Enclosure-PUF

Tamper Proofing Commodity Hardware and other Applications

Christian Zenger[1,2], Lars Steinschulte[1,2], David Holin, Johannes Tobisch[2], Christof Paar[2]

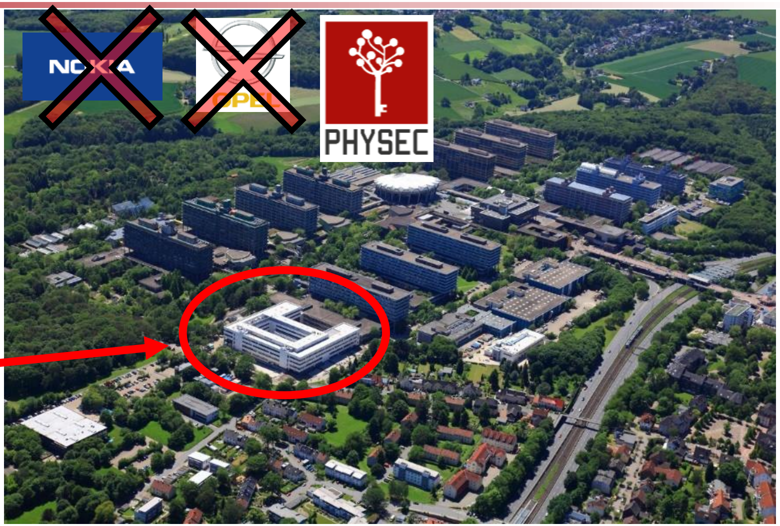
[1] PHYSEC GmbH

[2] Ruhr-Universität Bochum

hardwear.io 26.09.2019

Hacker Hochburg Bochum – alias *Security Valley*

RUHR UNIVERSITÄT BOCHUM RUB



hgi
Horst Görtz Institut
für IT-Sicherheit

26x

>100/Jahr

>15

TÜViT
Google
ROHDE&SCHWARZ
BOSCH

heise Security

Deutsche Forscher knacken RFID-Karten

11.10.2011 14:05 Uhr – Christian Kirsch

Wissenschaftler der Ru…

Forscher knacken Auto-Codes

Funkschlüssel: BMW greift Ruhr-Uni an

Zugangscode für Gebäude entschlüsselt

Funkschlösser für Hacker kein Problem

WESTFÄLISCHE RUNDSCHAU

Ein Schlüssel, der überall passt

Funkcodes von Autoschlüsseln geknackt

DÜSSELDORF. Funkfernbedienungen für Schlösser von Autotüren oder Garagentoren sind zwar bequem – aber nicht wirklich sicher. Wissenschaftlern der Ruhr-Universität Bochum ist es gelungen, einen der weltweit am häufigsten bei Funkschlüsseln verwendeten Codes …

Handelsblatt
WIRTSCHAFTS- UND FINANZZEITUNG

… wie er typischerweise in Autoschlüssel eingebaut wird, und einem Empfänger, der sich in der Fahrzeugsteuerung befindet. Beide Seiten – Sender und Empfänger – verschlüsseln ihre Funk-Kommunikation mit einer sogenannten KeeLoq-Chiffre. Das Verschlüsselungssystem wurde vom US-amerikanischen Halbleiterhersteller Micro…

Süddeutsche Zeitung

Einbruch auf Knopfdruck

Deutsche Forscher knacken Codes von Funkschlüsseln für Autos und Garagen

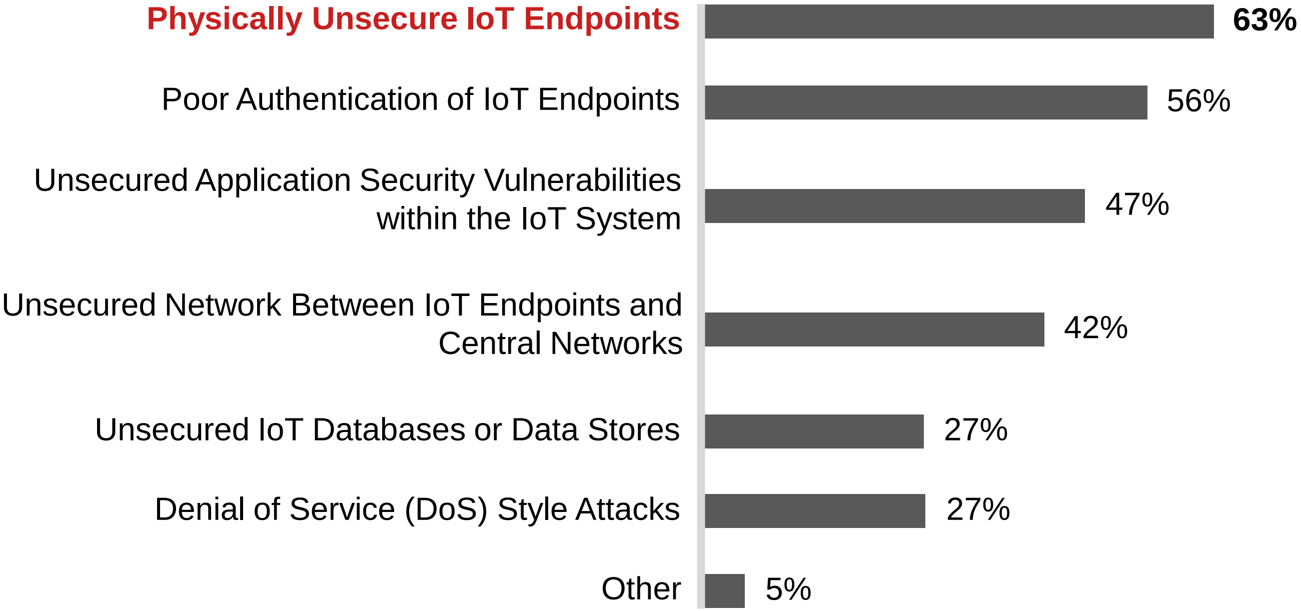
MAX-PLANCK-GESELLSCHAFT

eurobits
Europäisches Kompetenzzentrum
für IT-Sicherheit • Bochum

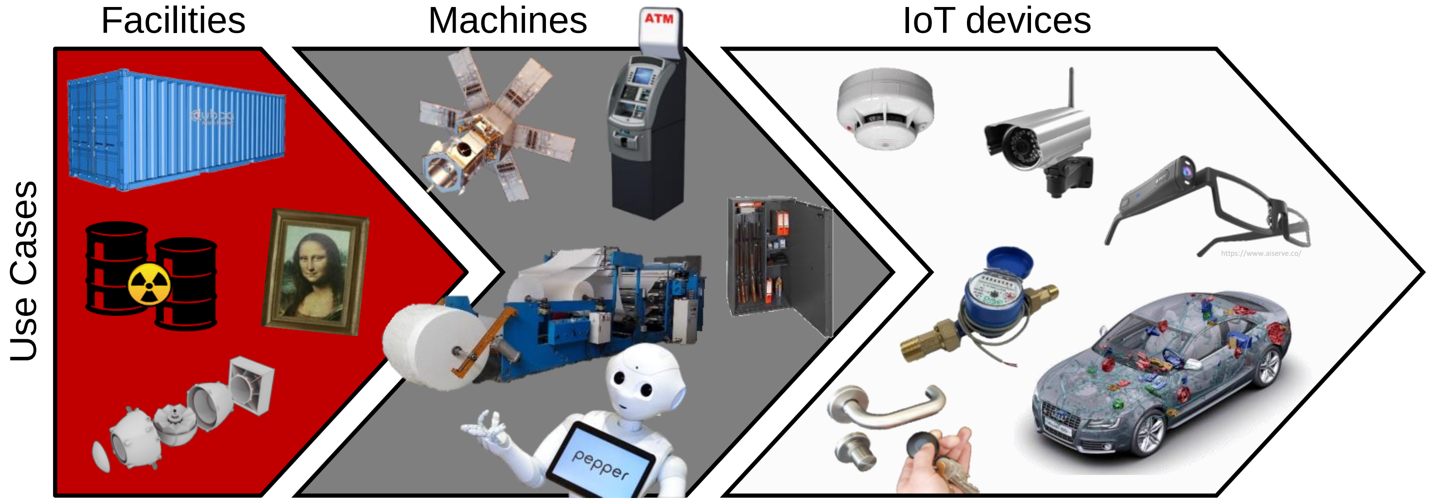
FluxFingers
:RUHR-SiDE HACKiNG:

Icons made by Eucalyp from https://www.flaticon.com is licensed by Creative Commons BY 3.0

Which of the following are the greatest IoT Security Concerns?

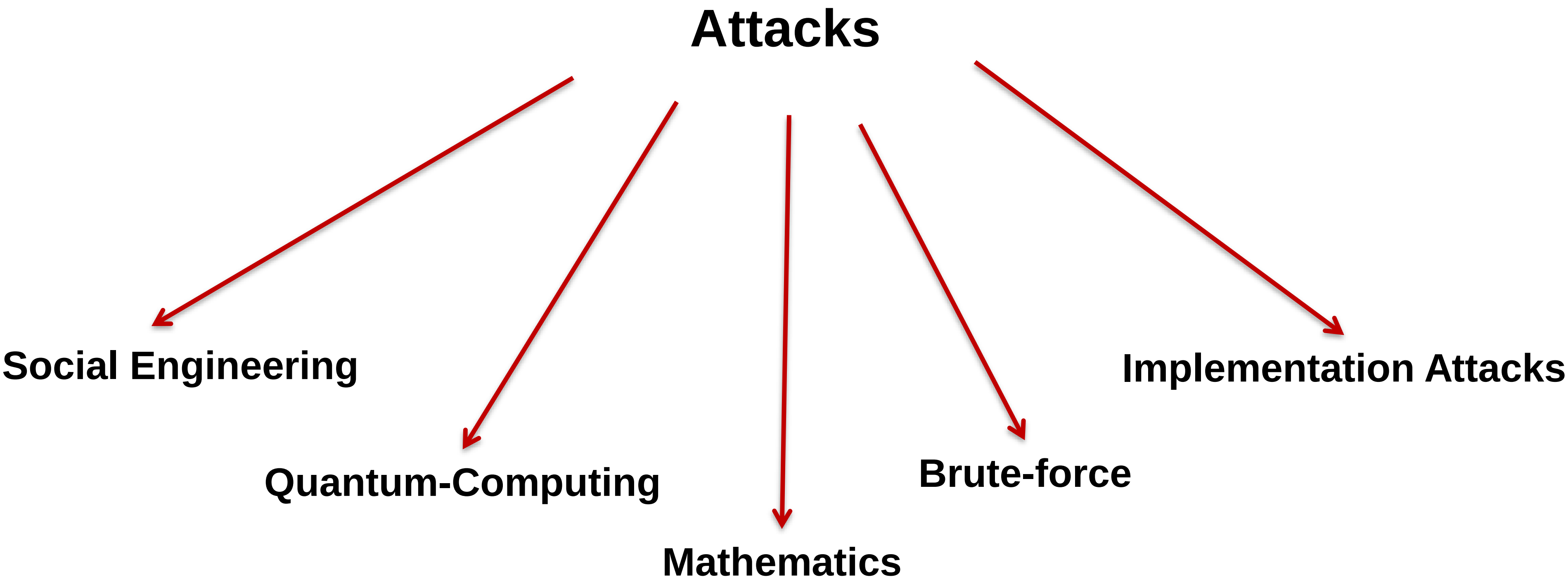


How to tamper protect systems from physical attacks?



Still an open question and topic of this talk.

Classification of Cryptoanalysis



Attacks

Social Engineering

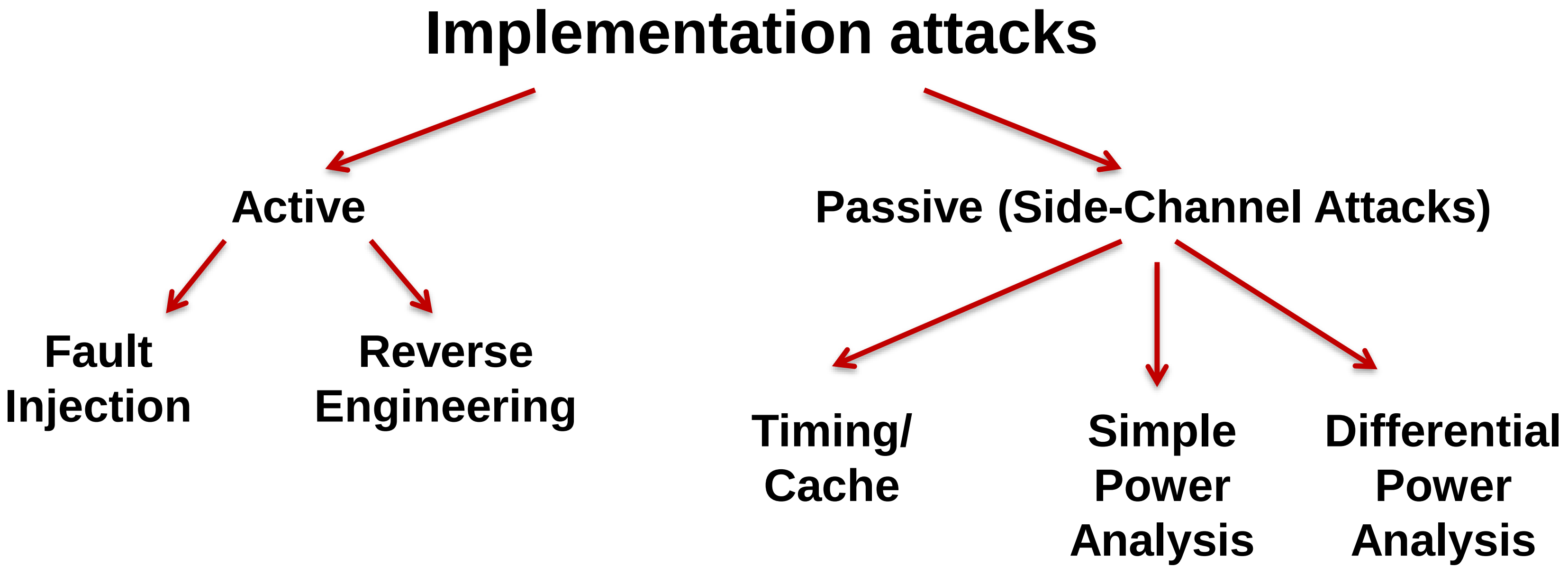
Quantum-Computing

Mathematics

Brute-force

Implementation Attacks

Classification of Implementation Attacks



Implementation attacks

Active

Fault Injection

Reverse Engineering

Passive (Side-Channel Attacks)

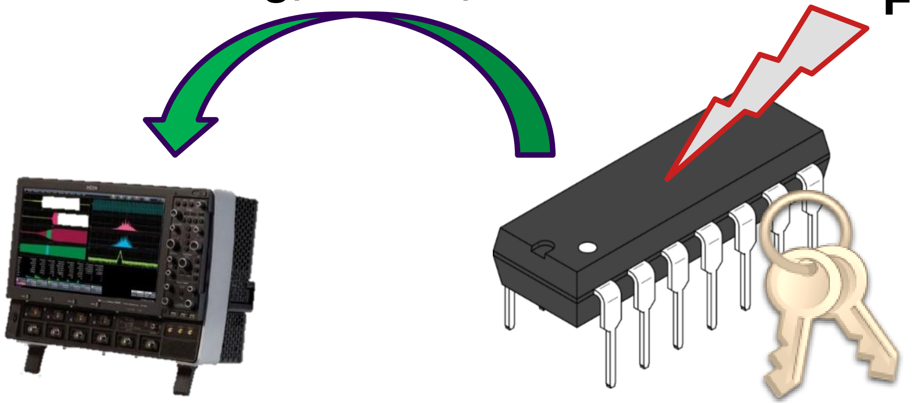
Timing/ Cache

Simple Power Analysis

Differential Power Analysis

Physical attacks are independent of mathematical security/proofs and work for almost every cipher.

