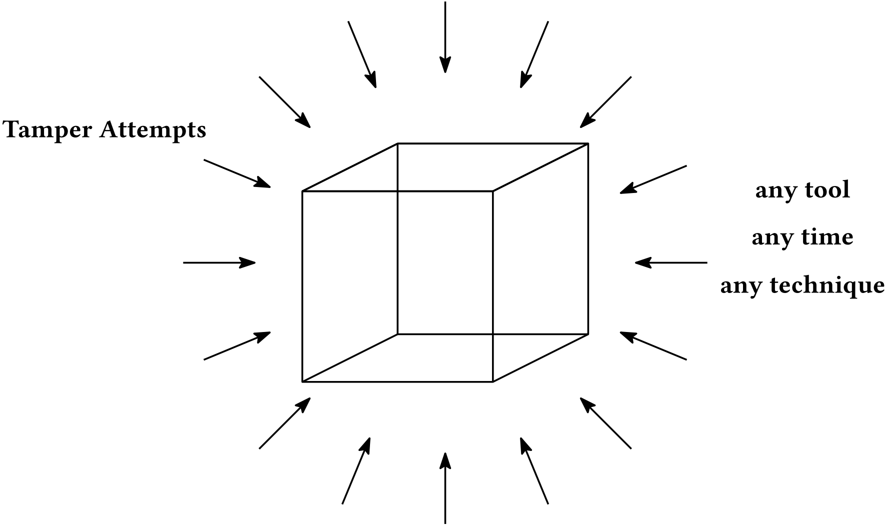
Secure Physical Enclosures from Covers with Tamper-Resistance

Vincent Immler, Johannes Obermaier, Kuan Kuan Ng, Fei Xiang Ke,
JinYu Lee, Yak Peng Lim, Wei Koon Oh, Keng Hoong Wee, Georg Sigl

Conference on Cryptographic Hardware and Embedded Systems, Atlanta, Aug 26, 2019

The Physical Security Challenge



Where We Stand in Physical Security

"Security outside the black-box model" by Ventzi Nikov at CARDIS 2016 (Invited Talk)

- Protecting crypto HW implementations in the grey-box model
  - Side channel attacks, Fault attacks, Combined attacks, Coupling, Reverse-engineering
- LR crypto in HW and SW in the grey-box model
- Protecting crypto SW implementations in the grey-box model
  - Side channel attacks, Fault attacks, Combined attacks
- Protecting crypto SW implementations in the white-box model
  - Grey-box attacks, White-box attacks, Reverse-engineering
- Protecting any SW execution in the white-box model
  - SW attacks, Physical attacks, Reverse-engineering
- Protecting any platform in the white-box model
  - SW attacks, Physical attacks, Reverse-engineering

Where We Stand in Physical Security

"Security outside the black-box model" by Ventzi Nikov at CARDIS 2016 (Invited Talk)

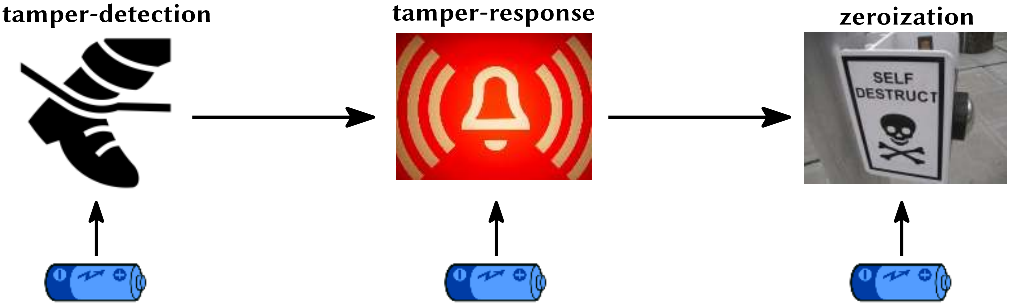
- Protecting crypto HW implementations in the grey-box model
  - Side channel attacks, Fault attacks, Combined attacks, Coupling, Reverse-engineering

skip the rest, let's make this green (at least try)

