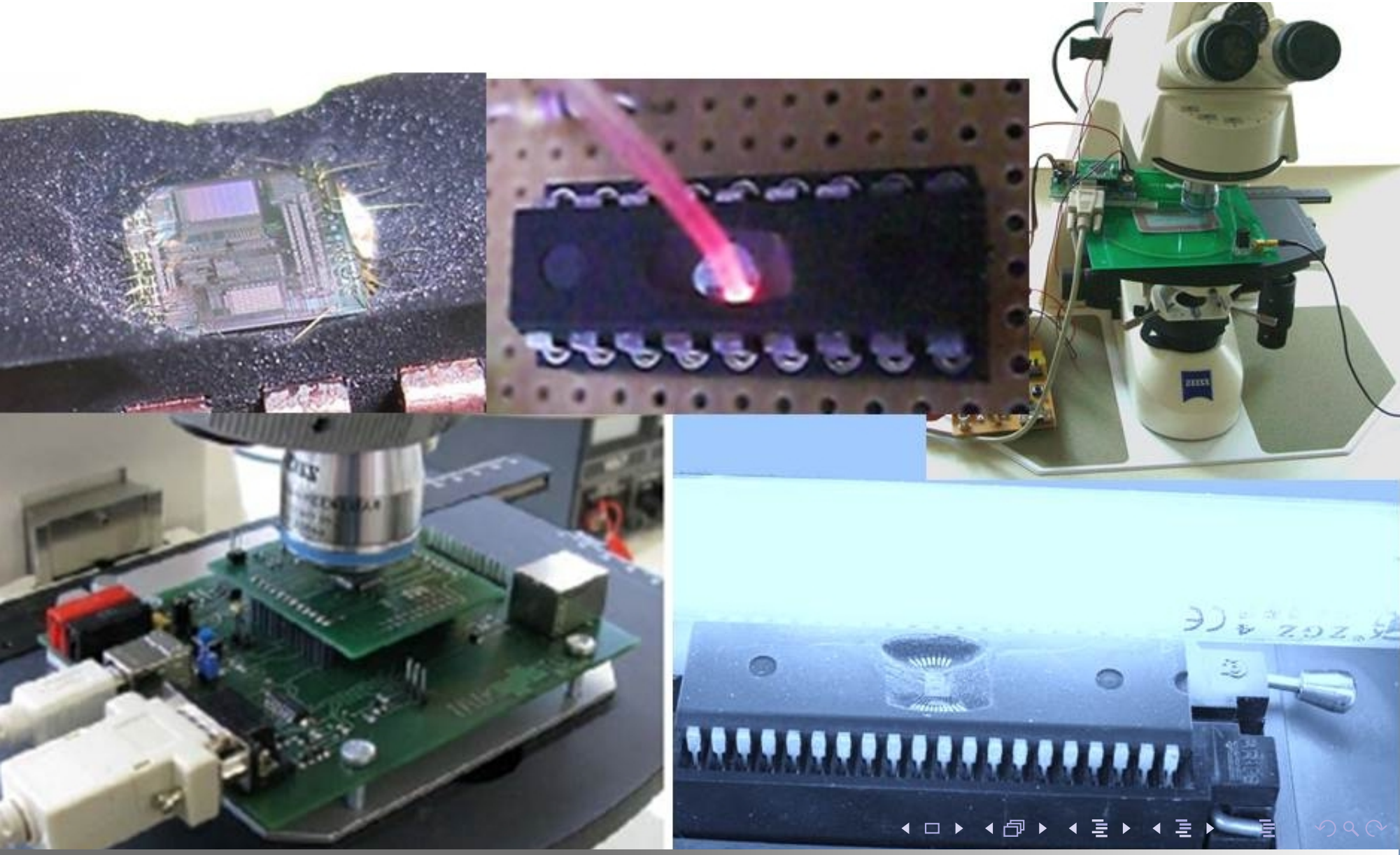
High-Temperature Fault Attacks - Example

