Understanding physics to break ESP32 AES encryption

... using custom hardware to perform side channel attacks

Roman Korkikian & Mathieu Stephan

Hello!

We are Roman Korkikian & Mathieu Stephan

embedded security pentester / embedded systems engineer

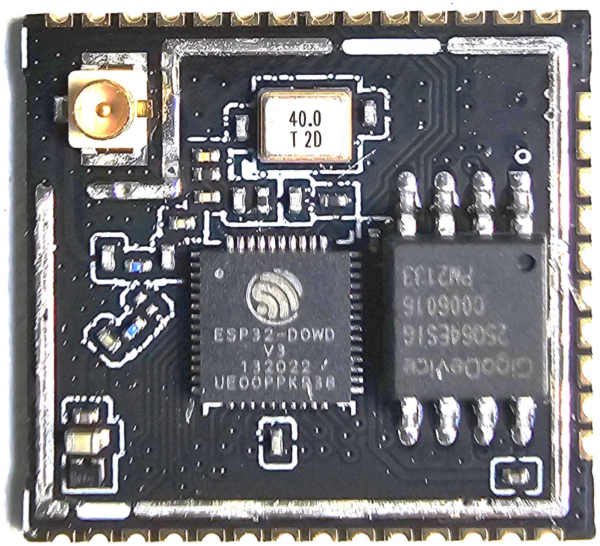
www.usec.ch / www.limpkin.fr

/ www.themooltipass.com

Presentation Outline

- Side channel attack setup presentation
- Study and measure the impacts of:
  - Wires
  - Decoupling capacitors
  - Probes
  - Noise
  - Power supply
- … to find the ideal testing setup
- … break the ESP32 AES engine
- … while designing 2 different devices

In this presentation…



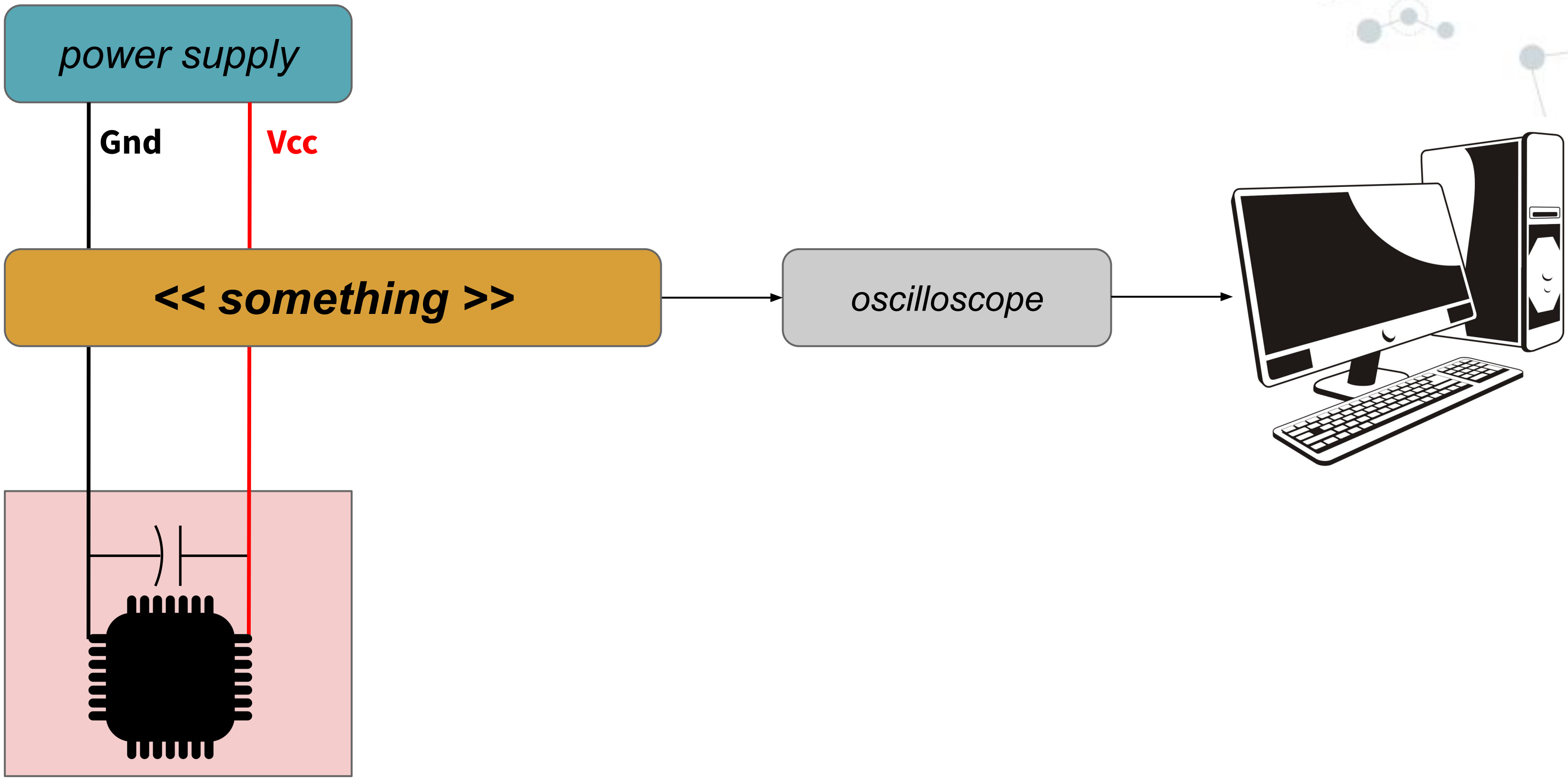
This presentation explores diverse power measurement scenarios for the ESP32 to perform correlation with the hardware AES engine