- Protecting any platform in the white-box model
  - SW attacks, Physical attacks, Reverse-engineering

Security Enclosures = Access Denial Systems

goal: detect and counteract physical attacks

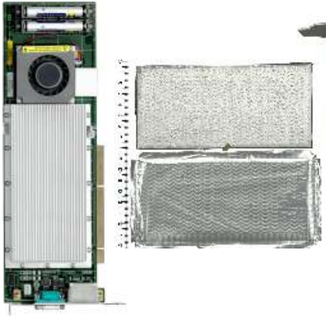


battery-backed mechanism for continuous protection
zeroization wipes volatile memory containing critical security parameters

Access Denial Systems: Commercial Examples

ADP Gauselmann

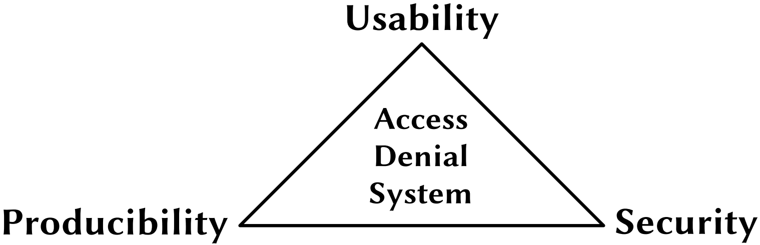
HP Atalla



IBM Cryptographic Coprocessor

countermeasures: active meshes, obfuscation, light sensors, switches, potting, …

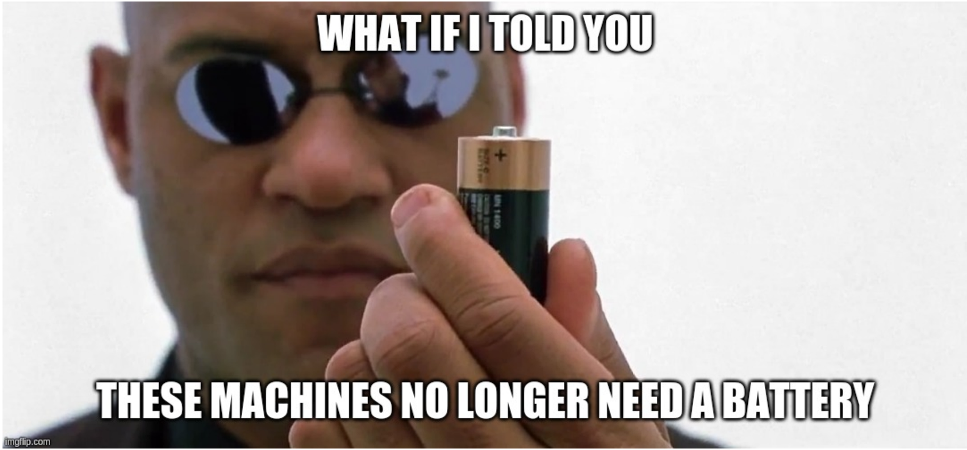
High-Level Goals of Access Denial Systems



desired level of security: no demonstrable way to circumvent
→ secure in the field; prevent HW trojans in distribution chain

Selected Properties of Shown Examples

- **Producibility:**
  - **Envelopes: complex manufacturing but highest geometrical security**
  - **Covers/shells/housings: less complex but also less secure**
- **Usability:**
  - **Battery typically limits operating range w.r.t. temperature**
  - **Shelf life is limited or necessitates additional service**
- **Security:**
  - **Energy-preserving approach leads to crude measurement resolution**
  - **Prone to single point of failure at PCB-level (e.g., cut-off alarm, fake check signal)**
  - **Security mostly based on <u>black-box</u> model**


