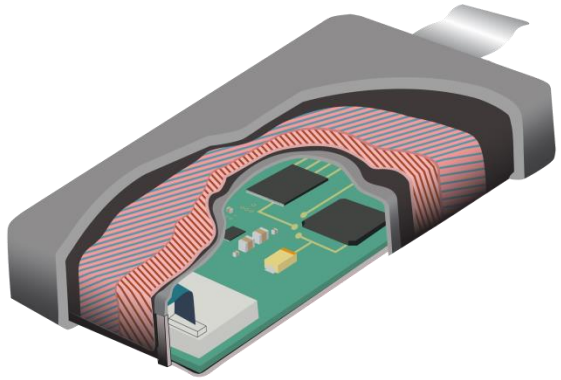
NEXT-GENERATION ANTI-TAMPER ENVELOPES FOR CYBER PHYSICAL DEFENSE SYSTEMS

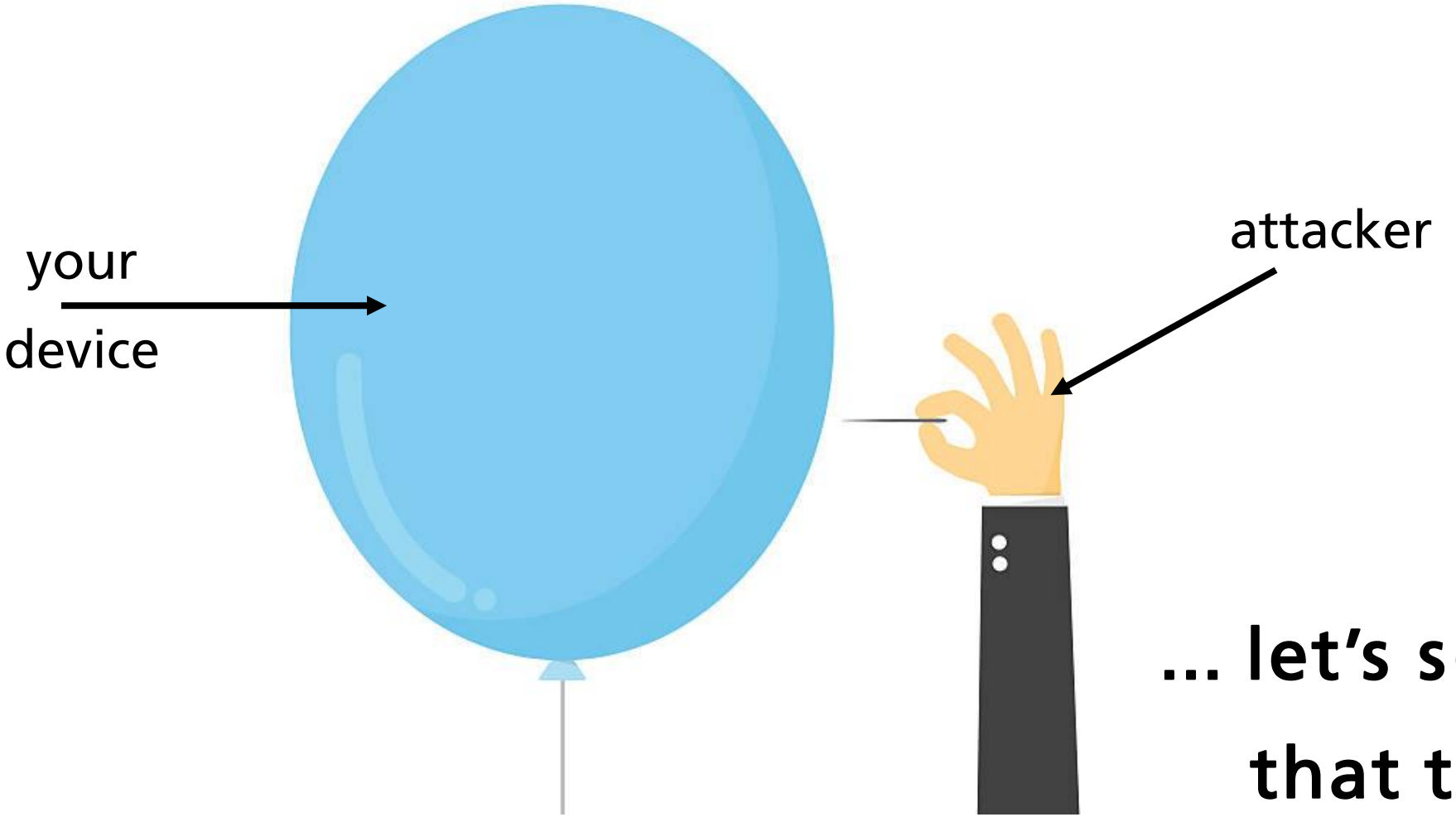
2018-05-08

Vincent Immler, Johannes Obermaier, Martin König, Matthias Hiller and Georg Sigl



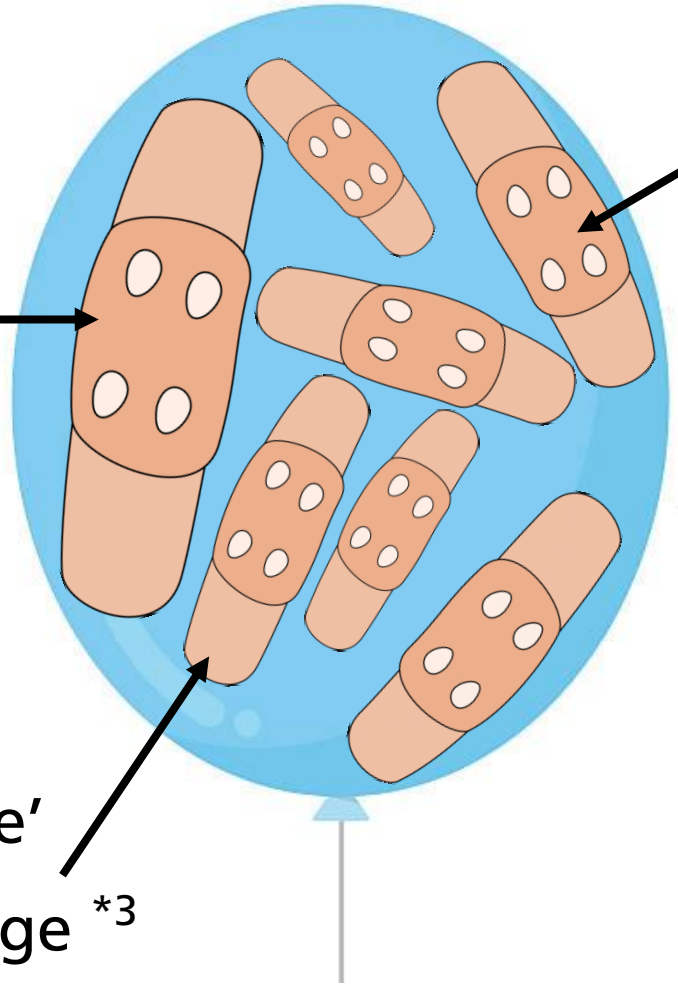
"Tamper-Resistant Envelope based on Physical Unclonable Function (PUF)"

This is the physical security challenge



... let's secure that thing!