Side-channel attack on ESP32 hardware engine was previously presented: <link>

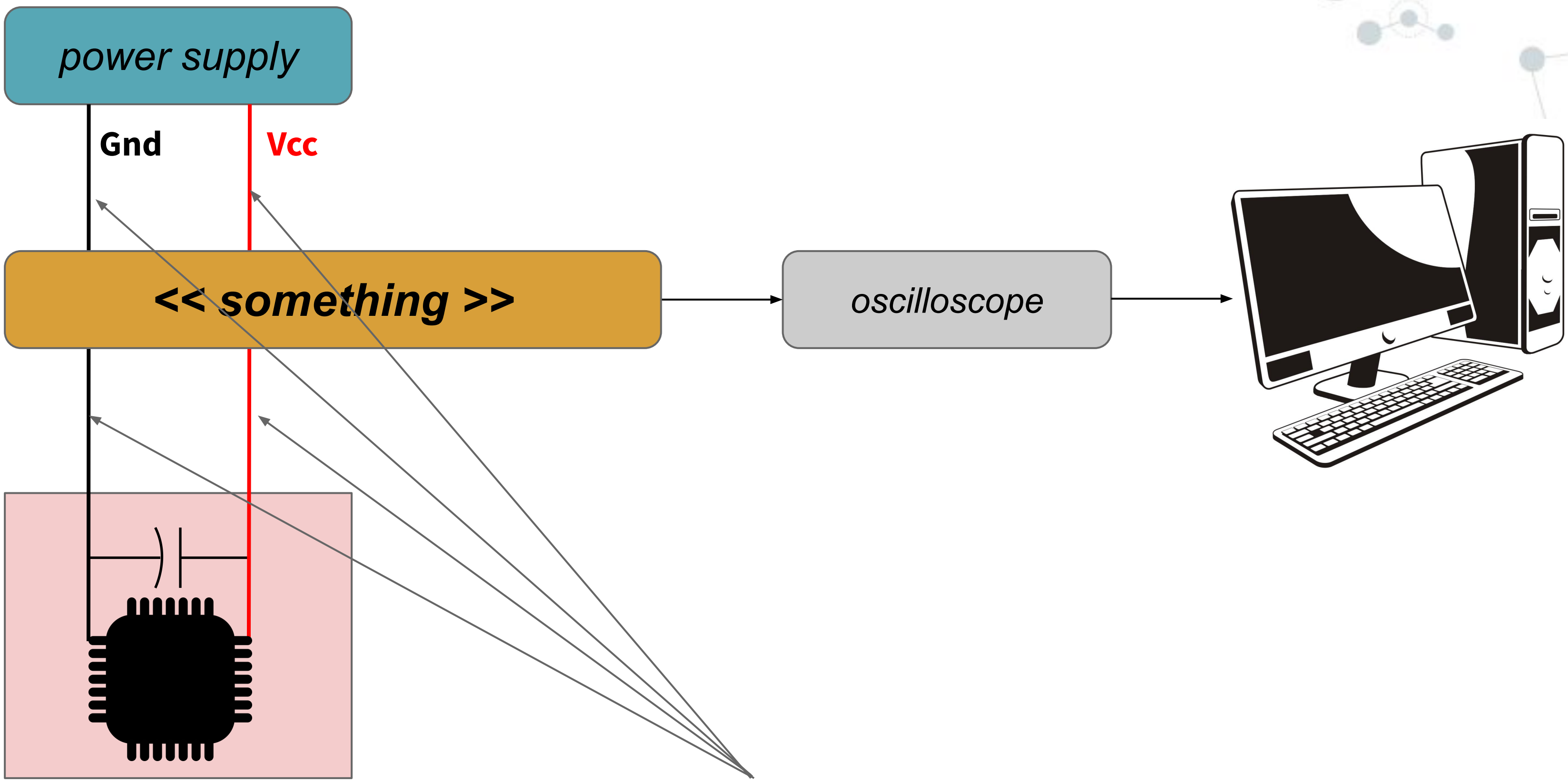
In this presentation…

- Measurements:
  - Fit the trace into vertical oscilloscope resolution (100 mV/div, 50 mV/div…)
  - 2us duration at 5 GS/s sampling (1GHz BW)
  - 300’000 traces (10’000 samples per trace)
  - One data set measurement took approximately 1h45
- Analysed parameters:
  - Raw traces
  - Fourier Power Spectral Density
  - Pearson Correlation Coefficient for AES key recovery