Implementation Attacks



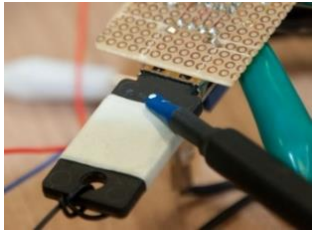
Timing, Power, EM

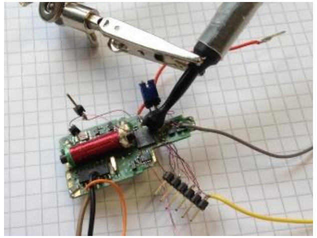
Invasive Attack, Fault-Injection

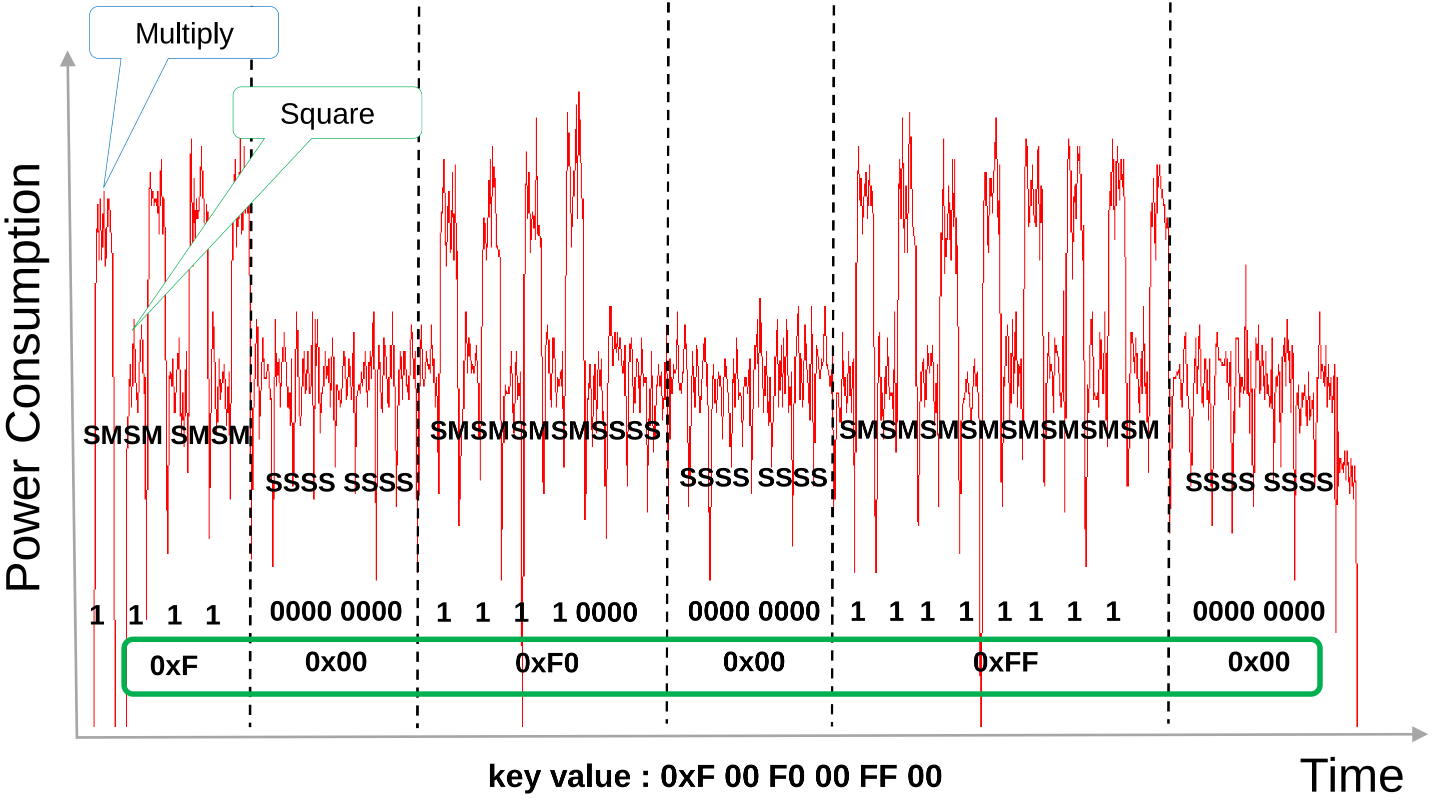
Side-Channel Analysis

Security IC / Device

Simple Power Analysis

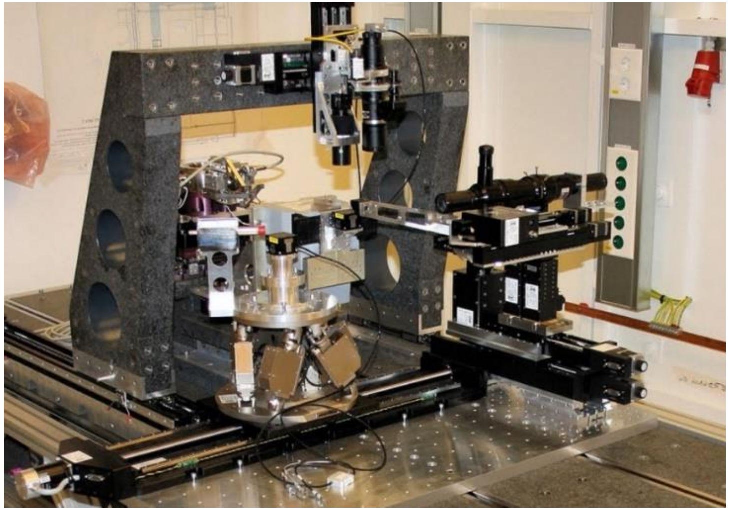


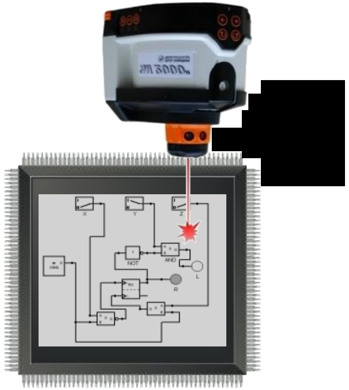




Fault-Injection Attack (FIA)

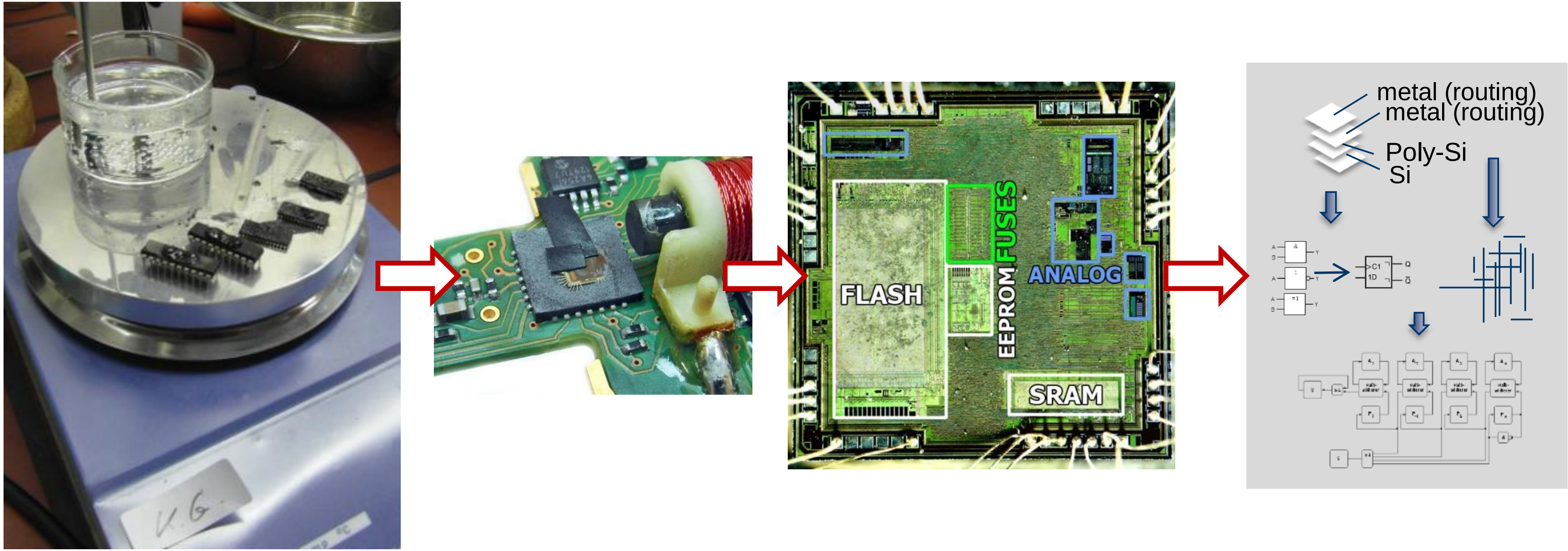
Semi-invasive FIA through systematic shooting with photons on circuits while the system is in operation





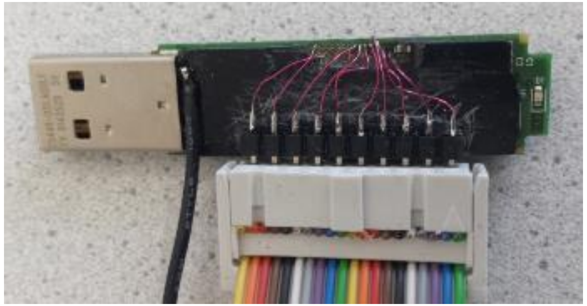
https://dblp.org/pers/hd/s/Schellenberg:Falk

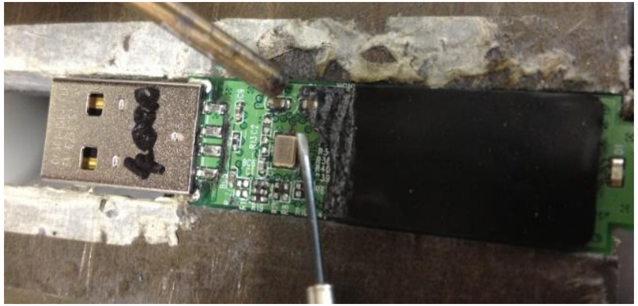
Software and hardware reverse engineering



https://dblp.org/pers/hd/s/Schellenberg:Falk

Implementing a hardware Trojan on a High-Security USB-Stick





[1] Swierczynski et al., Interdiction in Practice – Hardware Trojan Against a High-Security USB Flash Drive, Journal of Cryptographic Engineering, Springer, 2016.

Implications of Physical Attacks on Sensitive Devices

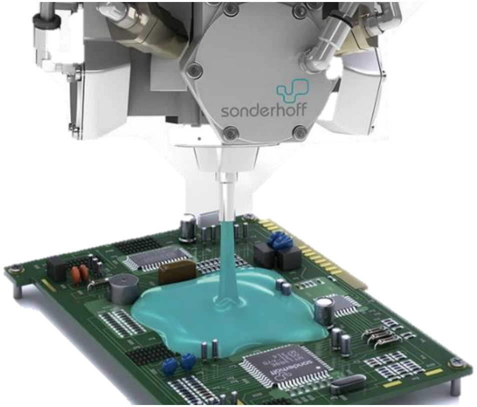
- Physical access enables multiple attack vectors
  - Side-channel attacks
  - Manipulating and exchanging modules
  - Probing conductors and bus lines
  - Over-/undervoltage
  - Opening chips and advance reverse engineering
  - Environmental influence: Temperature, X-Ray etc.
- Leakage: Adversary observes physical output of the device
- Tampering: Adversary modifies internal state and interacts with tampered device

Defining Levels of Physical Integrity

- Four different approaches of Tamper Resilience exist:
  - Tamper Resistance: Tamper is made difficult
  - Tamper Evidence: Intrusion (attempts) must be evident
  - Tamper Detection: The user is notified about tamper attacks
  - Tamper Responsiveness: Countermeasures are engaged when tamper occurs
- NIST FIPS 140-2 defines four increasing levels of anti-tamper security
  - Level 4 is demanded for highly sensitive environments of the US Government
    - Any attack must be detected (micro-intrusion, environmental attacks etc.)
    - Breaches must zeroize all CSP
    - CSP must be separated from the main system (red/black area)
    - Complete tamper-detection and response envelope
- No public benchmarks of what attacks are to be detected exists to the best of our knowledge

Approaches for Tamper Resistance

- Most approaches are based on hardening the encasement of the Environment under Protection (EUP)
  - Proprietary tools are required
  - EUP is potted in resin
  - All unnecessary openings are removed
  - Rivets are used for permanently closing latches
- Approaches are widely used, cheap, and **ineffective**



Potting of electronic components [1]

Totally secure one way screw [2]

[1] https://www.sonderhoff.com/fileadmin/assets/images/Technologies/Vergiessen/HEADER_SLIDER_Vergiessen.jpg
[2] https://manoffamily.com/how-to-remove-one-way-screws/

Approaches for Tamper Evidence

Warranty seal being carefully removed to be re-applied later on [2]

- Tamper Evidence aims to make tamper attempts visible upon inspection
- Most commonly used in cargo and consumables
  - Lead seal
  - Plastic tag
  - „Freshness“ seals
- Also widely used, cheap, and **ineffective** [1]

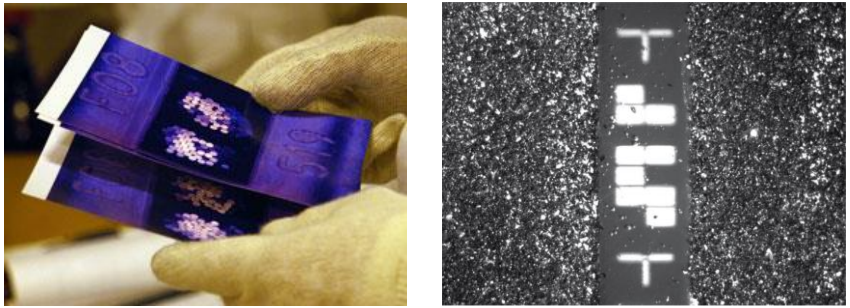
Freshness-seal on Tylenol medicine [3]

Polypropylen cargo seal [4]

[1] DEFCON 19: Introduction to Tamper Evident Devices
[2] https://www.youtube.com/watch?v=KGcNS5g9ygg
[3] https://www.pbs.org/newshour/health/tylenol-murders-1982
[4] http://www.imcolabel.de/Polycheck-Plombe-blau

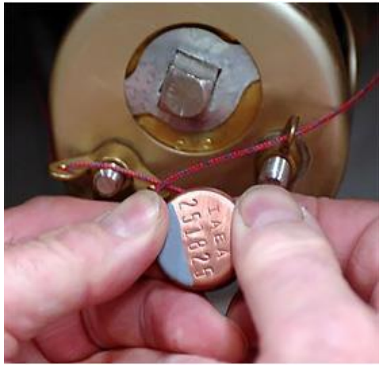
Approaches for Tamper Evidence and Unique Identifiers

