Can’t touch this

Inertial HSMs Thwart Advanced Physical Attacks

Jan Sebastian Götte <ihsm.m@jaseg.de>

Björn Scheuermann <scheuermann@kom.tu-darmstadt.de>

emergenCITY

Technische Universität Darmstadt

Alexander von Humboldt Institut für Internet und Gesellschaft

Philipps Universität Marburg

Universität Kassel

LOEWE – Exzellente Forschung für Hessens Zukunft

What is a Hardware Security Module?

A HSM is a computer that constantly monitors itself for attempts at physical attacks, and destroys its stored data when tampered.

- In contrast to a TPM or Smartcard, an HSM is **powered at all times** and will destroy its contents when power is lost.
- Usually, HSMs use **tamper-sensing membranes** that are much harder to bypass than simple lid switches.
- HSMs protect macroscopic circuits, where in a smartcard only the chip itself is protected
- HSMs often contain **multiple tamper sensors** (e.g. membrane, temperature sensors, light sensors, and contacts/switches)

Why would you want an HSM?

HSMs allow us to do things now that we cannot yet practically do using cryptographic techniques such as SMPC.

- Traditional HSMs usually offer proprietary APIs (e.g. for key generation / signing). This and their low speed limit their applications.
- Instead, custom software, or even custom hardware inside the HSM payload allows for exciting new applications!
- Example: Offloading entire applications into the HSM instead of only cryptographic parts

The History of Hardware Security Modules

1940ies: First ideas on HSMs

1950ies ~ 1970ies: Ciphering machines built into safes

1980ies ~ 1990ies: modern HSM tech in ATMs

1990ies ~ 2000s: modern HSM tech in payment processing terminals & payment processing datacenter applications

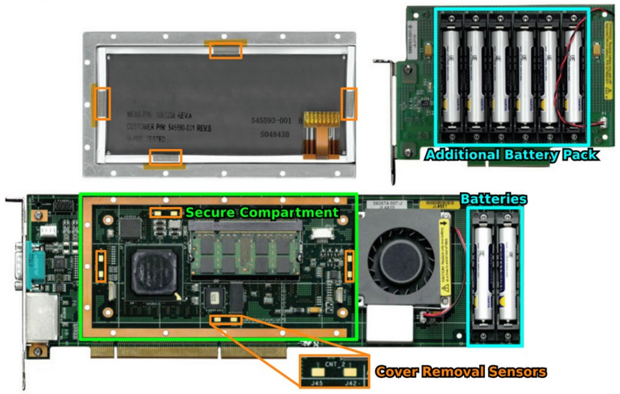
today: IHSM tech @ your lab?

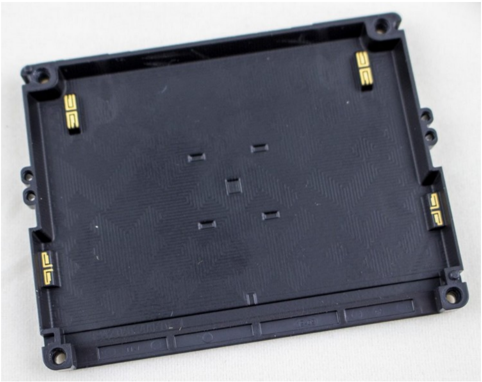
The History of Hardware Security Modules

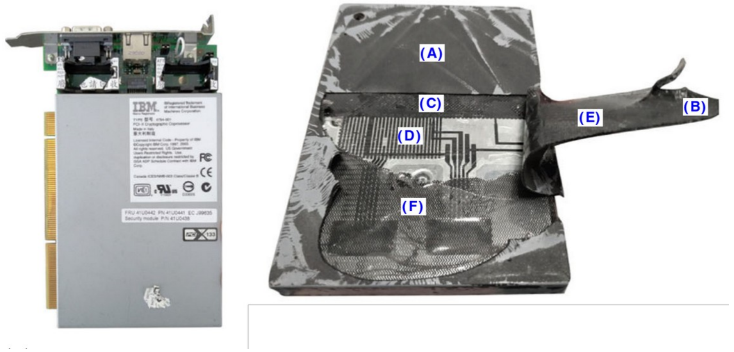
https://www.cryptomuseum.com/crypto/usa/ky9/index.htm

Hardware Security Modules: The State of the Art

Industrial designs exclusively use tamper-sensing membranes







middle: Colin O’Flynn 2020, Square Terminal Teardown (blog post): https://colinoflynn.com/2020/04/square-terminal-teardown/

left/right: Obermaier and Immler 2018, The Past, Present, and Future of Physical Security Enclosures. From Battery-Backed Monitoring to PUF-Based Inherent Security and Beyond. Journal of Hardware and Systems Security. https://doi.org/10.1007/s41635-018-0045-2

Hardware Security Modules: The State of the Art

Academic designs go beyond simple meshes, but do not cover the manufacturability / sensitivity sweet spot yet

easy to replicate / insensitive ⟷ **hard to replicate / sensitive**

Tobisch et al. (TRUDEVICE'20):
Use RF measurements as PUF

- Easy to manufacture / reproduce
- No sensitivity guarantees (relies on intractable RF cavity response)

This work

Immler et al. (CHES'19):
Use HSM mesh as capacitive PUF

- Very sensitive
- Hard to manufacture / reproduce

Commercially available HSMs

The state of the art in HSMs is an example of technological stagnation due to lack of competition.