Your typical measurement setup

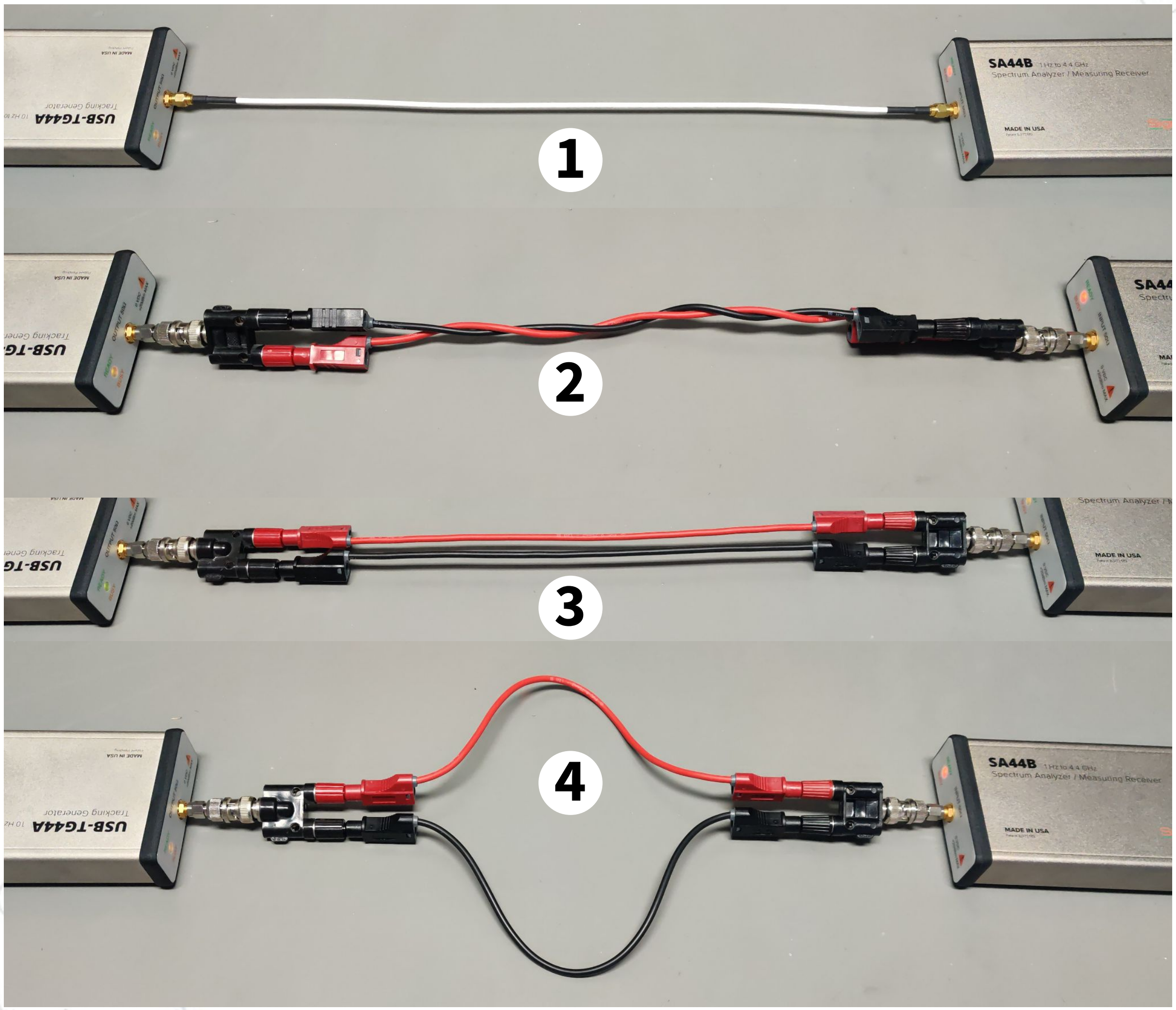


Your typical measurement setup

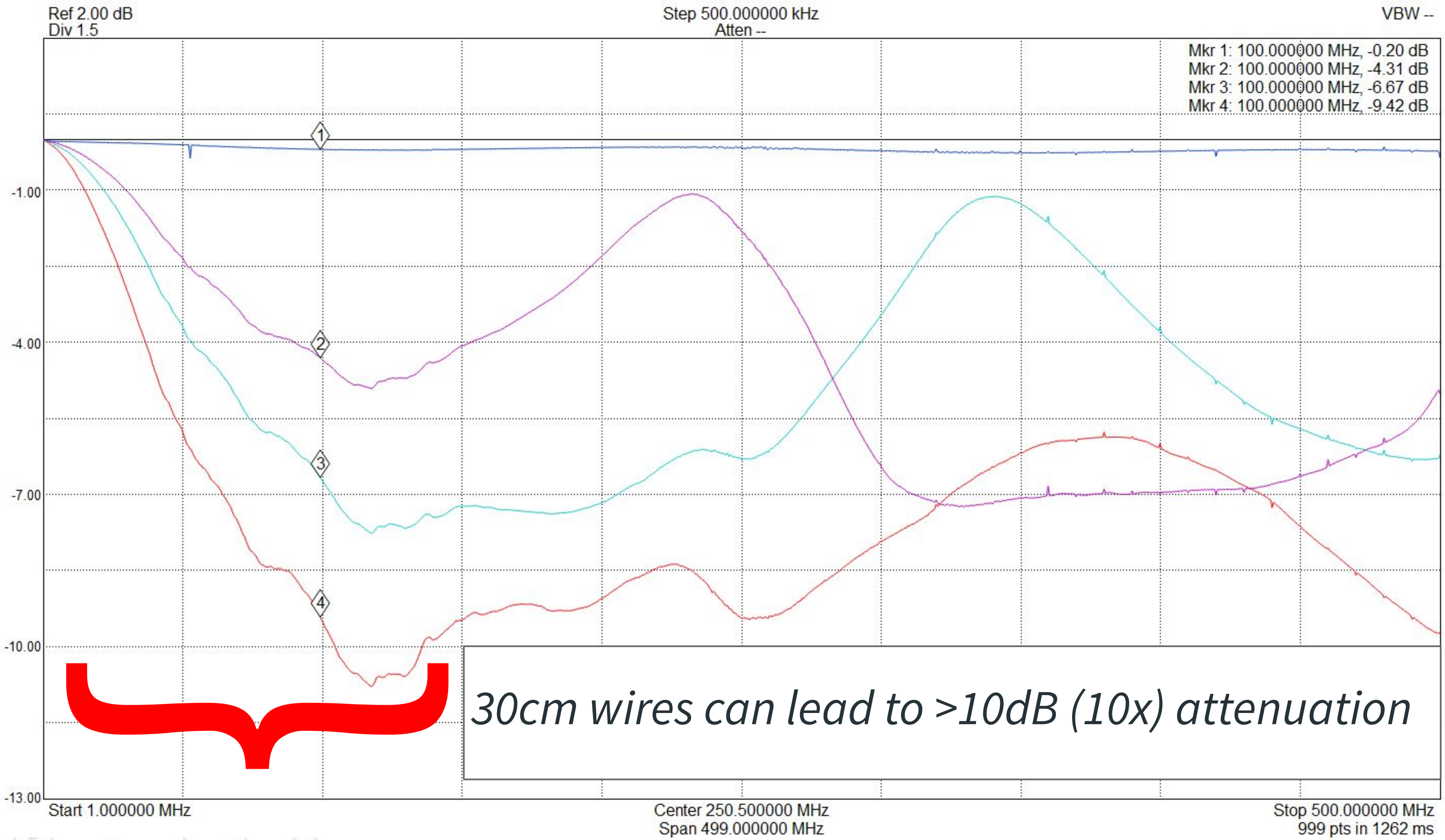


Should we care about wires?

~30cm wire length, different wirings



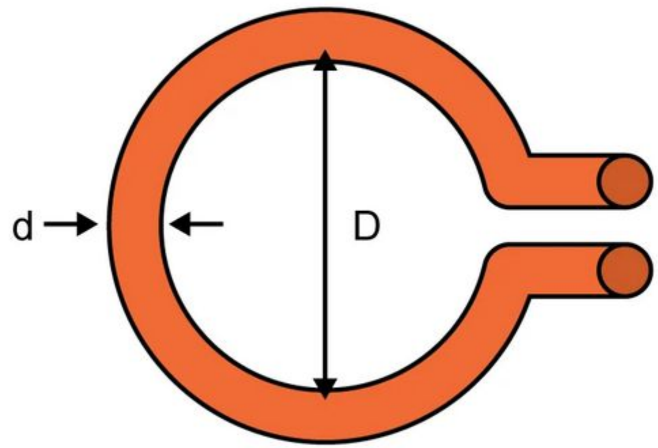