- Tamper Evidence and Unique Identifiers
- Technologies for Nuclear Warhead Disarmament Verification



Reflective Particle Tag [5]

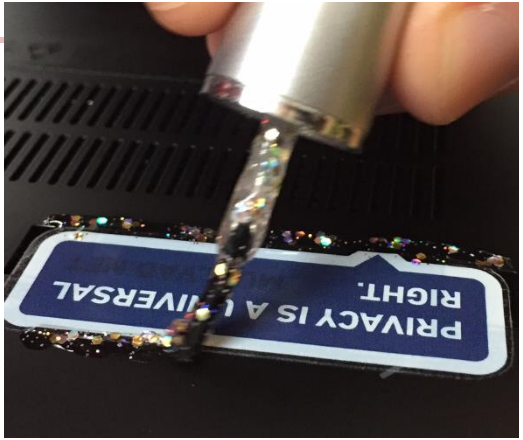
Laser based inspection of storage container [6]

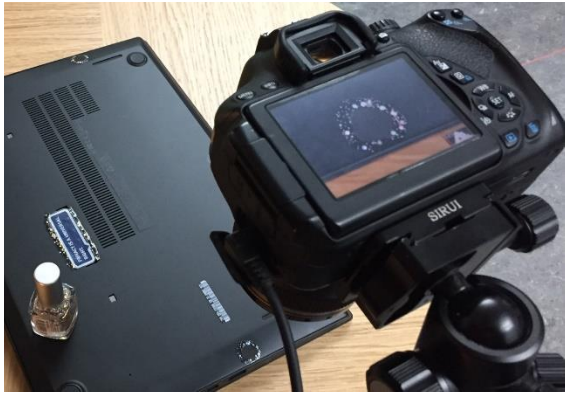


[5] H. A Smartt, etal. Noncontact handheld reader for reflective particle tags. Technical report, Sandia National Lab, 2014.
[6] International Partnership for Nuclear Warhead Disarmament Verification (IPNDV) 2019

Shine bright like a glitter nail polish

1. Cover all holes of a laptop with stickers
2. Cover sticker edges in nail polish
3. Make High Resolution Image of Glitter
4. Sign the image with you private key and upload the signature with the photo
5. Redo the photo if you want to check for tamper

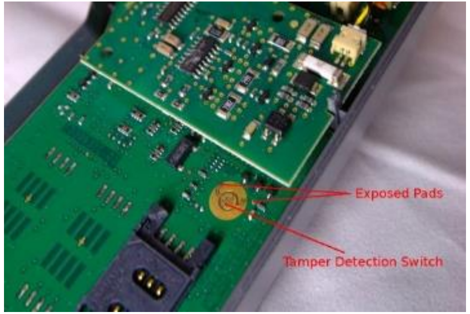




https://mullvad.net/de/blog/2016/12/14/how-tamper-protect-laptop-nail-polish/

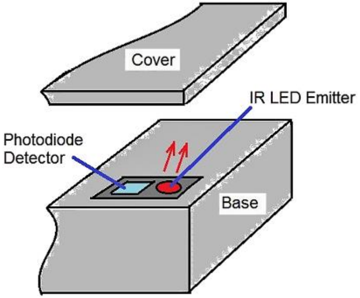
Approaches for Tamper Detection

- Tamper Detection methods aim to notify the user about intrusions
- Attacker is still able to conduct attack as no defence is activated
- Sensors are required:
  - Switches
  - Vibration sensors
  - Light sensors
  - **Tamper detecting mashes**
- No complex APIs are required
- False-Positives do not destroy CSP



Switches on a PCB for detecting tamper [1]

Digital seal for detecting openings of cargo containers through vibration sensors [2]

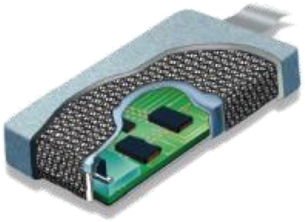


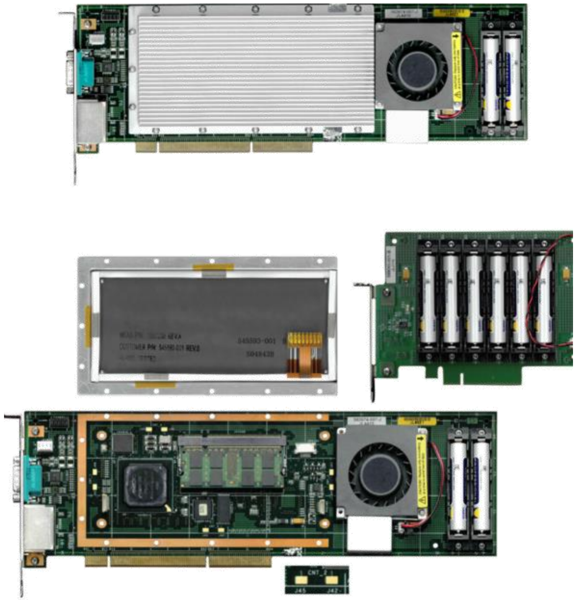
Photoelectric detection of case openings [3]

[1] https://thomascannon.net/chip-and-pin/
[2] https://www.babbler.io/
[3] https://www.sensorsmag.com/components/how-to-implement-reliable-tamper-detection-a-standard-proximity-sensor-module

Approaches for Tamper Responsiveness

- Attack detecting sensors notify deletion circuit about Tamper
  - False Positives are catastrophic
  - Trying to tamper with the system destroys any valuable information
- **Issue:** All approaches need constant power (battery) and leave blind spots, e.g., drilling new openings
- **State of the Art:**
  - Tamper detecting meshes are continuously measured
  - Rupture in mesh leads to zeroization





HP Atalla Cryptographic Subsystem

https://www-03.ibm.com/security/cryptocards/pciecc/overview.shtml
Immler et al., B-TREPID Batteryless Tamper-Resistant Envelope, HOST 2018

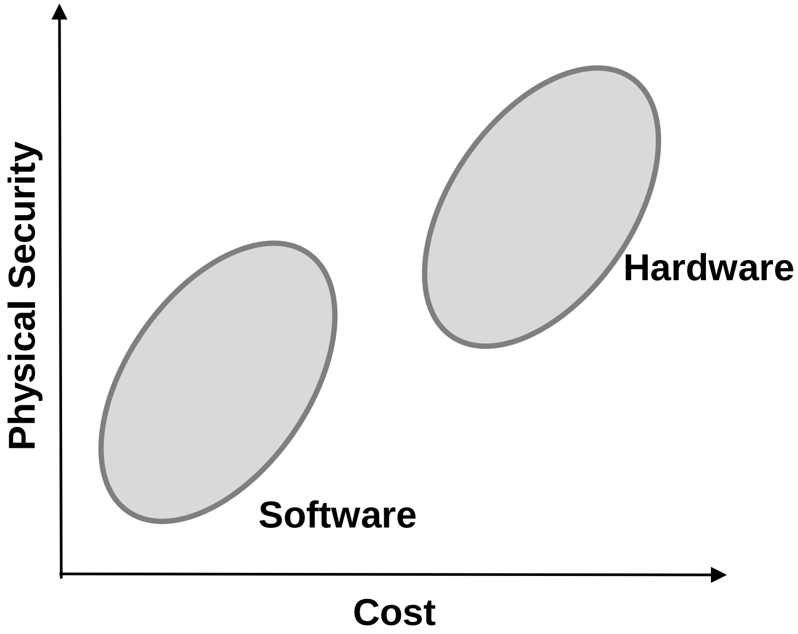
Issues with current solutions

- FIPS 140-2 Level 4 is a hard to reach certification
  - Only three modules (all HSM) worldwide are currently certified [1]
  - Fourteen modules have reached FIPS 140-2 Level 4 overall
- Constant need for power is troublesome
  - What happens when the battery runs empty?
- No OTS solution is currently available to the best of our knowledge
- Retrofitting existing machines is extremely hard to do
  (ATM, Server Units, IoT-devices, etc.)
- Current approaches cannot protect complete systems

[1] https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search

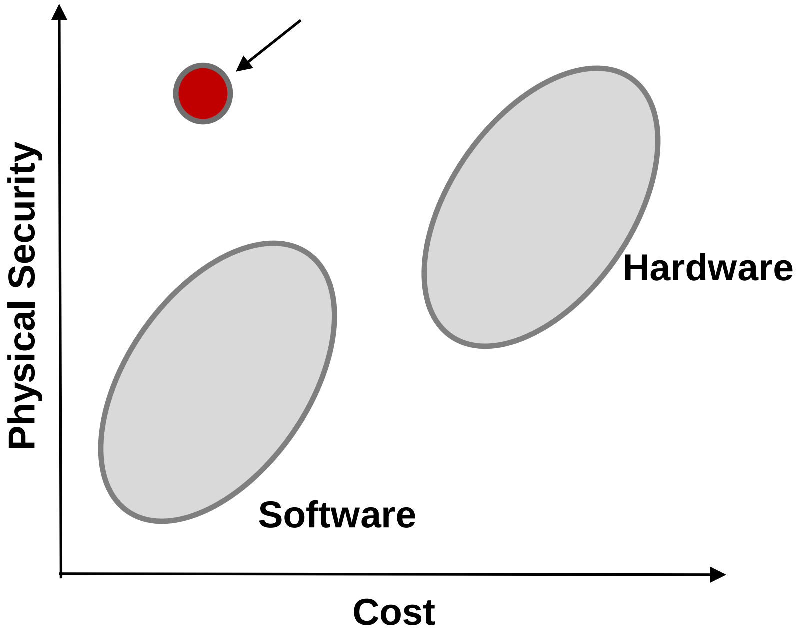
How are security parameters secured in chips or on PCB level?

- Software
  - Copyright notice and watermarking
  - Obfuscation
  - Proof-Carrying Code
  - Custom OS
  - Secret shares (online)
- Hardware
  - No security features at all
  - Write once read many memory
  - Proprietary code read out protection
  - Tamper-resistant packaging



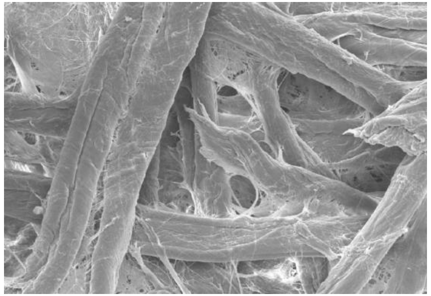
How are security parameters secured in chips or on PCB level?

- Software
  - Copyright notice and watermarking
  - Obfuscation
  - Proof-Carrying Code
  - Custom OS
  - Secret shares (online)
- Hardware
  - No security features at all
  - Write once read many memory
  - Proprietary code read out protection
  - Tamper-resistant packaging
  - **Physical Unclonable Functions**

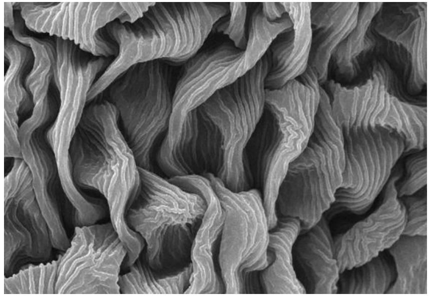


Physical Disorder based Security

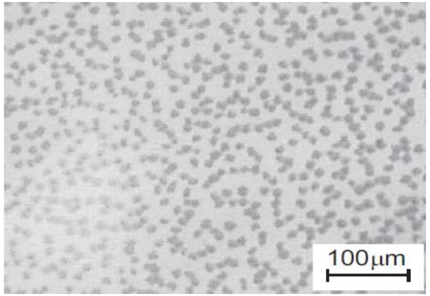
- The small-scale structure of almost any mesoscopic and macroscopic object is not perfectly smooth – but random, imperfect, unique, or physically disordered



Paper



Crimson Clover

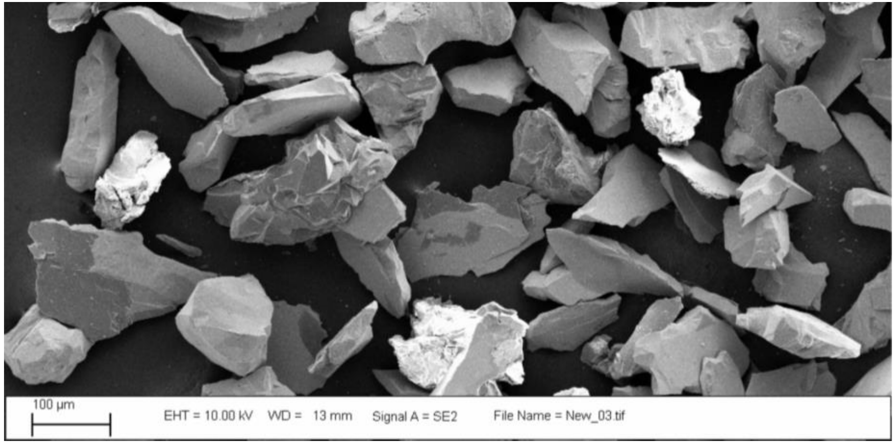


Silicon-aluminum substrate

[1] W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J.A. Halderman, E.W. Felten: Fingerprinting Blank Paper Using Commodity Scanners. IEEE S&P 2009.
[2] A. Sharma, L. Subramanian, E.A. Brewer: PaperSpeckle: microscopic fingerprinting of paper. ACM CCS 2011.
[3] C. Jaeger, M. Algasinger, U. Rührmair, G. Csaba, M. Stutzmann: Random p-n-junctions for physical cryptography. Applied Physics Letters 96, 172103 (2010)

Security-Relevant Features of Disorder

- **Physically disordered systems are very hard to duplicate or „clone“**
  - Even for their original manufacturer…
  - The technology for perfect duplication in 3D simply does not exist yet…
  - Ultimate security level: „Technological security“ against cloning
- Physical disorder is usually quite unwanted – but can we exploit it constructively, too?



H. A Smarttet al. Noncontact handheld reader for reflective particle tags. Technical report, Sandia National Lab., Albuquerque, NM (United States), 2014.

