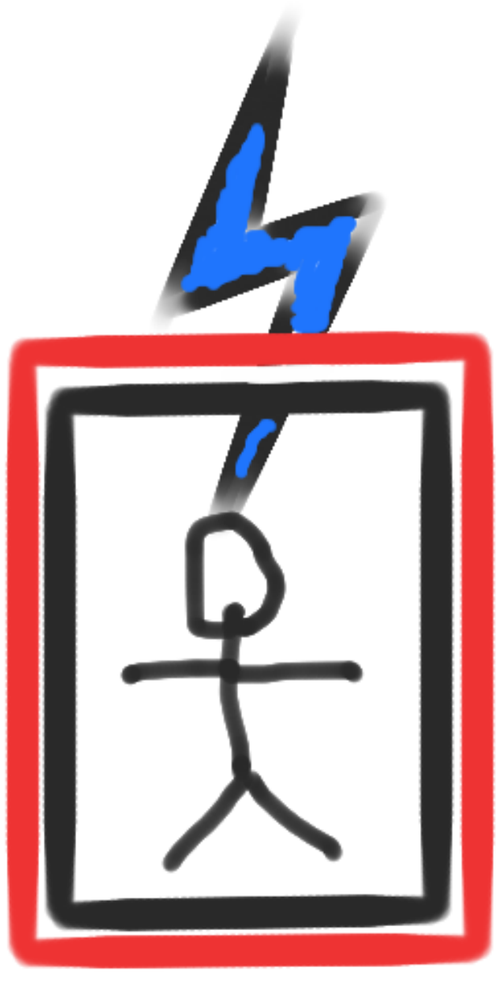
The inverse Faraday challenge

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

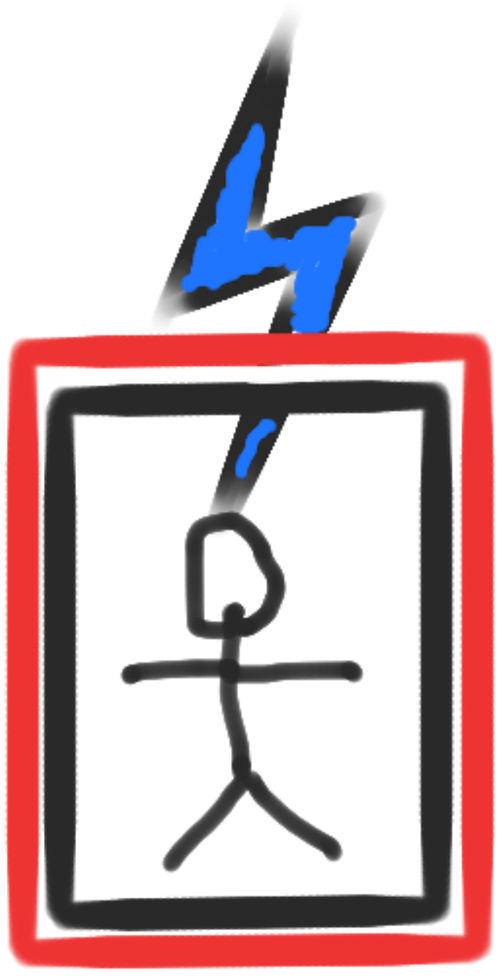


Myth: Faraday cage
(grounded or ungrounded)
eliminates some types of leakage.

The inverse Faraday challenge

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven



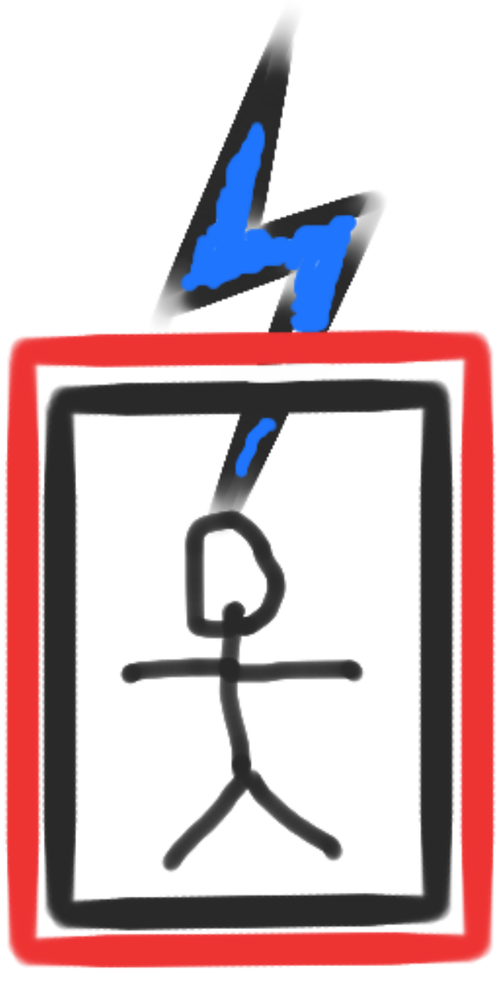
Myth: Faraday cage
(grounded or ungrounded)
eliminates some types of leakage.

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

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.