Result after *years* of *costly* hardware development = *Patchwork*



prevents certain fault attacks*2

mitigates side-channels*1

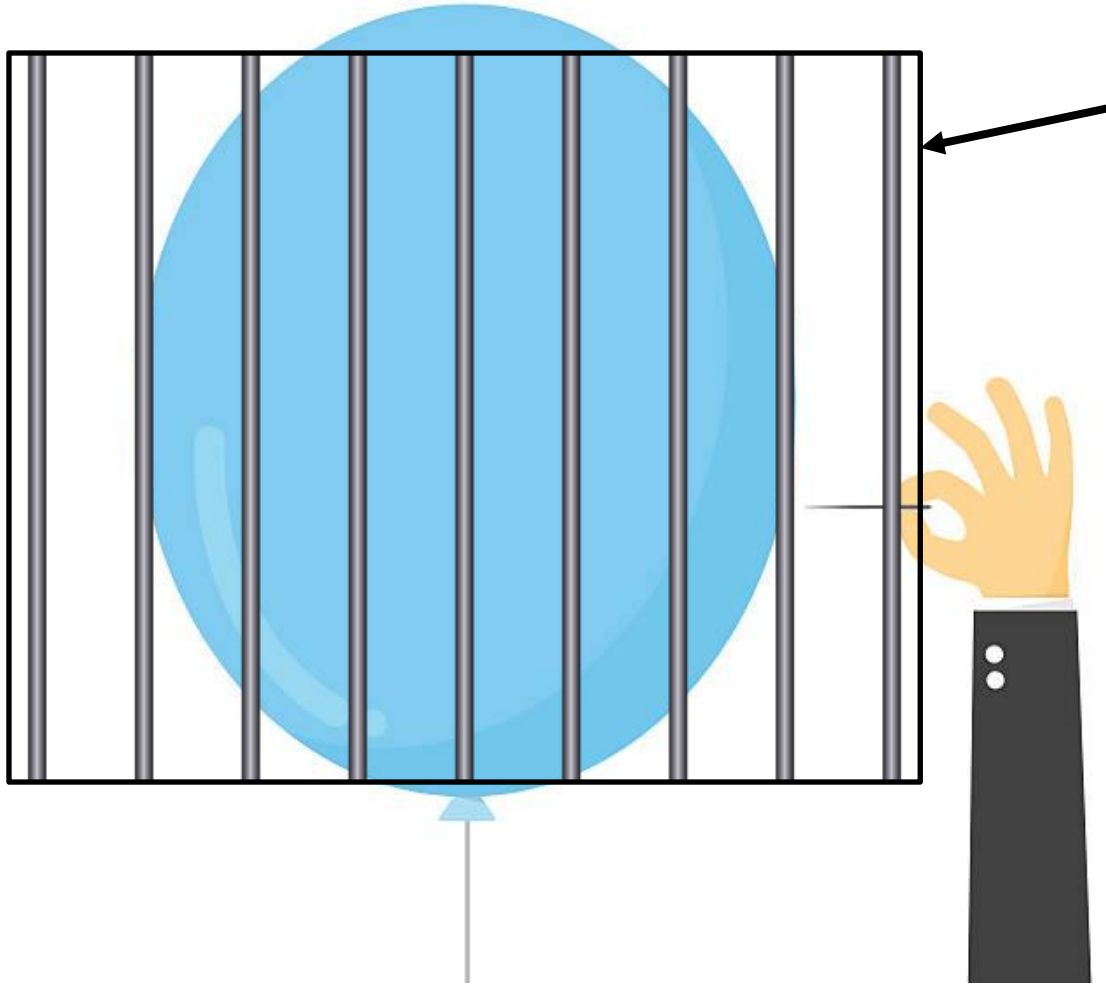
'secure' key storage *3

*1 HW crypto only

*2 iff error count = 1

*3 only obfuscation

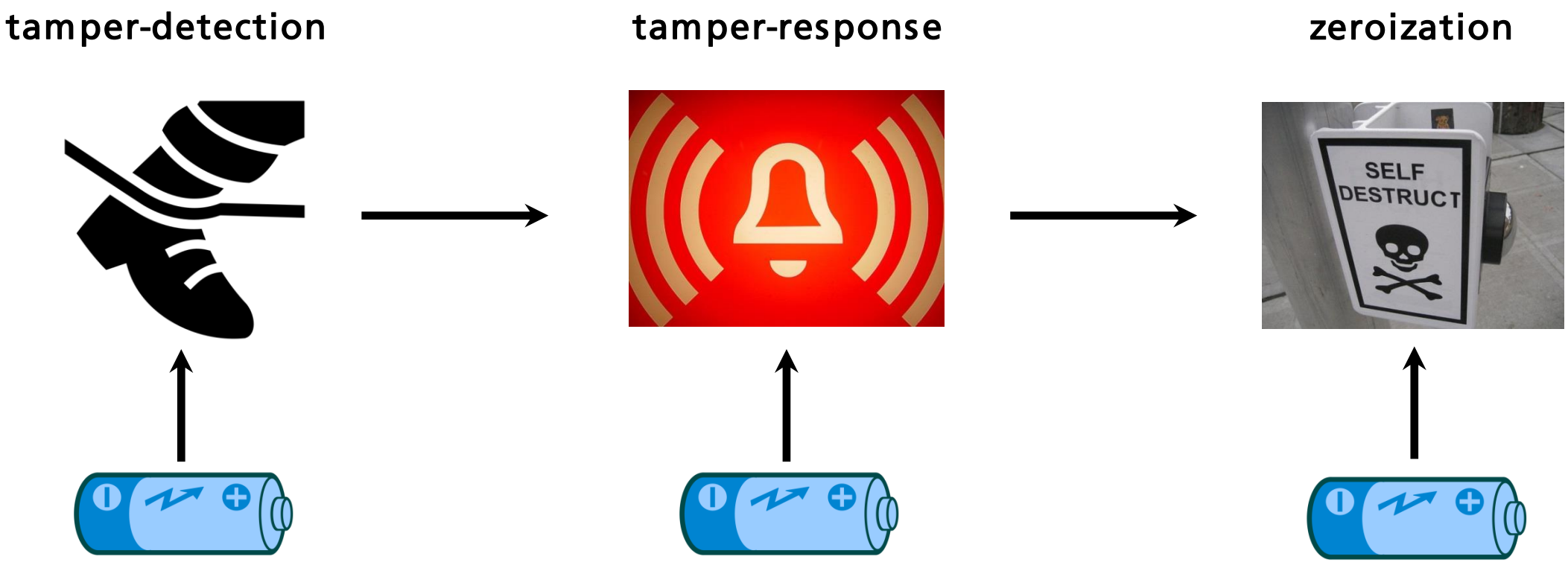
Alternatives? Locking balloon away from attacker's reach



... how can this be done?

Anti-tamper mechanisms = *active* physical security boundaries

goal: *detect and counteract* physical access