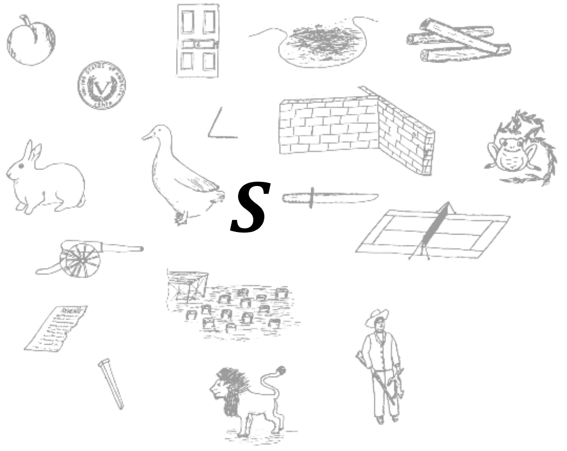
Physical Disorder based Security Example

PUF (Physically Unclonable Function)

Disordered, **unclonable**, physical system $\boldsymbol{S}$

Challenges $\boldsymbol{C_i}$

(External Stimuli)



Response $\boldsymbol{R_i}$

(Function of the challenge $\boldsymbol{C_i}$ and
The specific disorder $\boldsymbol{S}$)

$\boldsymbol{(C_i, R_i)}$

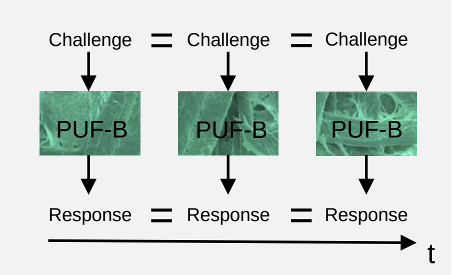
Challenge Response Pair (CRP)

Properties:

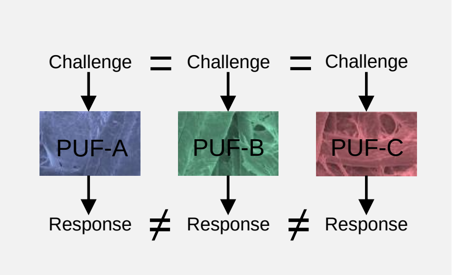
- Easy to evaluate but hard to predict
- Easy to manufacture but hard to duplicate

Physically Unclonable Function

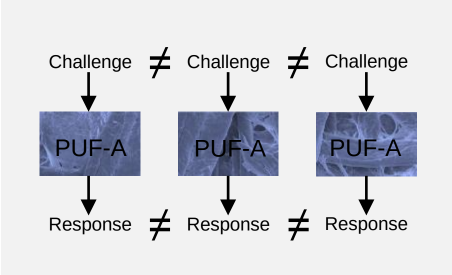
- Like a fingerprint, the PUF is an individual characteristic, which is bound to a physical object
- PUF properties
  - **Robustness**: how much two responses of the same PUF differ.
  - **Unclonability**:
    - Physical unclonability: The PUF can not be changed anymore and with a suitable design of the production process the probability of two identically PUFs disappears.
    - Mathematical unclonability: Attacker uses machine learning techniques (weapon of choice) which predicts PUF-behavior on unknown CRPs.
  - **Unpredictability**:
    - A PUF response to a challenge should be hard to predict if the responses of other PUFs to this challenge are known.
    - A PUF response should be hard to predict if a fixed number of PUF responses of the same PUF is already known
  - **Tamper-Evidence**: the PUF reacts to invasive manipulations (the response is no longer accepted)
- PUFs are (at least in theory!) a universal cryptographic primitive!



Challenge = Challenge = Challenge
PUF-B
PUF-B
PUF-B
Response = Response = Response
t



Challenge = Challenge = Challenge
PUF-A
PUF-B
PUF-C
Response ≠ Response ≠ Response



Challenge ≠ Challenge ≠ Challenge
PUF-A
PUF-A
PUF-A
Response ≠ Response ≠ Response

Algorithmic Tamper Proof (ATP)

- In [1], the authors examine the key storage from an algorithmic perspective, introduce the term Algorithmic Tamper Proof (ATP) and show that this can only be achieved with a device that has the following properties:
  - (E1) it has hardware from which an attacker cannot read information (readout secure storage),
  - (E2) it has the ability to destroy data (self-destruction) and
  - (E3) it has hardware that contains data that cannot be changed unnoticed by an opponent (tamper-proof hardware).

* The author focus on the security of smartcards. However, the underlying security principles can be applied for any use case.

[1] Gennaro, Rosario, et al. "Algorithmic tamper-proof (ATP) security: Theoretical foundations for security against hardware tampering." *Theory of Cryptography Conference*. Springer, Berlin, Heidelberg, 2004

Algorithmic Tamper Proof (ATP)

- The key can only be recovered from inside and if the integrity of the environment has not been violated
  - readout secure storage (E1) and
  - self-destruction (E2).

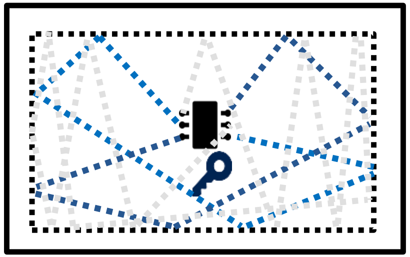
- The key can be used to encrypt stored data integrity-protected within the device
  - data that cannot be changed unnoticed (E3).

- No digital keys, no trusted HW

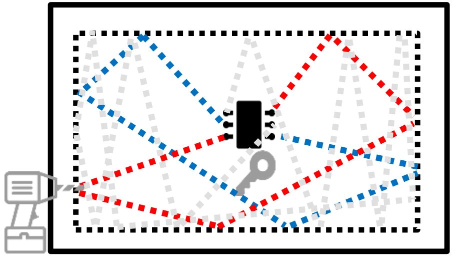
- No need for attack detecting circuit or data deleting circuit (no battery).

- Retrofitting of commodity hardware

Initially: Devices extract key from physical disorder

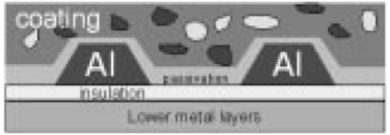


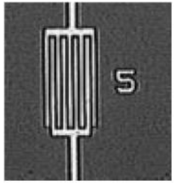
Later: Keys proof integrity of the entire system

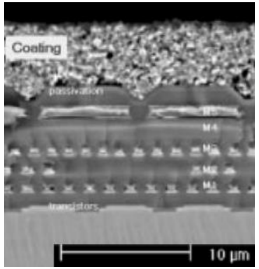


Interesting new approach: Cover with Tamper-Resistance

- Coating PUF [1]
  - **3bit per sensor**, 30 sensors overall = 90 bit of randomness







- Tamper-resistance PUF cover [2]
  - **5.5 bit per sensor**, 128 sensors = 704 bit

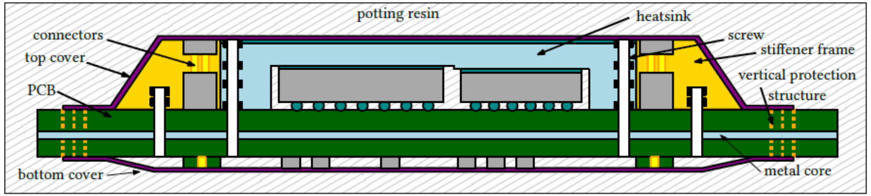
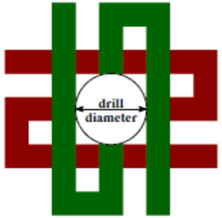


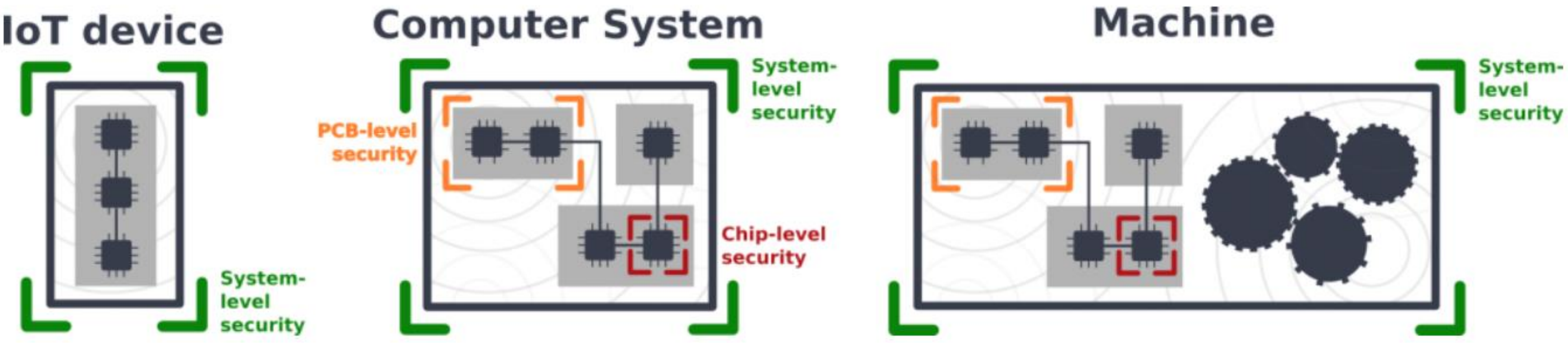
Figure 4: Packaging concept of a device enclosed by the proposed cover.



[1] Tuyls, Pim, et al. "Read-proof hardware from protective coatings." CHES, Heidelberg, 2006.
[2] Immler et al., Secure Physical Enclosures from Covers with Tamper-Resistance, CHES 2019

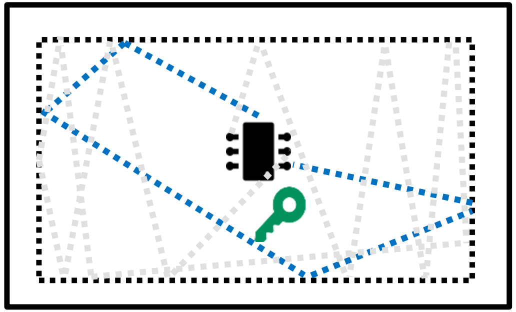
How to extend Physical Integrity Assessment to the System Level?

- Multiple-chip embedded systems are most commonly represented.



Tamper-Resistant Physical Enclosure

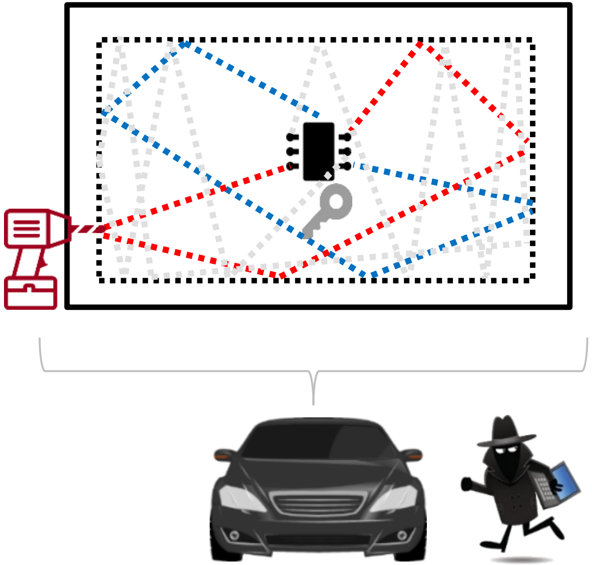
Devices extract key from physical disorder



e.g., control module of a car

Tamper-Resistant Physical Enclosure (2)

Devices extract key from physical disorder



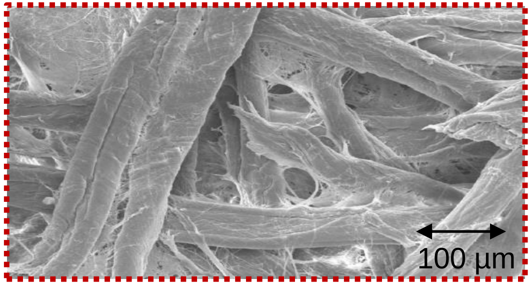
e.g., control module of a car

Key destroyed

An attack changes k_{phy} thereby rendering all encrypted data useless.

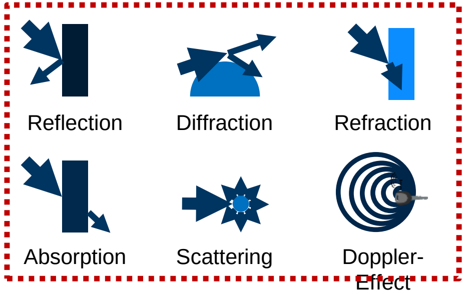
Our Key Idea:

- Making physically disordered systems (random, unique, unclonable) machine-readable by measuring their corresponding electromagnetic fingerprint…



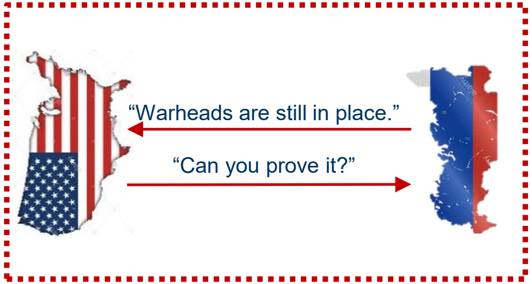
Object's physically disordered surface

+



Radio-wave propagation effects

+

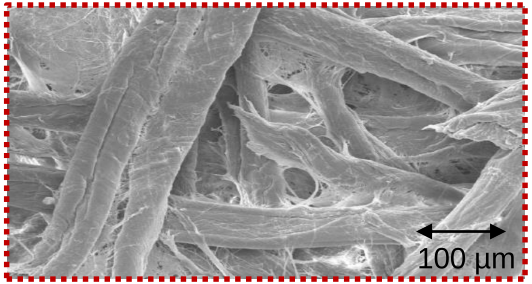


Cryptographic challenge-response protocol

- …to prove physical statements remotely without using classical tamper-resistant hardware and cryptographic keys.

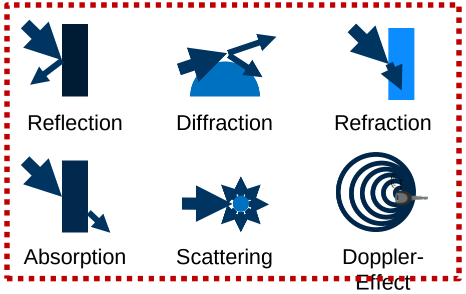
Our Key Idea:

- Making physically disordered systems (random, unique, unclonable) machine-readable by measuring their corresponding electromagnetic fingerprint…