- Low processing speed (smartphone-class ARM SoC)
- No bare-metal access, only proprietary API
- NDA requirements impede research & vulnerability disclosure
- High cost

If you can't buy it, make your own!

The difficult part about DIY'ing a HSM is the security barrier.

- To prevent attacks by probing and bridging, very fine features are needed
- To prevent disassembly, parts must be **engineered to be fragile**
- PCBs do not work, because PCBs are engineered to be robust (the exact opposite of what we need).

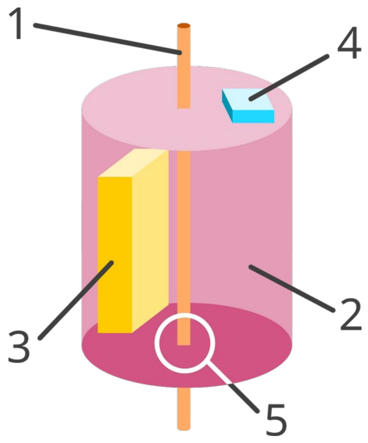
The Inertial Hardware Security Module

Core observation: You can’t tamper what you can’t touch

- To create a secure tamper barrier from commodity PCBs, we first create an insecure barrier that is vulnerable to probing, bridging and disassembly, which we then **spin it really fast**.

- We can tell if someone stops our spinning tamper sensing mesh by placing an accelerometer on it.

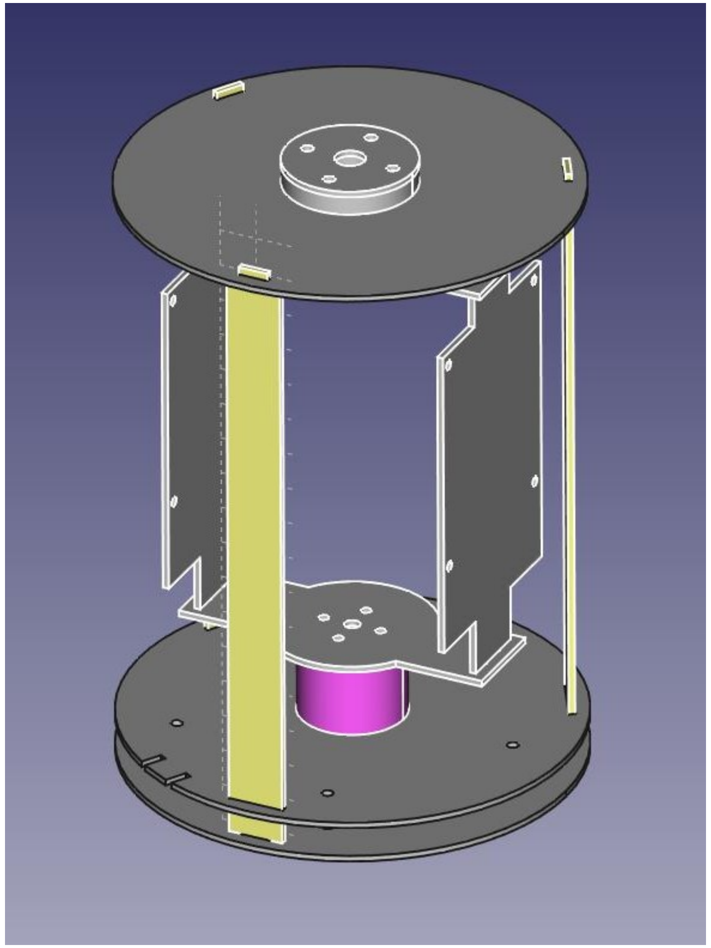
- Longevity / power consumption are unproblematic; see PC case fans or HDDs



