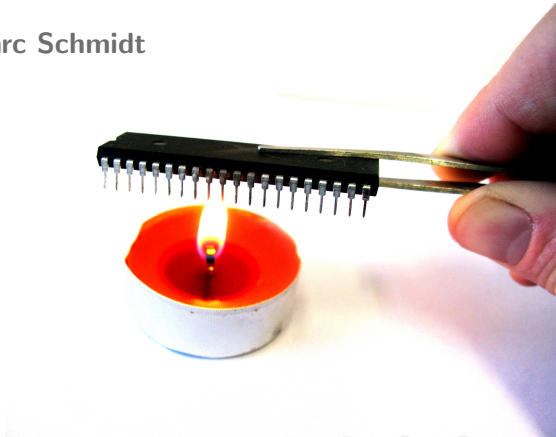


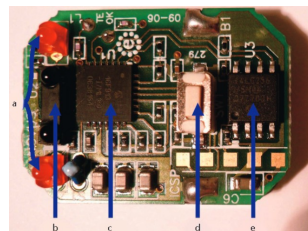
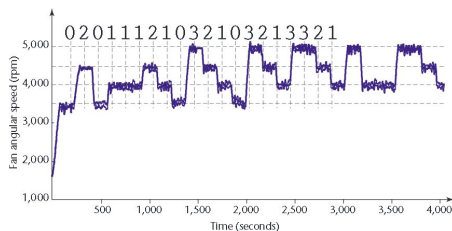
The Temperature Side Channel and Heating Fault Attacks

Michael Hutter and Jörn-Marc Schmidt



Related Work

- A. Shamir and E. Tromer - “Acoustic cryptanalysis” (2004) [12]
 - ▶ Heat causes mechanical stress expressed as low-level acoustic noise
 - ▶ Exploit the acoustic emissions to get information about processed data
- Several low-temperature attacks
 - ▶ S. Skorobogatov [13] and D. Samyde et al. [11]
 - ▶ Cooling down SRAM (-50°C) will *freeze* the data
 - ▶ Allows reading out of data even after seconds after power down
 - ▶ Similar to *cold-boot attacks* [10]
- J. Bouchier et al. - “Thermocommunication” (2009) [3, 4]
 - ▶ Cooling fan can carry information about the processed data

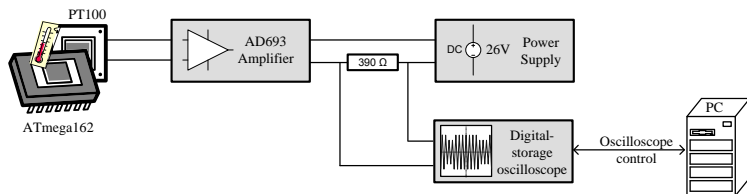


Outline

- 1 Introduction
- 2 Temperature Side Channel
- 3 High-Temperature Fault Attacks
- 4 Exploiting Data-Remanence Effects
- 5 Conclusions

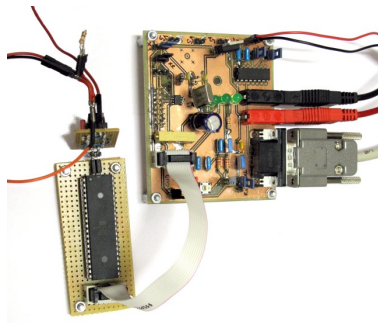
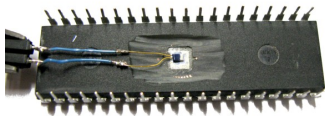
The Temperature Side Channel

- Electrical current causes heat
- Heat is proportional to the power consumption
- Temperature of the ATmega162 is measured using a Resistance Temperature Detector (PT100 RTD sensor)
- AD693 is an analog conditioning circuit to amplify the sensor signals (voltage to current converter, 4...20 mA to 0...104 °C)



The Measurement Setup

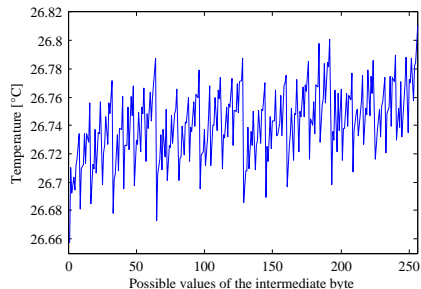
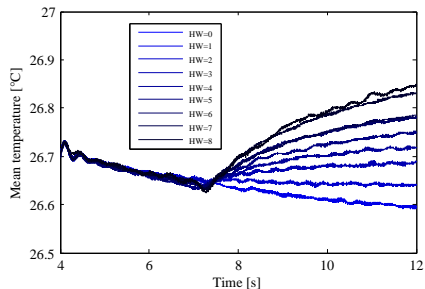
- Rear-side de-capsulated chip
- The silicon substrate offers a good thermal conductivity for the RTD sensor (about $150 \text{ W/m} \cdot \text{K}$)