Object's physically disordered surface

+



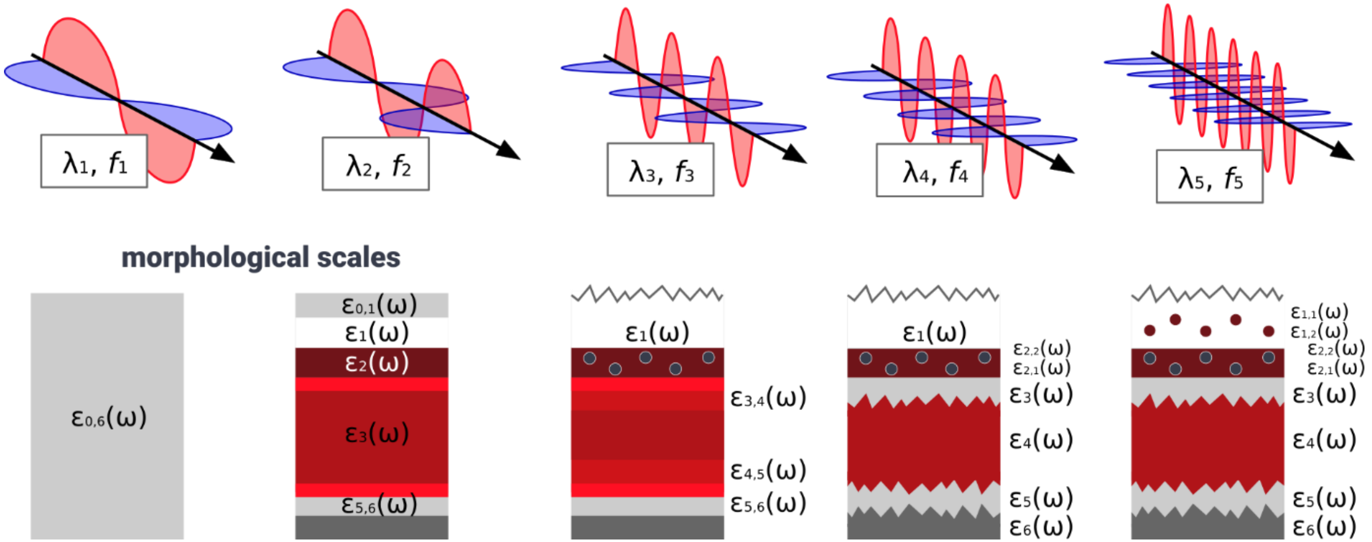
Radio-wave propagation effects

+

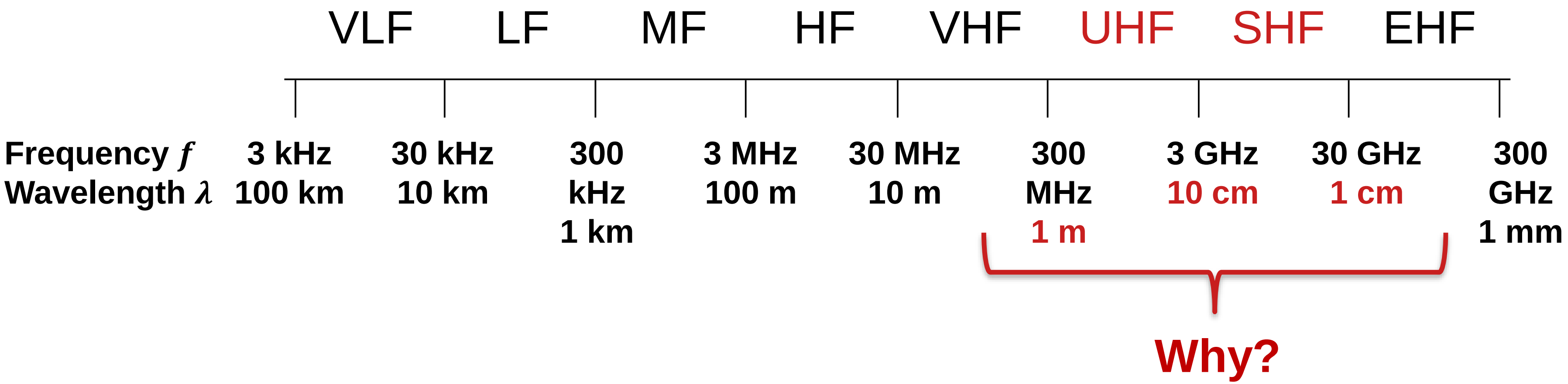
Cryptographic challenge-response protocol

- …to prove physical statements remotely without using classical tamper-resistant hardware and cryptographic keys.

Categorization of the Multi-scale Surface Model



Suitable Frequency Range?

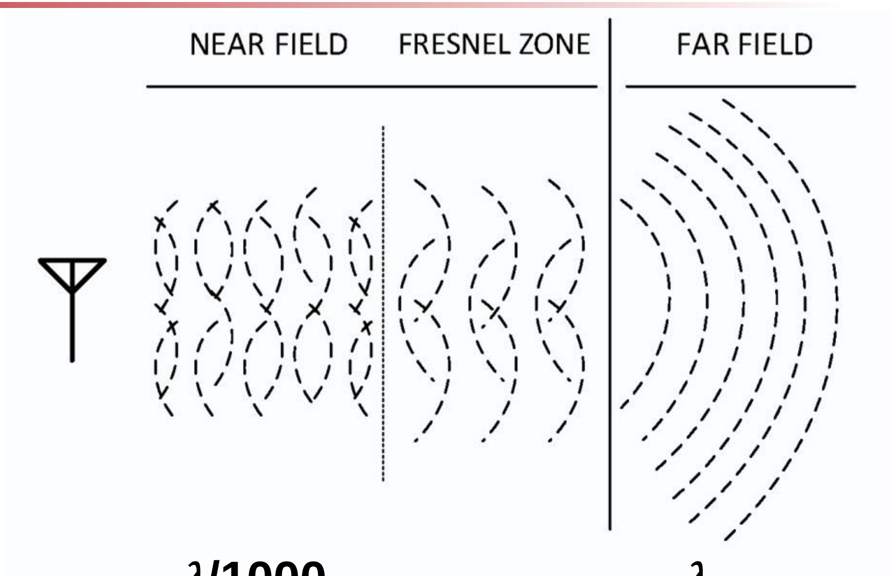


VLF LF MF HF VHF UHF SHF EHF

Frequency *f*	3 kHz	30 kHz	300 kHz	3 MHz	30 MHz	300 MHz	3 GHz	30 GHz	300 GHz
Wavelength *λ*	100 km	10 km	1 km	100 m	10 m	1 m	10 cm	1 cm	1 mm

Why?

Using the Near-Field to Increase the Security Sensitivity



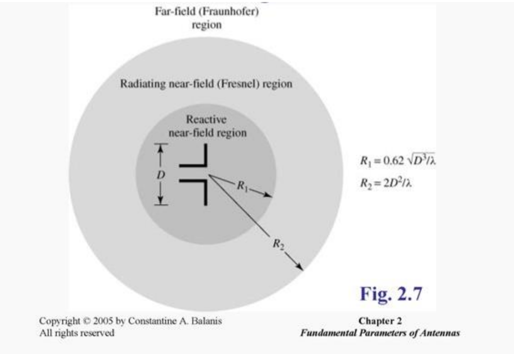
Object sizes that influence the wave propagation/antenna properties [1]:

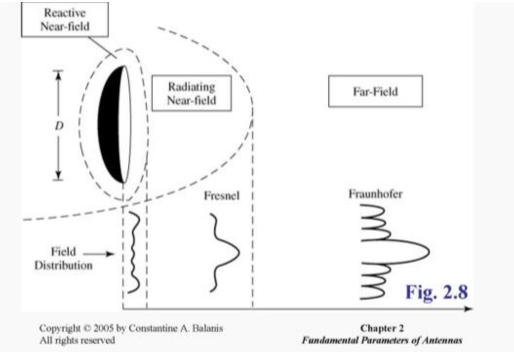
	$\lambda/1000$	λ
@433 MHz:	693 µm	69.3 cm
@868 MHz:	345 µm	34.5 cm
@2.4 GHz:	125 µm	12.5 cm
@5.5 GHz:	60 µm	6.0 cm

[1] Gerald DeJean and Darko Kirovski. 2007. RF-DNA: Radio-Frequency Certificates of Authenticity. CHES 2007, Vienna, Proceedings. 346–363.

Near-Field

- Reactive near-field
  - **In the reactive near-field, the relationship between the strength of the electric and magnetic fields is often too complex to predict**.
  - Either filed component may dominate at one point, ant the opposite relationship dominate at a point only a short distance away
  - Phase of electric and magnetic fields are nearly quadrature thus
    - Highly reactive wave impedance
    - High content of non-propagating stored energy near antenna
- Radiating near-field
  - Fields are predominantly in phase
  - Fields do not yet display a spherical wave front: thus a pattern varies with distance
  - These are regions where near-field measurements are made

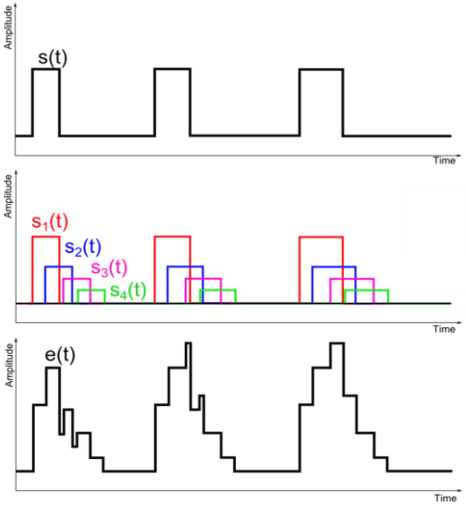

Far-field (Fraunhofer) region
Radiating near-field (Fresnel) region
Reactive near-field region
D
R_1
R_2
$R_1 = 0.62\sqrt{D^3/\lambda}$
$R_2 = 2D^2/\lambda$
Fig. 2.7
Copyright © 2005 by Constantine A. Balanis
All rights reserved
Chapter 2
Fundamental Parameters of Antennas

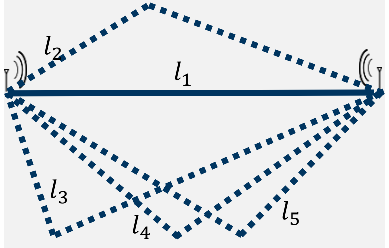


How to measure the influence of the environment to the signal?

- Channel Impulse Response (CIR)
  - Is capable to fully characterize the individual paths (including the sum of all multipath components according to the tapped-delay-line model)
  - $e(t)=s(t)*h(t)$

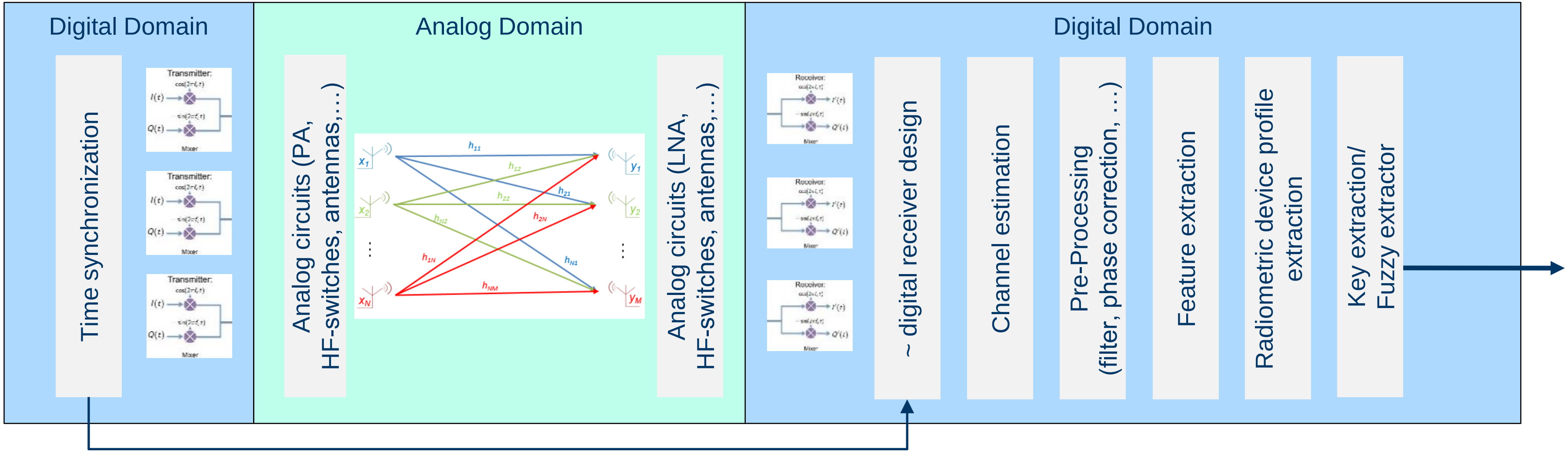
- Channel State Information (CSI)
  - Using CSI, a PHY-layer is able to discriminate multipath characteristics, and thus holds the potential for better equalization of the receiver and transmitter filters





$$H_{r,t}(f_k,t)=\sum_{l\in L}\alpha_l(f_k,t)e^{\frac{-2j\pi d_l(t)}{\lambda_k}}$$

How to measure the influence of the environment to the signal? (2)



Digital Domain

Time synchronization

Analog Domain

Analog circuits (PA, HF-switches, antennas,…)

Analog circuits (LNA, HF-switches, antennas,…)

Digital Domain

~ digital receiver design

Channel estimation

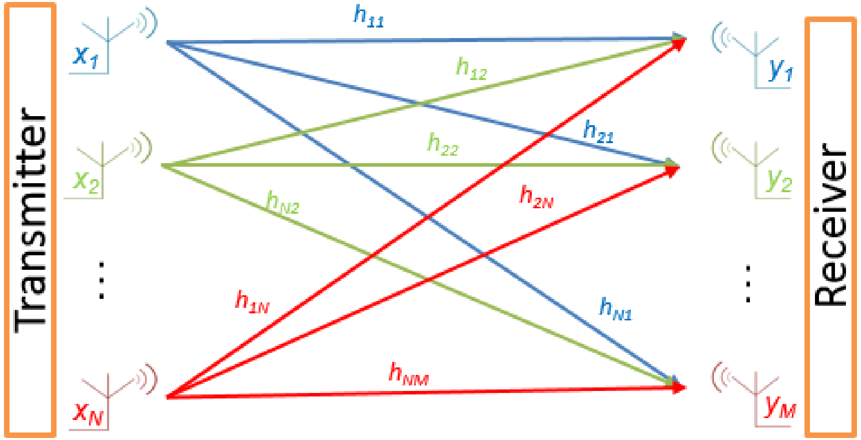
Pre-Processing (filter, phase correction, …)

Feature extraction

Radiometric device profile extraction

Key extraction/ Fuzzy extractor

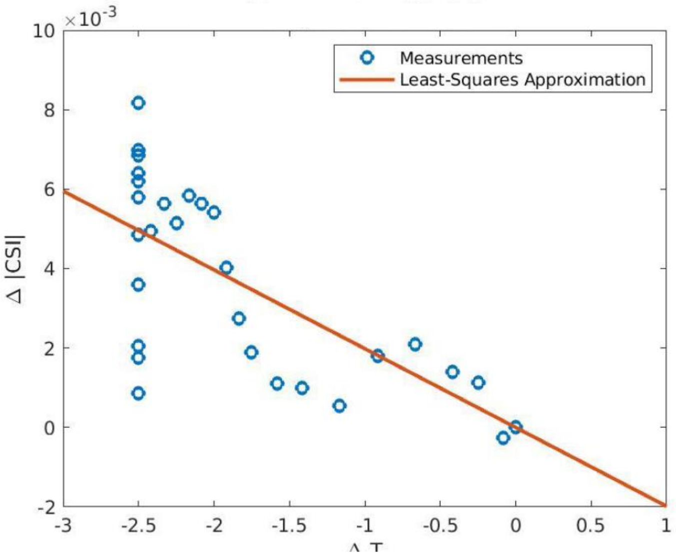
How to measure the influence of the environment to the signal? (3)

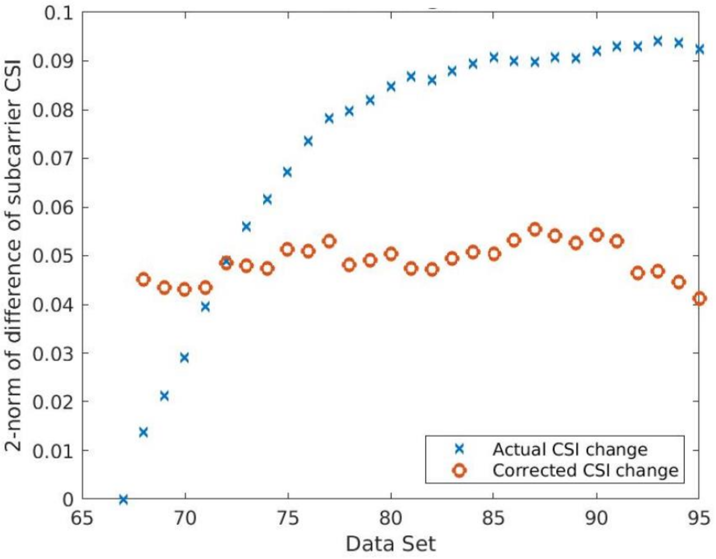


⇨ $\vec{Y} = H \times \vec{X} + \vec{n}$ $$H = \begin{bmatrix} h_{11} & h_{12} & h_{1M} \\ \vdots & \ddots & \vdots \\ h_{N1} & h_{N2} & h_{NM} \end{bmatrix}$$