WHAT IF I TOLD YOU
THESE MACHINES NO LONGER NEED A BATTERY
imgflip.com

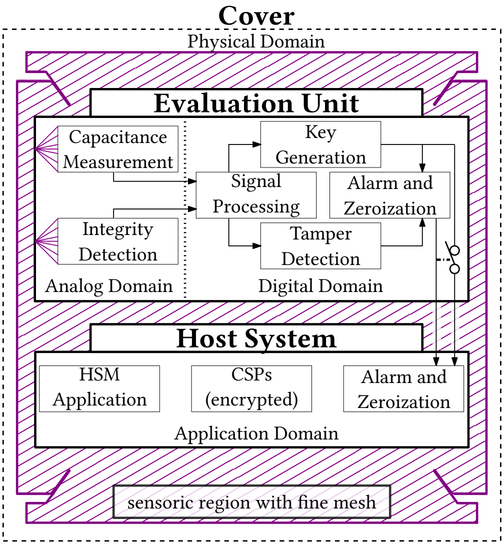
Tamper-Evident PUFs as Designated Alternative

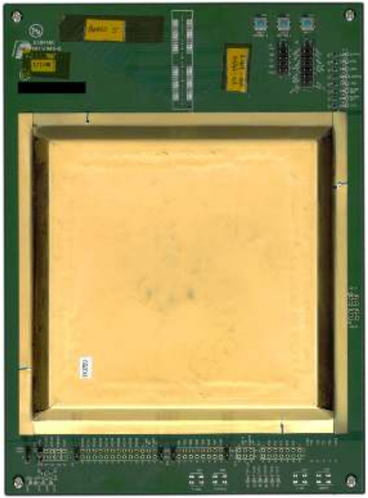
- “True” purpose of PUFs: tamper-detection w/o battery-backed sensors

- Upon power-on: key derivation from tamper-evident PUF enclosure
  - If it fails: goal achieved, still initiate further countermeasures
  - If it succeeds: decrypt system or unlock critical security parameters

- Unfortunately, very little (public) work in this area!
  - Move towards white-box PUF design w/o diminishing security
  - Additional obfuscation then makes it even more difficult to attack

Proof of Concept: Design Overview





Design Goals and Security Objectives

- **Design Goals:**
  - **Investigate how far we can get with COTS components**
  - **Check validity of concept and if it is worth developing further**
  - **Make physical integrity check complex and bury deep inside IC**
  - **Concept must scale with advancements in manufacturing**

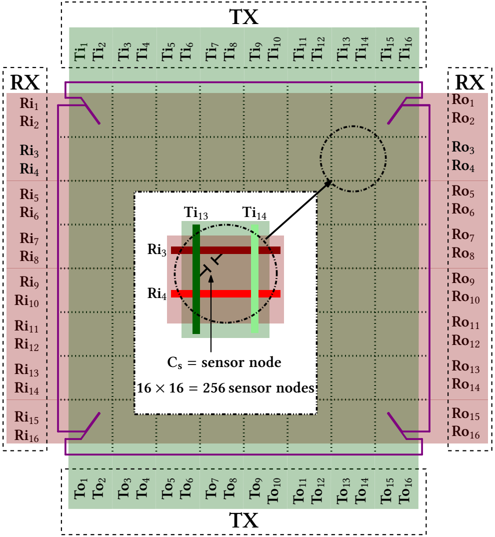
- **Security Objectives:**
  - **"Deny physical access" = disassembly is destructive; force multiple holes**
  - **Maximize distance from enclosure surface to insides of targeted chip**
  - **Entropy loss upon attack substantial, not possible to reconstruct**
  - **Increase need for customized tooling**
  - **Considered diameter =** $300\,\mu\text{m}$