Temperature Leakage Characterization

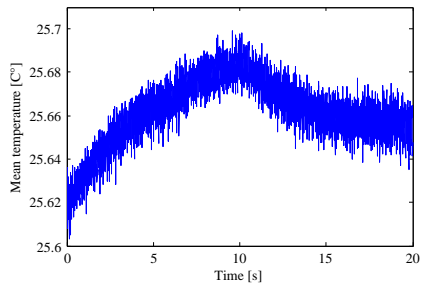
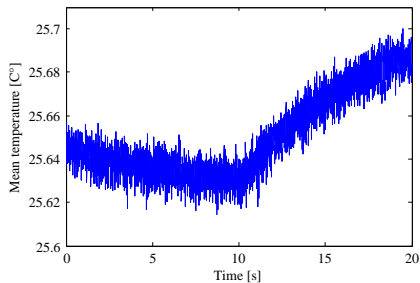
- We measured the temperature dissipation of various instructions, e.g. MOV, ADD, EOR, and MUL
- Evaluated the impact of thermal conductivity and capacitance
 - ▶ Targeted one byte that is processed and stored in 24 internal registers (and cleared before writing)
 - ▶ Executed the instructions in a loop
- Long acquisition window of 20 seconds
 - ▶ First 10 seconds: process zero values
 - ▶ Second 10 seconds: process all possible byte values (2^8)
 - ▶ We averaged 100 traces per value to reduce noise

AVR Results



- The temperature side-channel obviously leaks the Hamming weight of the processed data
- Data caused an averaged DC increase/decrease (0.3°C)

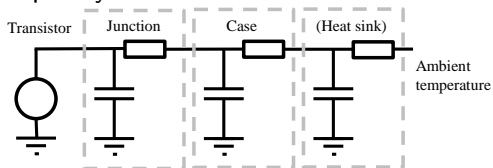
PIC16F84 Results



- Leakage of 0x00 → 0xFF (left plot) and 0xFF → 0x00 (right plot)
- No chip decapsulation
- RTD placed on top of package

Observed Characteristics

- Temperature variation is limited by the physical property of thermal conductivity
- Heat flow can be seen as a (low-pass) RC network with cut-off frequency of some kHz



- Higher frequency leakages are filtered
- Temperature sensor has limitations in response time and acquisition resolution (100 ms and 0.01 °C)

Attack Scenarios and Ideas

1 Loops and continuous leakages

- ▶ Implementation repeatedly checks a password (as similarly argued by Brouchier et al. [3, 4])
- ▶ Password is written continuously from memory into registers
- ▶ The dissipated temperature can then be exploited to reveal the password

2 Exploiting static leakage

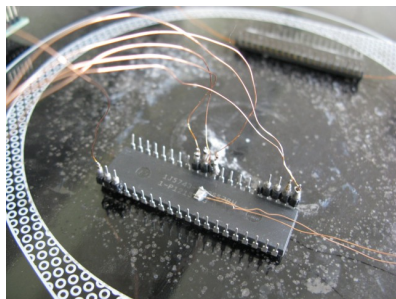
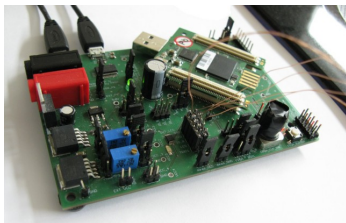
- ▶ Assuming a device is leaking information in the static power consumption (already shown by, e.g., Giogetti et al. [7] or Lin et al. [9])
- ▶ The clock signal can then be stopped, e.g., after the first AES S-box operation
- ▶ Intermediates can be extracted from the temperature side channel
- ▶ *Advantage*: plenty of time available to measure the temperature leak