With *n* as *AWGN*

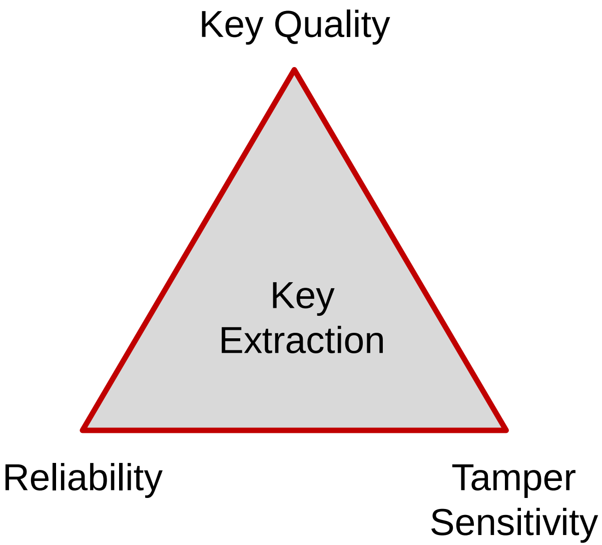
Temperature Correction (Example)



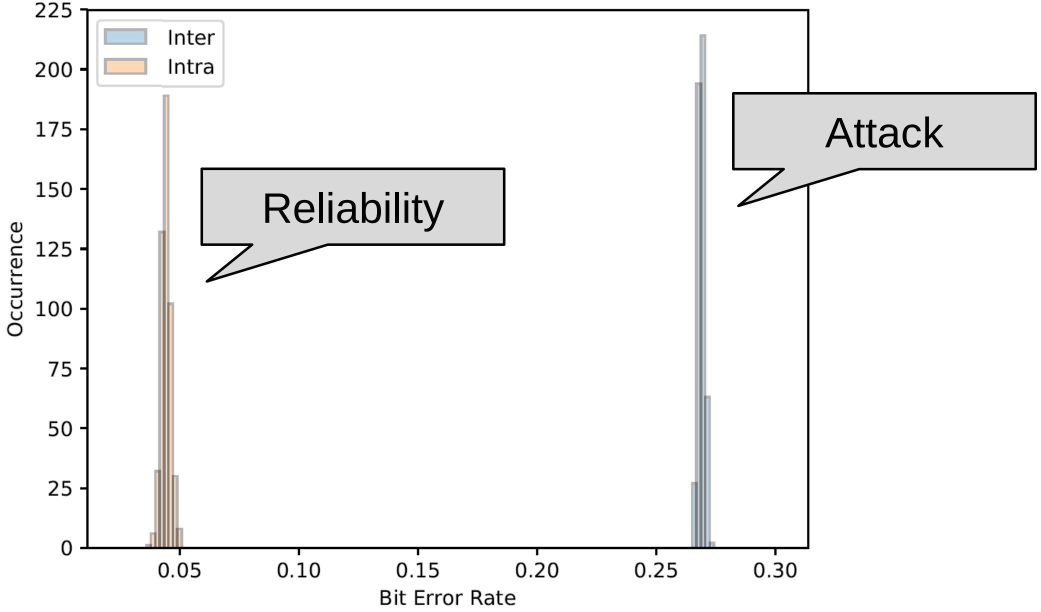


Design Requirement for Fingerprints

- Key Quality
  - The generated key must be highly random
  - >= 128 bit need to be extracted
- Reliability
  - The system must work under all circumstances
  - Legitimate Influences must not result in False-Positives
- Sensitivity
  - Even miniscule attacks shall be detected



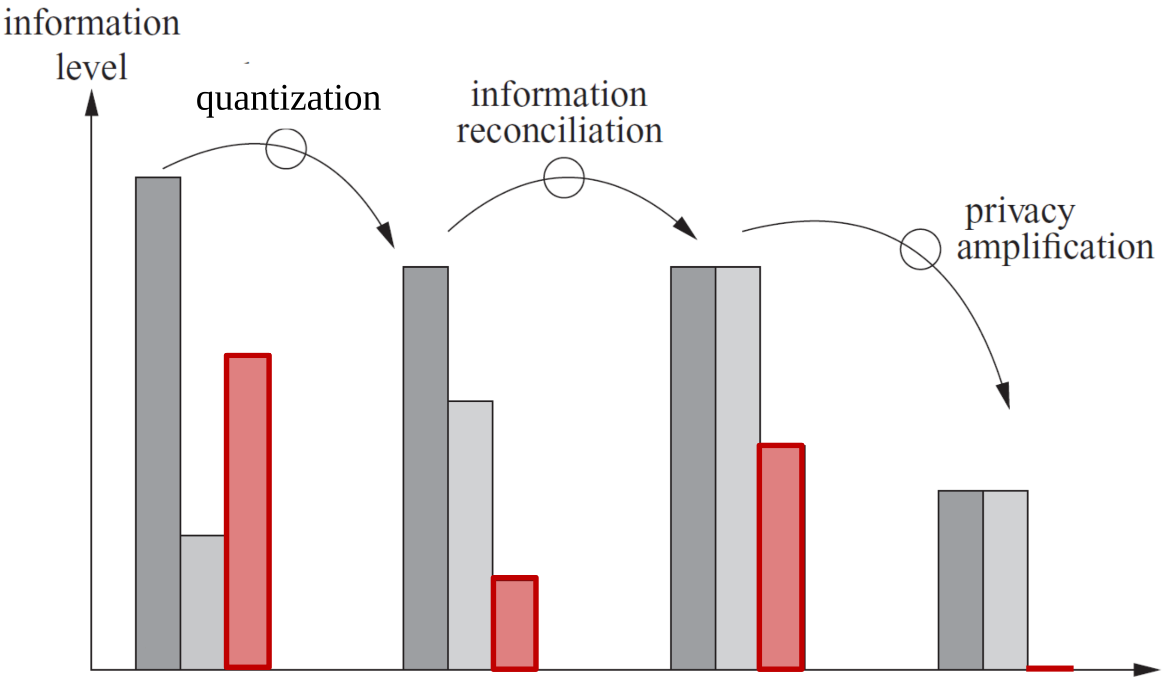
Reliability vs. Tamper Sensitivity



Reliability

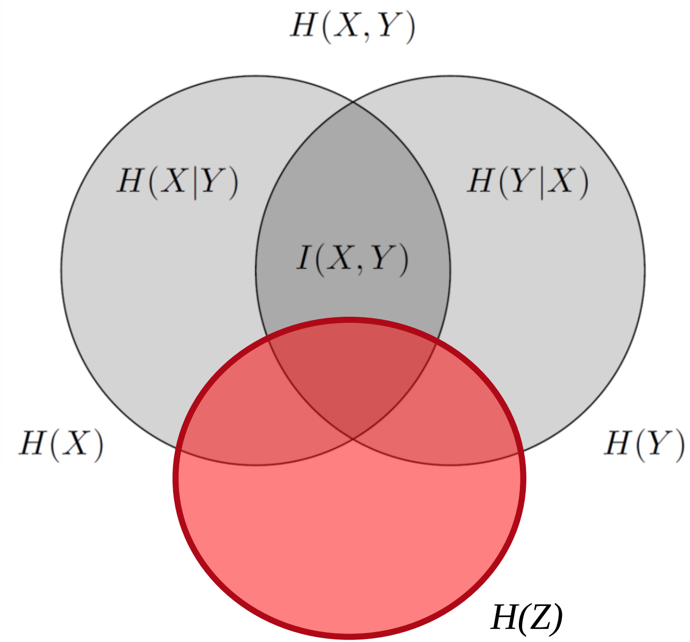
Attack

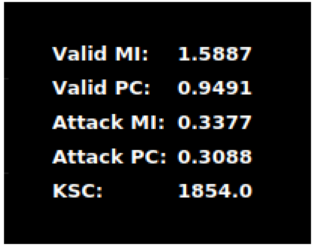
Evolution of information during the phases of a sequential key-generation strategy



Secret Key Capacity

$$C_{sk} \geq I(X;Y) - I(X;Z) \triangleq R_{sk}$$



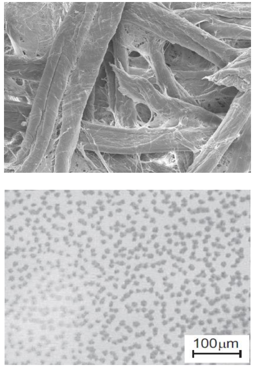


```
Valid MI:    1.5887
Valid PC:    0.9491
Attack MI:   0.3377
Attack PC:   0.3088
KSC:         1854.0
```

Testbed Example 1: Low-Cost Proof of Concept Demonstrator using a Lunch Box and Radio-Chips

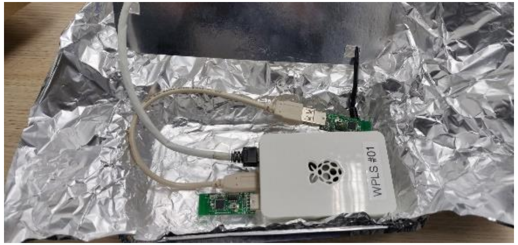
- Radio-enabled commodity hardware (with at least two transmitter)

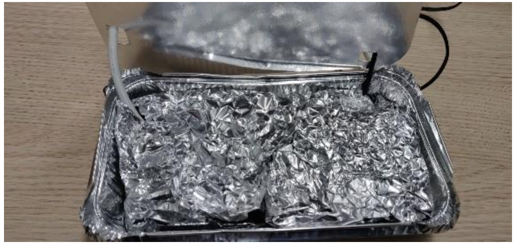
- Enclosure which is not perfectly smooth – but random, imperfect, unique, or physically disordered



Aluminium foil

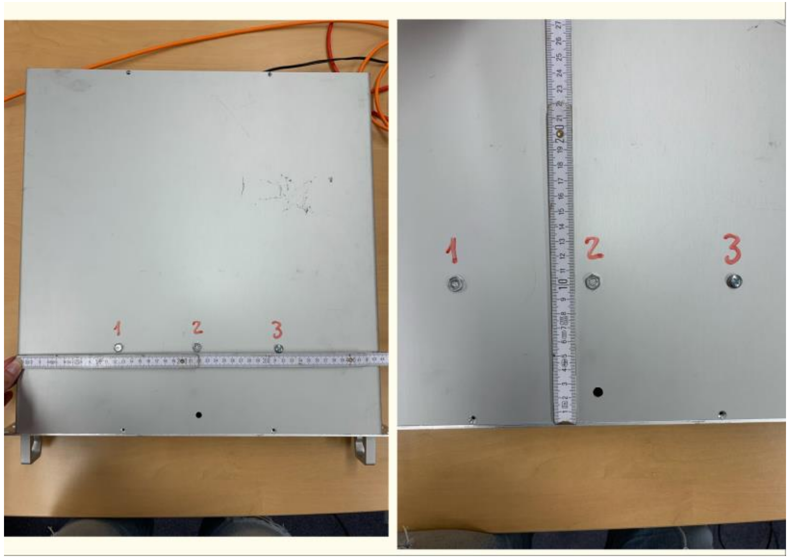
Aluminium lunch box





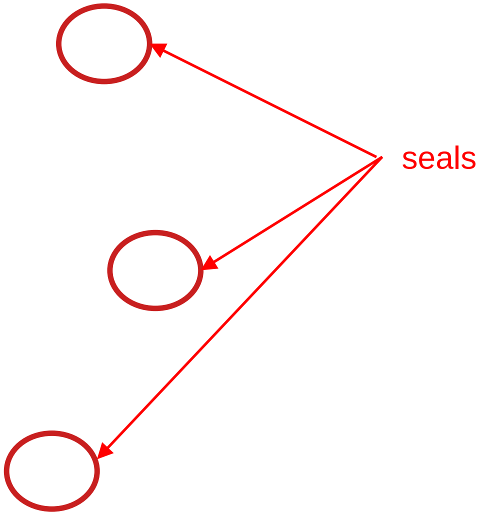
Testbed Example 2: 19” Server Rack

- Unfortunately we cannot present our real-world 19” appliances



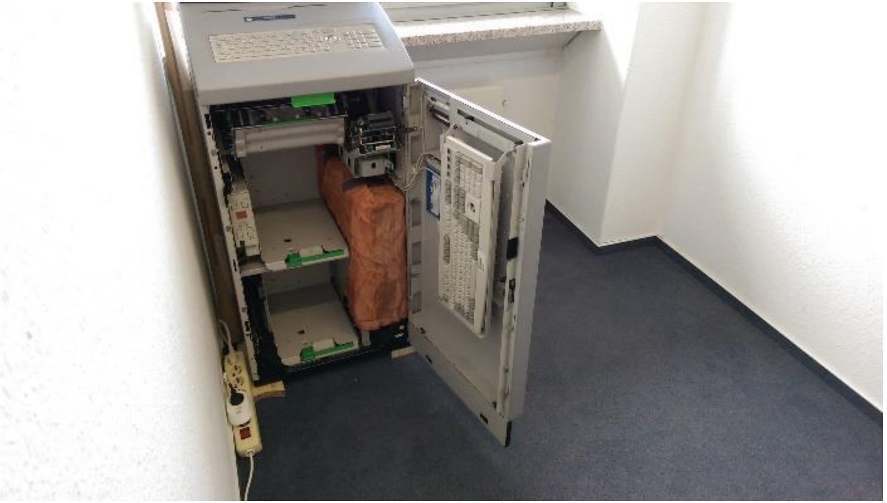
Testbed Example 3: Smart Meter

- Attack vectors of a smart meter:
  - Communication unit (upper part)
  - Meter
  - Connection terminals ←