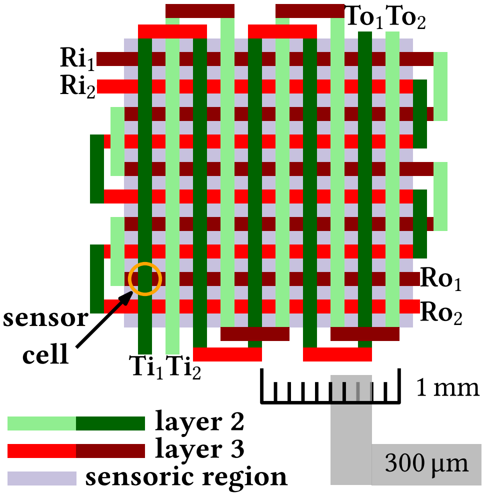
Physical Domain: Layer Stack-Up of Cover

PCB manufacturing process causes intrinsic variation in mutual capacitance C^{M}

Layer	Description	Comment
1	**Shield**	Facing to outside
	Bonding	
2	**Tx electrodes**	Driven electrodes
	Polyimide	⇕ **Mutual capacitance** C^{M}
3	**Rx electrodes**	Receiving electrodes
	Bonding	
4	**Shield**	Facing inside (to PCB)
	Polyimide	
5	**Connectors and routing**	

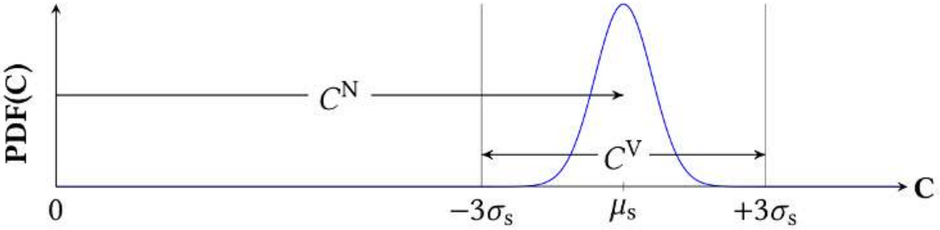
Physical Domain: Mesh with 16 RX × 16 TX Electrodes



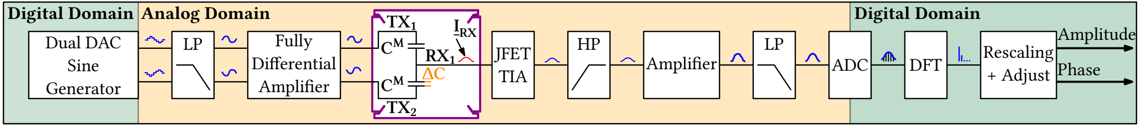


Stochastic Model of Sensor Nodes

- All tiny track overlaps behave like capacitors in parallel
- C^{M} comprised of nominal capacitance C^{N} and variation C^{V}
- Differential measurement needed to remove common offset C^{N}
- $C^{\mathrm{V}} <<< C^{\mathrm{N}}$ requiring high-resolution circuit

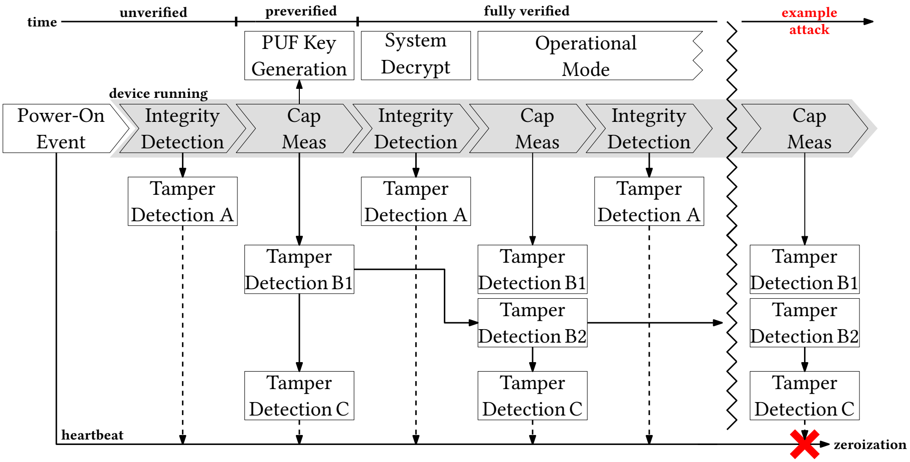


Analog/Digital Domain: Abs+Diff+Integrity Measurement



- Measurements of different nature, one cannot exist w/o the other:
  - Absolute capacitance measurement
  - Differential capacitance measurement
  - Integrity measurement (open/short circuit)
- Applications:
  - Integrity for rapid measurements and factory-initialization
  - Differential measurement for key generation and on-the-fly rate and range limits
  - Absolute measurement for additional tamper detection and temperature sensor