Exploiting Heating Faults

- Well known attack, but less details available in literature
- The device is exposed to extensive heating ($> 150^{\circ}\text{C}$)
 - ▶ ATmega162 operated beyond the maximum ratings
 - ▶ Target implementation was CRT-RSA
- Bellcore attack [2]
 - ▶ CRT allows computing two exponentiations in smaller sub-groups (faster)
 - ▶ Signature $S \equiv \text{CRT}((m^d \bmod p), (m^d \bmod q)) \bmod n$
 - ▶ Injection of a random fault Δ causes the device to output a faulty signature $\tilde{S} \equiv \text{CRT}((m \bmod p)^d, (m \bmod q)^d + \Delta) \bmod n$
 - ▶ Now $p = \gcd(\tilde{S} - S, n)$ can be calculated to factorize n and to reveal the RSA primes p and q

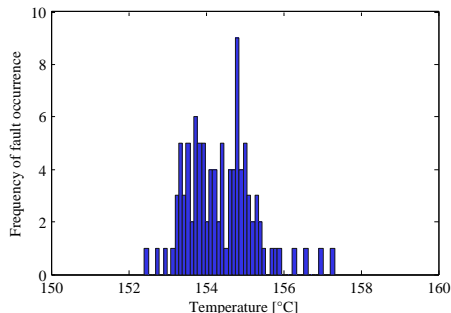
The Used Setup

- Laboratory heating plate from Schott instruments (SLK 1)
 - ▶ ATmega162 placed directly on top of the hot-plate surface
 - ▶ Temperature measured with two PT100s
- “Flying” connections
 - ▶ Exposed wires to avoid any contact to the hot plate: *serial connection, power supply, clock signal, and reset*
- Controller
 - ▶ Spartan-3 FPGA-based board
 - ▶ Allows turning off/on signals



Results

- ATmega162 does not respond after 160 °C
- Faults occurred between 152 and 158 °C
 - ▶ Within 70 minutes, we got 100 faults
 - ▶ 31 revealed one of the prime modulus: 15 revealed p , 16 revealed q
 - ▶ 7 faults produced the same RSA output
- Same result also for other ATmega162 devices
 - ▶ E.g., 182 faults within 30 minutes
 - ▶ Mean and fault temperature varies per device

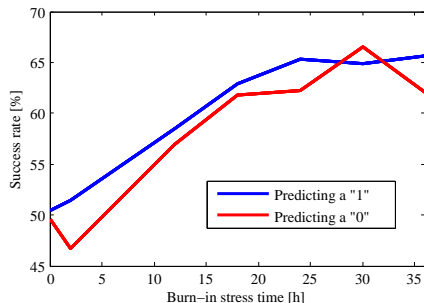


Exploiting Data-Remanence Effects

- Data stored in SRAM for a long period of time leaves a permanent mark, cf. P. Gutmann [8]
- Can be recovered by reading out the preferred power-up values
 - ▶ Practically exploited by R. Anderson and M. Kuhn [1] in 1997, recovered over 90 % of a DES key of a late 1980s bank card
 - ▶ Harder on newer SRAM structures, 18 % recoverable (cf. Cakir [5])
- Effect is due to aging where transistor parameters change (speed, current drive, noise margin)
- Extensive heating accelerates aging
 - ▶ **Negative Bias Temperature Instability (NBTI)**
 - ▶ SRAM cells get “weaker” and tend to a certain bit value
- Two NBTI degradation components: *permanent* and *transient* damage [6]

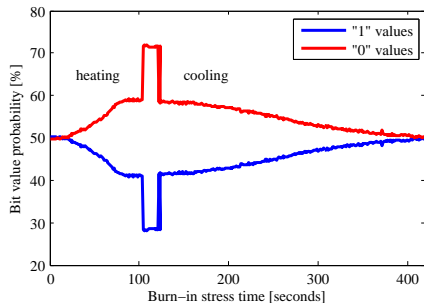
Permanent Data Remanence Effect

- 1 Tests performed on new ATmega162; preferred power-up values are around 50 %
- 2 We wrote randomly distributed data to SRAM (3072 bits to "1" and 3072 bits to "0", 6144 out of 8192 bits total)
- 3 Exposed the device to extensive burn-in stress
 - ▶ 100 °C for 36 hours at 5.5 volts
 - ▶ SRAM cells got biased:
52.24 % → 1, 47.75 % → 0
 - ▶ 919 bits (15 %) changed their state, i.e., 30 % are unstable
 - ▶ > 95 % of the bits tended to the correct value
 - ▶ In total, we can predict 63 % correctly



Transient Data Remanence Effect

- 1 Read out the SRAM content every 4 seconds during burn-in stress
- 2 Heated up to 170 °C and turned off heating afterwards
 - ▶ “Weak” SRAM cells tend to “0” during heating
 - ▶ They move back to preferred state after cooling
 - ▶ Can be used to identify “unstable” bits
 - ▶ Around 30% have been identified to be unstable



How to Exploit NBTI Degradation?