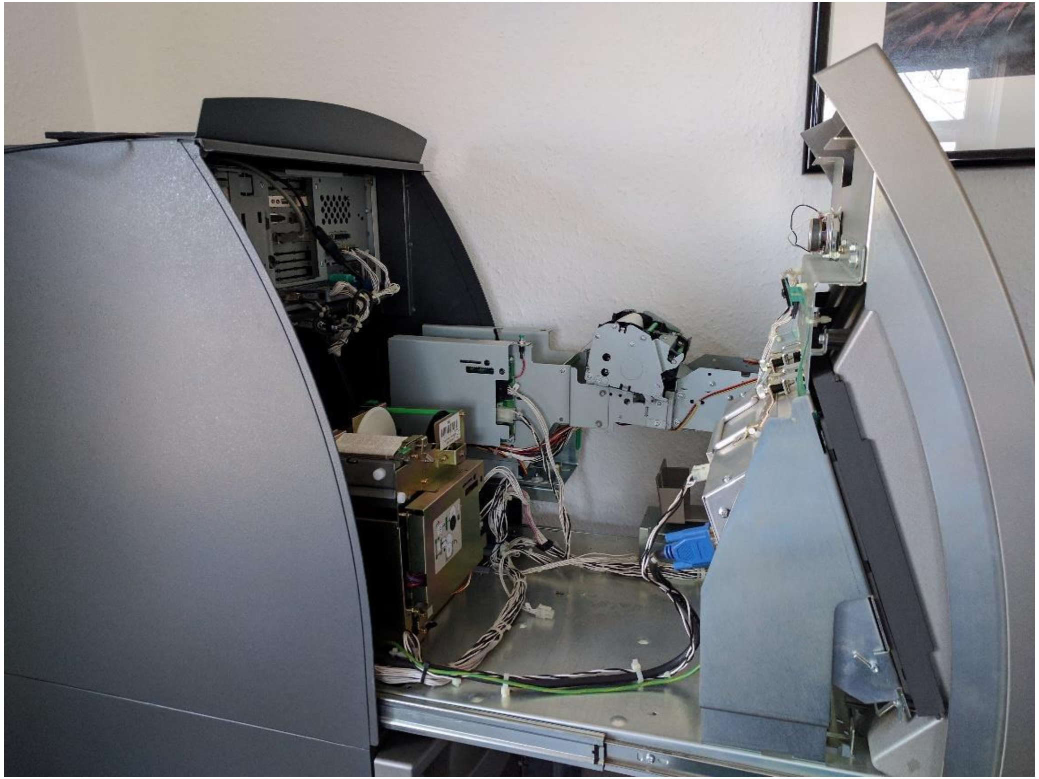


Testbed Example 4: Bank Statement Printer

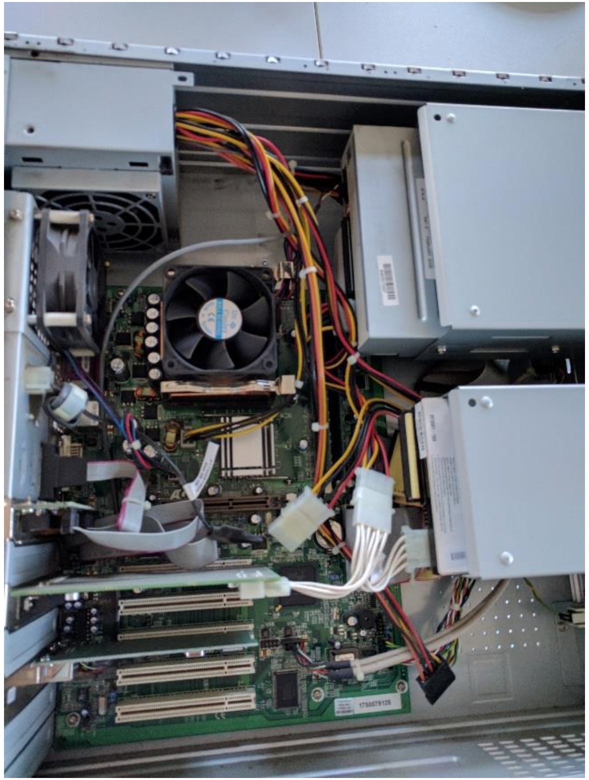
- Couper mesh for additional protection material

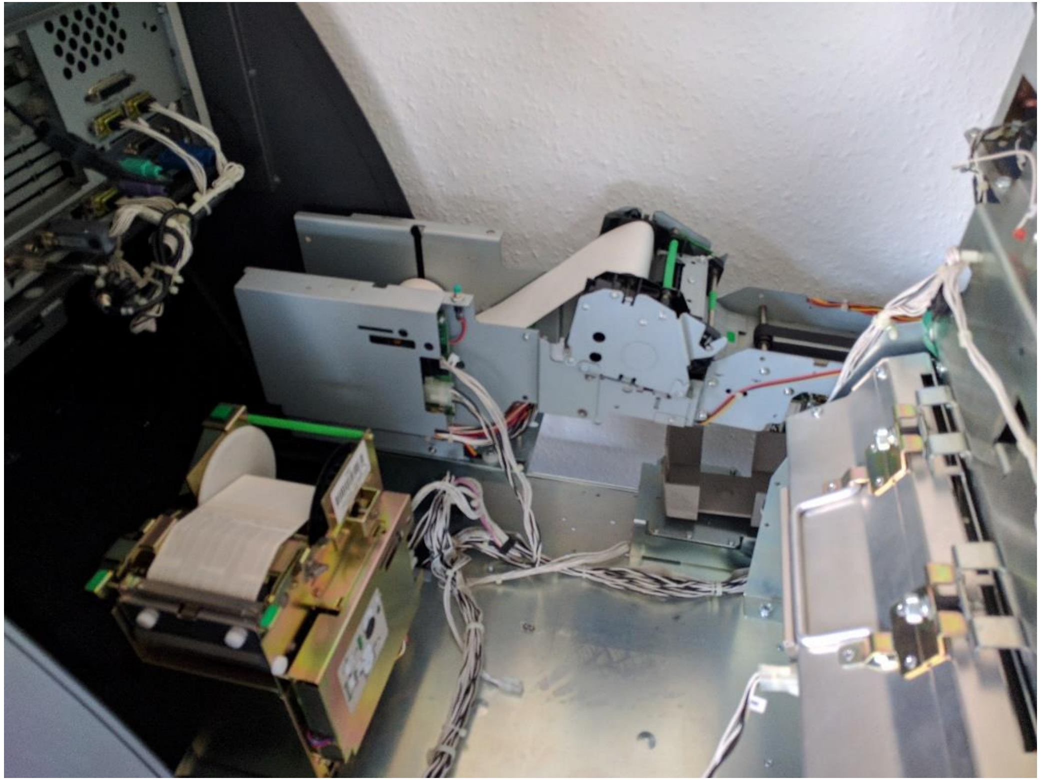


Testbed Example 5: ATM

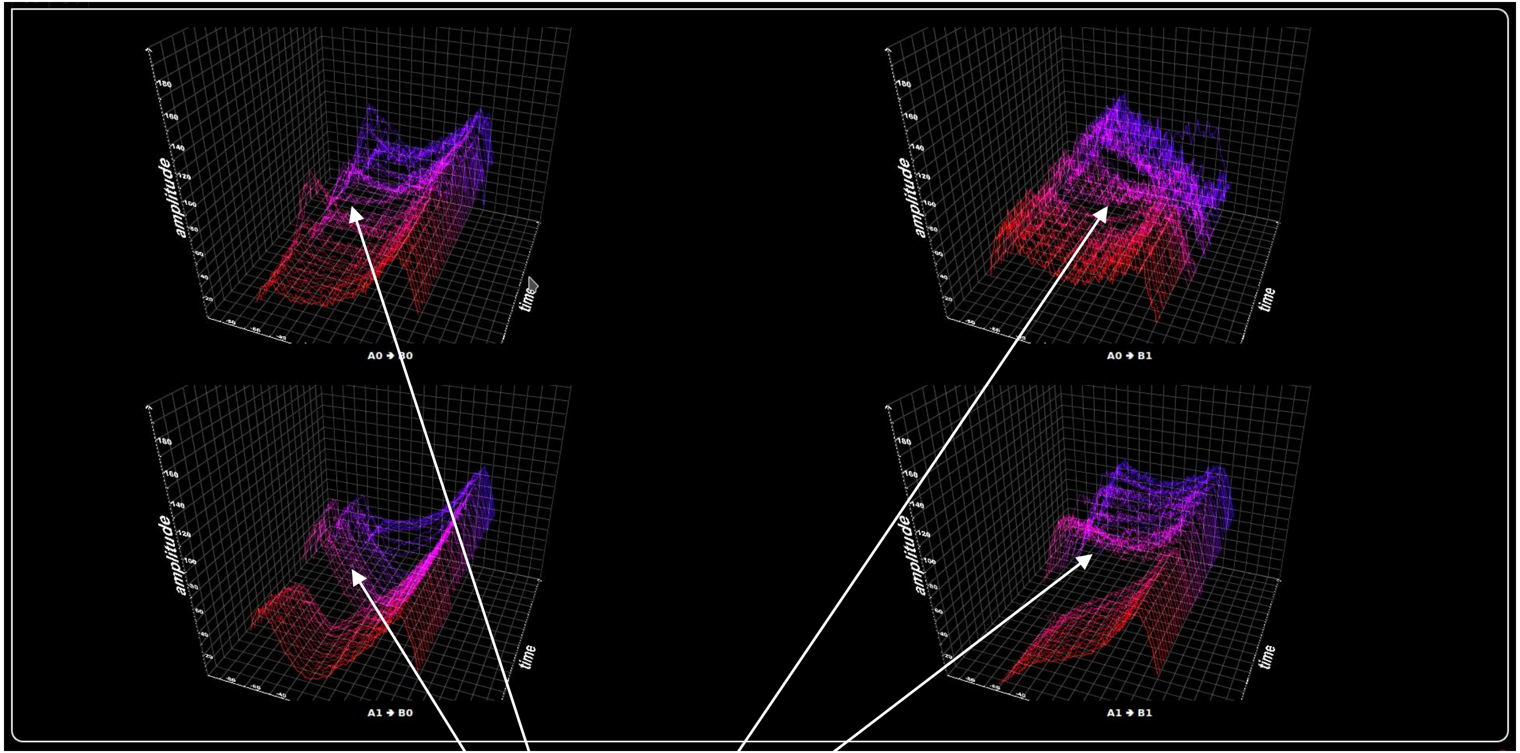


Testbed Example 5: ATM



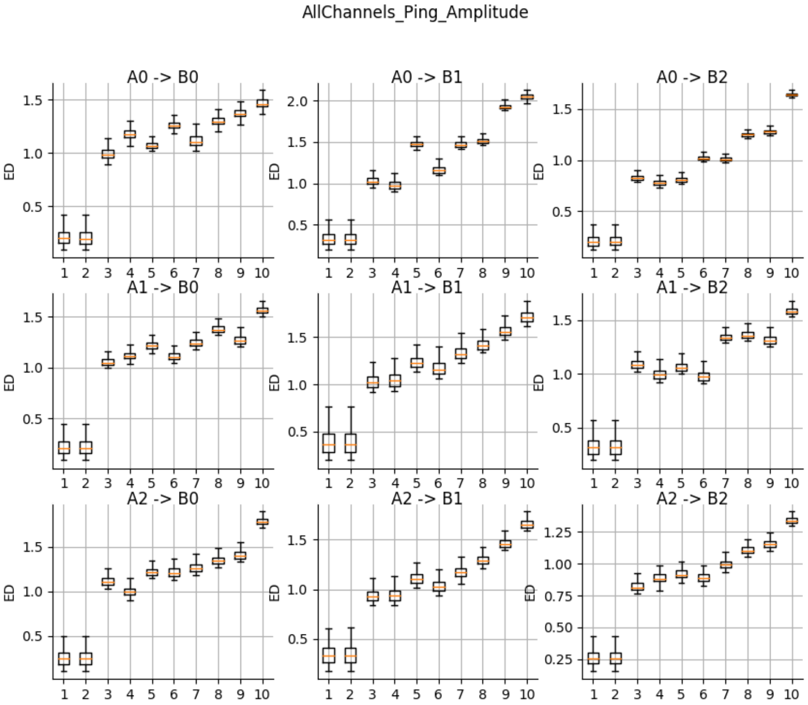


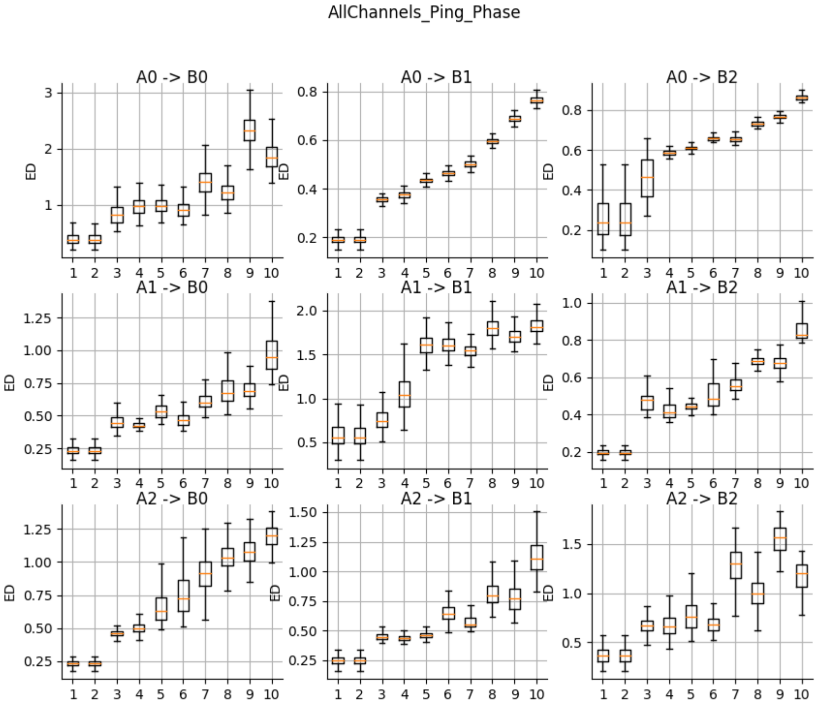
3D CSI Visualization



Needle penetration and retraction

Evaluation results ~60µm^2 to ~1 cm^2 environmental changes

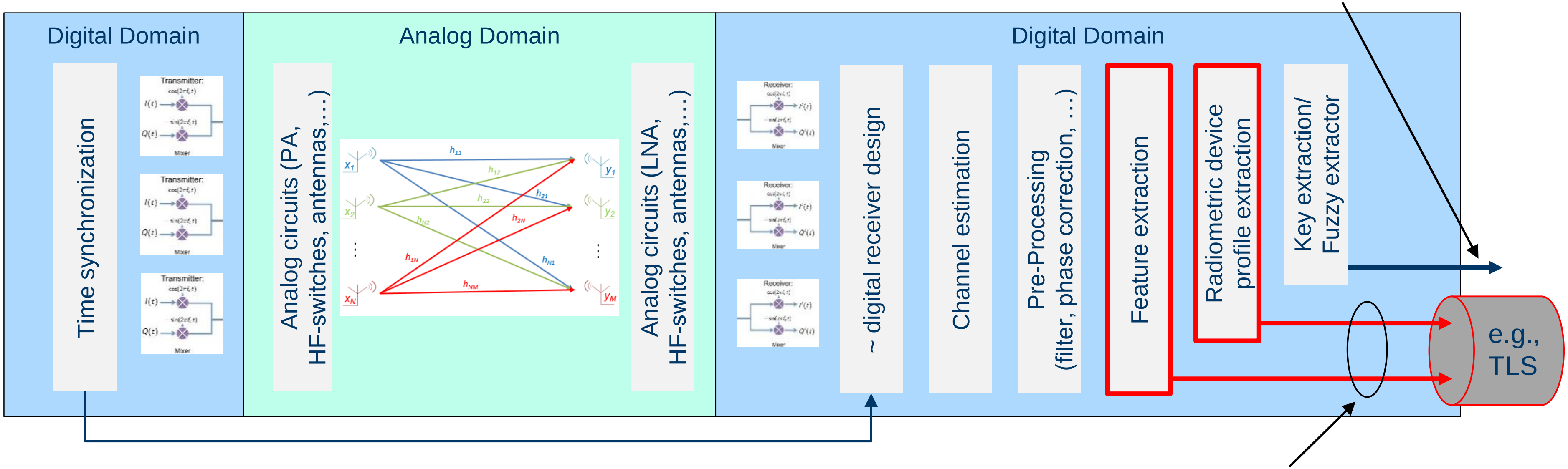




Questions during the development

- How do we deal with internal time-variant behaviours?
  - Based on cyclo-stationary processes, e.g., fan, HDDs, of a server.
  - Based on complex technical processes and equipment, e.g., the internal logbook printer of an ATM.
- How do we deal with external influences?
  - People moving around
  - Devices within the environment
  - Mechanical shocks on the device
- What about Electromagnetic Compatibility (EMC)?
- Unlike an ATP, the integrity of a complex real-world device is not easy to boil down to a binary decision.
  - Machine learning techniques for classification and anomaly detection

