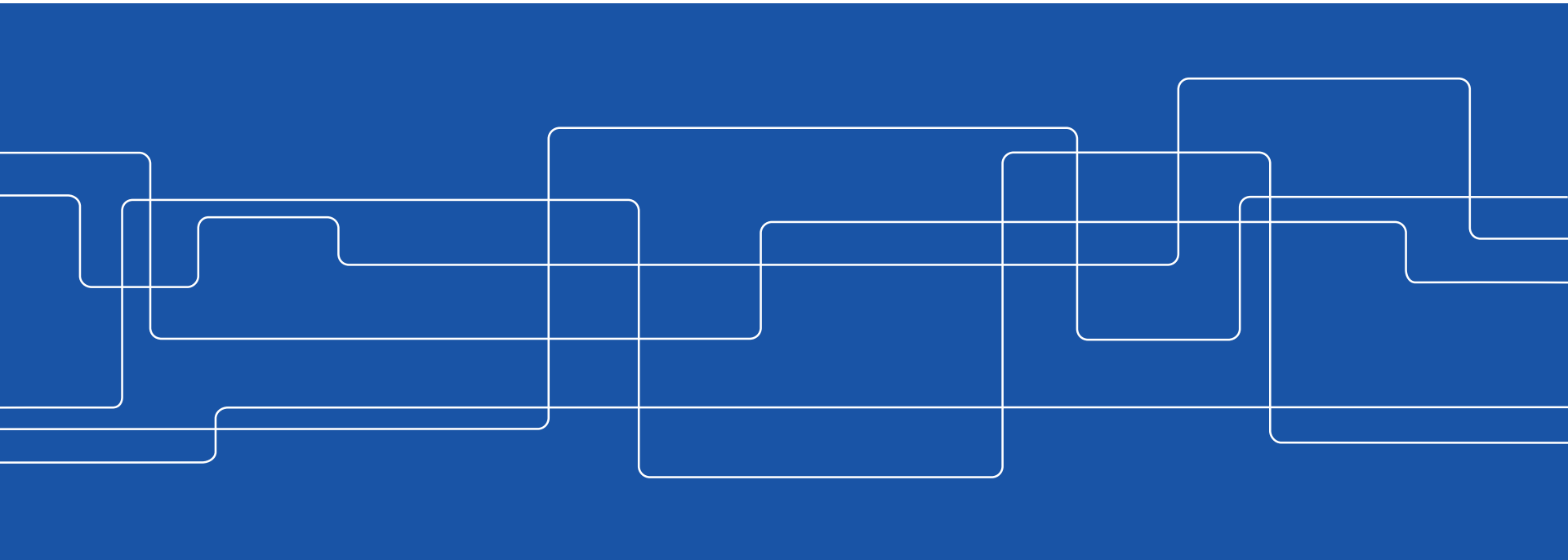
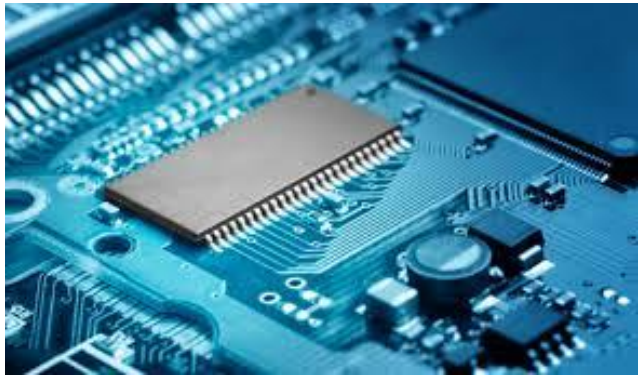
Hardware Security

Elena Dubrova
Royal Institute of Technology, Stockholm, Sweden



Overview



source: threatpost.com

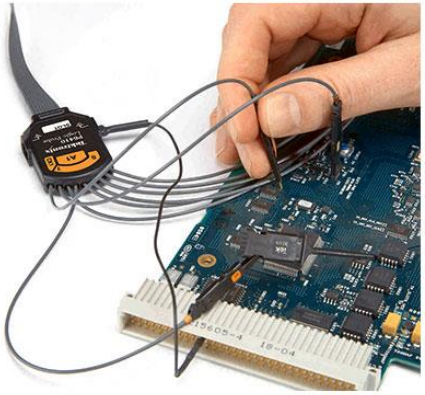
- Why hardware security is important?
- Threats to hardware
- Anti-tamper techniques
  - Tamper prevention
  - Tamper detection
  - Tamper response
  - Tamper evidence
- Summary

Sources: http://shoise.com/house-images/charming-house-images-with-house, https://fineartamerica.com/featured/southern-swamp-ester-

Why attacking hardware?

source: www.clearwater-fl.com

- Theft of service
  - Getting a service for free
    - pay-TV, parking cards, electricity meters, …
- Prevent others from getting service (denial of service attack)
  - Dishonest competition
- Theft of Intellectual Property (IP)
  - Reverse engineering/cloning/counterfeiting for marketplace advantage
- Theft of sensitive data/personal information
  - Steal secret keys, medical records, …


source: www.tek.com

How to attack?

- Break into a board/chip to reverse-engineer /clone
- Physically intrude or measure side-channel signals to extract secret keys
- Inject malicious hardware into a system
- A compromised device can potentially be used as a stepping stone to attack other devices connected to the network, or the network itself

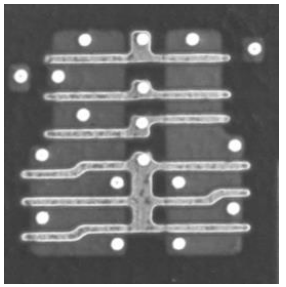
First cyberattack based on smart home appliances

Between Dec. 23, 2013 and Jan 6, 2014, more than 100.000 “smart” home appliances were used to send out more than 750.000 malicious emails targeting enterprises and individuals worldwide [1]

- home-networking routers, connected multi-medial centers, TVs, at least one refrigerator

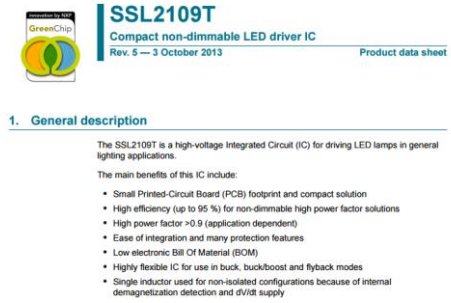
No more that 10 emails were initiated from any single IP address, making the attack difficult to block based on location

Reverse engineering



SEM image, source: [2]

source: lednews.org



SSL2109T

Compact non-dimmable LED driver IC

Rev. 5 — 3 October 2013 Product data sheet

1. General description

The SSL2109T is a high-voltage Integrated Circuit (IC) for driving LED lamps in general lighting applications.

The main benefits of this IC include:

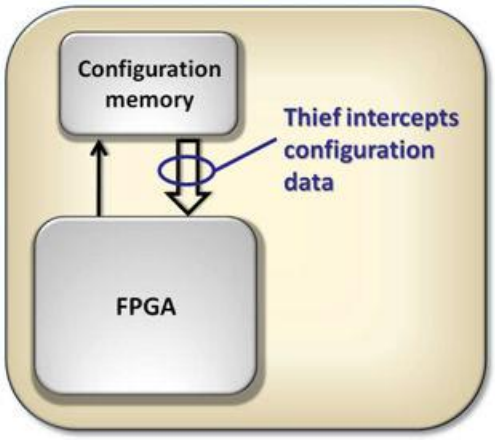
- Small Printed-Circuit Board (PCB) footprint and compact solution
- High efficiency (up to 95 %) for non-dimmable high power factor solutions
- High power factor >0.9 (application dependent)
- Ease of integration and many protection features
- Low electronic Bill Of Material (BOM)
- Highly flexible IC for use in buck, buck/boost and flyback modes
- Single inductor used for non-isolated configurations because of internal demagnetization detection and dV/dt supply

source: www.nxp.com/documents/data_sheet/SSL2109T.pdf

- Re-construct a netlist of the target design
  - sub-components are identified one by one
- Integrated Circuits (ICs) usually carry manufacturer's logo and part number
  - a mark (round or square) indicates pin order
- Data sheets are typically publicly available
- Debug interfaces, e.g. JTAG, can be used to access the internal content of a chip
  - extract program code/data
  - read or modify memory content
- There are many tools for signal monitoring and analysis (e.g. see [3-5])