Attenuation across frequency



30cm wires can lead to >10dB (10x) attenuation

But why?

- Ask Mr Faraday



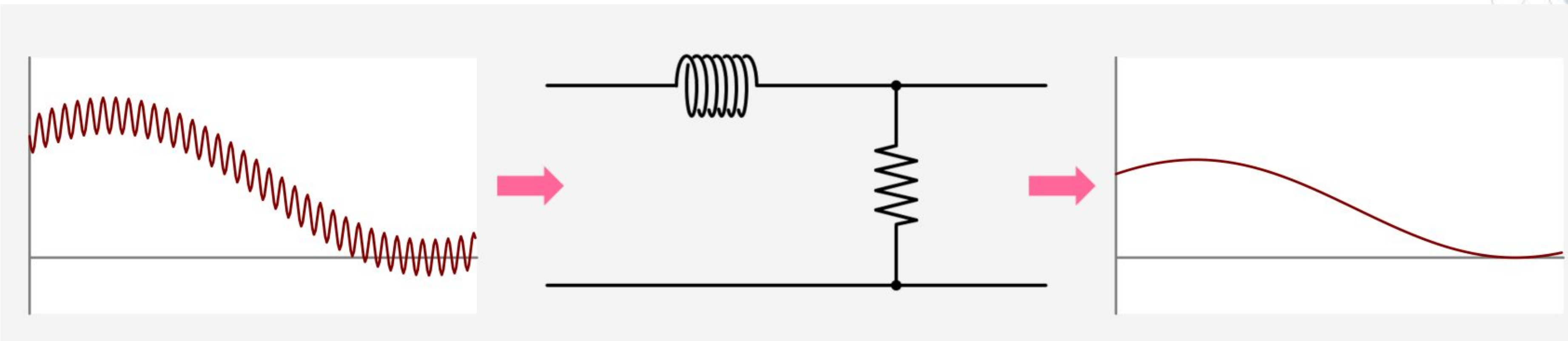
Equations

$$L_{loop} \approx \mu_o \mu_r \left(\frac{D}{2}\right) \cdot \left[\ln\left(\frac{8 \cdot D}{d}\right) - 2\right]$$