battery-backed mechanisms for continuous protection

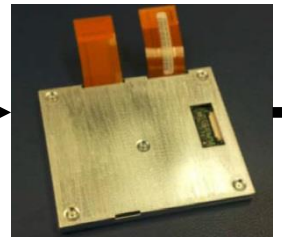
20 years of dominance: GORE envelope – *now discontinued*!

Envelope with mesh

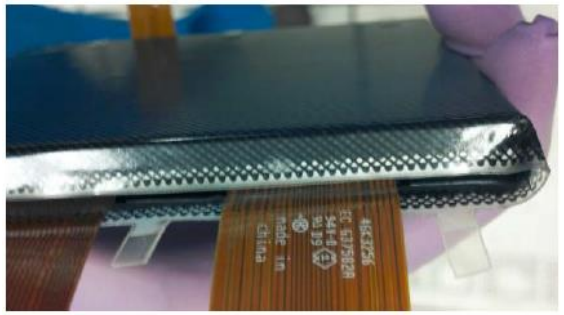
+

PCB with components

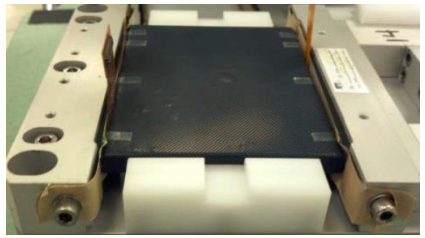
Inner case



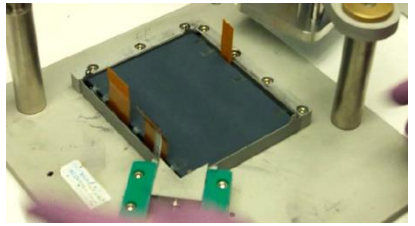
Tamper respondent sensor



Finalized wrapping



Outer case



Encapsulation with resin

Connection to carrier PCB

Finalized HSM

Pictures from: TAMPER PROOF, TAMPER EVIDENT ENCRYPTION TECHNOLOGY (2013)