Reverse engineering/cloning of FPGAs

source: www2.hdl.co.jp



source: www.eetimes.com/document.asp?doc_id=1274656

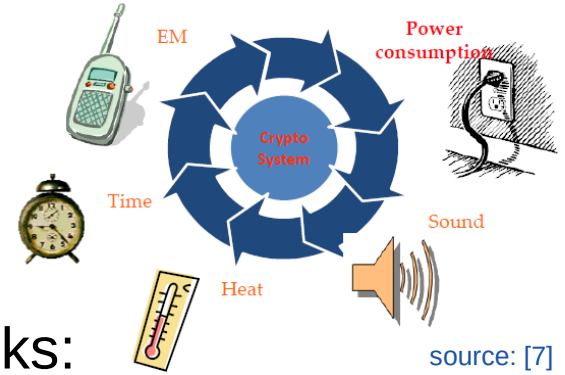
Field Programmable Gate Array (FPGA) is an IC which can to be configured by a customer after manufacturing

- contains an array of programmable logic blocks and reconfigurable interconnects
- configuration bit stream is stored in an external or internal memory and loaded on power on

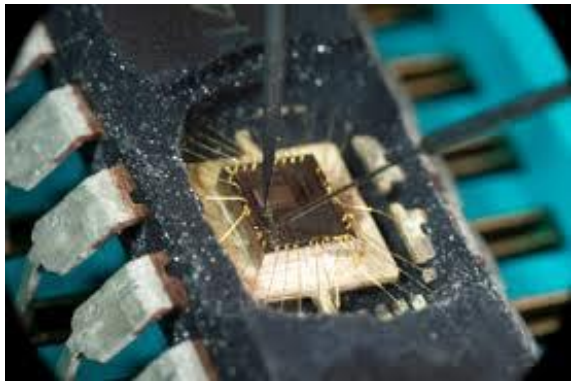
If bit stream is stored unencrypted in an external memory, it can be easily cloned

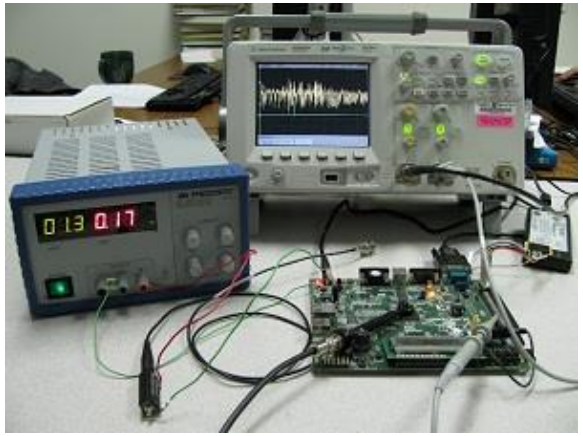
There are tools for bit stream reverse engineering, e.g. [6]

Physical attacks



source: [7]


source: sec.ei.tum.de


source: hackaday.com

- Types of physical attacks:
  - $$$ Invasive: microprobing, fault injection
  - $ Non-invasive: measuring side-channel signals (power consumption, timing, etc.), fault generation by changing supply voltage and clock signal
- The equipment to do physical attacks becomes cheaper continuously
  - With a $2,000 piece of equipment an adversary can extract practically any data from a chip if the chip is not hardened against side-channel attacks [8]

Hardware Trojans

source:www.thice.nl/hide-your-data-in-plain-sight-usb-hardware-hiding/

Malicious modifications (hardware Trojans) can open backdoors into a system in spite of cryptographic protection

source: venturesafrica.com

- Lenovo PCs are suspected to contain malicious modifications in their circuitry that could allow adversaries to remotely access devices without the users' knowledge [9]
- Some processors manufactured by Intel and Via Technologies are suspected to contain backdoors in their hardware-based Random Number Generators (RNGs) that could allow adversaries to predict RNG's output [10]

source:hardwarebbq.com

Anti-tamper techniques

- Anti-tamper techniques attempt to:
  - Prevent tampering
    - Security bits, coatings, security fuses, ...
  - Detect tampering
    - Anti-tamper sensors
  - Respond to tampering
    - Erase memory
    - Destroy chip
  - Provide evidence of tampering

I. Tamper Prevention

Tamper prevention mechanisms

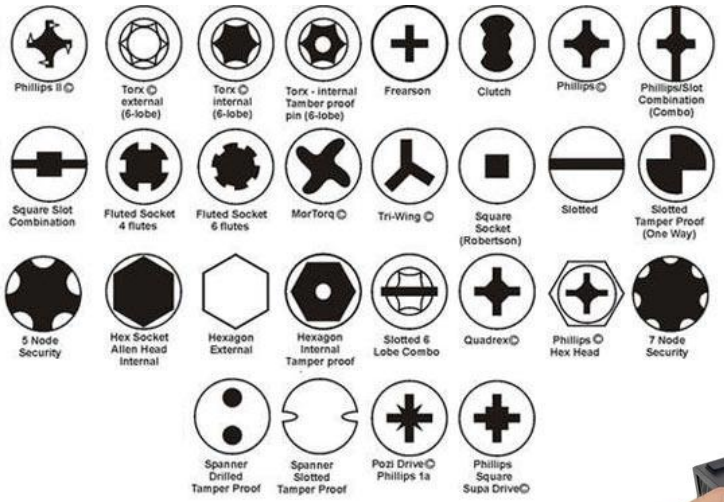
- Making housing difficult to open
- Encapsulation/Coating
- Using security fuses to prevent unauthorized access
- Layout and data bus scrambling

Tamper prevention I:
Making housing difficult to open

Make housing difficult to open by using:

- Security bits
- Adhesives
- Ultrasonic welding

Security bits



source: http://justinpaulin.com/tag/security-bits/

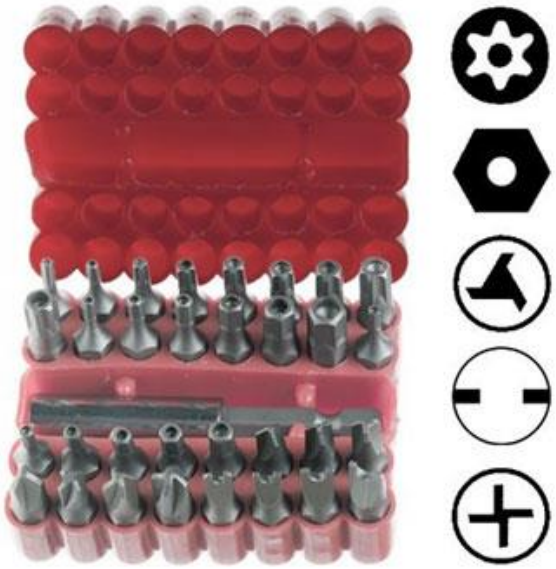
- Security bits are intended to protect outer shells from being open
- Often rubber feet or labels are used to hide them

source: [11]

source: https://www.ifixit.com/Teardown/Xbox+One+Teardown/19718/

source: http://www.androidcentral.com/how-upgrade-ram-your-hp-chromebox/

Defeating security bits



source: toolguyd.com/cheap-security-bit-sets/

- Screwdriver sets for opening security bits are easy to purchase
- The head of a security bit can be drilled out
- 3D printer can be used to create a required screwdriver

Adhesives

- High strength glue is used to hold the housing together

source: www.ifixit.com/Teardown/iPad+4+Wi-Fi+Teardown/11462

Defeating adhesives

source: www.ifixit.com

- Unless the glue is high-temperature, it will soften when heat is applied
  - Use a heat gun to soften the adhesive
  - Ran a sharp knife/plastic opening tool ($3) around the edge to separate the adhesive

Ultrasonic welding

- Applies high-frequency ultrasonic vibrations to pieces pressed together to create a one-piece outer shell
  - There are no connective bolts, nails, soldering materials, or adhesives
- Outer shell is difficult to open without a noticeable damage
  - Cooling with liquid nitrogen and filling with compressed air may crack the weld in some cases

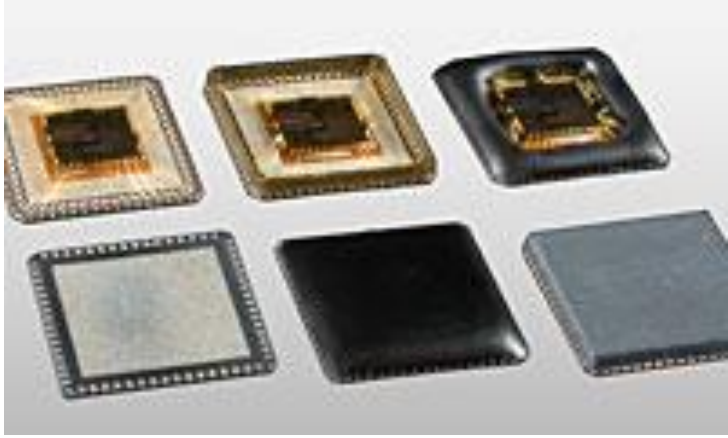
source: http://www.ebay.com/gds/How-to-Repair-a-USB-Stick-/

Tamper prevention II: Encapsulation/Coating

Encapsulation/coating is used to protect integrated circuits or boards from:

- Dust, moisture, corrosion, etc.
- Tampering, reverse engineering, cloning

Encapsulation



http://www.icproto.com/capabilities-services/ic-assembly/encapsulation-options/

Types of encapsulation include:

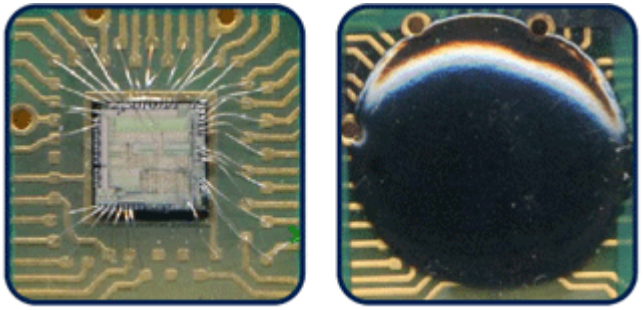
Fully Closed:

- Flattened: Packages are fully encapsulated with filled epoxy
- Glob Top: Packages are fully encapsulated with filled epoxy and have a domed surface
- Clear Encapsulant: Packages are fully encapsulated with non-filled epoxy (for bonding verification, visual samples and optical applications)

Partially Closed:

- Partial Encapsulation: Packages are encapsulated with filled epoxy in selected areas (i.e. around leads only.)