- 1 Combine revealed SRAM content of several devices
 - ▶ Assume all devices share the same secret
 - ▶ Reveal parts of the data of many devices and combine the information
 - ▶ Identify constant data, i.e., related to the key with high probability
- 2 Apply partially key exposure attacks
 - ▶ Apply burn-in stress for several hours
 - ▶ Read out the memory
 - ▶ Exploit transient NBTI effect to identify “unstable” bit locations
 - ▶ Now use previously revealed bits at these locations to obtain correct SRAM content with high probability
 - ▶ Apply cryptanalytic attacks to reveal the entire secret

Further Research Suggestions

- More NBTI tests
 - ▶ Accelerate aging while device is performing crypto operations (realistic scenario)
 - ▶ Are SRAM cells that stored constant data (key) “unstable” during transient NBTI?
- Heat penetrates through different materials (through shielding?)
- Heating or cooling will change the characteristics not only for *memory* but also for *logic*...
 - ▶ Increase/decrease threshold voltages, e.g., of watchdog circuits
- Exploit static power/temperature leakages on newer CMOS processes

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, 5th International Workshop*, 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, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceedings*, volume 1233 of *LNCS*, pages 37–51. Springer, 1997.




J. Bouchier, N. Dabbous, T. Kean, C. Marsh, and D. Naccache.

Thermocommunication.

eprint, 2009.

References II

 J. Brouchier, T. Kean, C. Marsh, and D. Naccache.
Temperature Attacks.
Security Privacy, IEEE, 7(2):79–82, 2009.

 C. Cakir, M. Bhargava, and K. Mai.
6T SRAM and 3T DRAM Data Retention and Remanence Characterization in 65nm bulk CMOS.
In Custom Integrated Circuits Conference – CICC 2012, USA, San Jose, 9-12 September, 2012, pages 1–4, 2012.

 M. Ershov, S. Saxena, H. Karbasi, S. Winters, S. Minehane, J. Babcock, R. Lindley, P. Clifton, M. Redford, and A. Shibkov.
Dynamic Recovery of Negative Bias Temperature Instability in P-type MetalOxideSemiconductor Field-Effect Transistors.
Applied Physics Letters, 83(8):1647–1649, 2003.

References III

 J. Giogetti, G. Scotti, A. Simonetti, and A. Trifiletti.

Analysis of Data Dependence of Leakage Current in CMOS Cryptographic Hardware.

In *Proceedings of the 17th ACM Great Lakes Symposium on VLSI, Stresa-Lago Maggiore, Italy, March 11-13, 2007*, pages 78–83. ACM, 2007.

 P. Gutmann.

Data Remanence in Semiconductor Devices.

In *USENIX 2001 – Proceedings of the 10th Conference on USENIX Security Symposium, USA, Washington, D.C., August 13-17, 2001*, Berkeley, CA, USA, 2001. USENIX Association.

 L. Lin and W. Burleson.

Leakage-Based Differential Power Analysis (LDPA) on Sub-90nm CMOS Cryptosystems.

In *ISCAS 2008 – IEEE International Symposium on Circuits and Systems, USA, Seattle, 18-21 May, 2008*, pages 252–255, 2008.

References IV



T. Müller and M. Spreitzenbarth.

FROST - Forensic Recovery of Scrambled Telephones.

In M. Jacobson, M. Locasto, P. Mohassel, and R. Safavi-Naini, editors, *Applied Cryptography and Network Security-ACNS 2013, 11th International Conference, Banff, AB, Canada, June 25-28, 2013. Proceedings*, volume 7954, pages 373–388, 2011.



D. Samyde, S. P. Skorobogatov, R. J. Anderson, and J.-J. Quisquater.

On a New Way to Read Data from Memory.

In *IEEE Security in Storage Workshop (SISW02)*, pages 65–69. IEEE Computer Society, 2002.



A. Shamir and E. Tromer.

Acoustic cryptanalysis - On nosy people and noisy machines.

<http://www.wisdom.weizmann.ac.il/~tromer/acoustic/>.

References V



S. Skorobogatov.

Low temperature data remanence in static RAM.

Technical report, University of Cambridge Computer Laboratory, June 2002.

Thanks for attention!

Questions?



Michael Hutter

michael.hutter@iaik.tugraz.at

Graz University of Technology