→ the bigger the loop area, the bigger the <u>inductance</u>

→ the <u>less high frequencies</u> you'll get

Equivalent Circuit



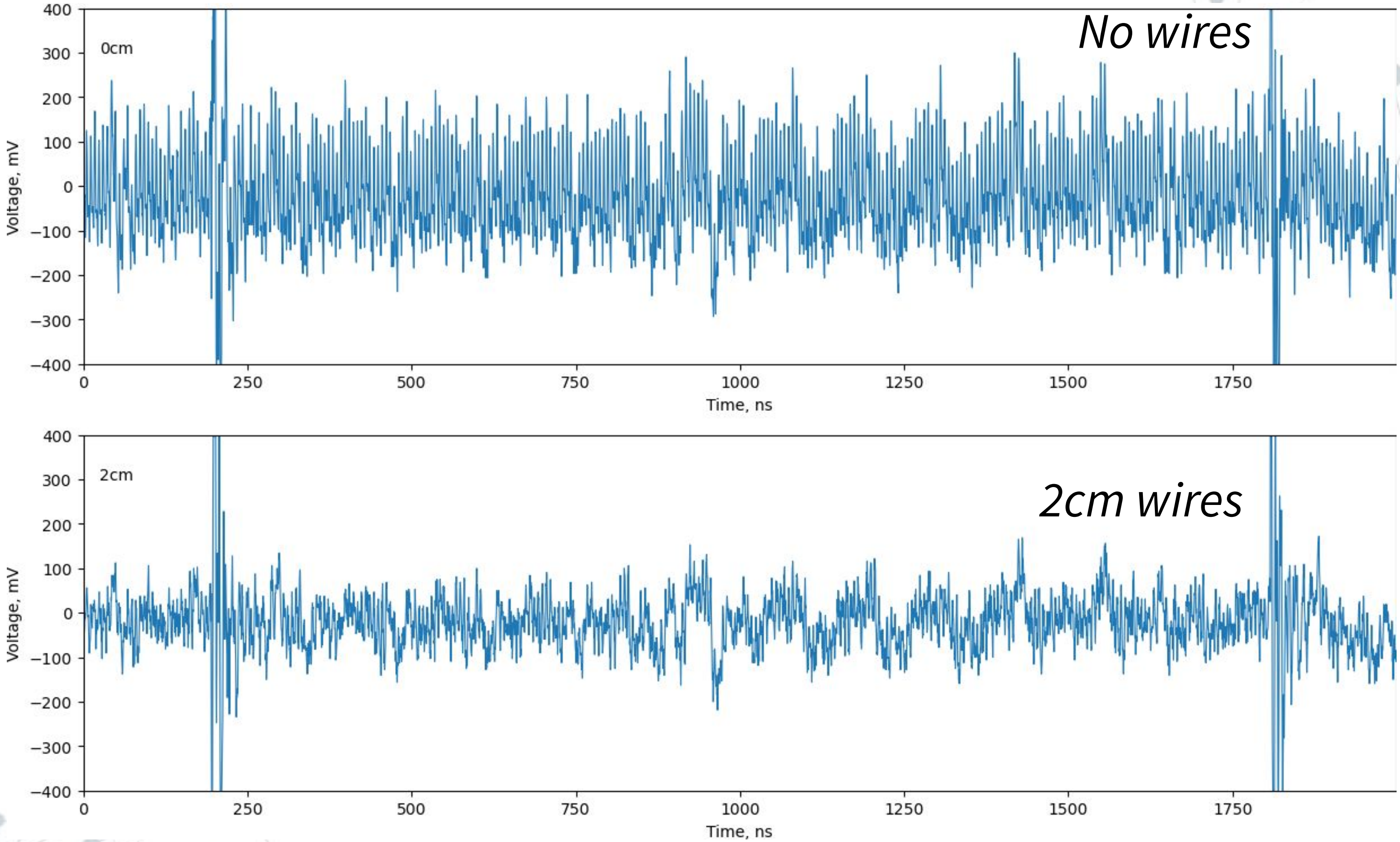
→ the bigger the loop area, the bigger the inductance

→ the less high frequencies you'll get

And on an actual platform?

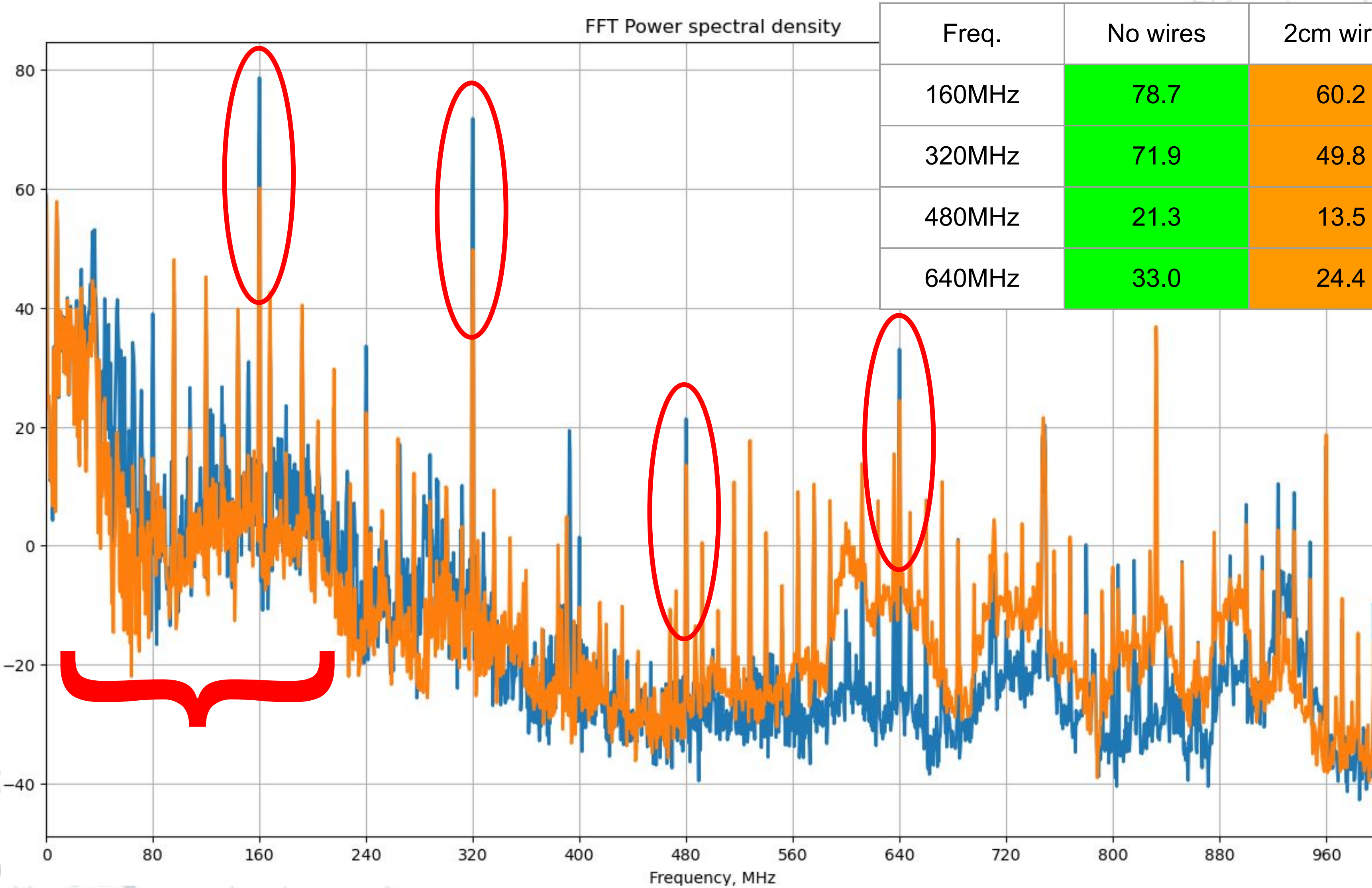
2 test cases: directly connected / with 2 cm wires