- CARDIS 2013 [6] or [16]
- μC placed on top of a heating plate
  - No response beyond 160 °C
  - Within 70 minutes, we got 100 faults (between 152 and 158 °C)
  - Attacking CRT-RSA: 31 revealed one of the prime modulus: 15 revealed p, 16 revealed q
- Exploiting **data-remanence effects** [5, 1]
  - Extensive heating accelerates aging (Negative Bias Temperature Instability)
  - Experiment: 100 °C for 36h at 5.5 V
  - SRAM cells got biased to either 1 or 0
  - 30 % of memory change after heating
- Data-retention attacks by cooling [20]

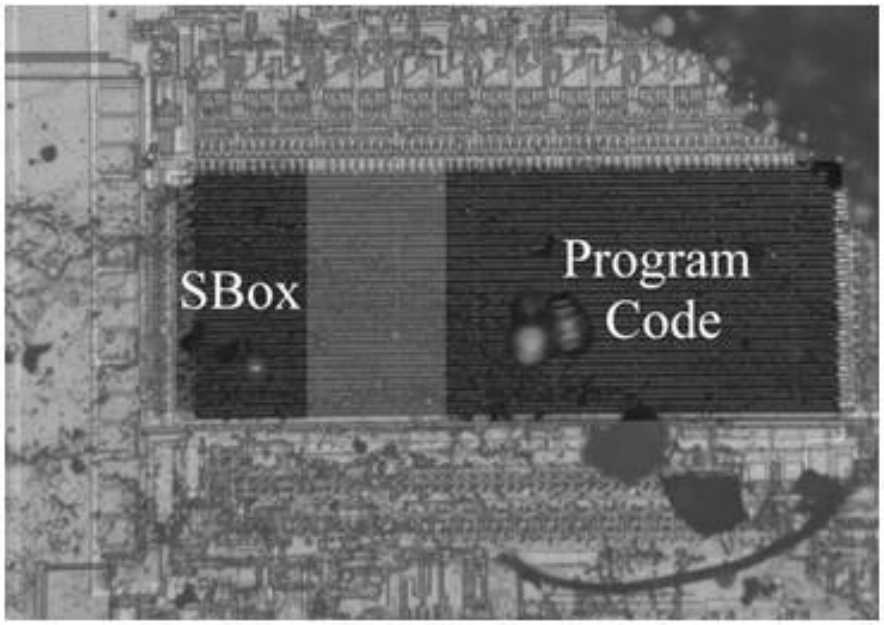


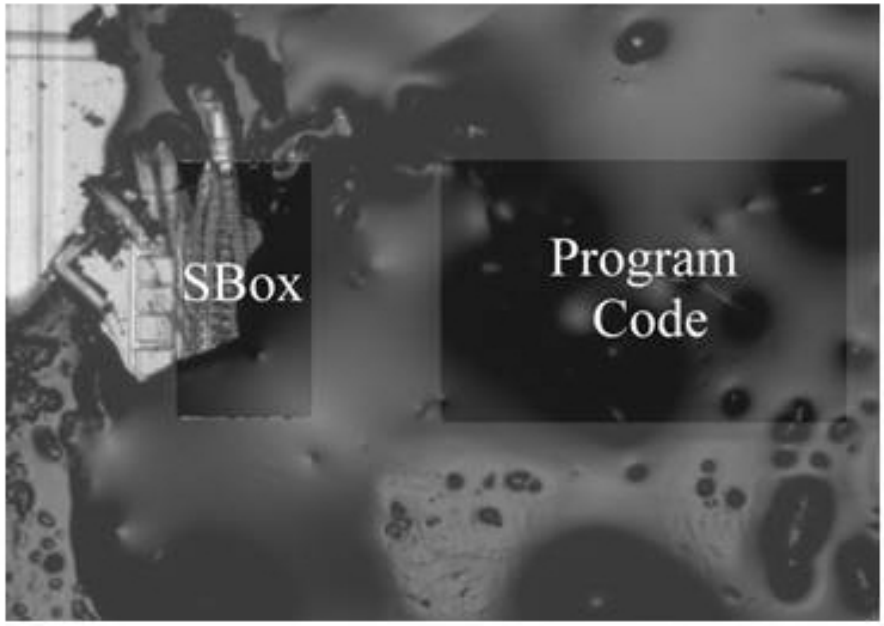


Semi-Invasive Attack Setups



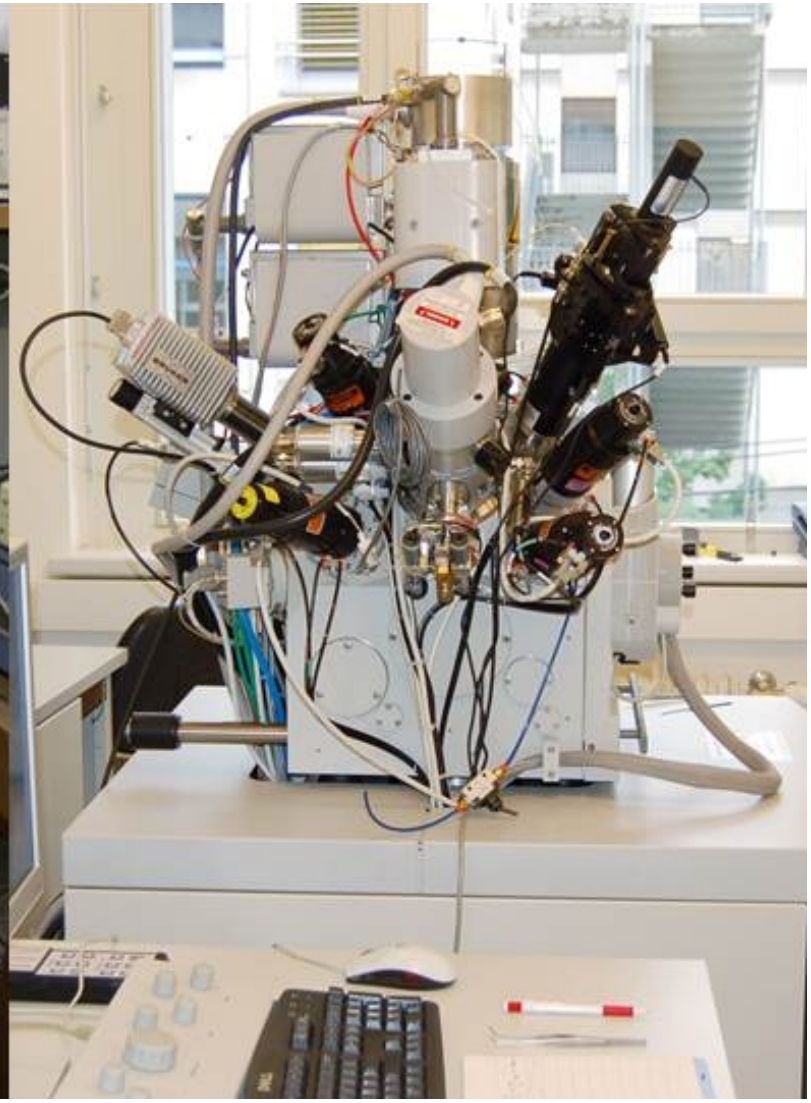
Semi-Invasive Attack - Example