Strong regulatory need for generic countermeasures

FIPS 140-2 Level 4

*"**Tamper detection envelope with tamper response and zeroization circuitry**"*

DoDI 5000.02 Enclosure 14

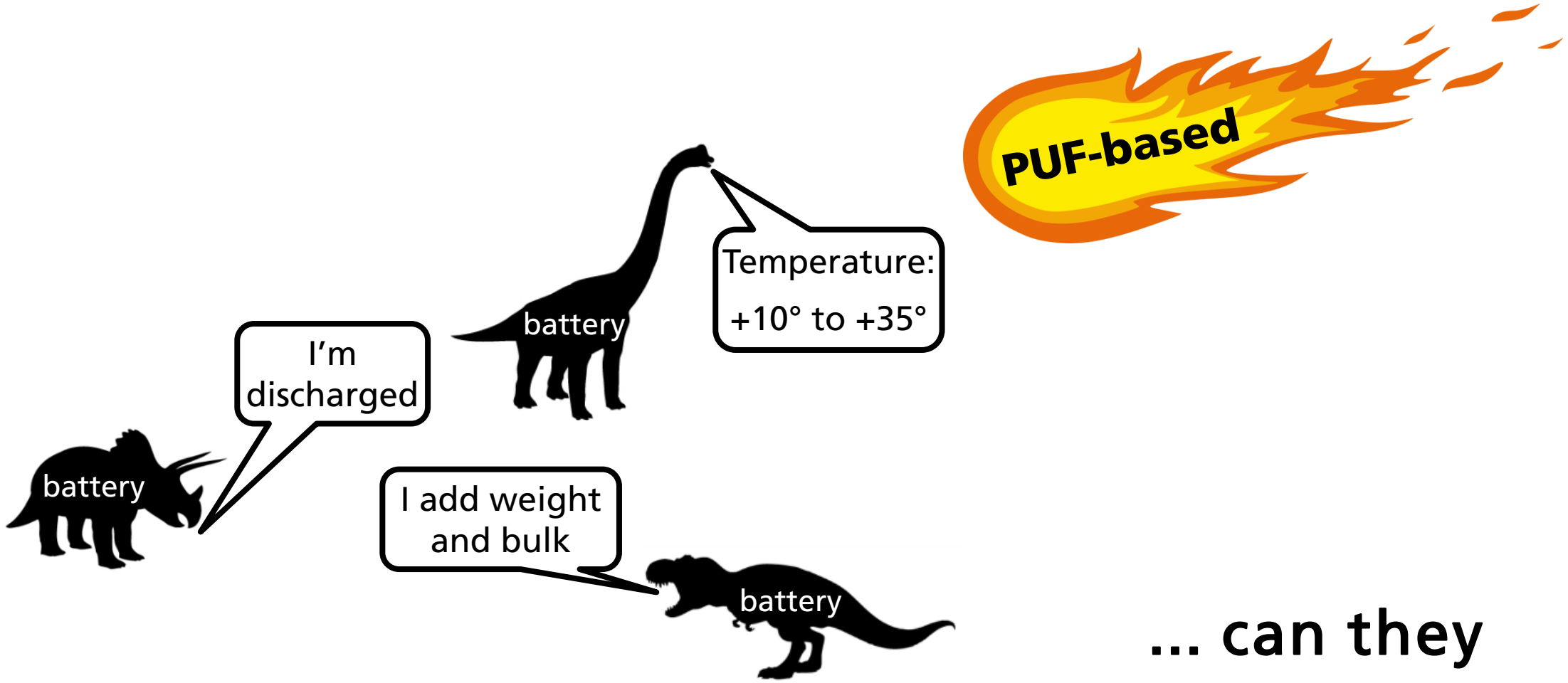
*"Appropriate cyber threat protection measures include, ..., **anti-tamper (AT)**, ..."*

PCI POS

*"The device **uses tamper-detection and response mechanisms** ..."*

unfortunately, very little public work in this area

Is the future of anti-tamper with batteries?



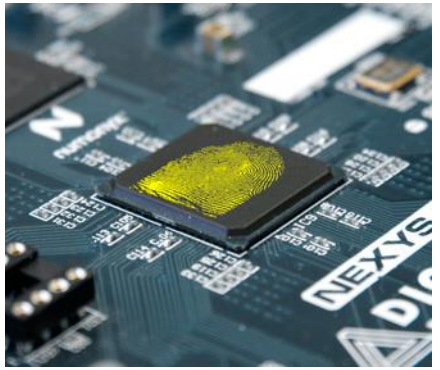
... can they survive the future?

What is a Physical Unclonable Function?

- Solving the problem of key storage:
  - Keys stored in Secure Non-Volatile Storage (SNVS)
  - *However:* Delayering and optical analysis can defeat this

How to prevent these “offline attacks”?

- “Physical Unclonable Functions” (PUFs)
- Basic idea: manufacturing variations cause ‘fingerprint’
- Example: start-up patterns of SRAM are unique
- Error-Correcting Codes required to derive robust key



What is a Physical Unclonable Function? (Cont'd)

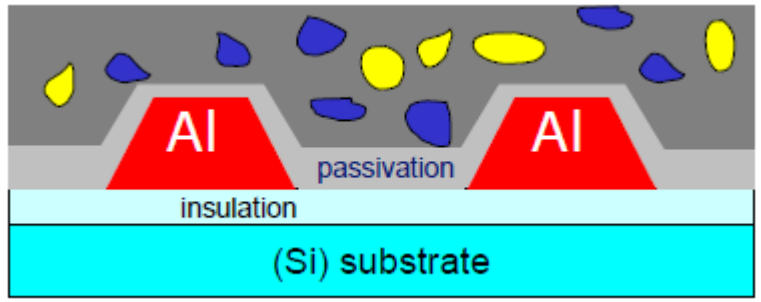
- Silicon PUFs included in some commercial designs (Intrinsic-ID, Verayo)
- FPGA-based PUFs available, too (Enthentica, AISEC)

- *Warning*: silicon PUFs cannot prevent "online attacks"!
  - At runtime, key is generated and transferred over, e.g., data bus
  - Probing can extract key from data bus

- *Solution*: tamper-evident PUFs that enclose significant portions of system

Related Work: Coating PUF (Tamper-Evident)

