



Bootstrapping Physical Security with Inertial Hardware Security Modules

Darmstadt • 2026-06-16 • Jan Sebastian Götte • research@jaseg.de



Research Questions



Why secure hardware?

- Computing systems increase in complexity with time. The LLM bubble makes this *a lot* worse.
- Physical separation helps compartmentalizing complex systems across interfaces that are easy to reason about
- At interfaces, proofs, testing and fuzzing reduce logical flaws, but physical attacks remain to directly target what's behind
- Decades of research show circuit-level defenses are complex, costly and brittle
- Thus, we need secure enclosures to prevent physical attacks from ever reaching their target (CPU, memory, etc.)



Secure hardware use cases

- Germany's national Electronic Health Record system ("ePA") stores sensitive healthcare data about millions of people
- keys are derived from system-wide low-entropy root secret
- root secret stored in secure hardware

Deutsches
Ärzteblatt
Politik

Neustart für elektronische Patientenakte für 2023 geplant

Mittwoch, 28. Dezember 2022



/picture alliance, FotoMedienService, Ulrich Zillmann

Berlin – Arztbefunde, Röntgenbilder, Medikamentenlisten: Seit zwei Jahren gibt es die elektronische Patientenakte (ePA), mit der Versicherte Gesundheitsdaten parat haben können – abrufbar am Smartphone. Doch die Nachfrage hält sich in engen Grenzen.



Research Questions

RQ1: What is the state of the art in commercial tamper sensing mesh implementations?

RQ2: What are criteria and approaches for the design of secure tamper sensing meshes?

RQ3: Can we achieve physical security without a bespoke tamper-sensing mesh?

RQ4: Can we improve tamper-sensing meshes monitoring performance?

RQ5: Can we improve the ripple voltage performance of Wireless Power Transfer to power IHSMs?

RQ6: What applications do IHSMs open up through increased power dissipation and size?



Research Questions

RQ1: What is the state of the art in commercial tamper sensing mesh implementations?

RQ2: What are criteria and approaches for the design of secure tamper sensing meshes?

RQ3: Can we achieve physical security without a bespoke tamper-sensing mesh?

RQ4: Can we improve tamper-sensing meshes monitoring performance?

RQ5: Can we improve the ripple voltage performance of Wireless Power Transfer to power IHSMs?

RQ6: What applications do IHSMs open up through increased power dissipation and size?



Publications



Inertial Hardware Security Modules



Hardware Security Modules (HSMs)

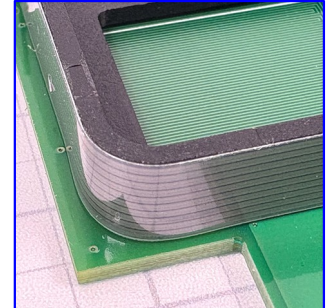
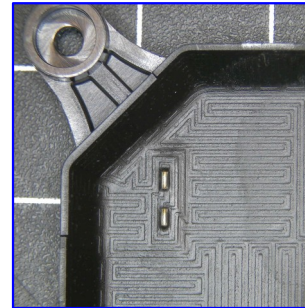
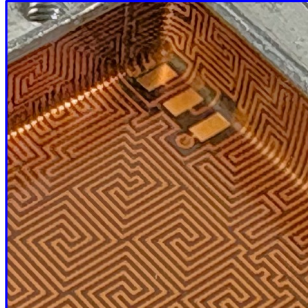
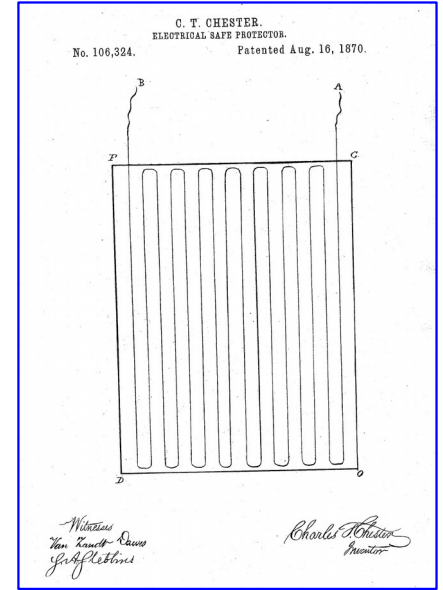
- Physically secured cryptographic coprocessor
- Surrounded by Tamper-Sensing "Mesh" detecting cutting
- Computational power limited because heat transfer through the mesh is difficult
- HSMs operate as peripheral to regular computers





