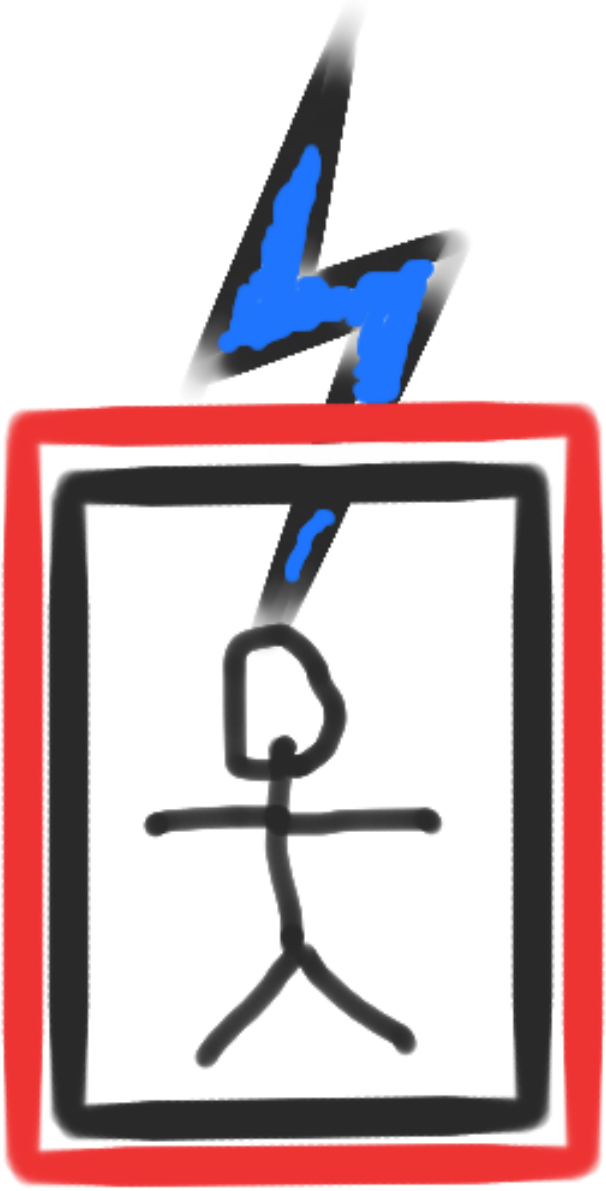
The inverse Faraday challenge

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven



Myth: Faraday cage
(grounded or ungrounded)
eliminates some types of leakage.

Myth: Faraday cage
(grounded or ungrounded)
eliminates some types of leakage.

Fact for each m:
All information inside Faraday
cage is visible m meters away.

Myth: Faraday cage
(grounded or ungrounded)
eliminates some types of leakage.

Fact for each m:
All information inside Faraday cage is visible m meters away.

Hard proof: Messy calculations using laws of electromagnetism.

Myth: Faraday cage
(grounded or ungrounded)
eliminates some types of leakage.

Fact for each m:
All information inside Faraday cage is visible m meters away.

Hard proof: Messy calculations using laws of electromagnetism.

Easy proof: This is a special case of the "holographic principle".

Typical EM attack:

Use sensors to extract EM data from chip. Compute secret key.

Typical EM attack:
Use sensors to extract EM data from chip. Compute secret key.

Countermeasure:
Put Faraday cage around chip.
Sensors fail.

Typical EM attack:
Use sensors to extract EM data from chip. Compute secret key.

Countermeasure:
Put Faraday cage around chip.
Sensors fail.

Challenge:
Surround Faraday cage with an **inverse Faraday cage** that rebuilds the original EM data.
Sensors work again.

Should be able to build

inverse Faraday cage from

- many EM sensors;
- the messy calculations;
- many EM generators.

Should be able to build
inverse Faraday cage from

- many EM sensors;
- the messy calculations;
- many EM generators.

Probably easier: Directly build
a many-sensor EM attack against
a chip inside a Faraday cage.

Should be able to build
inverse Faraday cage from

- many EM sensors;
- the messy calculations;
- many EM generators.

Probably easier: Directly build
a many-sensor EM attack against
a chip inside a Faraday cage.

Maybe harder, maybe impossible:
Build inverse Faraday cage as a
simple physical device.

Technical note added to slides after the talk: My understanding of the primary Faraday effect is that waves inside the Faraday cage are converted into movements of electrons on the cage, creating magnetic fields outside the cage, which EM sensors outside the cage should be able to see. For grounded Faraday cages it should also be helpful to tap the ground. Electromagnetic waves can also be converted into other forms of information, so using other types of sensors might also be helpful.