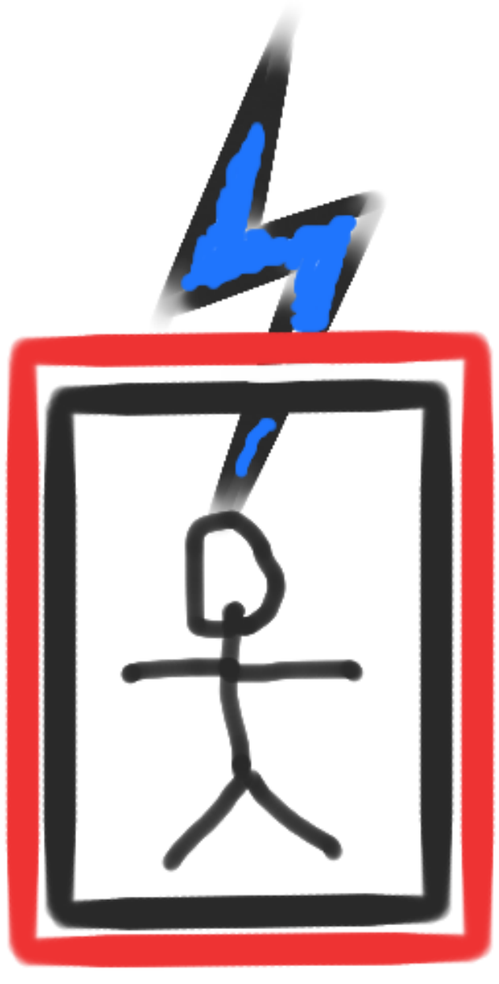
Fact for each m:
All information inside Faraday
cage is visible m meters away.

Hard proof: Messy calculations
using laws of electromagnetism.

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.

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

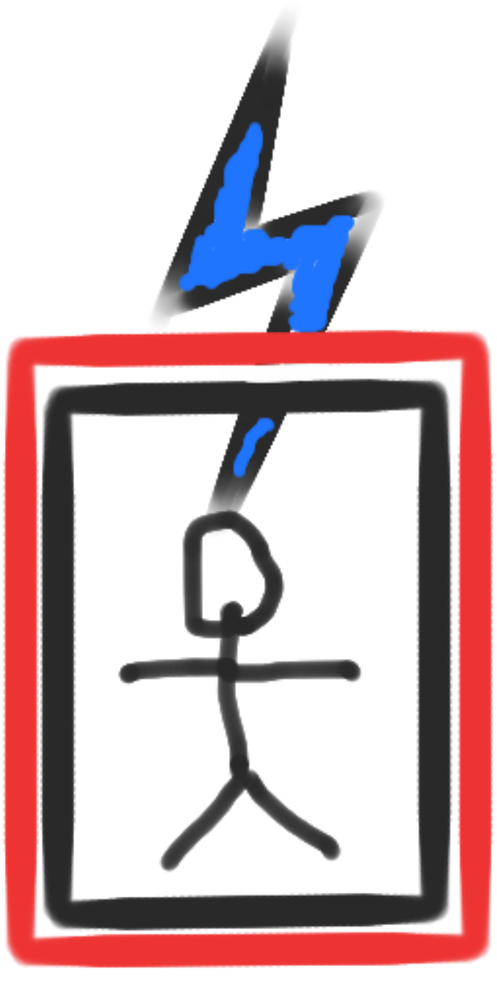
Hard proof: Messy calculations
using laws of electromagnetism.

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

erse Faraday challenge

. Bernstein

ty of Illinois at Chicago &
che Universiteit Eindhoven



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
Use sens
from chi

ay challenge

n

is at Chicago &

siteit Eindhoven

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 ext
from chip. Compu

ge

ago &
hoven

1

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".

2

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

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.

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.

Countermeasure:
Put Faraday cage around chip.
Sensors fail.

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.

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.

Faraday cage
ed or ungrounded)
es some types of leakage.

each m:
rmation inside Faraday
visible m meters away.

oof: Messy calculations
ws of electromagnetism.

oof: This is a special case
holographic principle".

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 b
inverse F
- many
- the me
- many

ge
ounded)
ypes of leakage.

nside Faraday
neters away.

y calculations
romagnetism.

s a special case
c principle".

2

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.

3

Should be able to
inverse Faraday ca
- many EM senso
- the messy calcul
- many EM genera

kage.

day

y.

ons

ism.

l case

e".

2

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.

3

Should be able to build inverse Faraday cage from

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

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.

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.

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

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.

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.

EM attack:

sors to extract EM data

p. Compute secret key.

measure:

aday cage around chip.

fail.

ge:

d Faraday cage with

rse Faraday cage that

the original EM data.

work again.

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
the talk:
primary Fa
inside the
into move
cage, crea
the cage,
cage shou
Faraday ca
tap the gr
can also b
of informa
sensors mi

k:

ract EM data

ute secret key.

around chip.

cage with

ay cage that

al EM data.

n.

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
the talk: My understa
primary Faraday effect
inside the Faraday cag
into movements of ele
cage, creating magnet
the cage, which EM s
cage should be able to
Faraday cages it shoul
tap the ground. Elect
can also be converted
of information, so usin
sensors might also be

lata
key.

ip.

nat
a.

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 afte
the talk: My understanding of the
primary Faraday effect is that wav
inside the Faraday cage are conver
into movements of electrons on th
cage, creating magnetic fields outs
the cage, which EM sensors outsid
cage should be able to see. For g
Faraday cages it should also be he
tap the ground. Electromagnetic w
can also be converted into other f
of information, so using other type
sensors might also be helpful.

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.