Coatings



source: http://electronics.stackexchange.com/questions/56649/what-is-a-die-package

Common coating types are [12]:

- **Acrylic**

  + Good resistance to chemicals, moisture, and abrasion (surface wear caused by rubbing), temperature resistance 150°C

  - Very easy to rework

- **Epoxy**

  + Excellent resistance to chemicals and abrasion, fair resistance to moisture, temperature resistance 150°C, hard to rework

- **Silicone**

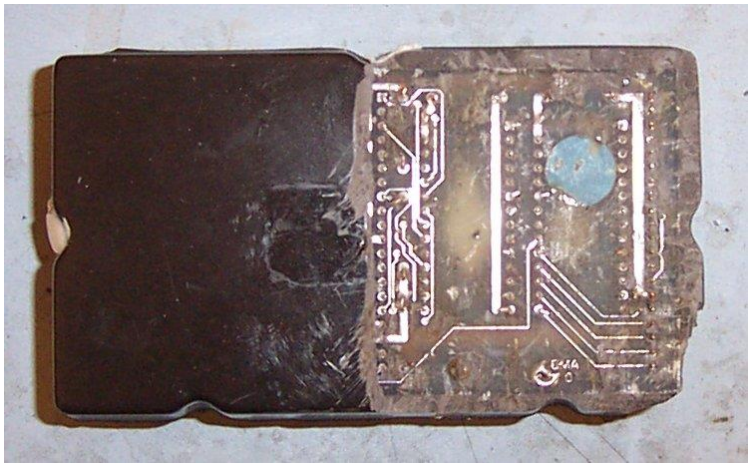
  + Good resistance to chemicals, excellent resistance to moisture, fair resistance to abrasion, temperature resistance 200°C

  - Easy to rework

Removing coating by abrasion

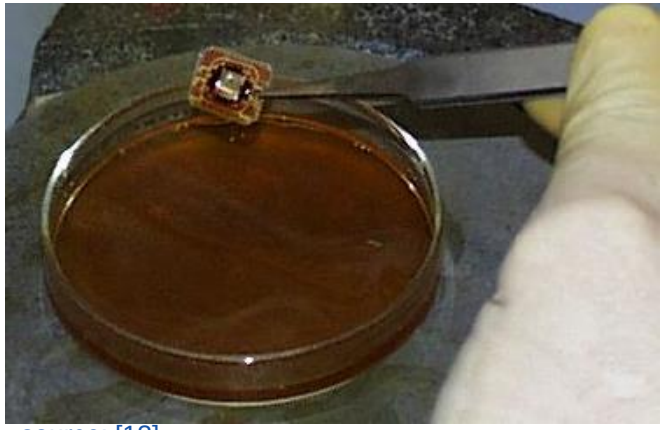
www.dremel.com/en-us/Tools

A protective layer can be often removed by rubbing the surface with knife, sand paper, using dremel tools or milling machine



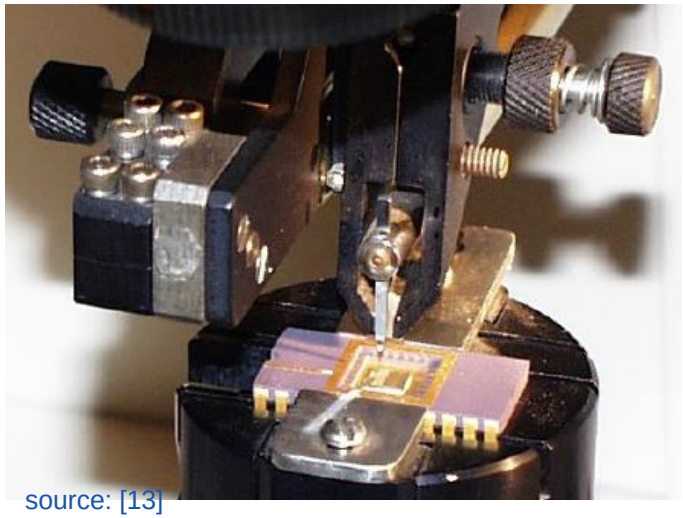
source: http://www.kevtris.org/Projects/votraxpss/unpot.html

Removing coating by chemicals



source: [13]

Hot fuming nitric acid dissolves the smartcard package without affecting the chip [13]

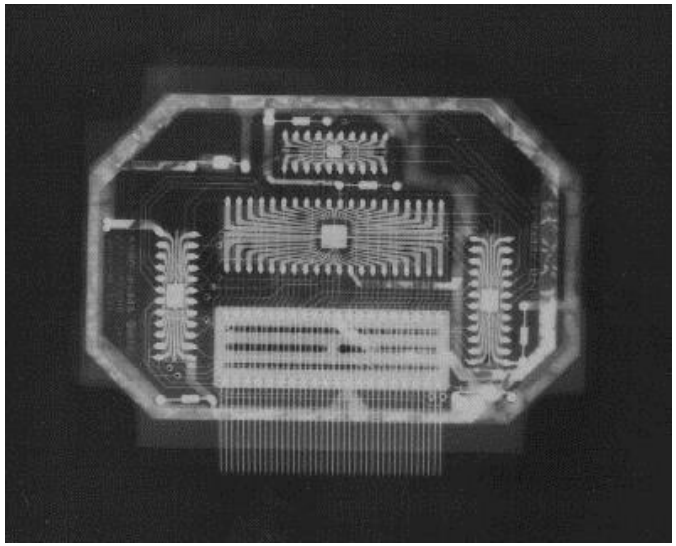


source: [13]

The de-packaged smartcard is glued into a test package, whose pins are connected to the contact pads of the chip with fine aluminum wires in a manual bonding machine [13]

Defeating encapsulation by X-ray or acoustic microscopy

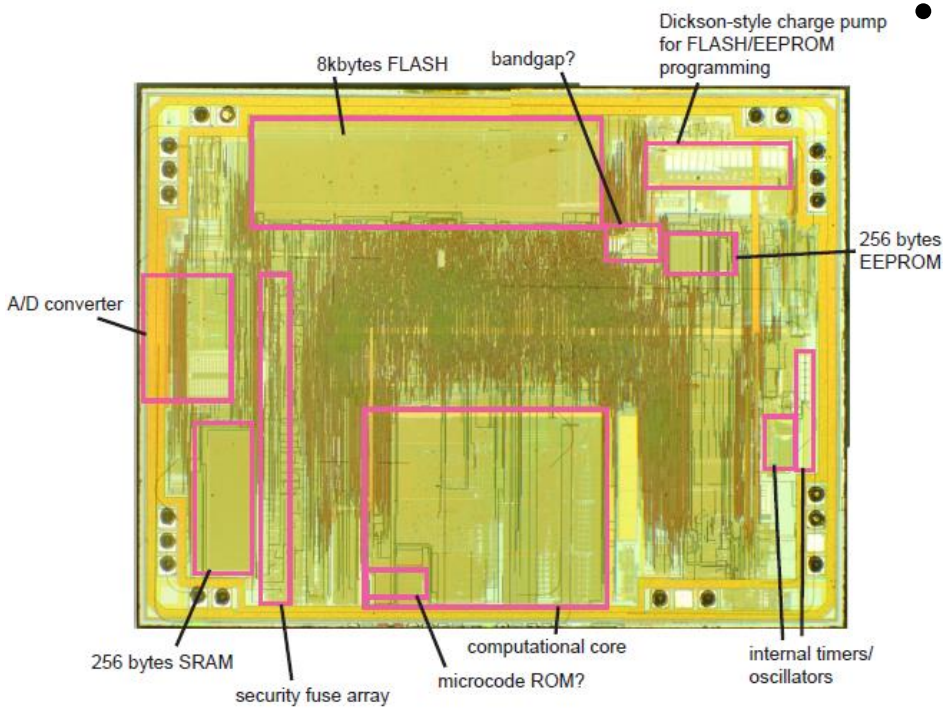
- X-ray or acoustic microscopy can be used to get images of a chip
- Helps to find out component location, hidden sensors, etc.