Security Meshes

- Tamper-Sensing Meshes cover a surface with circuit traces to detect physical cuts
- Basic approach dates back to the 1800s
- Modern Meshes usually constructed as flexible printed circuits





Mechanical Motion Makes Meshes Mightier

- Mesh security proportional to difficulty of manipulation
- A steady hand with a scalpel under a microscope can accomplish amazing feats (cheaply!)

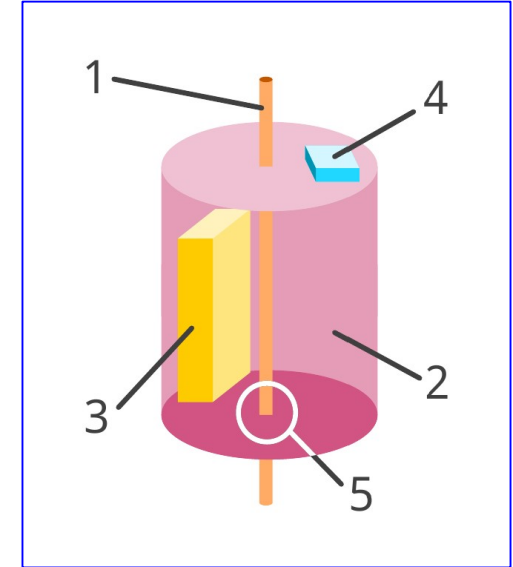
The core idea in *Inertial* HSMs:
Move the mesh!

Moving the mesh makes it much harder to manipulate



IHSM Construction

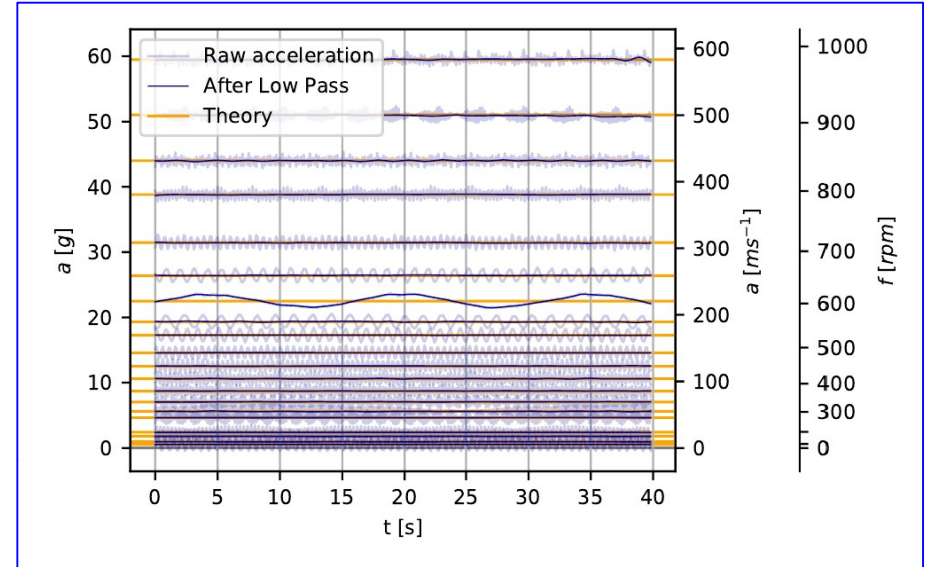
- Place the payload to be protected inside a *rotating* cage covered in a tamper-sensing mesh
- The mesh can have holes!
- The payload does not need to rotate, only the mesh
- Place an accelerometer on the mesh to ensure it is rotating
- Link mesh and payload using a cryptographically secured heartbeat protocol





Braking Detection

- An accelerometer is used to detect attackers trying to slow down the mesh
- At 1000 rpm, an accelerometer at $r=100\text{mm}$ measures 100g
- Thus, the system is insensitive to environmental noise such as shocks, vibration, and earthquakes
- Speed can be varied over time to detect failure of the accelerometer