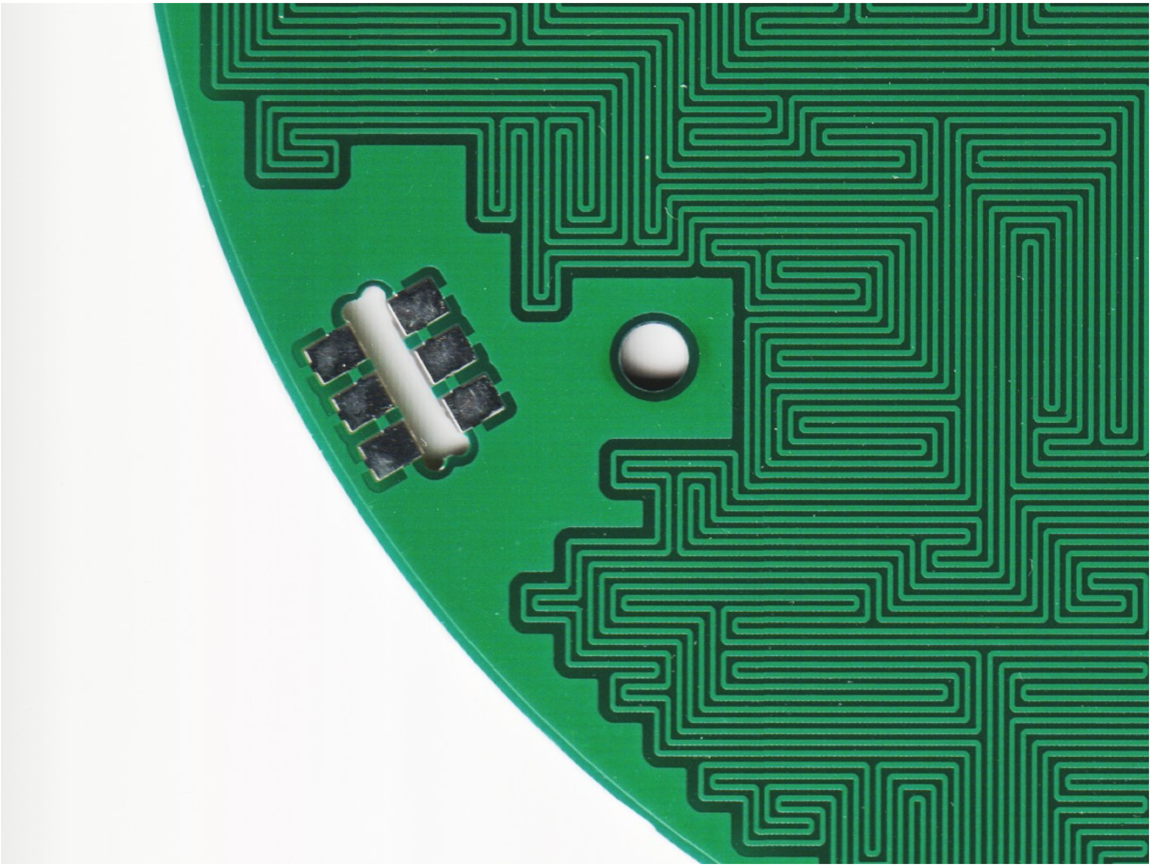
The Inertial Hardware Security Module

Key components of an Inertial HSM

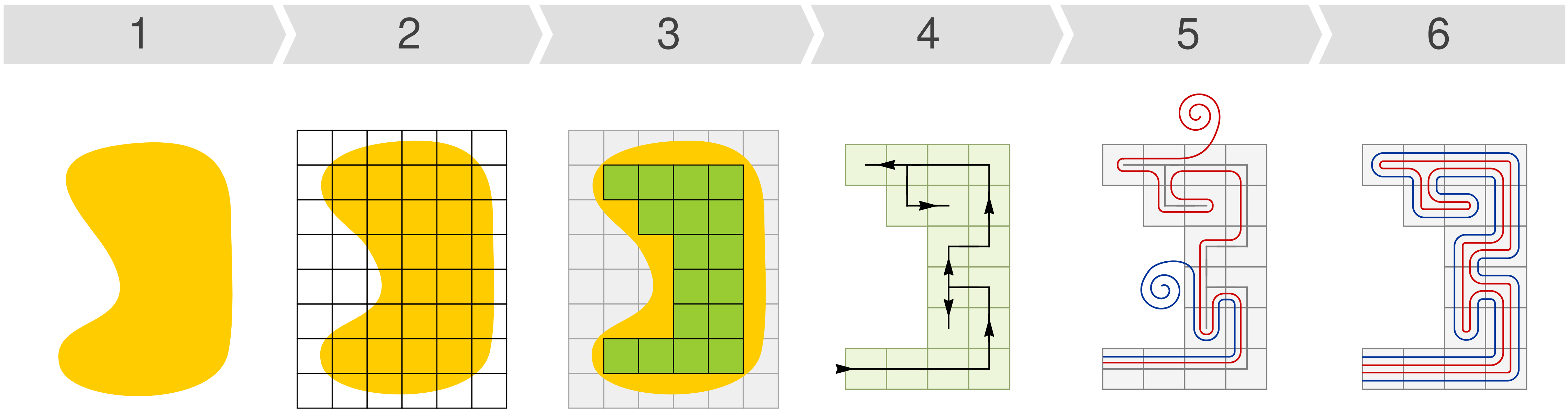
- Low-tech security mesh
- Accelerometer
- Rotating data + power coupling
- Motion subsystem (motor + digitally controlled driver)