source: www.multigame.com/pacplus.html

Tamper prevention III: Using security fuses to prevent non-authorized access

- Security fuses can be used to protects on-chip memories from non-authorized access

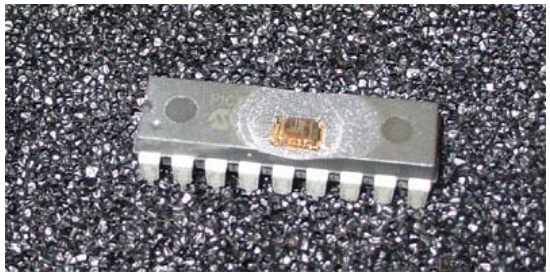


http://www.bunniestudios.com/blog/?page_id=40

- ID authentication is performed when an access is attempted; if the authentication fails, the access is not allowed
  - Modification or readback of certain regions of memory is prevented

Defeating security fuses

- Security fuses can be erased with UV light [14]
  - Metal shields over the security fuses can be surpassed by placing the chip at an angle
- To prevent the erasure of data from the Flash memory, a piece of electrical tape can be placed over the Flash
- With fuses disabled, the code stored in the Flash can be read out



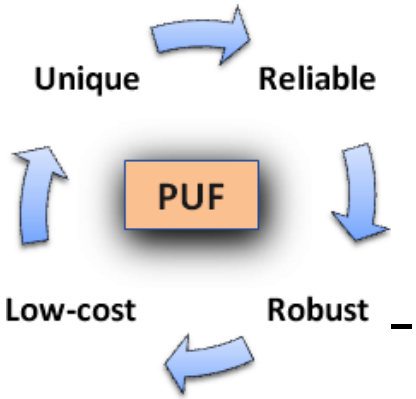
PIC 18F1320 microcontroller

http://www.bunniestudios.com/blog/?page_id=40

Countermeasures to the attack in [14]

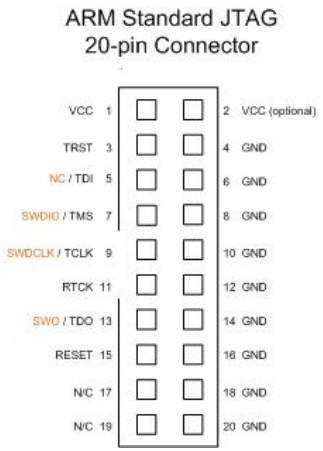
The attack presented in [14] can be mitigated using more secure methods for key storage, including

- Encode a key in a Finite State Machine (FSM) and implement the FSM on-chip by a sequential circuit [15]
  - Reverse-engineering of the chip netlist will be required to defeat this method
- Store a key using a Physical Unclonable Function [16]



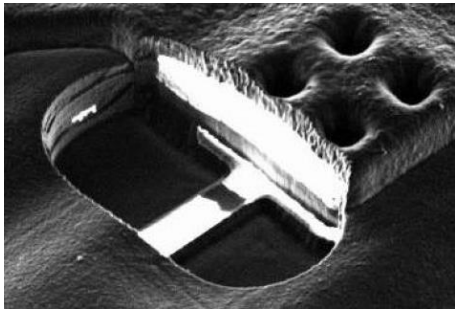
source:http://rijndael.ece.vt.edu/puf/main.html

Using security fuses to disable debug interfaces



http://www.keil.com/support/man/docs/ulinkpro/conjtag.png

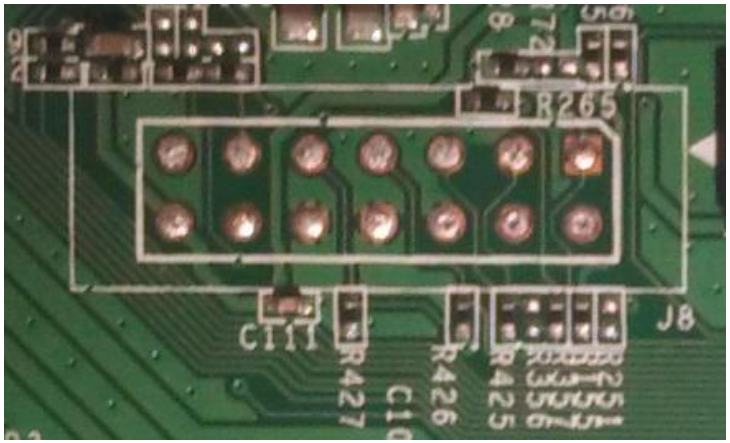
- Debug interfaces, such as JTAG, are created for chip-level testing
- Can be used to [17]:
  - Access all pins via boundary scan
  - Extract program code
  - Modify memory content
- Security fuses can be used to temporary disable or destroy debug interfaces



⇦ Focused ion beam image of a blown polysilicon fuse next to a test pad (interrupted white line at the bottom of the cavity) [13]

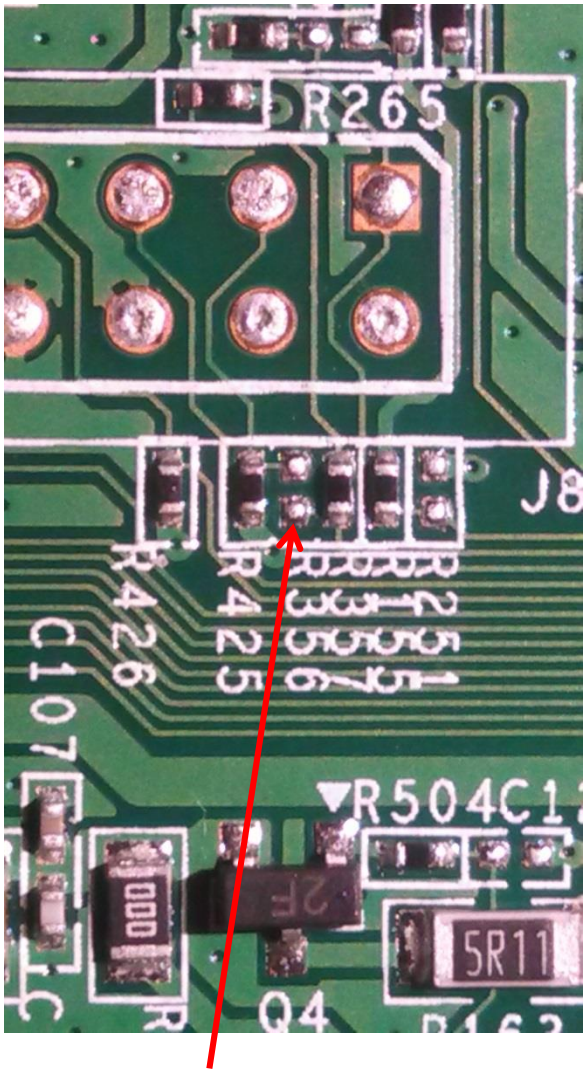
Defeating JTAG security fuses

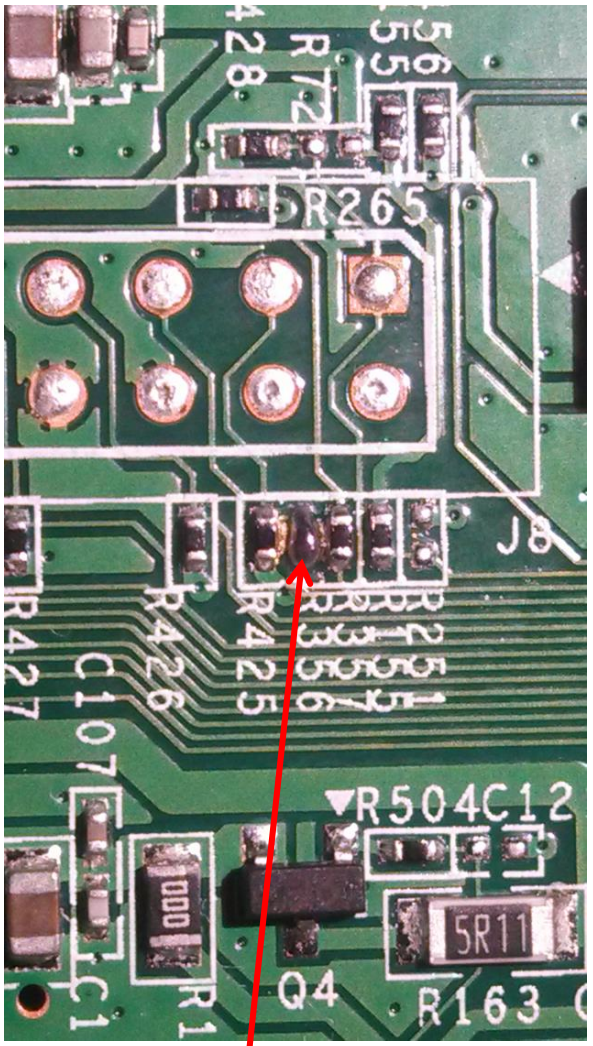
- However, destroying JTAG removes debugging capabilities, which is undesirable
- Usually JTAG is disabled rather than destroyed
  - can be enabled again