Attacks on IHSMs

- Side-channel attacks are mitigated through physical distance between payload and mesh
- At IHSM speeds, the mesh cannot be manipulated by a human
- A robotic manipulator attacking an IHSM mesh is conceivable, but presents a formidable engineering challenge
- The IHSM shaft must be protected to prevent insertion of probes at its entry points into the mesh
- Fast and violent attacks should be considered during mechanical design to ensure secure failure modes

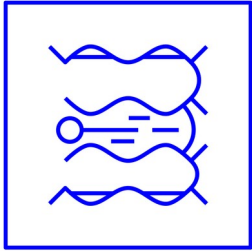


Related Work



A Summary of the IHSM Design Approach

- We showed how mechanical motion allows standard PCBs to be used as tamper-sensing meshes
- The approach is unaffected by environmental factors such as vibration and shocks
- IHSMs scale to larger volumes compared to conventional HSMs
- IHSMs permit airflow to pass through the mesh, enabling larger power dissipation in computationally intensive applications



Security Mesh Monitoring using Low-Cost Time Domain Reflectometry



Security Mesh Sensing Approaches

- Widespread approach: basic binary continuity sensing detects breaks
- Sometimes augmented with pulsing patterns to detect short circuits
- One commercial implementation measures voltage deviations using a bridge circuit
- Academic approaches use capacitive sensing and (cite TODO), frequency response among others

To our knowledge, no commercial approach exceeds
~16 bit of entropy total, and no academic approach
has found industry adoption



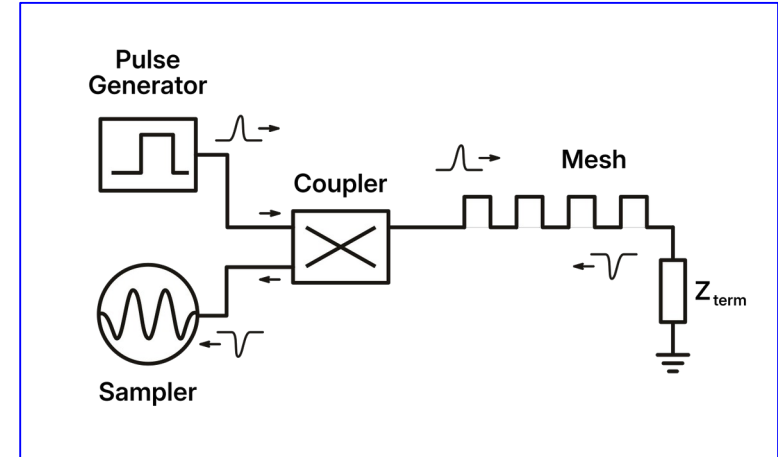
Better Sensing With Time Domain Reflectometry (TDR)

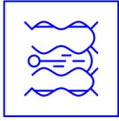
- TDR measures reflections of a *fast* electrical impulse traversing a conductor at speed of light
- TDR on a Mesh provides a *fingerprint* with multiple kilobits of entropy
- Sensing of reflections at any impedance discontinuity, not just breaks or short circuits
- Faults locatable in space by calculating distance from speed of light
- **Critical challenge:** Rise time determines spatial resolution