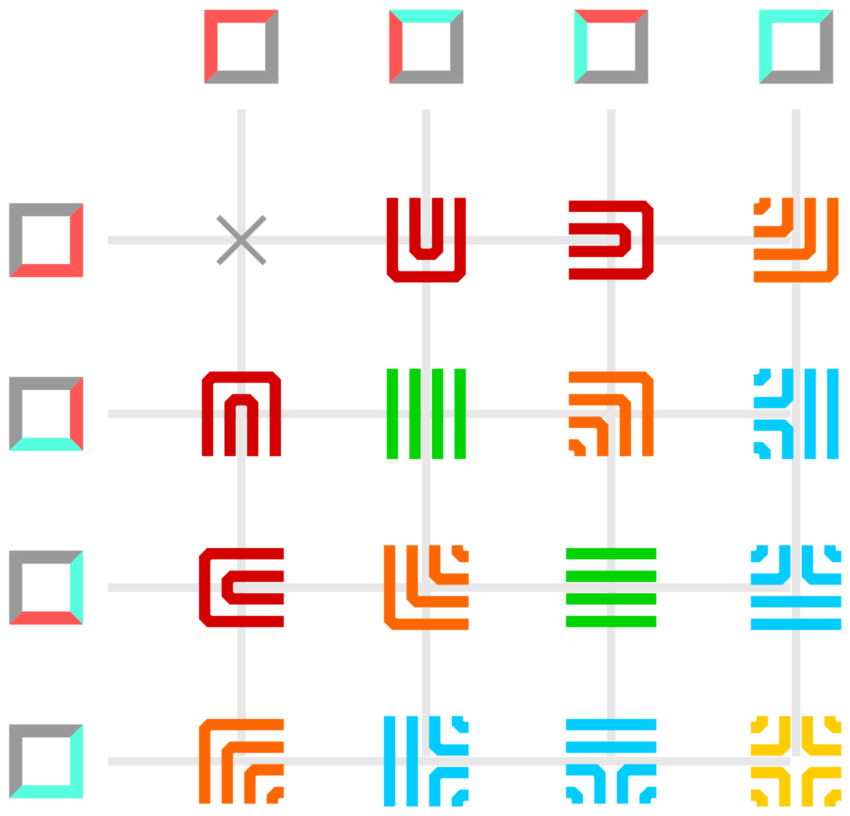
Open-source Mesh Generation Workflow using Kicad