Time domain traces



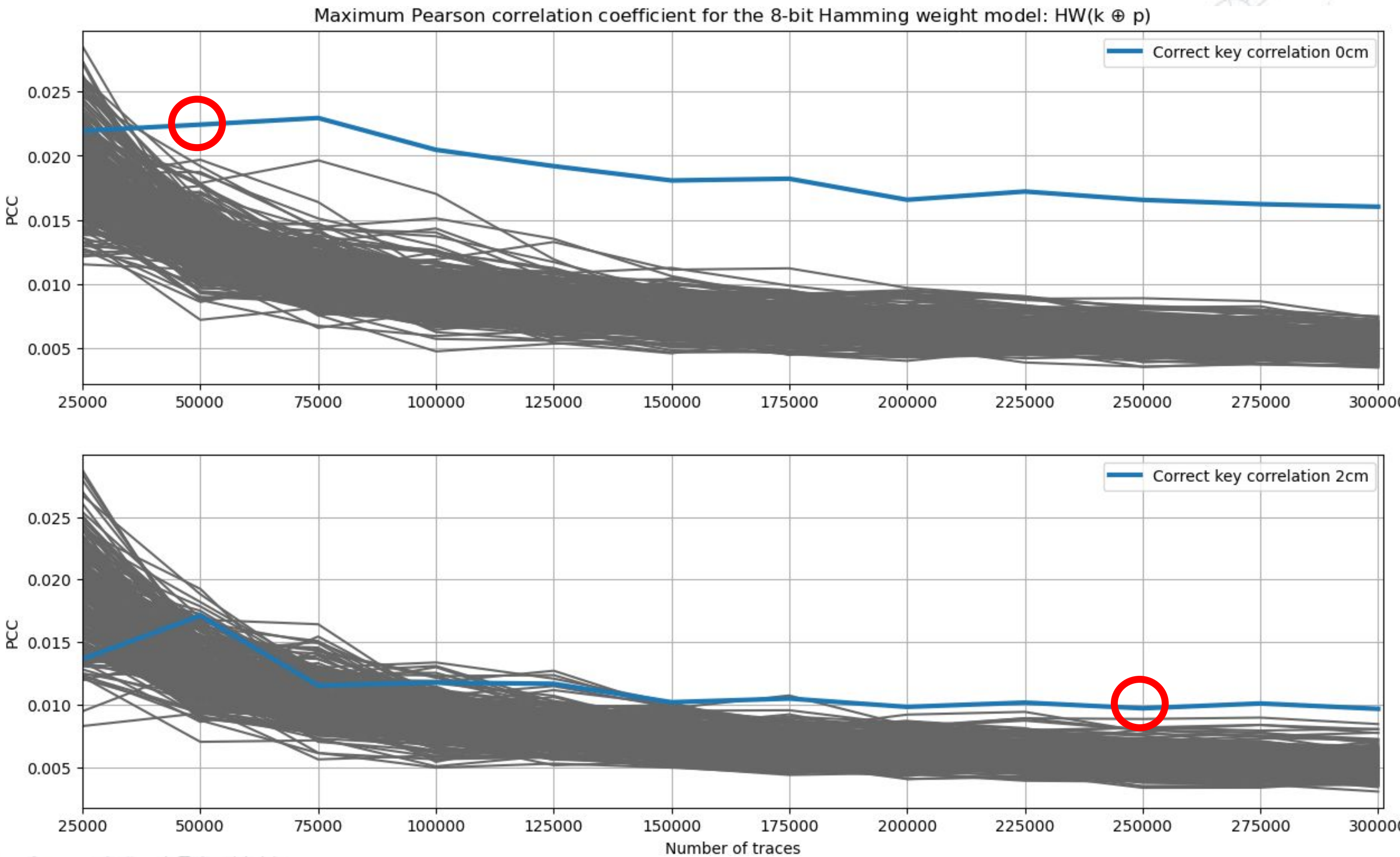
longer wires → more inductance → less high frequencies

Frequency contents vs wiring type



Freq.	No wires	2cm wires
160MHz	78.7	60.2
320MHz	71.9	49.8
480MHz	21.3	13.5
640MHz	33.0	24.4