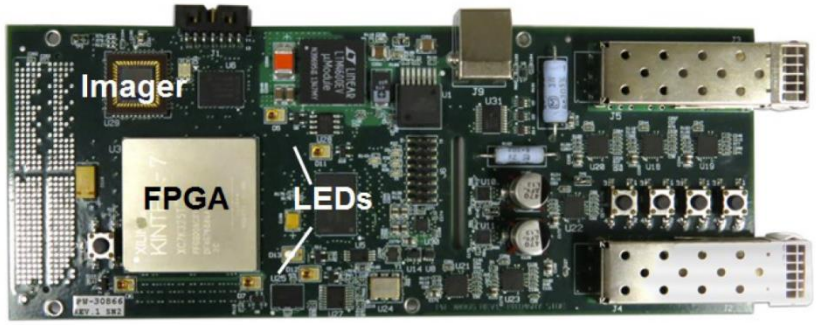
- An IC is covered with an opaque coating containing random particles with high dielectric constant
- Orientation and distribution of particles within the coating cannot be controlled
- Random properties of coating → suitable structure for a PUF
- Array of capacitive aluminum sensors in upper metal layer detects local coating properties



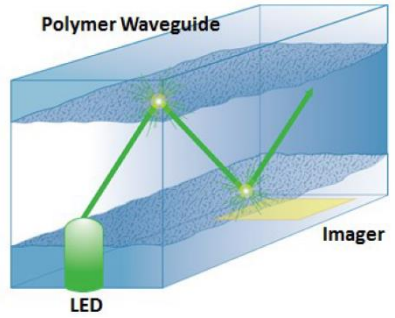
Source: Tuyls et al., "Read-Proof Hardware from Protective Coatings", 2006

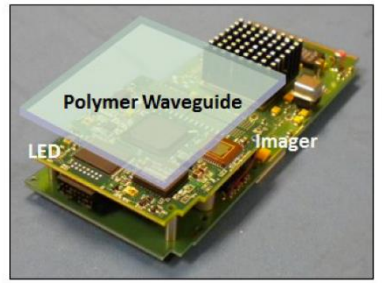
Related Work by MIT Lincoln Labs (Tamper-Evident)

- Key generation takes ~ 620ms
- No runtime tamper detection
- No backside protection
- No integrity check
- Insufficient data to assess properties

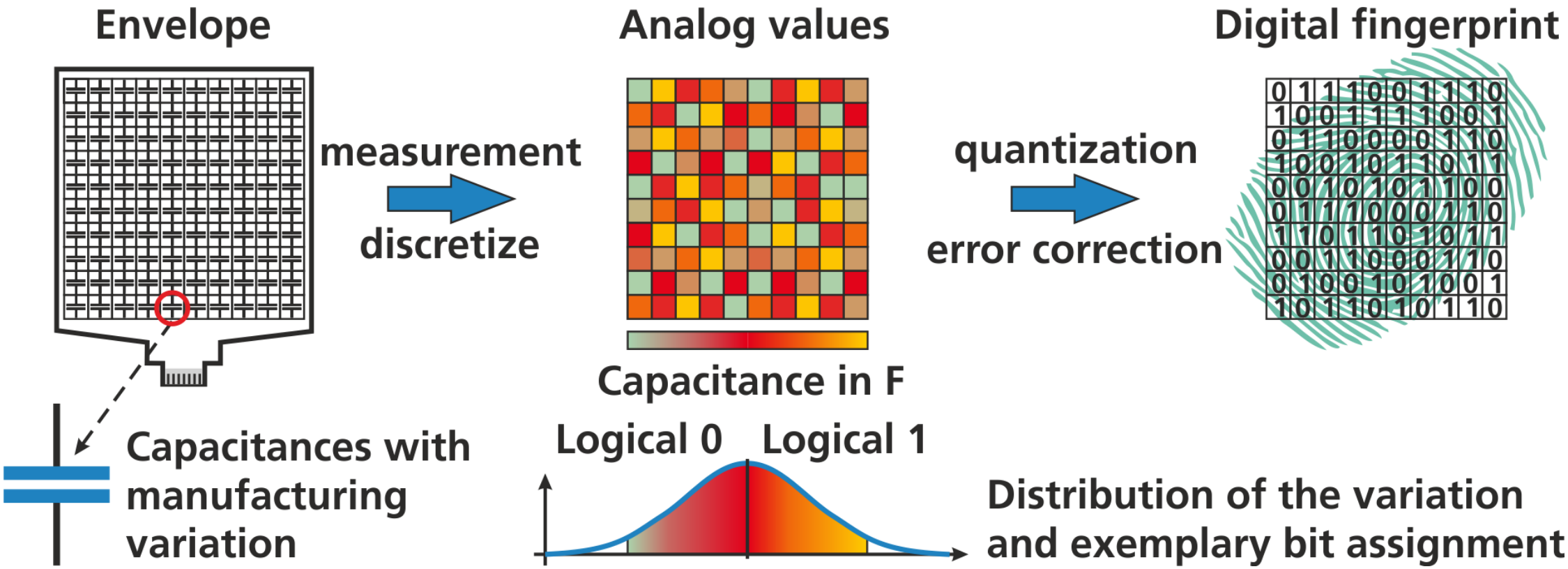


(a)





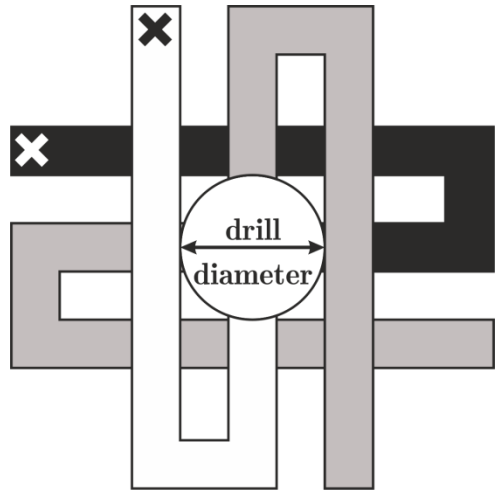
Our approach: a PUF-based envelope – no battery required!