The WRT120N JTAG header

source: http://www.devttys0.com/2014/02/re-enabling-jtag-and-debugging-the-wrt120n/





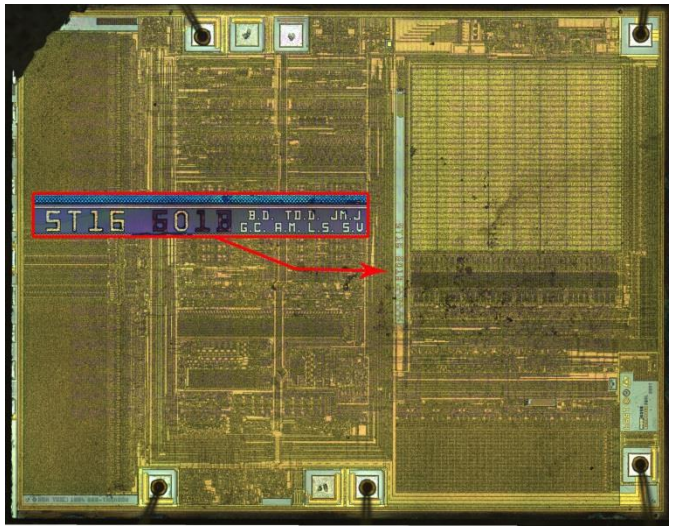
JTAG is disabled by removing jumper R356

A solder blob enables JTAG back

source: http://www.devttys0.com/2014/02/re-enabling-jtag-and-debugging-the-wrt120n/

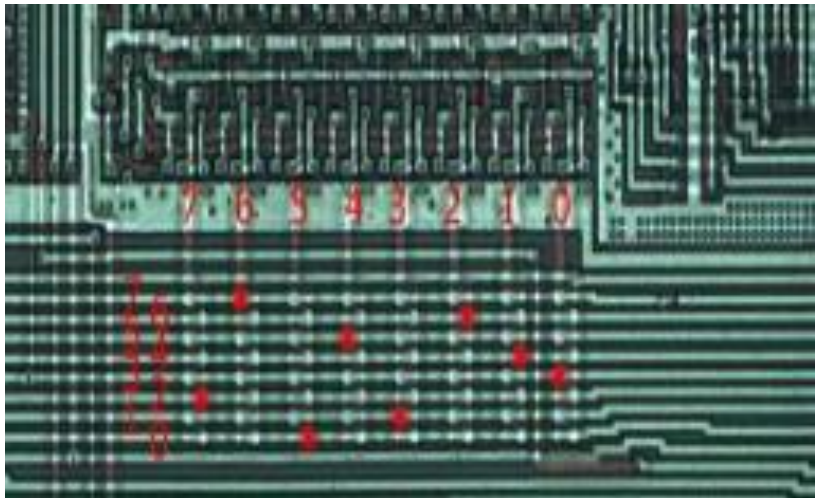
Tamper prevention IV: Layout and data bus scrambling

Layout and data bus scrambling can be used to confuse an attacker



source: [9]

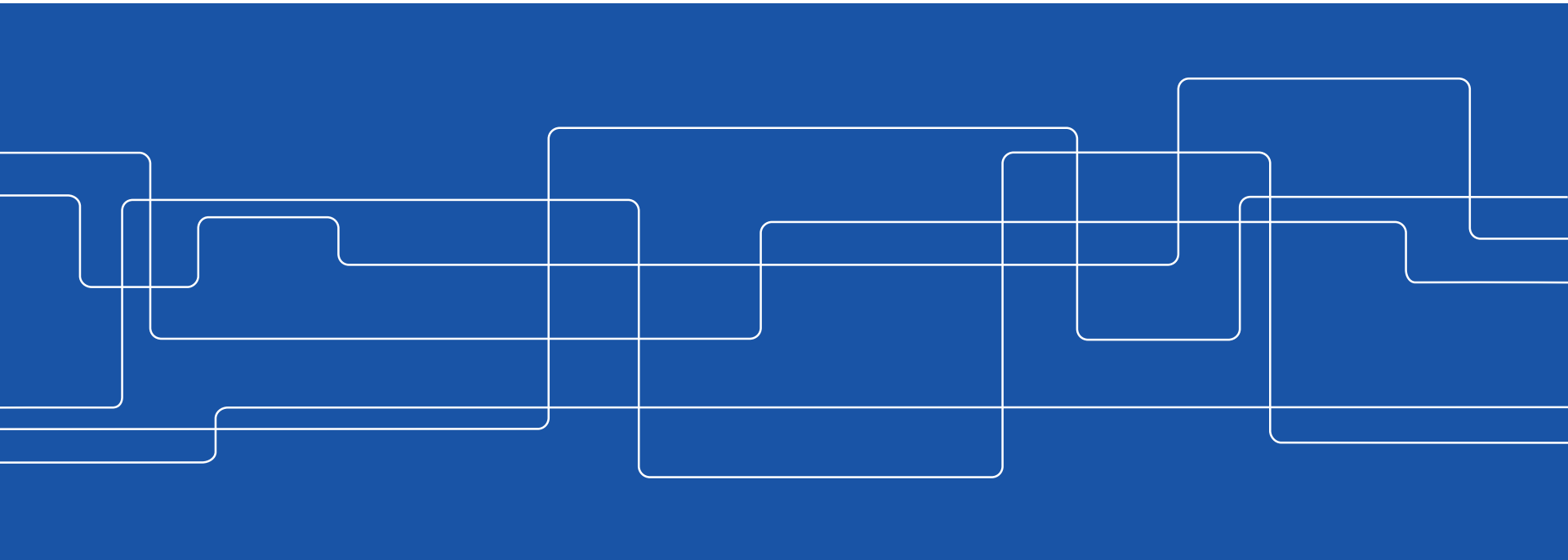
STMicroelectronics ST16601 smartcard MCU



source: [8]

Motorola SC27/28 smartcard MCU

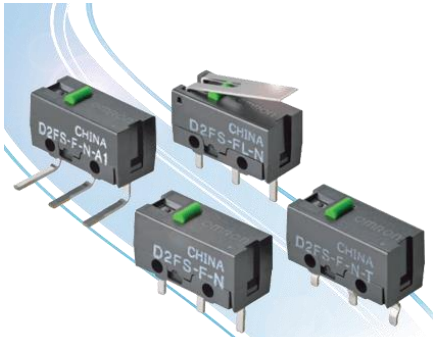
II. Tamper Detection



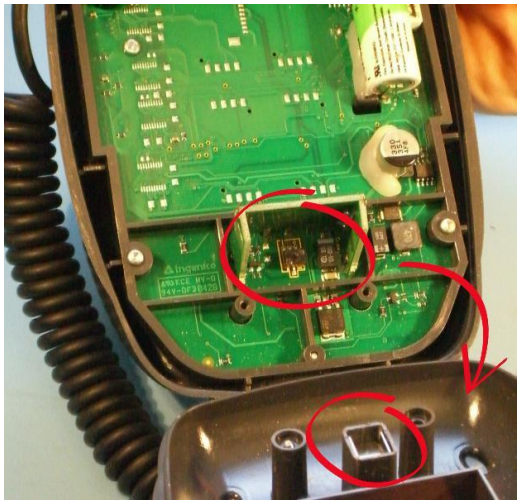
Tamper detection mechanisms

- Anti-tamper switches
- Anti-tamper sensors
- Anti-tamper circuitry

Tamper detection I: Anti-tamper switches



source: uk.farnell.com



source: ethicalhackernet.blogspot.com

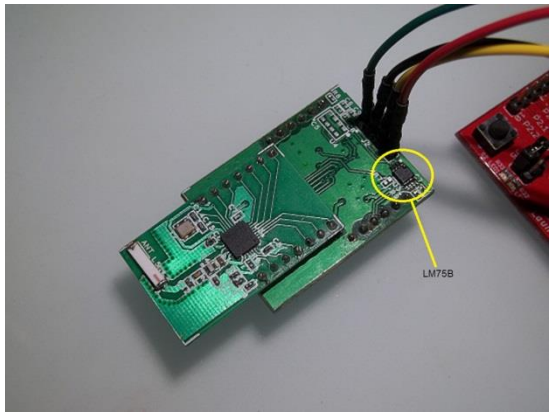
Various switches can be used to detect tampering when a cover is removed, some component is moved, or a physical security barrier is breached