Performing the actual attack…



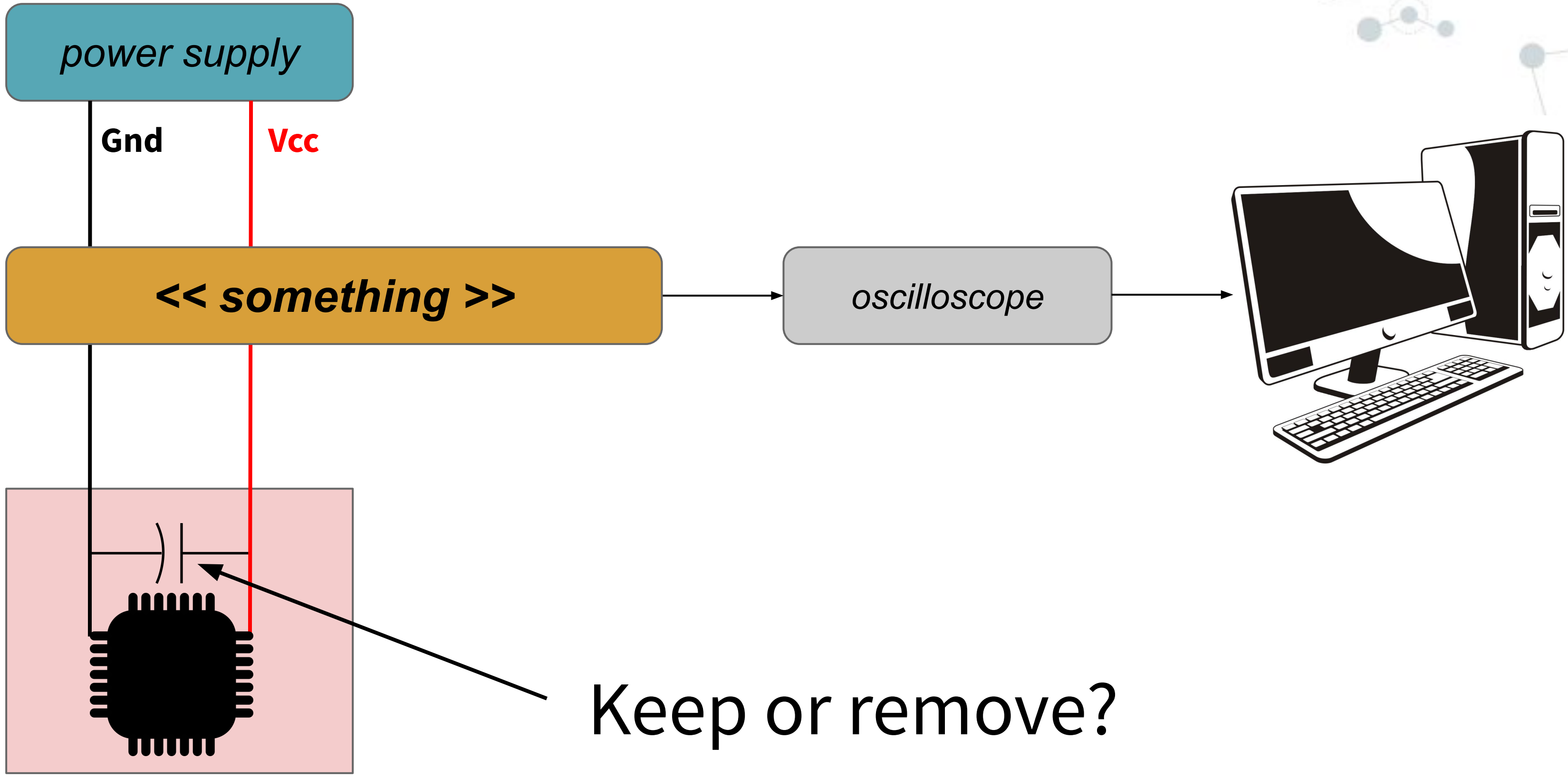
no wires: <u>50k traces</u> needed vs <u>250k traces</u> with wires

“

Conclusion?

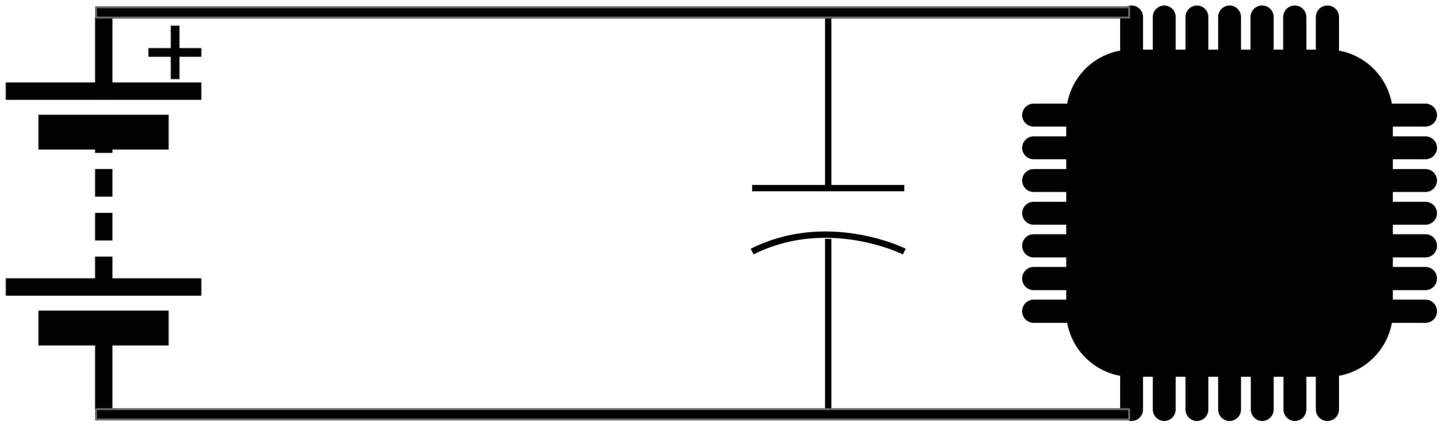
No wires.