Open-source Mesh Generation Workflow using Kicad

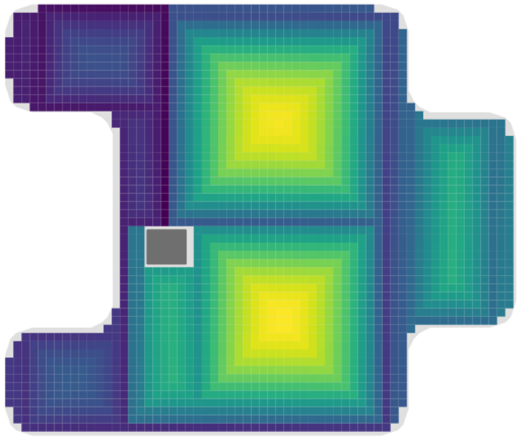


Open-source Mesh Generation Workflow using Kicad

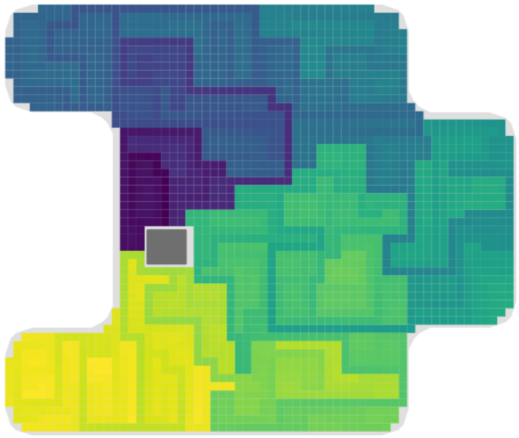


Open-source Mesh Generation Workflow using Kicad

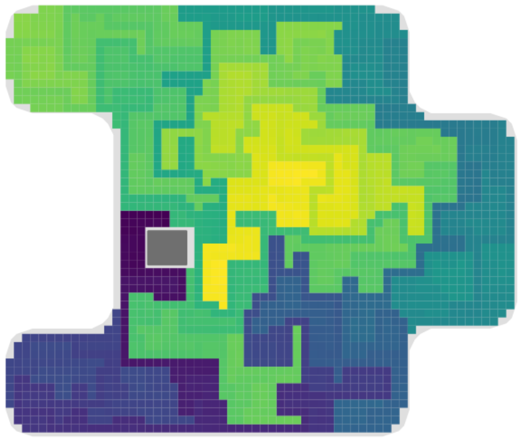
0%



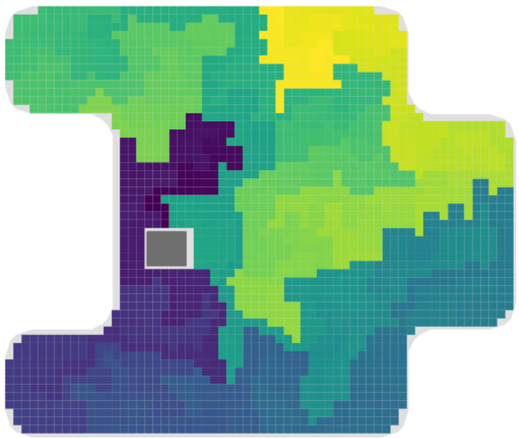
25%



50%

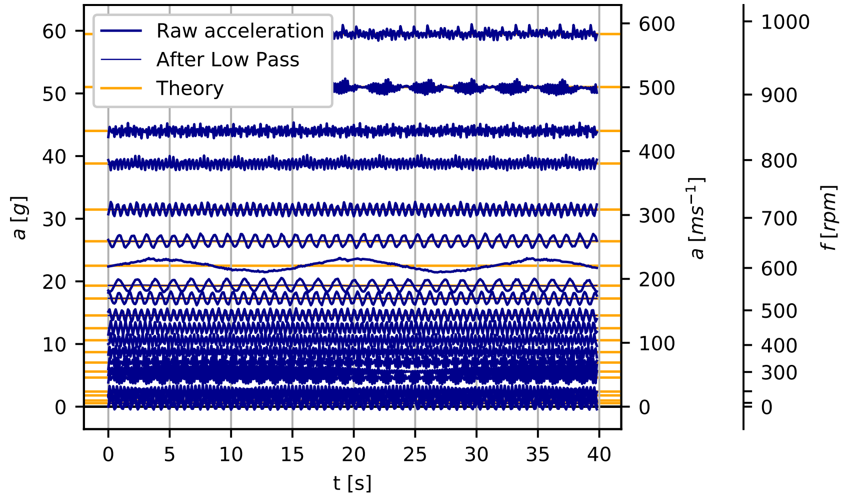


100%



Accelerometer accuracy

- Off-the-shelf automotive accelerometer has ample precision
- External influences (shock, vibration, earthquakes, ...) are smaller by orders of magnitude
- All accelerometers produce relative measurements and drift, so periodic re-calibration through speed changes is necessary