How to measure the influence of the environment to the signal? (2)



For local tamper proof (Enclosure-PUF)

Digital Domain

Time synchronization

Analog Domain

Analog circuits (PA, HF-switches, antennas,…)

Analog circuits (LNA, HF-switches, antennas,…)

Digital Domain

~ digital receiver design

Channel estimation

Pre-Processing (filter, phase correction, …)

Feature extraction

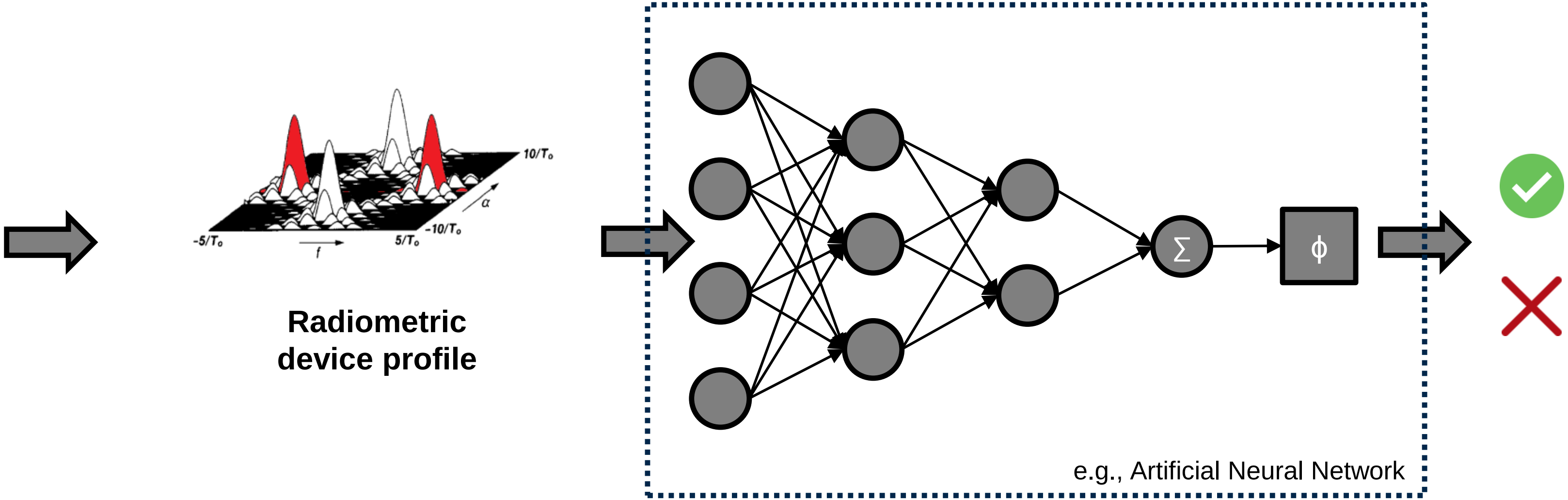
Radiometric device profile extraction

Key extraction/ Fuzzy extractor

e.g., TLS

For remote integrity assessment

Classification of Physical-Layer Information using Machine Learning

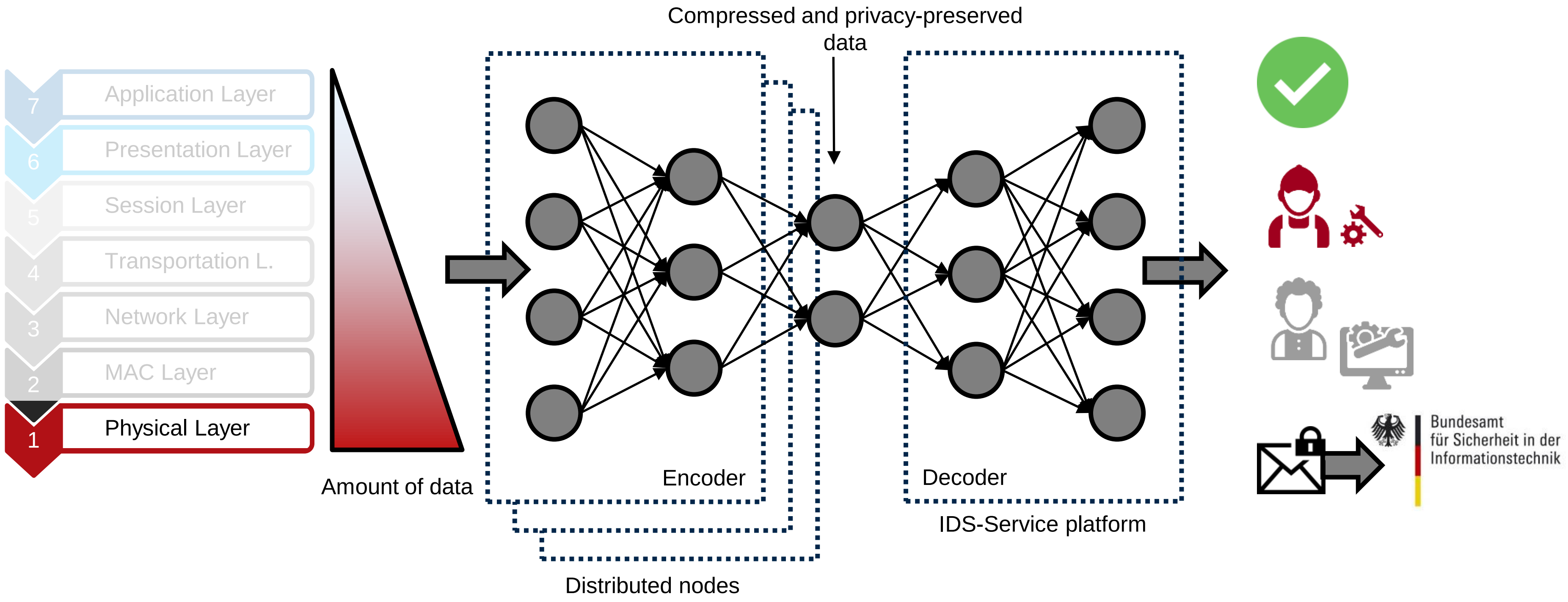


Radiometric device profile

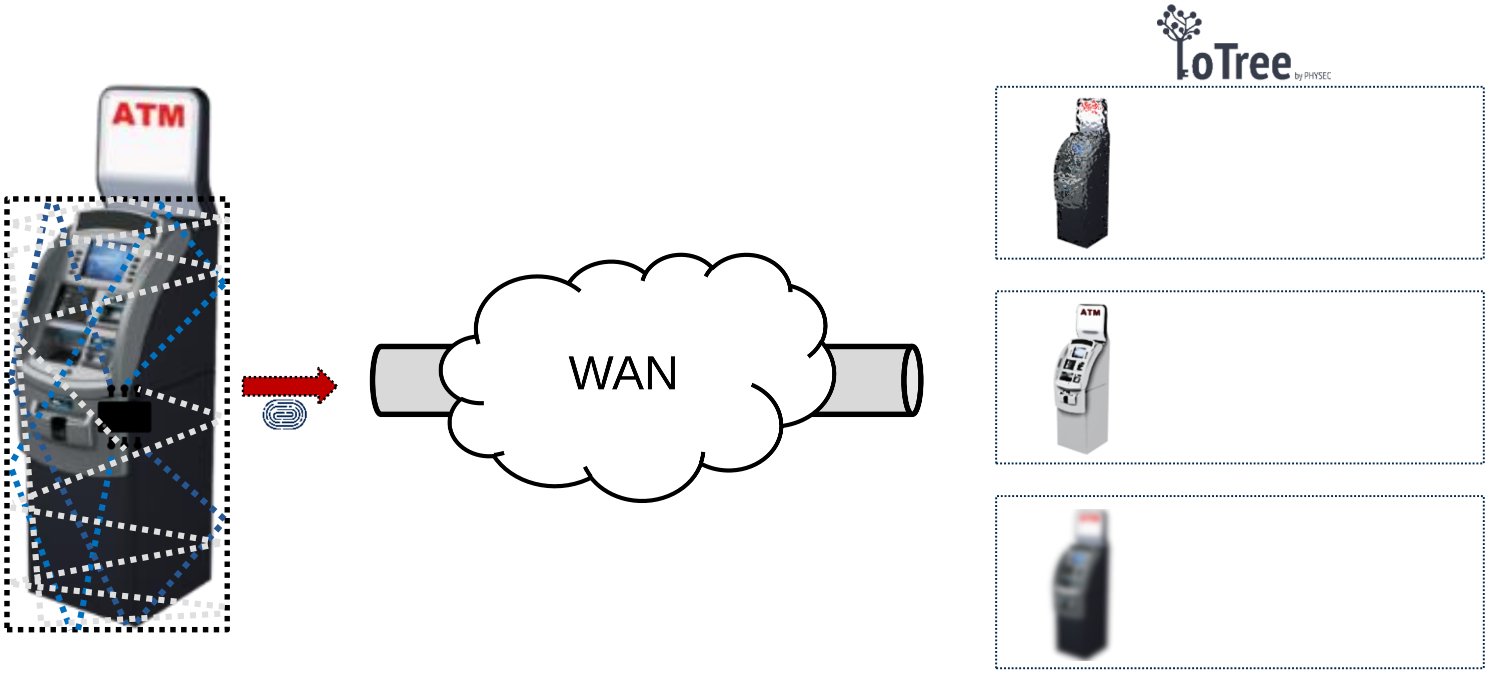
e.g., Artificial Neural Network

Verifying the authenticity, integrity, and other **physical statements** of a complex system.

Physical-Layer Information for Managed Security Solutions



Physical Integrity Assessment

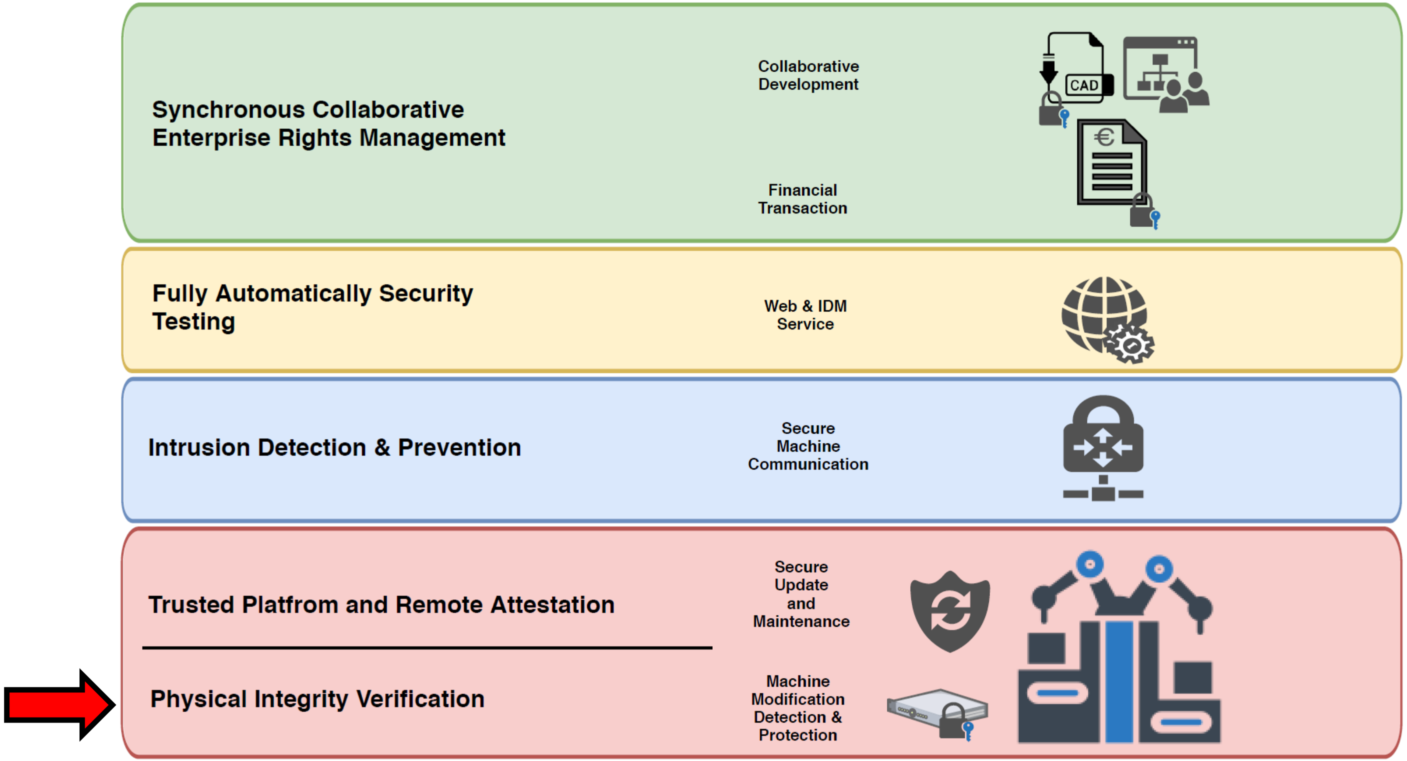


Anomaly detection

(Un-) supervised state classification

Information theoretical assessment

PHYSEC in an Overall Security Concept



Synchronous Collaborative Enterprise Rights Management

Collaborative Development

Financial Transaction

Fully Automatically Security Testing

Web & IDM Service

Intrusion Detection & Prevention

Secure Machine Communication

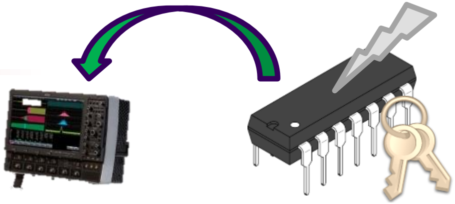
Trusted Platfrom and Remote Attestation

Secure Update and Maintenance

Physical Integrity Verification

Machine Modification Detection & Protection

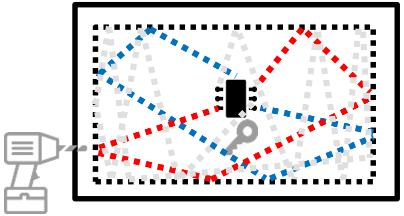
Summary

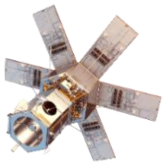


- Physical access enables tampering and leakage

- System-level tamper-protection (or integrity assessment) for commodity hardware is a need

- We presented a solution called Enclosure-PUF that:
  - Is based on standard hardware and cheap enclosure
  - Can be deployed on systems (extends IC/PCB-security)
  - Fulfils an ATP
  - Provides physical state assessment of complex systems





Remote Inspection through Physical Layer Technology
Virtual Proof of Reality for Nuclear Warhead Disarmament Scenarios
https://vpor.rub.de
A joint project by
RUB
HARVARD
PHYSEC
281021
22G1
FRONT
REAR

Dr. Christian Zenger

Prof. Dr. Christof Paar

Dr. Heiko Koepke

We are looking for cooperations

Many thanks for your attention!

Questions?

… or maybe later:
christian.zenger@physec.de

https://www.physec.de