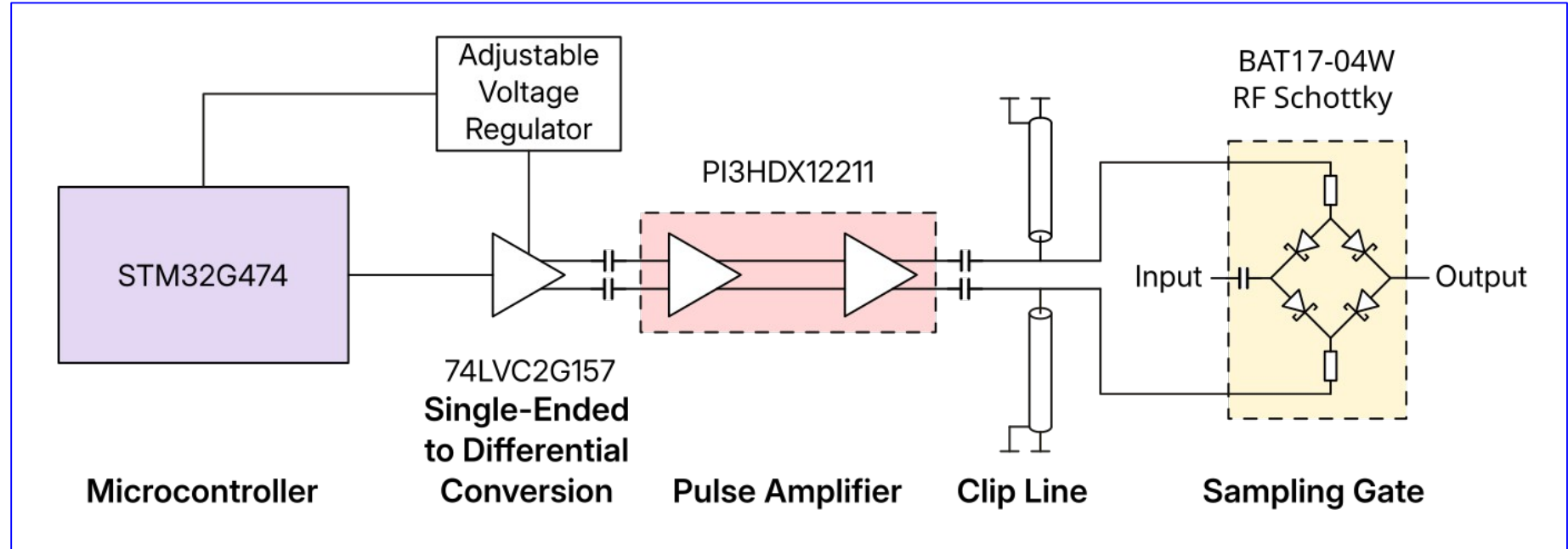
TDR Principle

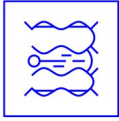
- Send a fast pulse through a coupler into the channel
- Wait for the pulse to be reflected at a discontinuity in the channel
- Couple the reflection into a sampler
- Sample the reflection at a precise point in time
- Usually done sampling because the pulse generator is already halfway to a sampling gate





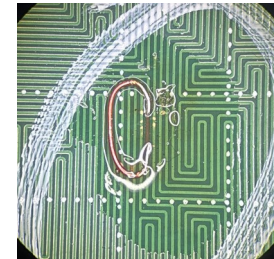
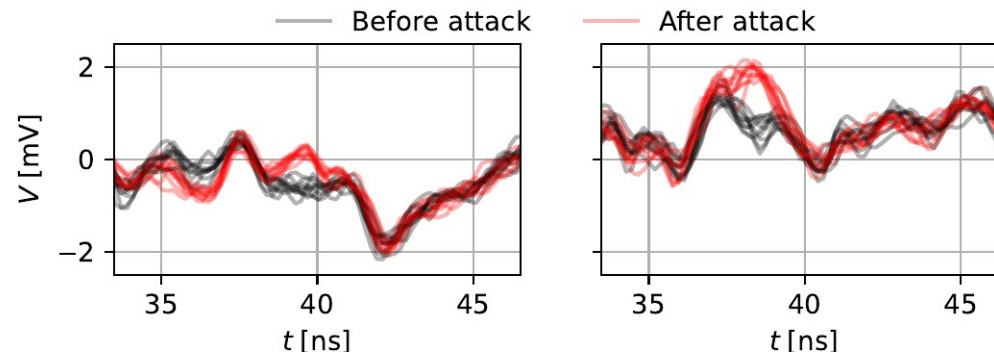
Generating Picosecond Edges

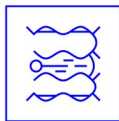




TDR Trace of a Mesh

The pictured attack causes a difference at a specific point in time along the TDR trace





Automated Analysis Using Pearson Correlation

Pearson Correlation can be used as a simple similarity measure for TDR time vectors