Envelope based on strong design rationale

- A *PUF-only* enclosure is deemed *insufficient*
  - How to distinguish variation from defects?
  - How to enable rapid measurements during runtime?

- *Solution*: interleaved mechanisms of different nature
  - Entropy of capacitance
  - Structural integrity of mesh
- Protection against well-defined drill sizes (0.3mm)
- Stochastic model for capacitance

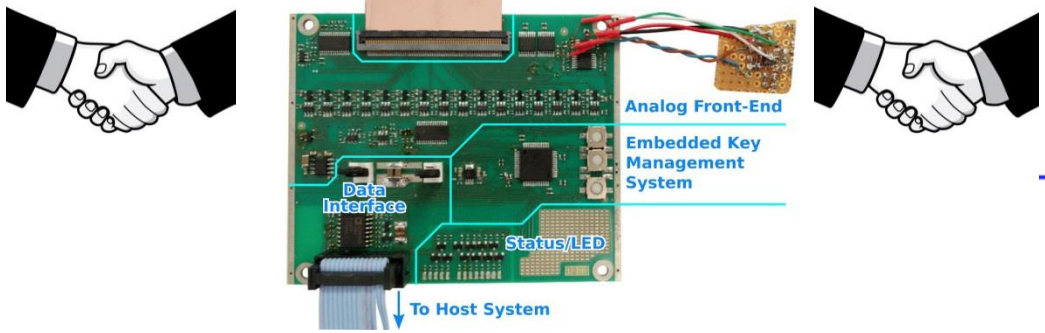


Key aspects of a full-stack approach to physical security

Physical Enclosure

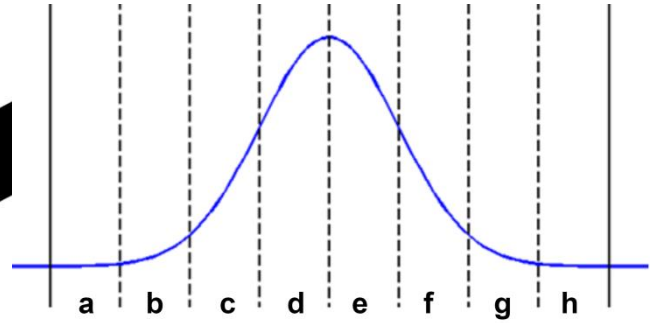
- Four conductive layers
- Capacitive sensoric mesh
- 16x16 electrodes
- Variation from etching etc.

Measurement Circuit



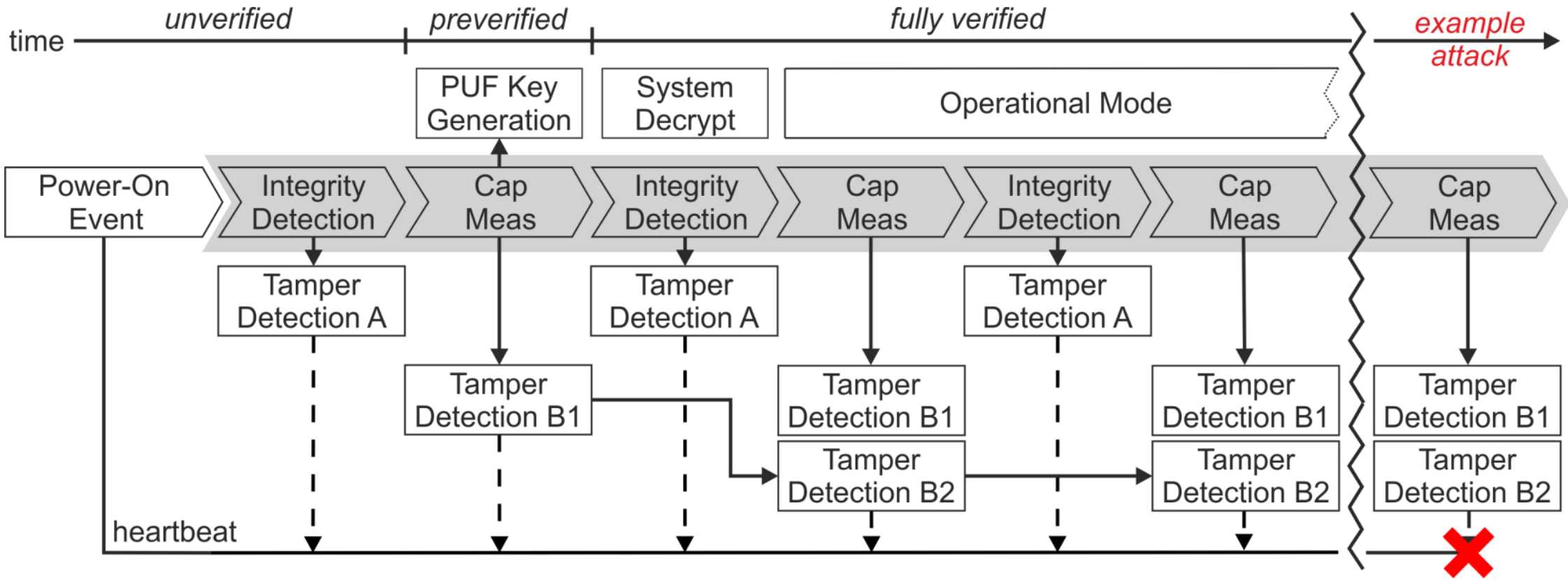
- Early prototype based on discrete components
- IC in next revision
- *to appear* at DAC'18