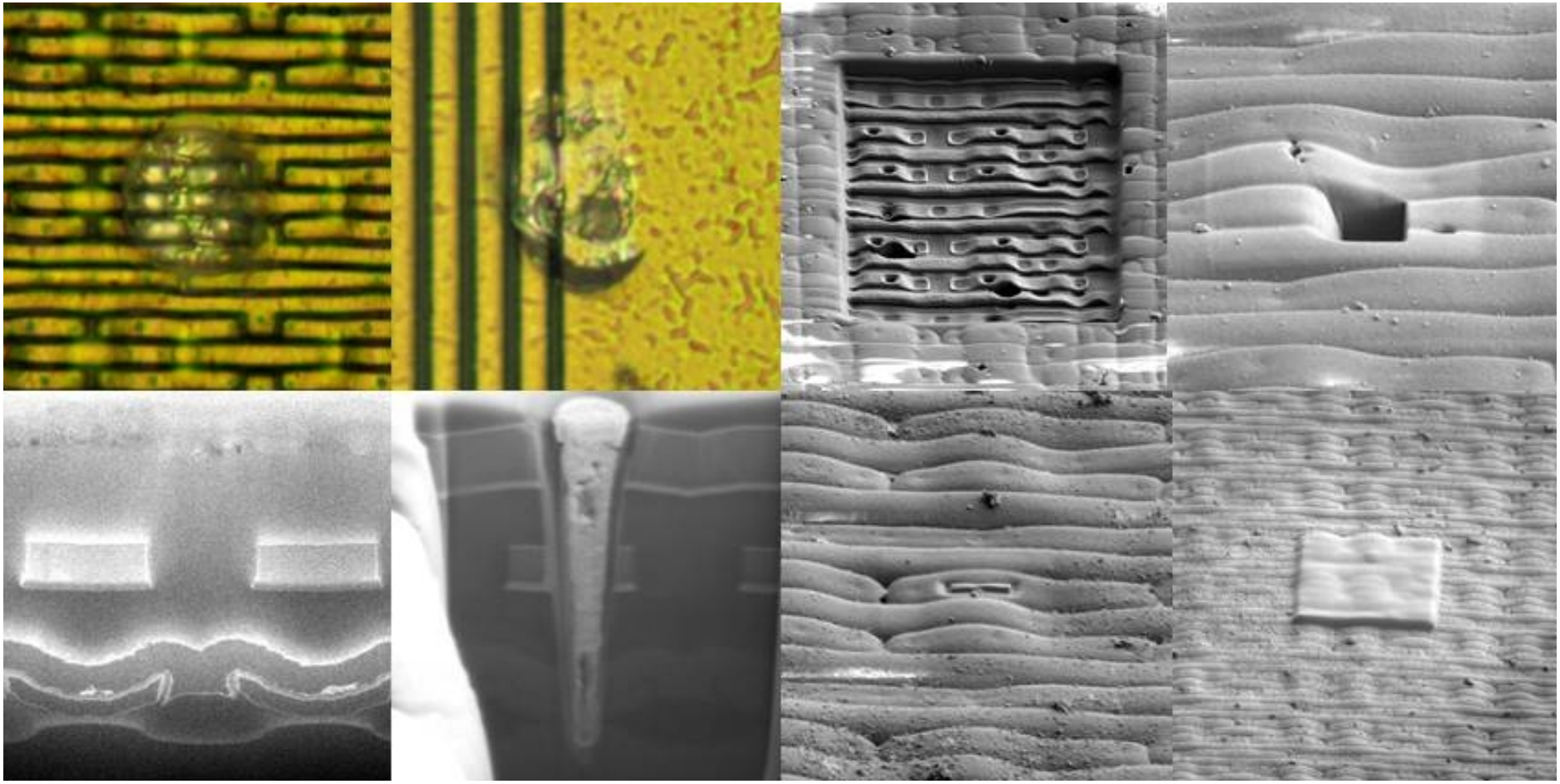


- AES on an 8-bit microcontroller (FDTC 2009 [19])
- Modifying 256-bit S-box table stored in flash memory using a low-cost UV lamp
  - UV-light resistant marker protects remaining memory
- Byte fault allows recovering of entire key (using 2 500 pairs of correct and faulty encryptions)

Invasive Attack Setups (1)



Invasive Attack Setups (2)