Application Domain / Boot Process



Basic Statistics

Data acquired from 115 flexPCB covers at constant environmental conditions.

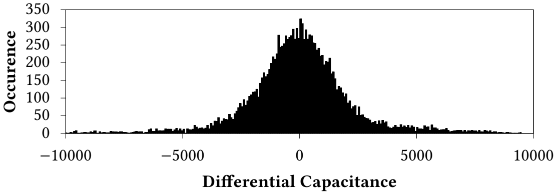


Figure: PDF of differential capacitance.

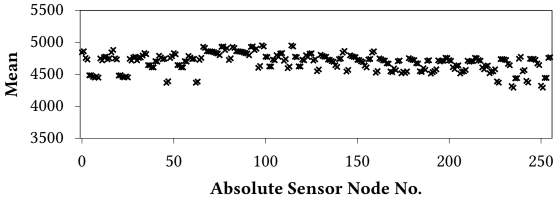


Figure: Absolute capacitance per node position.

Data in line with expectations. Low noise essential for tamper-evident application.

Entropy and PUF Assessment (Global)

Shannon entropy over PUF population: 5.2 bit per node / 4.17 bit (with temperature)

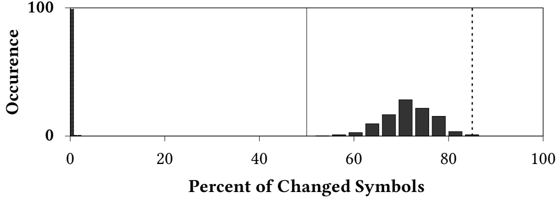


Figure: Uniqueness computed via Hamming distance over symbols (higher-order alphabet).

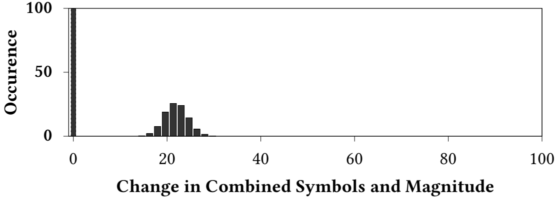


Figure: Uniqueness computed via Manhattan distance over symbols (higher-oder alphabet).

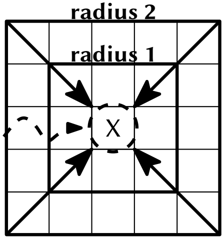
Uniquess for tamper-evident PUFs: think beyond Hamming over binary responses!

Entropy Assessment (Localized) – Spatial Context-Tree-Weighting

Investigate

- Spatial entropy dependencies
- Context around drill hole
- Worst-case (on average)

Tamper-Evident PUF



Results

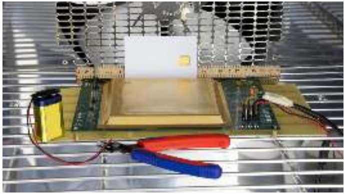
- Entropy = 3.7 bit (radius 1)
- Entropy = 3.1 bit (radius 2,3)
- Degradation exists due to crude layout and PCB process

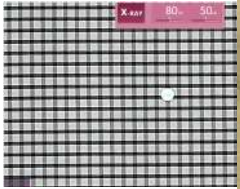
strong attack: given information around drill hole, complexity to reconstruct X