Algorithmic Processing

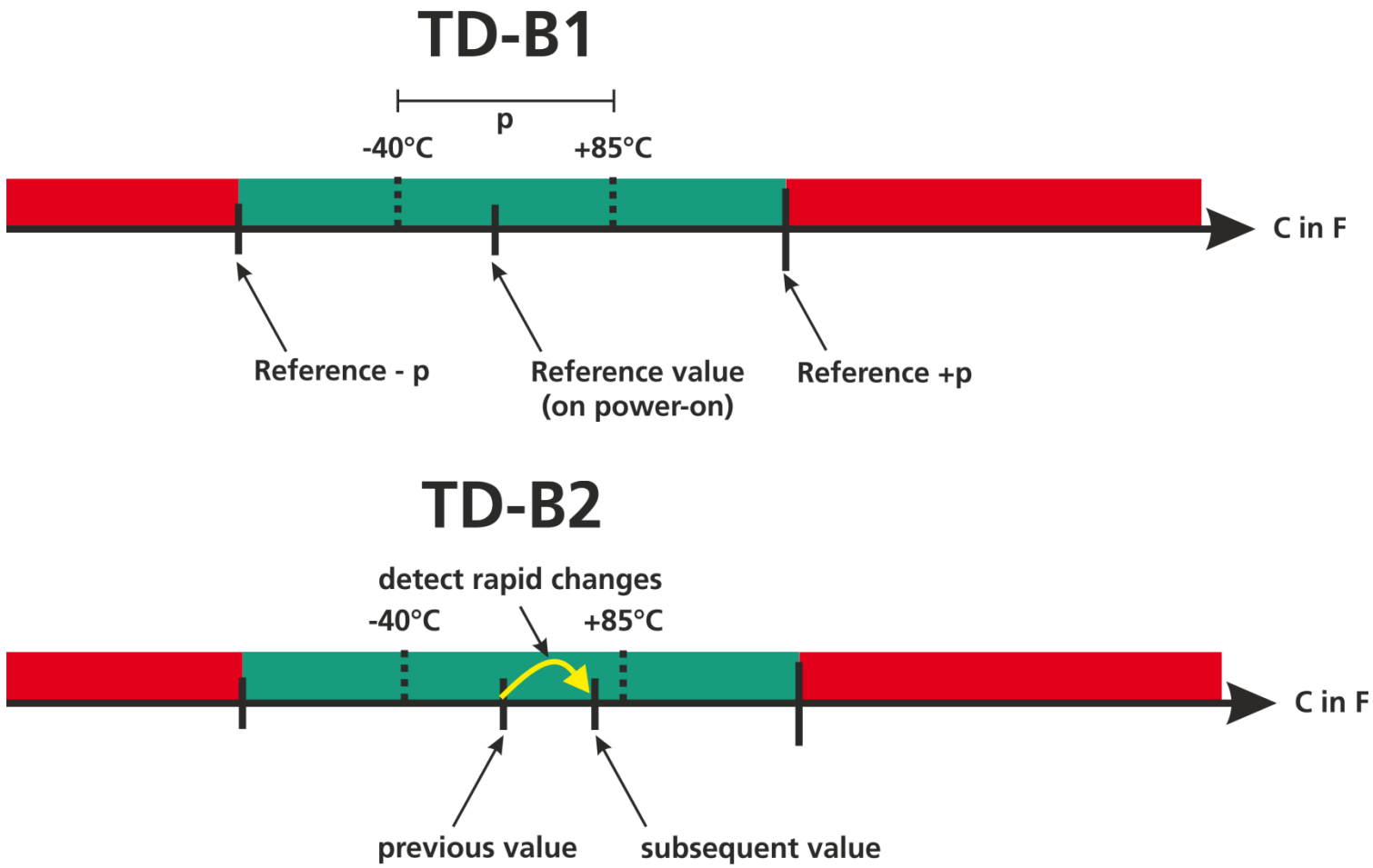


- Equidistant quantization
- Symbols from higher-order alphabet as output
- Additional ECC

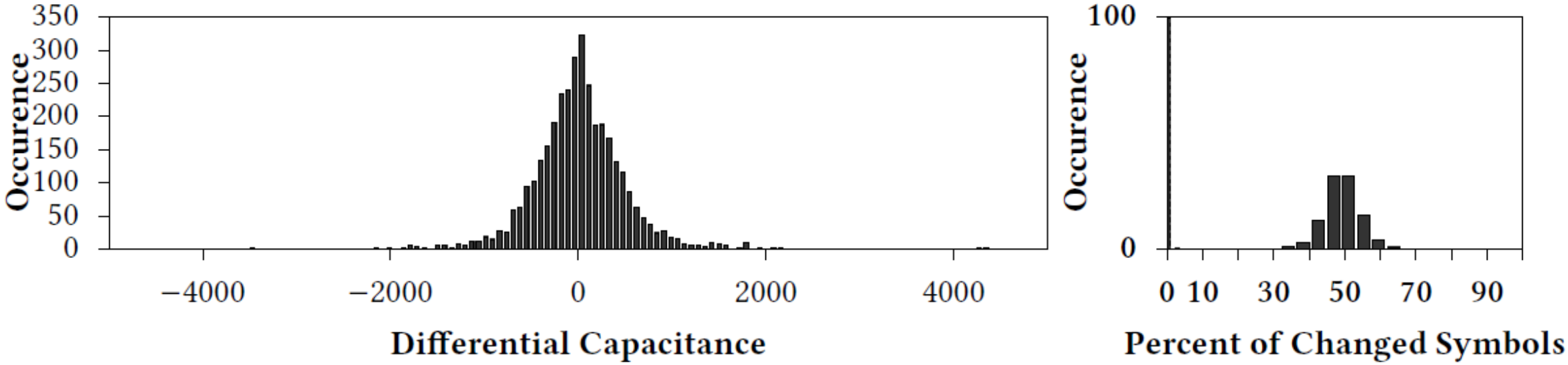
Secure bootstrap with PUF key generation *and* tamper detection