Power and Data Transfer

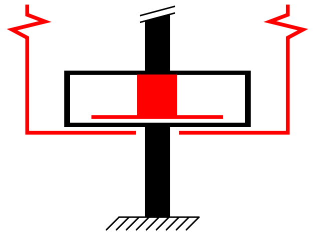
Optical data/power is easy to build, performs well

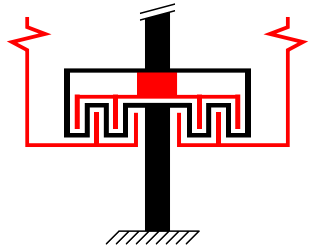
Optical	Magnetic	Mechanical
Photodiode / Solar cell	Modified motor	Slip ring
+ Off-the-shelf components	+ Compact	+ Off-the-shelf components
+ Simple implementation	+ Simple implementation	+ Simple implementation
- Only low power transfer	+ High power capability	- Low maximum speed
- Mechanically complex	- Specialized component	- Expensive

Additional defenses

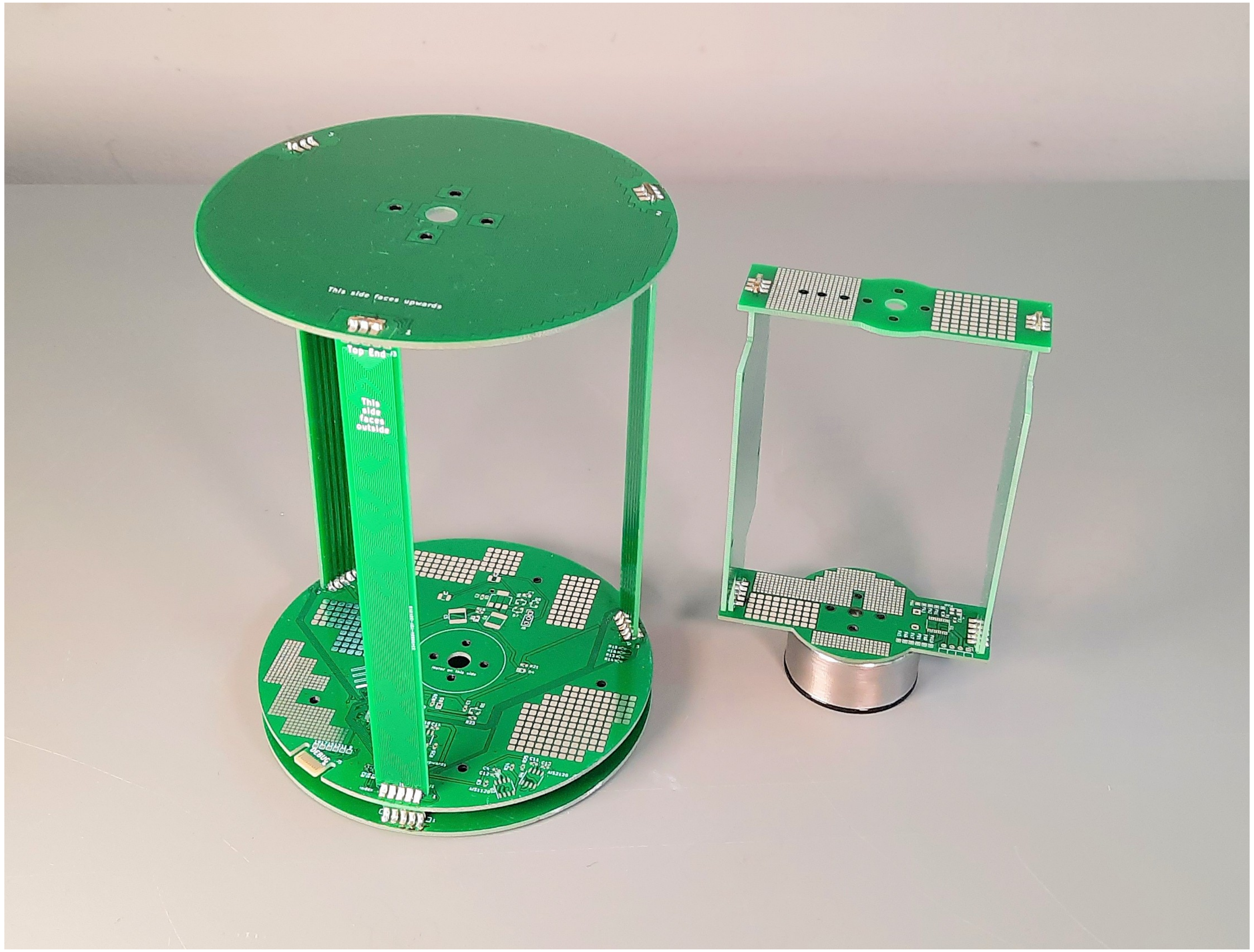
Our prototype has a weak point where the shaft goes through the mesh