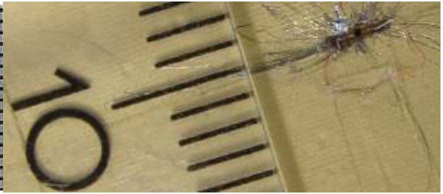
prevent attacker from obtaining PUF output; consider helper data leakage

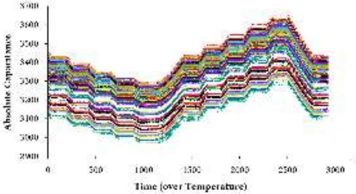
(joint work with Michael Pehl of TU Munich; to be published)

More Data/Attacks/Inspection/Environmental Tests – See Paper









Conclusions

- Still, only a tiny step towards access denial systems without battery
- Full stack approach needed for tamper-evidence/resistance
- COTS-based approach has its limits, especially regarding repairs
- Development of access denial systems in white-box model challenging
- Always use a layered approach to security!

Selected Future Work

- **Layout Randomization:**
  - Increase # of electrode pairs, recombination based on challenge
  - Naturally translates to layout randomization; breaks up local dependencies
- **Customize PDF:**
  - Impregnation of paired nominal C^N values without altering variation C^V
  - Bimodal or arbitrary PDF for improved circuit and tamper behavior
- **Tailored Materials:**
  - Increase C^V and reduce C^N to improve local entropy loss
  - Make repairs more difficult

…and so much more!

Contact Information

Vincent Immler

Central Office for Information Technology
in the Security Sector (ZITiS)

For government inquiries only:
vincent.immler@zitis.bund.de

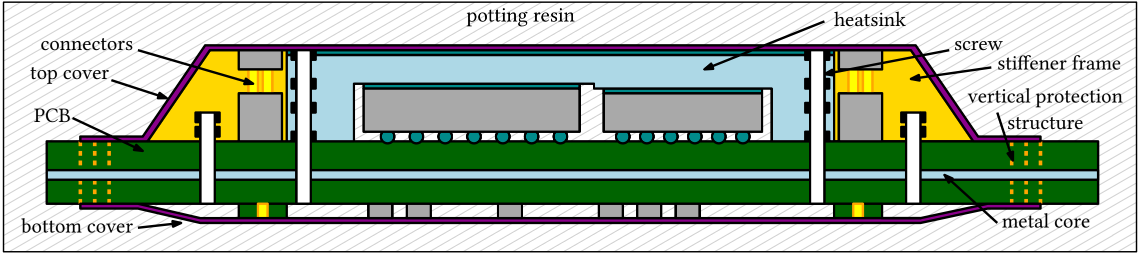
All other inquiries:
science+ches2019@mm.st

This work was performed while with Fraunhofer Institute AISEC.

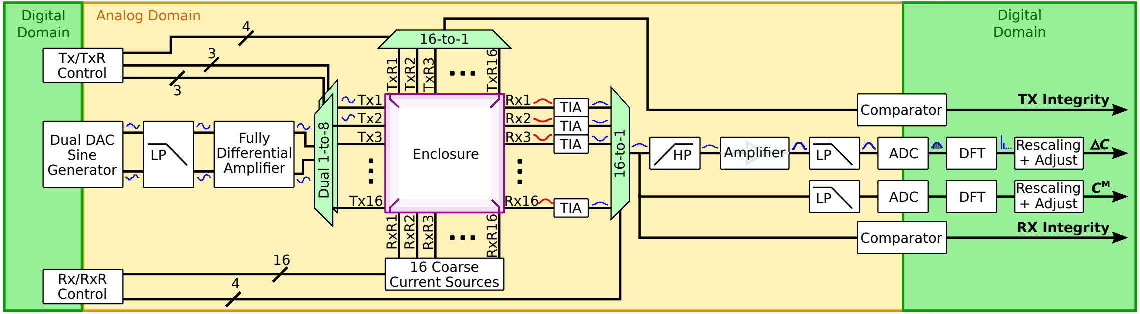
Thank You!
Questions?

Backup

Packaging Concept



Measurement Chain



Data Processing Chain