Picture courtesy of Dr. Jörn-Marc Schmidt

Exploitation of Faults

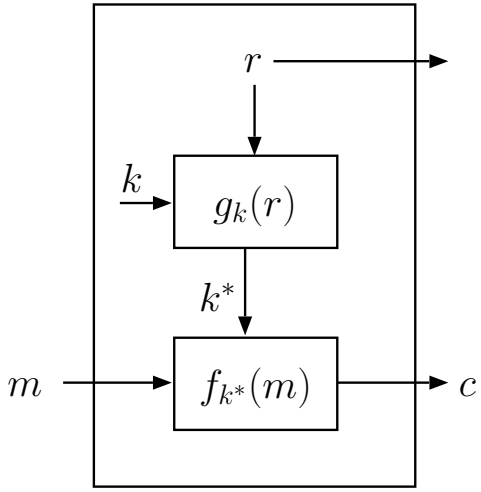
- Algorithm-specific attacks, e.g., in ECC
  - Manipulation of input parameters, e.g., base point [3]
  - Operations are done on a twist where ECDLP is easier to solve
  - Recover ephemeral key in ECDSA [14]
- Differential Fault Analysis (DFA)
  - Exploitation of differential information
  - Collection of correct and faulty outputs
  - Solve differential fault equations with cryptanalysis techniques
- Instruction-skipping attacks
  - E.g., skip square-and-multiply operations of RSA [17]
- Safe-error attacks
  - Exploit faults in key-dependent operations
  - Faults in computational part: C safe-errors
  - Faults in memory: M safe-errors

Hardware Countermeasures

- Sensors and filters
  - Detection of frequency changes
  - Power watchdogs, light detectors, temperature sensors, ...
- Hardware redundancy
  - Parallel computation, check result at the end
  - Double memory, e.g., dual-rail logic
- Hiding and masking
  - Randomize the computation (dummy random cycles, asynchronous designs, unstable clocks, ...)
  - Obfuscation: bus scrambling, memory encryption, glue logic, ...
- Shielding
  - Active shielding (wire mesh on chip surface that detects interruptions)
  - Passive shielding (metal plate, additional metal layers, ...)
- Switch to newer CMOS process technology
  - Smaller transistors are usually harder to attack...

Software Countermeasures (1)

- General countermeasures [10]
  - Checking input/output parameters (e.g., ECC point-validity checks)
  - Loop counters (use invariants, calc round signature)
  - Cyclic redundancy checks (checksum is stored together with data)
  - Hiding and masking (randomization limits precision)
  - Time redundancy (calc twice and check, but: permanent faults?)
  - Inverse computations (decrypt after encryption and check input)
- Protocol-level countermeasures
  - Fresh re-keying [13]
  - "all-or-nothing" transforms [11]
  - Message modifications [4]



Software Countermeasures (2)

- Information redundancy
  - Add parities
    - E.g., with linear codes
    - Problems: not compatible with non-linear functions like AES S-box
  - Ring embeddings [12]
    - Idea: perform operations on both data and check elements
    - E.g., embed AES field into a larger ring with data and check algebra
  - Infective computations [21]
    - Idea: output only random data if there was a fault
    - E.g., add *secret error* and remove it again at the end (or apply bit scrambling [9])

Conclusions

- There is NO 100% protection!
  - Fault attacks are very powerful
  - If you have enough resources, there are almost no limits
- Countermeasures are needed to make attacks harder
  - Designer needs to know attack types and techniques
  - Attacks are always improving - countermeasures too
- Future work
  - Passive and Active Combined Attacks (PACA)

References I

R. J. Anderson and M. G. Kuhn.

Low Cost Attacks on Tamper Resistant Devices.

In B. Christianson, B. Crispo, M. Lomas, and M. Roe, editors, *Security Protocols*, volume 1361 of *LNCS*, pages 125–136. Springer, 1997.

D. Boneh, R. A. DeMillo, and R. J. Lipton.

On the Importance of Checking Cryptographic Protocols for Faults (Extended Abstract).

In W. Fumy, editor, *EUROCRYPT '97, Konstanz, Germany, May 11-15*, volume 1233 of *LNCS*, pages 37–51. Springer, 1997.

M. Ciet and M. Joye.

Elliptic Curve Cryptosystems in the Presence of Permanent and Transient Faults.

Des. Codes Cryptography, 36(1):33–43, 2005.

Available online at `http://eprint.iacr.org/2003/028.pdf`.

References II

S. Guilley, L. Sauvage, J.-L. Danger, and N. Selmane.

Fault Injection Resilience.

In *Fault Diagnosis and Tolerance in Cryptography – FDTC, Santa Barbara, California, USA*, pages 51–65, 2010.

P. Gutmann.

Data Remanence in Semiconductor Devices.

In *USENIX 2001, USA, Washington, D.C., August 13–17, 2001*, Berkeley, CA, USA, 2001.