- Microswitches
- Magnetic switches
- Pressure contacts

source: [1]

Tamper detection II: Anti-tamper sensors

- Temperature sensors can detect changes in operating temperature (cold boot attack)
- Voltage sensors can detect changes in operating voltage (glitch attacks)
- Radiation sensors can detect for X-rays and ion beams

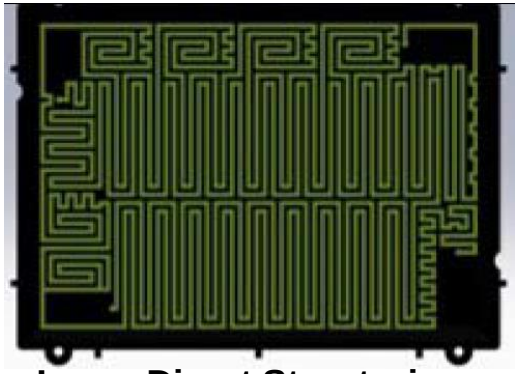


source: https://wisense.wordpress.com/2013/12/02/lm75b-temperature-sensor/

Tamper detection III: Anti-tamper circuitry

- Intrusion detection meshes such as
  - Wire meshes
  - Piezo-electric sheets
  - Fiber optics

  can be wrapped around critical hardware areas to detect an attempted intrusion
- Sensors monitoring these meshes recognize small changes in mesh's capacitance or resistance

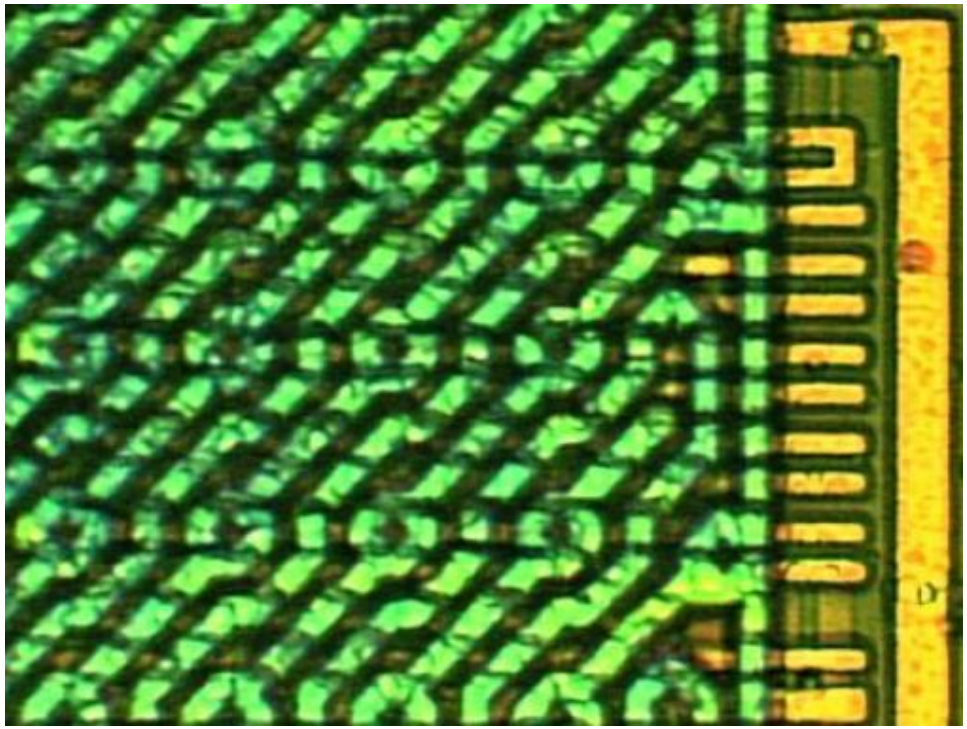


Laser Direct Structuring (LDS) circuitry shield

http://www.ecnmag.com/article/2012/04/robust-hardware-security-devices-made-possible-laser-direct-structuring

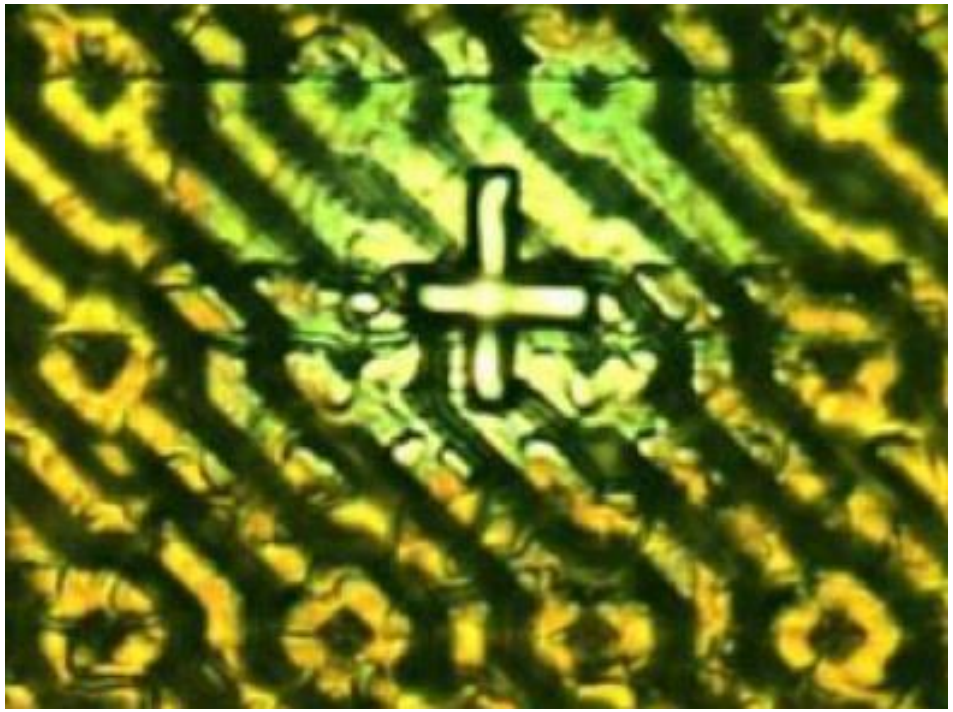
http://zch5584.buy.reelisor.com/pz5084ee1-pvdf-piezo-film-pvdf-piezo-sensor.html

Defeating anti-tamper circuitry



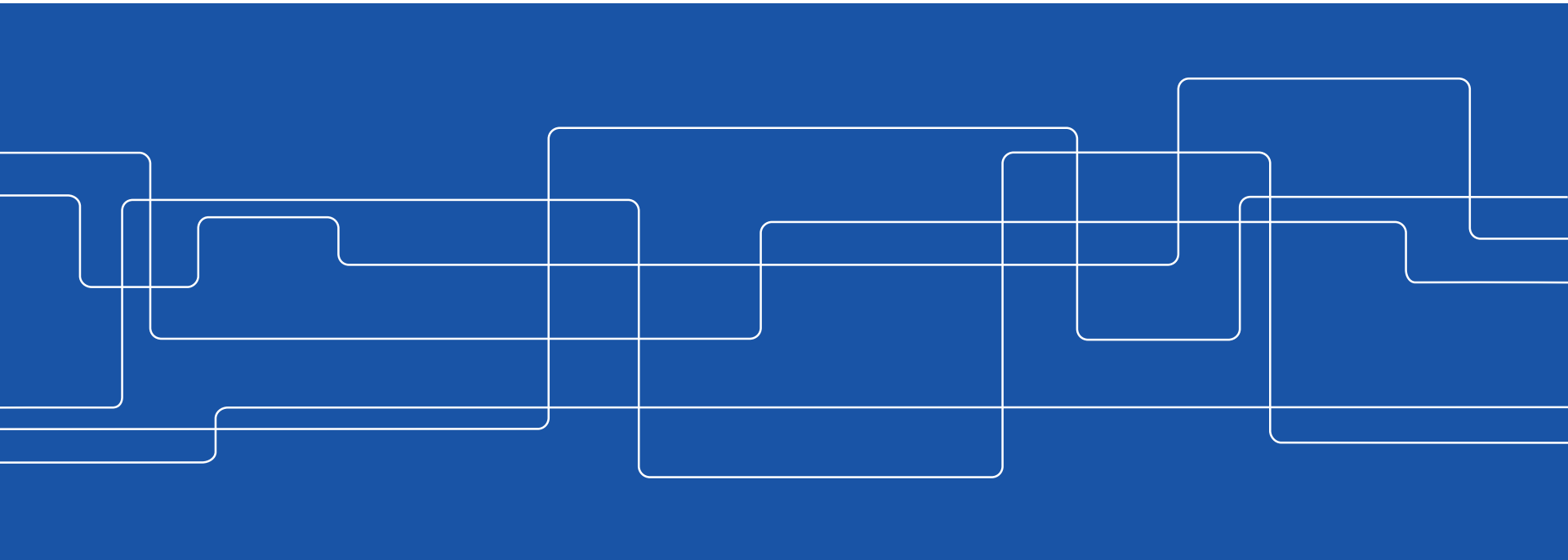
The ST16SF48A data bus extends several micrometers beyond the protected mesh area, providing easy probing access [13]

Defeating anti-tamper circuitry, cont.