Tamper Detection B1 = limit range of values
Tamper Detection B2 = limit discrete rate of change



Statistical results support a good PUF behavior

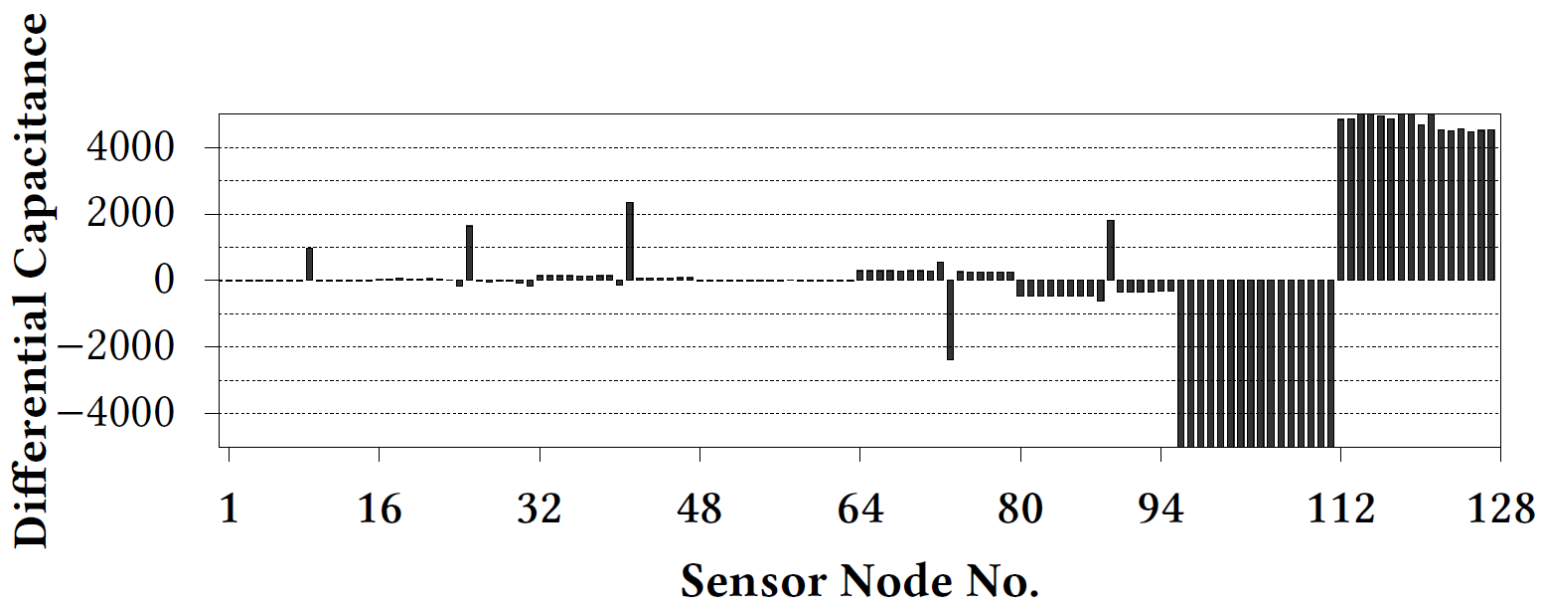


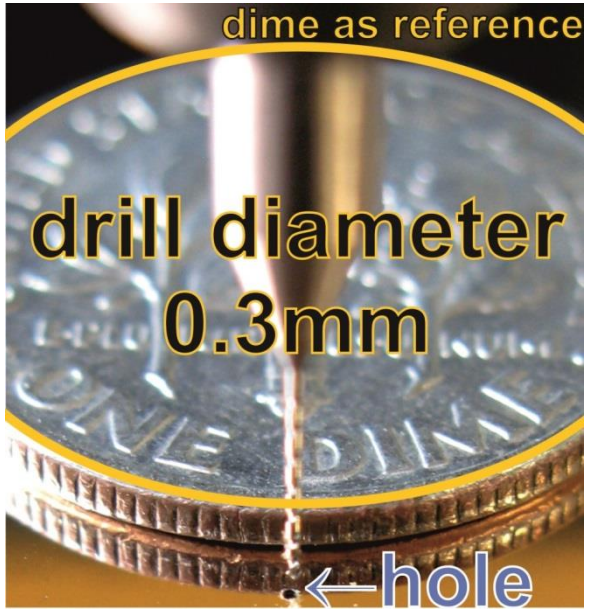
(a) Histogram of sensor node data.

(b) Uniqueness and reliability.

- Result of 50 measured envelopes
- Full-scale range of measurement circuit [-73fF;+73fF]
- σ of PDF = 6.25 fF; σ of measurement noise = 0.19 fF

Attack Results





Conclusion and future work

- **Conclusion**
  - A first step towards strong anti-tamper mechanisms without battery
  - Development of ad-hoc physical countermeasures challenging
  - Much more work in this area needed

- **Future work**
  - Scale from prototype to real-world product
  - More detailed entropy assessment
  - Improving material properties

Thank you very much for your attention!
Questions?

Contact Information

Vincent Immler
Physical Security Technologies Group

Fraunhofer Institute for
Applied and Integrated Security (AISEC)

Parkring 4
85748 Garching (near Munich)
Germany

www.aisec.fraunhofer.de

Phone +49 (0)89 3229986-185
vincent.immler@aisec.fraunhofer.de