M. Hutter and J.-M. Schmidt.

The Temperature Side-Channel and Heating Fault Attacks.

In P. Rohatgi and A. Francillon, editors, *CARDIS 2013, Berlin, Germany, November 27-29*. Springer, 2013.

References III


M. Hutter, J.-M. Schmidt, and T. Plos.
RFID and its Vulnerability to Faults.
In E. Oswald and P. Rohatgi, editors, *CHES 2008, Washington DC, USA, August 10-13*, volume 5154 of *LNCS*, pages 363–379. Springer, August 2008.


M. Hutter, J.-M. Schmidt, and T. Plos.
Contact-Based Fault Injections and Power Analysis on RFID Tags.
In *European Conference on Circuit Theory and Design 2009, ECCTD*, 2009.


M. Joye, P. Manet, and J.-B. Rigaud.
Strengthening Hardware AES Implementations against Fault Attacks.
IET Information Security, 1(3):106–110, Sept. 2007.


M. Joye and M. Tunstall.
Fault Analysis in Cryptography.
Springer, 2012.

References IV

R. P. McEvoy, M. Tunstall, C. Whelan, C. C. Murphy, and W. P. Marnane.

All-or-Nothing Transforms as a Countermeasure to Differential Side-Channel Analysis.

Cryptology ePrint Archive, Report 2009/185, 2009.

M. Medwed and J.-M. Schmidt.

A Continuous Fault Countermeasure for AES Providing a Constant Error Detection Rate.

In L. Breveglieri, M. Joye, I. Koren, D. Naccache, and I. Verbauwhede, editors, *FDTC, Santa Barbara, California, 21 August*, volume 7, August 2010.

M. Medwed, F.-X. Standaert, J. Großschädl, and F. Regazzoni.

Fresh Re-keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices.

In D. J. Bernstein and T. Lange, editors, *AFRICACRYPT, Stellenbosch, South Africa, May 3-6*, volume 6055 of *LNCS*, pages 279–296. Springer, 2010.

References V

D. Naccache, P. Q. Nguyen, M. Tunstall, and C. Whelan.

Experimenting with Faults, Lattices and the DSA.

In S. Vaudenay, editor, *PKC 2005, Les Diablerets, Switzerland, January 23-26*, volume 3386 of *LNCS*, pages 16–28. Springer, January 2005.

M. Otto.

Fault Attacks and Countermeasures.

PhD thesis, Universität Paderborn, 2005.

J.-J. Quisquater and D. Samyde.

ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards.

In I. Attali and T. P. Jensen, editors, *Smart Card Programming and Security, E-smart 2001, Cannes, France, September 19-21*, volume 2140 of *LNCS*, pages 200–210. Springer, 2001.

References VI

J.-M. Schmidt and C. Herbst.

A Practical Attack on Square and Multiply.

In *FDTC*, pages 53–58, 2008.

J.-M. Schmidt and M. Hutter.

Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results.

In K. C. Posch and J. Wolkerstorfer, editors, *Austrochip 2007, October 11, Graz, Austria*, pages 61–67. Verlag der Technischen Universität Graz, October 2007.

J.-M. Schmidt, M. Hutter, and T. Plos.

Optical Fault Attacks on AES: A Threat in Violet.

In D. Naccache and E. Oswald, editors, *FDTC 2009, Lausanne, Switzerland, September 6*, pages 13–22. IEEE-CS Press, September 2009.

References VII

S. P. Skorobogatov.

Data Remanence in Flash Memory Devices.

In J. R. Rao and B. Sunar, editors, *CHES 2005, Edinburgh, UK, August 29 - September 1*, volume 3659 of *LNCS*, pages 339–353. Springer, 2005.

S.-M. Yen, S.-J. Moon, and J. Ha.

Hardware Fault Attack on RSA with CRT Revisited.

In *ICISC 2002, Seoul, Korea, November 28-29*, volume 2587 of *LNCS*, pages 374–388. Springer, 2003.

Thanks for attention!

Questions?

Michael Hutter
michael.hutter@iaik.tugraz.at
Graz University of Technology