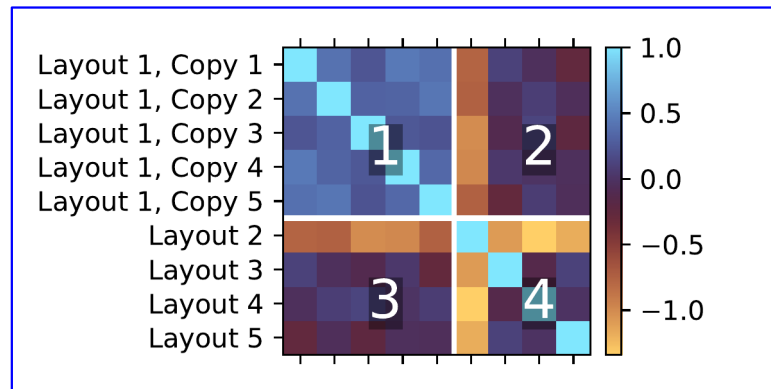
$$\rho_{X,Y} = \frac{\text{cov}(X, Y)}{\sigma_X \sigma_Y}$$

$$r_{X,Y} = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}}$$



Can TDR Distinguish Mesh Patterns?

- Correlation plot shows four zones
- Control experiments on (1)
- Experiment group on (2)
- (2) and (3) show error probability
- FNR 18% @ 0.1% FPR → Yes!





Analysis Results for Simple Attacks

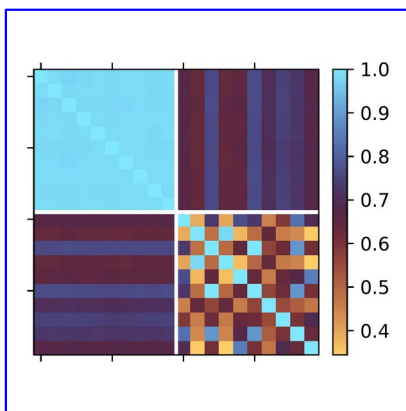
No false negatives in all cases!