A FIB was used here to drill a fine hole to a bus line through the gap between two wires [13]

III. Tamper Response



Tamper response

Tamper response is the actions taken upon the detection of tampering with a device

Possible responses include:

- Shut down or disable the device
- Erase critical parts of memory
- Physically destroy the device

Tamper response I: Memory zeroization

- Erasing critical parts of memory in response to tampering is called zeroization
- However, zeroization mechanisms often require a continuous power supply
  - the attacker can disable them before powering up a chip
- Another problem is data remanence – residuals of data remain after erasure

Data remanence in volatile memories

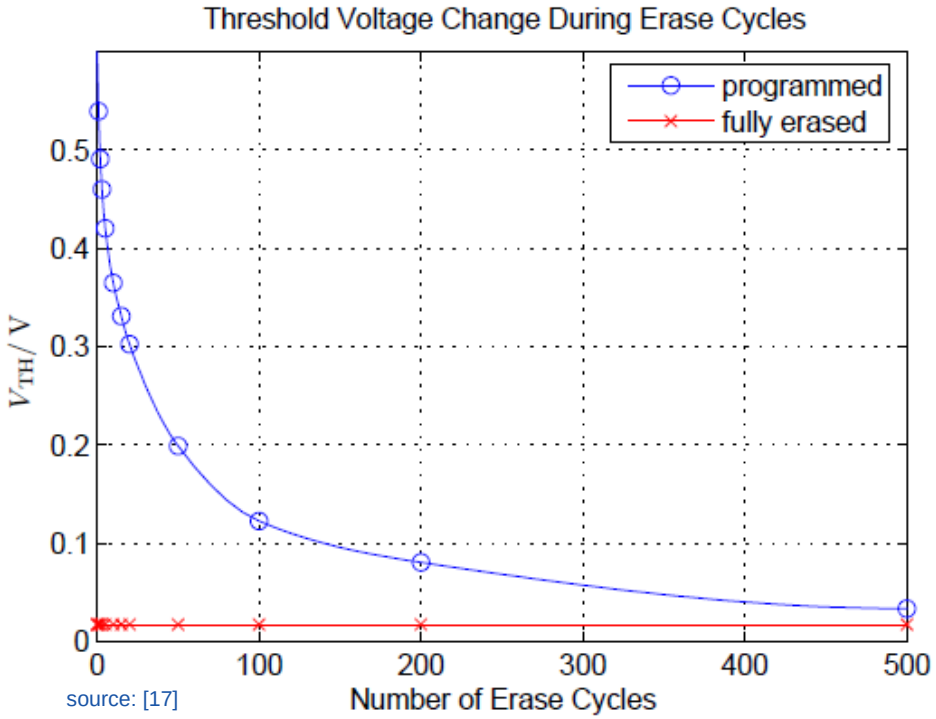
Contrary to conventional belief, volatile memories (SRAM, DRAM) do not entirely lose their contents when power is turned off [21]

- for SRAM, at room temperature the data retention time varies from 0.1 to 10 sec
- cooling SRAM to -20ºC increases the retention time to 1 sec to 17 min
- at -50ºC the retention time is 10 sec to 10 hours

source: revision3.com

Data remanence in non-volatile memories

It may take many cycles to erase data from a non-volatile memory (EEPROM, Flash, etc.)

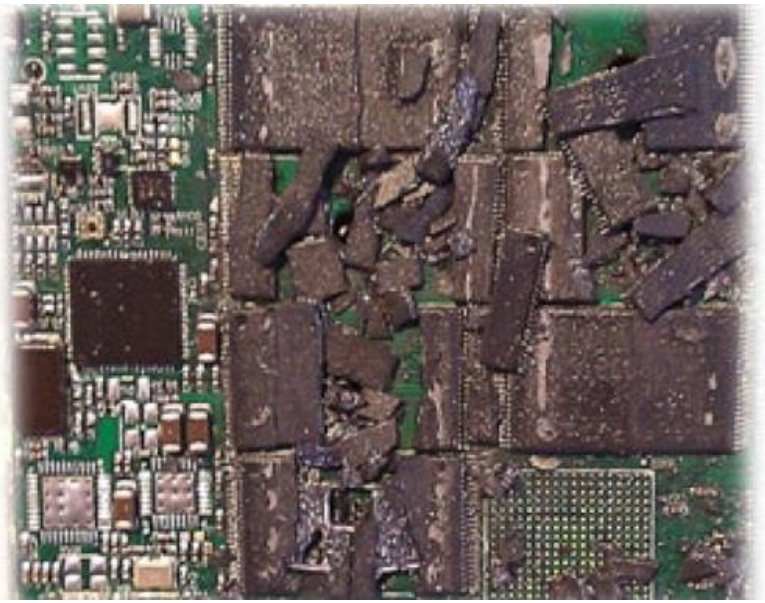


source: [17]

Data was successfully recovered from the Flash memory PIC16F84 after 10 erase cycles [22]

To overcome this problem, it is recommended to erase data by writing all-0, all-1, and random data in the memory

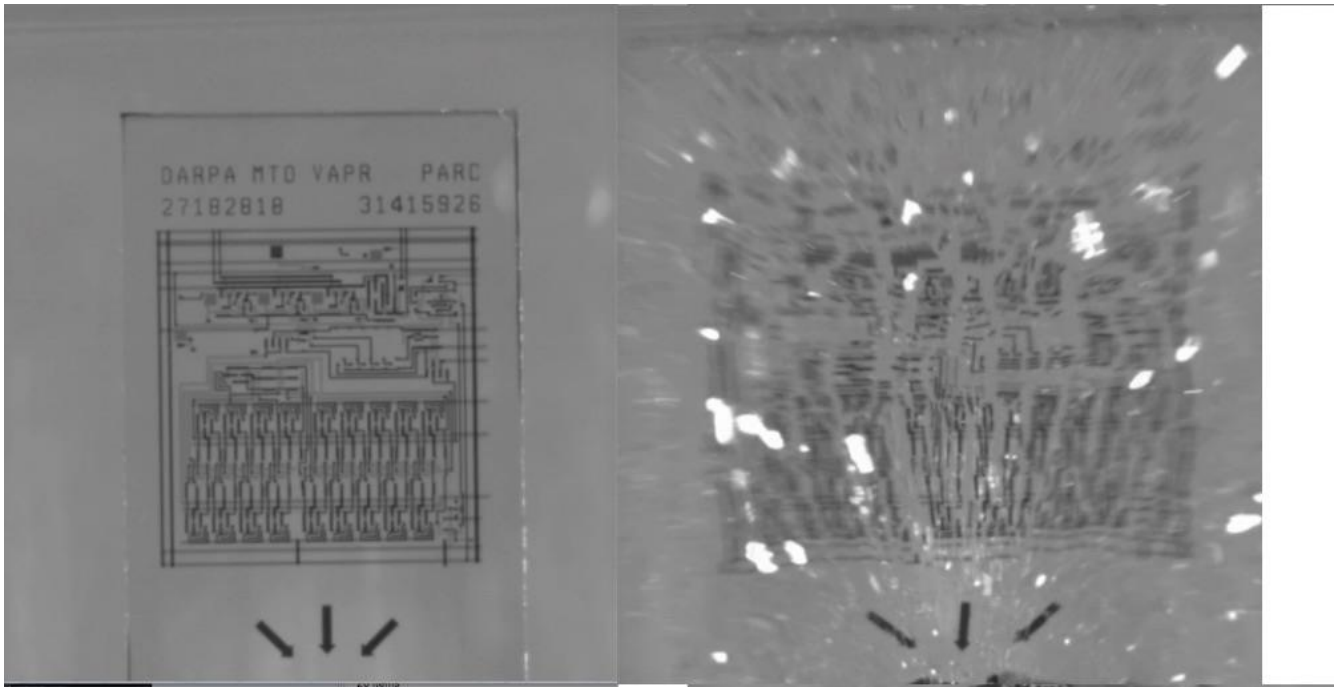
Tamper response II: Physical destruction



source: www.alphr.com

- Devices requiring very high security can be physically destroyed using, e.g. a small explosive charge
- But this option is not practical for consumer electronics
  - a chip on the left is destroyed in response to tamper detection [23]
  - $1500 hard drive,128GB