- Defense at rotation axis through nested meshes / precession
- Defense against non-contact attacks through mechanical and EM shielding
- Internal power filtering for conducted-mode EM
- Additional tamper sensing through motor current monitoring, light/radiation/temperature sensors, vibration monitoring

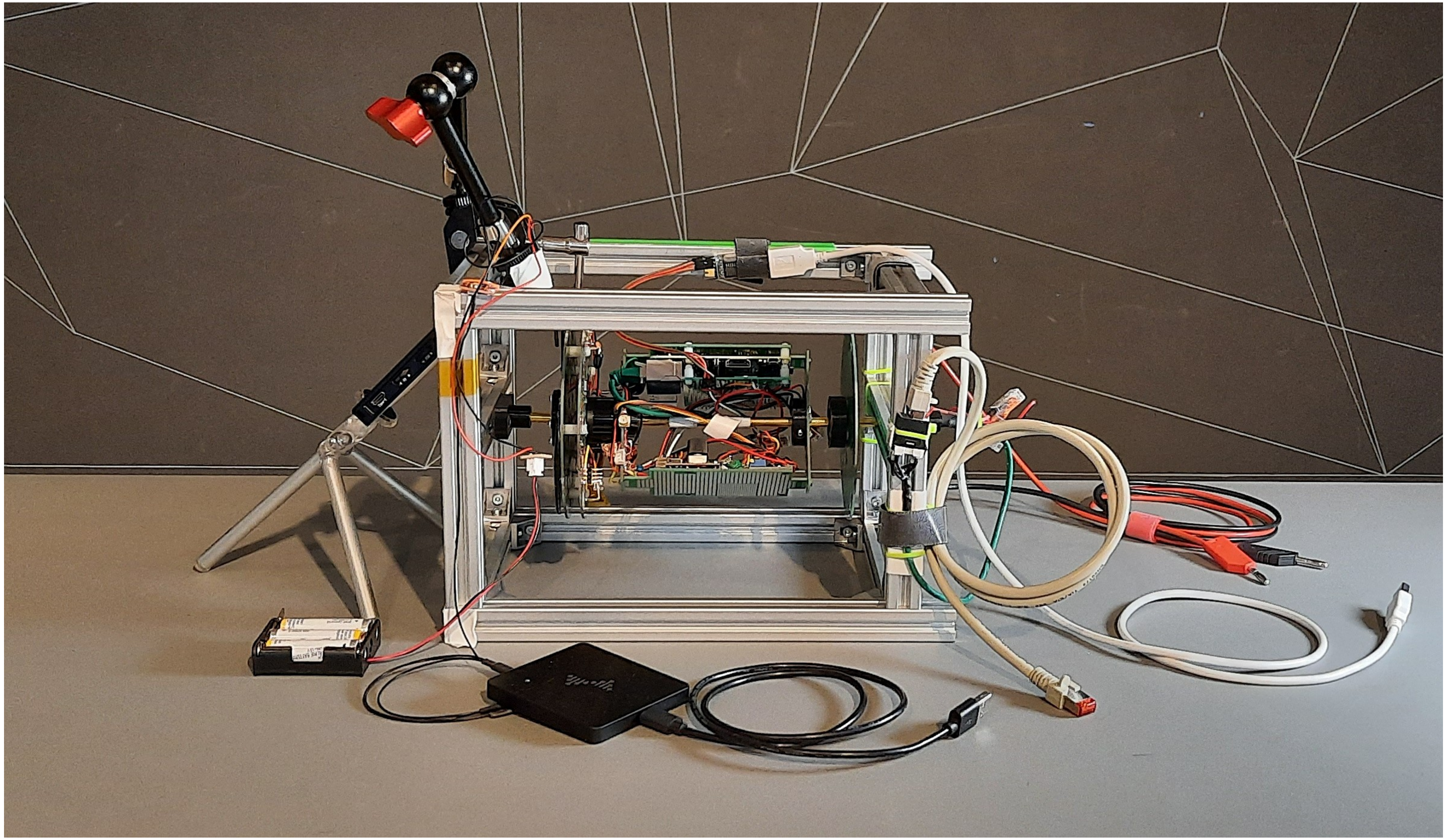




Prototype #1



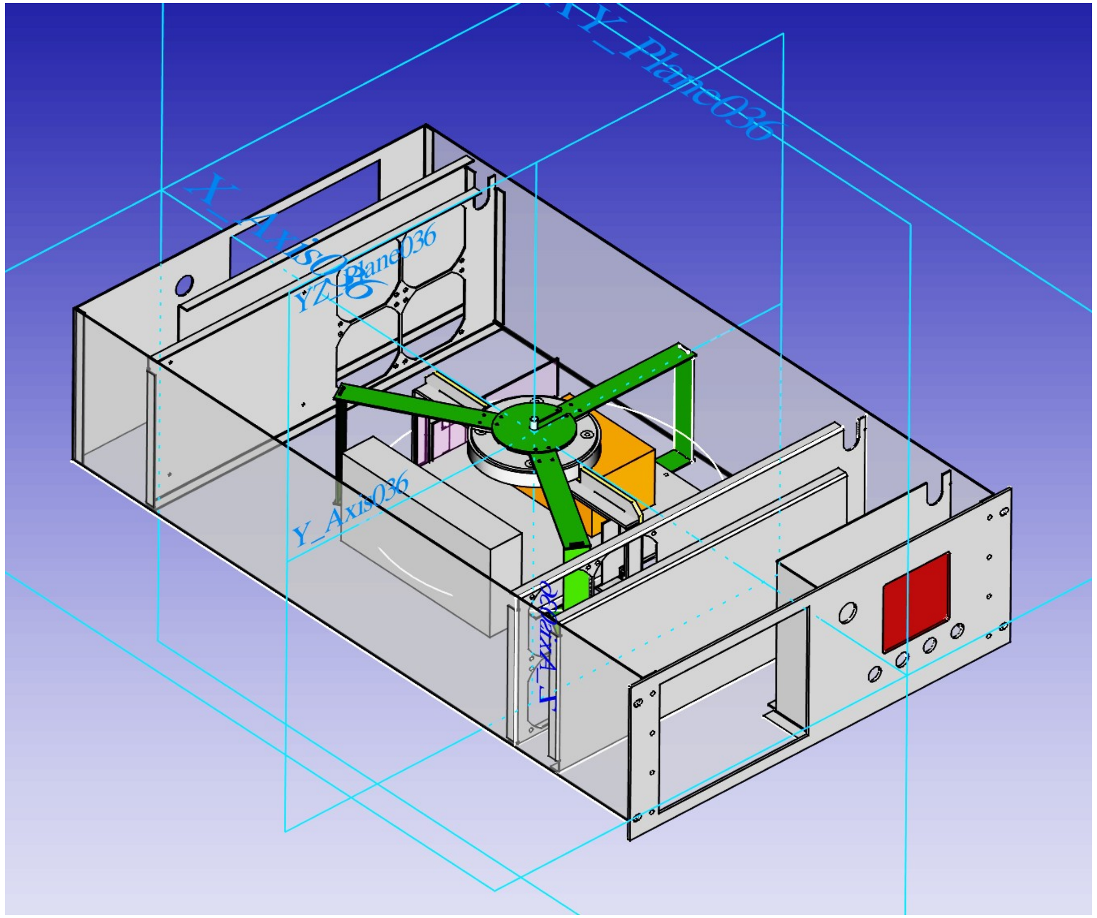
Prototype #1

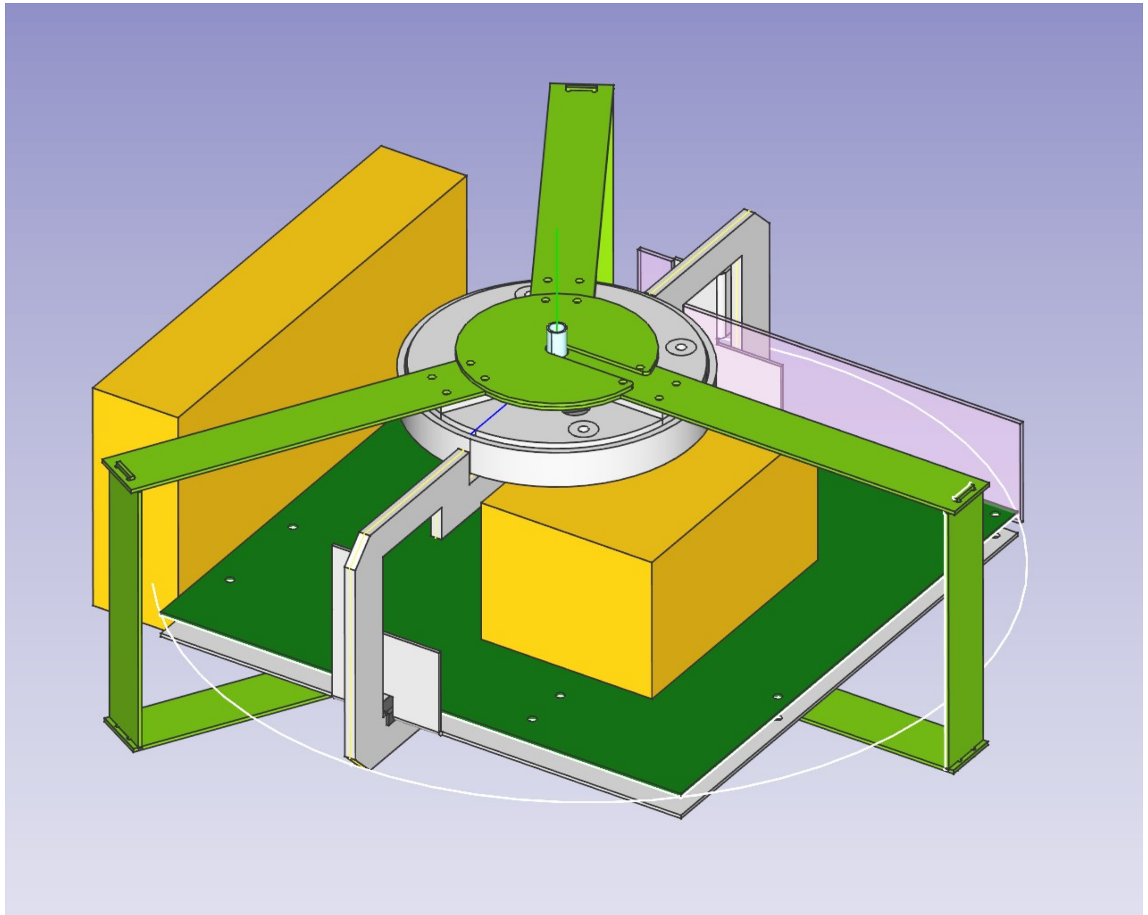


Future Work

Mission: Enable research, new applications by making IHSMs open-source accessible to anyone with a basic mechanical / electronics workshop.

Rackmount high-power IHSM prototype





Resources

Our design: hw (Kicad, FreeCAD), firmware (C), Paper (LaTeX):

`https://git.jaseg.de/ihsm.git`

Recommended reading:

David G. Boak. *A History of U.S. Communications Security, Volumes I and II*. Lecture Notes. 1973

Ross Anderson. *Security Engineering*. Sept. 16, 2020. ISBN: 978-1-119-64281-7

Saar Drimer, Steven J Murdoch, and Ross Anderson. “*Thinking inside the box: System-level failures of tamper proofing*”. In: 2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE. 2008, pp. 281–295

Vincent Immler et al. “*Secure Physical Enclosures from Covers with Tamper-Resistance*”. In: IACR Transactions on Cryptographic Hardware and Embedded Systems (2019). issn: 2569-2925. doi: 10.13154/tches.v2019.i1.51-96.

Johannes Tobisch, Christian Zenger, and Christof Paar. “*Electromagnetic Enclosure PUF for Tamper Proofing Commodity Hardware and other Applications*”. In: TRUDEVICE 2020: 9th Workshop on Trustworthy Manufacturing and Utilization of Secure Devices

emergenCITY

About us

The LOEWE center emergenCITY, established in **2020**, combines the extensive research in Hesse on resilient and crisis-proof infrastructures in digital cities.

emergenCITY is an interdisciplinary and multi-site collaboration led by **Technische Universität Darmstadt, Universität Kassel, and Philipps-Universität Marburg**. Twenty-six professors from the fields of computer science, electrical engineering and information technology, mechanical engineering, social sciences and history, architecture, economics, and law conduct research in four interlinked program areas: City and Society, Information, Communication, and Cyber-Physical Systems.