One Trace Interrupted

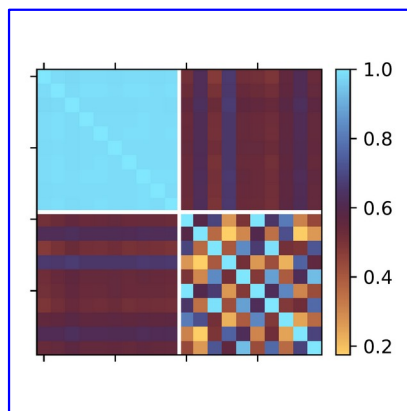
Traces Shorted

One Trace Interrupted

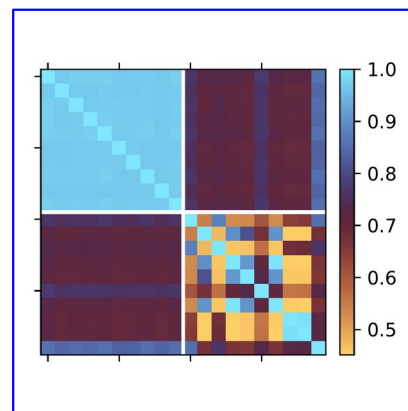
Traces Shorted



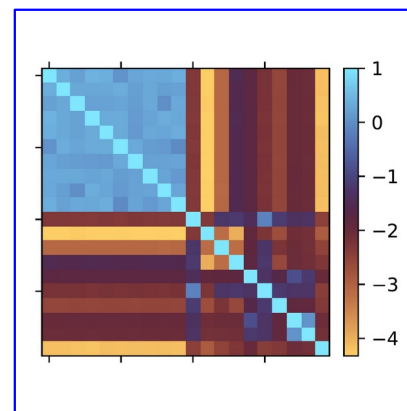
0.3mm pitch mesh



0.3mm pitch mesh



0.4mm pitch mesh

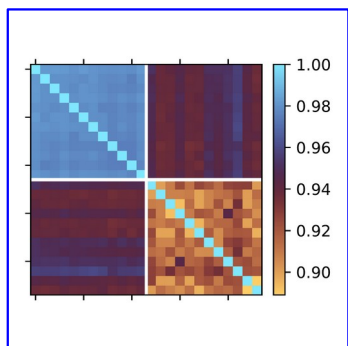


0.4mm pitch mesh



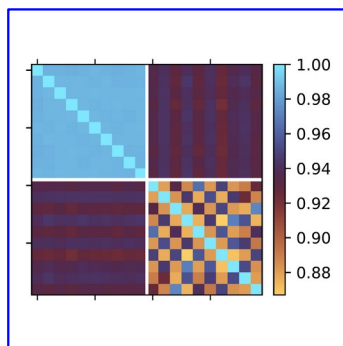
Analysis Results for Advanced Attacks

Oscilloscope Probe



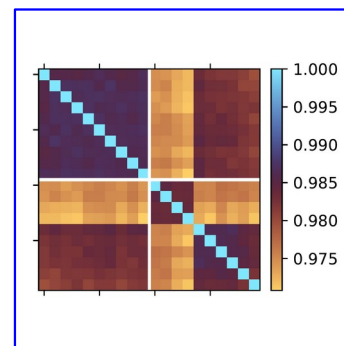
FNR 0.0%

Soldering Iron



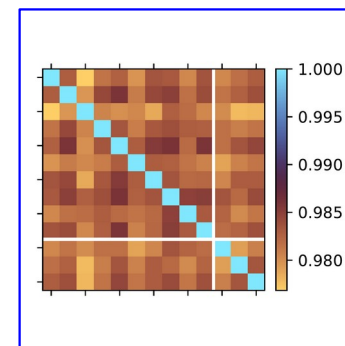
FNR 0.0%

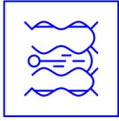
30mm wire



FNR 9.6%

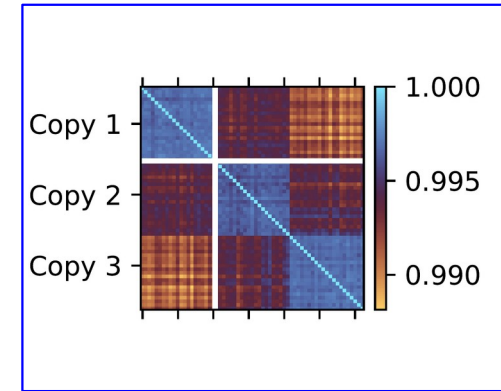
(baseline)





Oops, We Have Made a PUF!

- It turns out the circuit can distinguish identical copies of the same mesh from manufacturing tolerances
- This is called a PUF, a Physically Unclonable Function
- PUFs have applications in cryptography and supply-chain security
- Future work!



FNR 1.7%



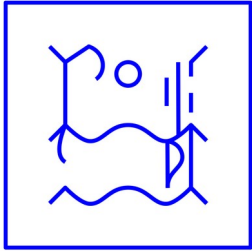
Related Work

- To Do



A Summary of TDR-Based Mesh Monitoring

- We showed a simple, inexpensive circuit can perform Time Domain Reflectometry with better than 200 ps resolution
- We showed how a tamper-sensing mesh can be monitored using TDR
- We experimentally demonstrated our approach detects several types of attacks
- We show our approach additionally exhibits PUF-like behavior and is capable of distinguishing identical copies of the same mesh



Results



Research Questions

RQ1: What is the state of the art in commercial tamper sensing mesh implementations?

RQ2: What are criteria and approaches for the design of secure tamper sensing meshes?

RQ3: Can we achieve physical security without a bespoke tamper-sensing mesh?

RQ4: Can we improve tamper-sensing meshes monitoring performance?

RQ5: Can we improve the ripple voltage performance of Wireless Power Transfer to power IHSMs?

RQ6: What applications do IHSMs open up through increased power dissipation and size?



Research Results

We surveyed a large selection of real-world tamper-sensing meshes

We designed a layout algorithm and a set of design rules for tamper-sensing meshes

We developed the IHSM approach for tamper-sensing using moving meshes

We designed a low-cost, high-fidelity TDR mesh monitoring system

We designed a planar inductor geometry with improved rotational symmetry

We explored two IHSM use cases in case studies, adapting the approach



Use Cases & Future Work

- Quantum Key Distribution requires physically secure, remote *relay* nodes handling cleartext key material
 - These can be secured using IHSMs
- Secure Multiparty Computation suffers from extreme network communication / performance tradeoffs
 - IHSMs allow co-locating nodes with short, fast, local network links without node operators trusting one another
- Jan has received two small grants funding one year of work implementing this research in a turnkey, open-source product



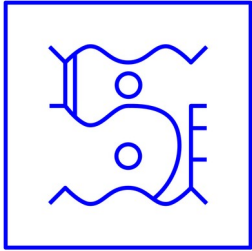
Interested?

research@jaseg.de

yasec

 ashen

Thank you!