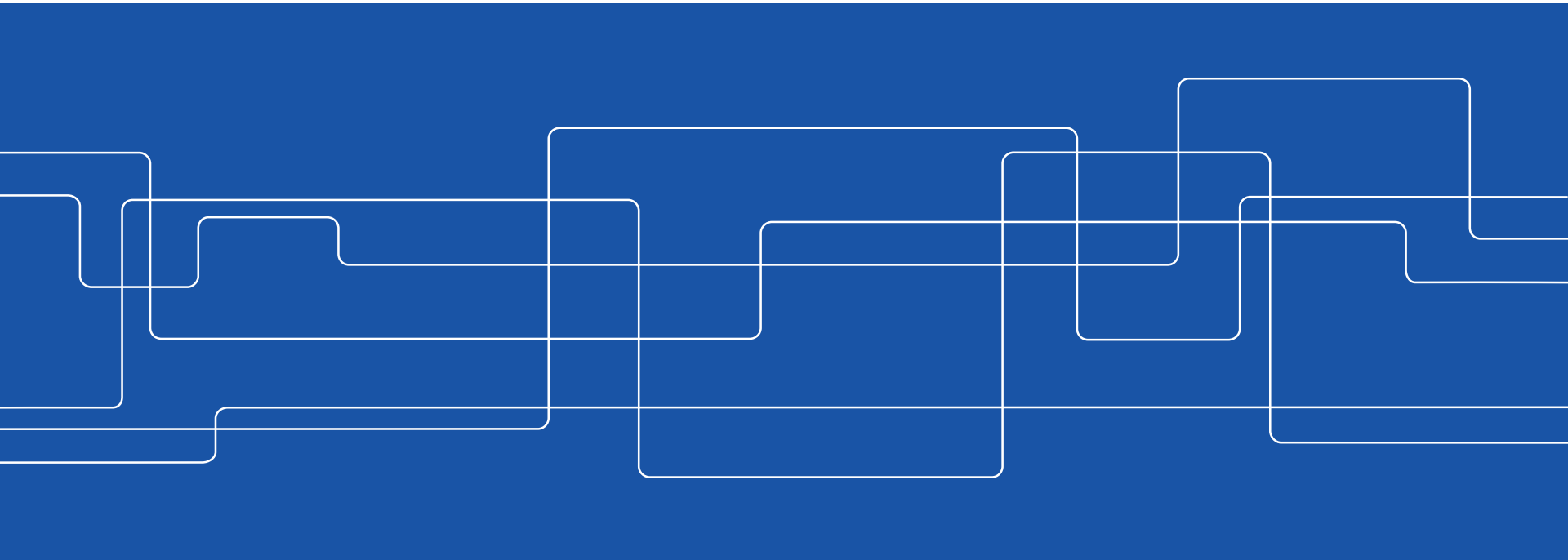
Tamper response II: Physical destruction



source: PARC, a Xerox company

Chip made of tempered glass can be triggered remotely to self destruct. The silicon computer wafers is attached to a piece of tempered glass that breaks when heated in one spot [24]

IV. Tamper Evidence



Tamper Evidence

The goal is to ensure that visible evidence is left behind when tampering occurs

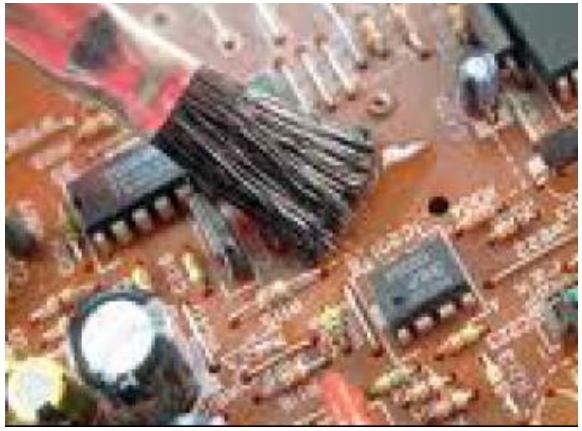
- Tamper evidence may be provided by:
  - Tamper-evident housing, e.g. ultrasonic welding creates a housing which is difficult to open without a noticeable damage

source: http://www.eprovided.com/data-recovery-blog/common-flash-drive-failure/

Tamper Evidence

- Enclosures with tamper-evident seals or locks
- Tamper-evident encapsulating materials or coatings

source: [11]



source: [11]

- "Bleeding" paint - paint of one color is mixed with micro-balloons containing paint of a contrasting color. If the painted surface is damaged, the colors blend and tampering is easy to identify [25]

Tamper Evidence, cont.

- Logging the type of detected attack and its time
  - For example, tamper detection mechanisms in electricity meters can record a tamper event in the memory and report it during the next meter reading by an authorized personnel. A tamper LED is enabled and date is recorded [26]

source: [27]

Summary

- Do not assume hardware to be trustworthy
  - Instead, design a system to be tamper-resistant
- Use a combination of anti-tamper techniques
  - A hacker will search for the weakest link and exploit it

source: rocketgirlsolutions.com


Öppna inte kaffe-maskinen
Do not open the coffee machine

Research on hardware security at KTH

- Countermeasures against hardware Trojans
- Side-channel and fault attacks and countermeasures
- Energy-efficient cryptographic primitives
  - True random number generators
  - Physically Unclonable Functions (PUFs)
- Energy-efficient cryptographic algorithms
  - Encryption
  - Message authentication

References

[1] Proofpoint Inc., ”Proofpoint Uncovers Internet of Things Cyberattacks”, Report Jan 16, 2014

[2] Advanced IC Reversed Ingeneering Techniques: In Depth Analysis of a Moder Smart Card, BlackHat USA 2015

[3] Logic Analyser, http://www.tek.com/learning/logic-analyser-tutorial

[4] OpenVizsla (USB), http://openvizsla.org

[5] Dasho (Ethernet, USB 3.0, HDMI), http://ossmann.blogspot.com/2013/05/introducing-daisho.html

[6] F. Benz et al, “Bil: A tool-chain for bitstream reverse-engineering”,*Field Programmable Logic and Applications, 2012* pp.735-738

[7] J. Liu et al, “Cloning 3G/4G SIM Cards with a PC and an Oscilloscope: Lessons Learned in Physical Security”, BlackHat USA 2015

[8] E. Worthman, “ChaoLogix: Integrated Security”, Semiconductor Engineering, 13 April 2015

[9] S. Shah, ”NSA, GCHQ ban Lenovo PCs due to security concerns, Computing, 29 July 2013

[10] D. Goodin, “We cannot trust Intel and Via’s chip-based crypto, FreeBSD developers say”, Dec. 10, 2013, http://arstechnica.com/security/2013/12/we-cannot-trust-intel-and-vias-chip-based-crypto-freebsd-developers-say

References, cont.

[11] “Physical Protection: Anti-Tamper Mechanisms in CC Security Evaluations”, http://www.yourcreativesolutions.nl/ICCC10/proceedings/doc/pp/ALVARO_ORTEGA_EPOCHE&ESPRI_Physical_protection_Anti_tamper_mechanisms.pdf

[12] Printed Circuit Design & Fab Magazine, May 2012

[13] O. Kömmerling, “Design Principles for Tamper Resistant Smartcard Processors”, Smartcard’ 99

[14] Hacking the PIC18F1320, http://www.bunniestudios.com/blog/?page_id=40

[15] N. Li, et al., “Secure Key Storage Using State Machines” **,** ISMVL'2013, pp. 290-295

[16] S. Tao et al., “An Ultra-Energy-Efficient Temperature-Stable Physical Unclonable Function in 65nm CMOS”, Electronics Letters, 2016

[17] Joe Grand, Practical Secure Hardware Design for Embedded Systems, http://www.grandideastudio.com/wp-content/uploads/secure_embed_paper.pdf

[18] Securit Failures in Secure Devices, C. Tarnovsky, Black Hat 2008

[19] http://blog.ioactive.com/2007_12_01_archive.html

[20] http://www.adnas.com/sites/default/files/apdn.press.release.hi-rel.10.26.2015.pdf

References, cont.

[21] S. Skorobogatov, “Physical Attacks on Tamper Resistance: Progress and Lessons”, Special Workshop on HW Assurance, 2011

[22] S. Skorobogatov, “Data Remanence in Flash Memory Devices”, CHES’2005

[23] Securedrives, http://securedrives.co.uk/

[24] http://www.livescience.com/52397-self-destructing-chip-secures-data.html

[25] M. Aarts, “Hardware Attacks Tamper Resistance, Tamper Response and Tamper Evidence”, http://maurice.aarts.info/papers/tamper_resistance_evidence.pdf

[26] M. Arora, P. Bhargava and S. Pickering, “MCF51EM256 Anti-tamper features : A leap towards robust smart metering solutions”

[27] M. Ford, “Lead Generation Tips – Things You Do Not Tell Prospects”, http://www.business2community.com/ sales-management/lead-generation-tips-things-you-do-not-tell-prospects- 0422837 #OMBu1jkkPAmByVsp. 99