Also, the **Federal Office of Civil Protection and Disaster Assistance (BBK), the City of Darmstadt, the German Aerospace Center (DLR)**, and more than 40 other partners from industry and science are involved in the center.

Contact

Prof. Dr. Matthias Hollick
Scientific Coordinator

Anne Hofmeister
Manager

www.emergencity.de
manager@emergencity.de

Hochschulstraße 1
64289 Darmstadt

+49 6151 16-25482

TECHNISCHE UNIVERSITÄT DARMSTADT

Philipps Universität Marburg

UNIKASSEL VERSITÄT

LOEWE
Exzellente Forschung für Hessens Zukunft

Über uns

Das in **2020** etablierte LOEWE-Zentrum emergenCITY bündelt die langjährige hessische Forschung zu resilienten und krisenfesten Infrastrukturen in digitalen Städten.

emergenCITY ist als interdisziplinäre und standortübergreifende Kooperation organisiert, an der die Universitätspartner **Technische Universität Darmstadt, Universität Kassel und Philipps-Universität Marburg** beteiligt sind. 26 Professorinnen und Professoren aus den Fachrichtungen Informatik, Elektrotechnik und Informationstechnik, Maschinenbau, Gesellschafts- und Geschichtswissenschaften, Architektur, Wirtschaftswissenschaften sowie Rechtswissenschaften forschen in vier miteinander verzahnten Programmbereichen: Stadt und Gesellschaft, Information, Kommunikation und cyberphysische Systeme.

Darüber hinaus sind das **Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), die Wissenschaftsstadt Darmstadt, das Deutsche Zentrum für Luft- und Raumfahrt (DLR)** sowie mehr als 40 weitere Partner aus Wirtschaft und Wissenschaft in das Zentrum eingebunden.

Kontakt

Prof. Dr. Matthias Hollick
Wissenschaftlicher Koordinator

Anne Hofmeister
Geschäftsführung

www.emergencity.de
manager@emergencity.de

Hochschulstraße 1
64289 Darmstadt

+49 6151 16-25482

TECHNISCHE UNIVERSITÄT DARMSTADT

Philipps Universität Marburg

UNIKASSEL VERSITÄT

LOEWE Exzellente Forschung für Hessens Zukunft