Questions & Answers



Bonus Slides



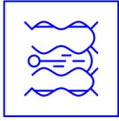
Multiparty Computation vs. Secure Hardware



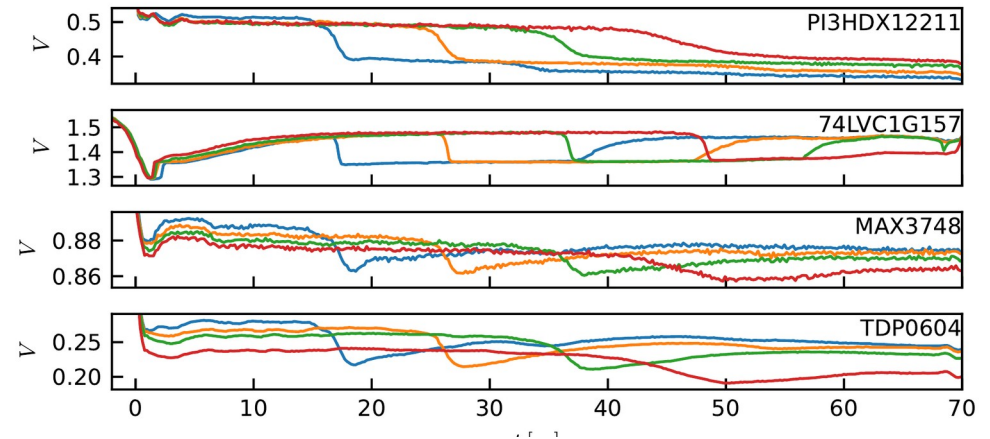
Environmental Factors in TDR Mesh Monitoring

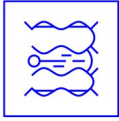


More Mesh Photos

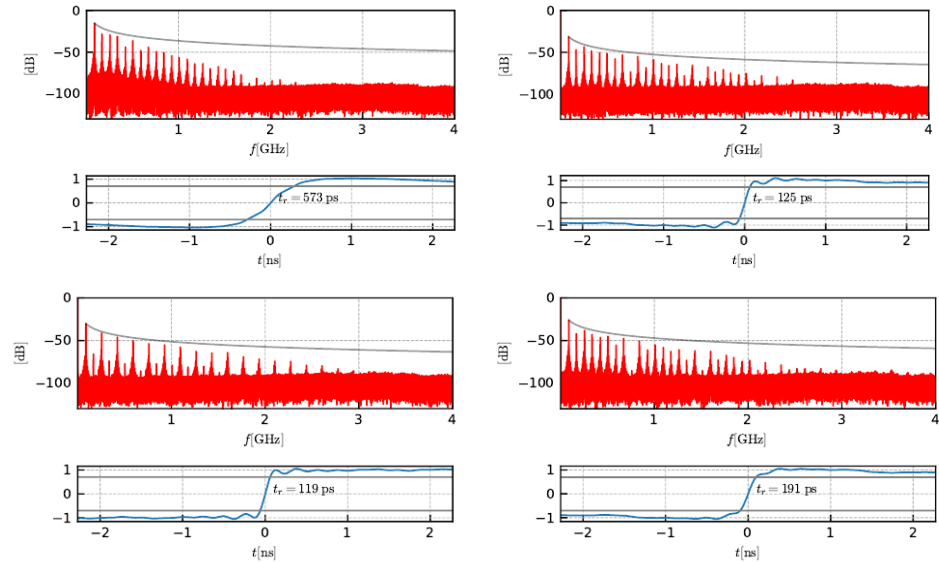


Speed of Light in a Typical TDR Response





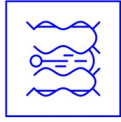
TDR Rise Time Results





IHSM Data & Power Transfer

- The rotating mesh needs a continuous power supply and a communication link to the payload
- Batteries unnecessarily limit lifetime
- Mechanical slip rings are unsuitable for IHSM speeds
- Standard Wireless Power Transfer (WPT) can be applied
- Data can be transmitted e.g. optically or through an electrostatic slip ring



Signal Routing and Modes of Sensing