Your typical measurement setup



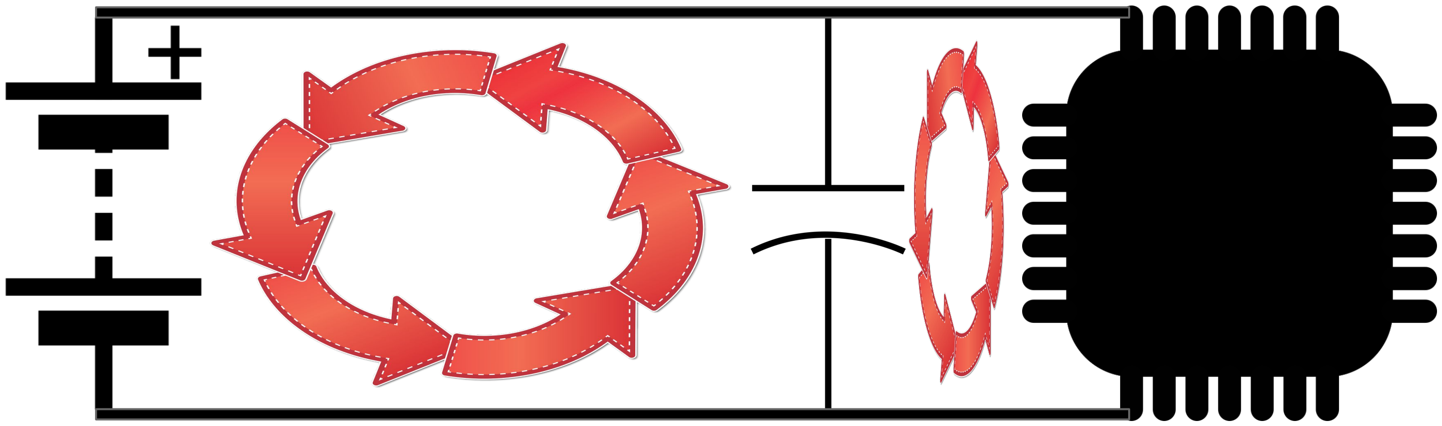
Removing decoupling capacitors…. why?

After all… the energy comes from your supply, right?



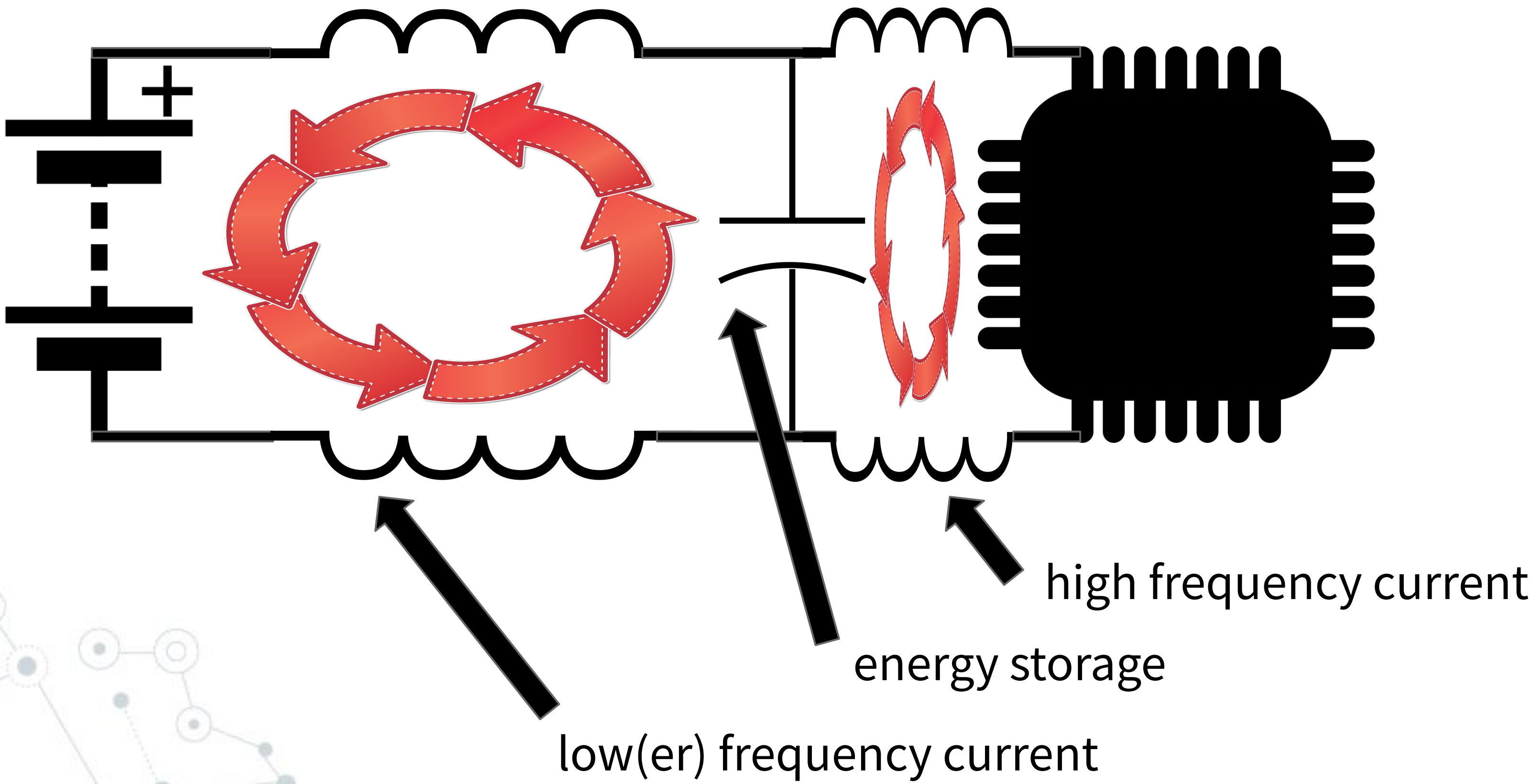
Removing decoupling capacitors…. why?

After all… the energy comes from your supply, right?



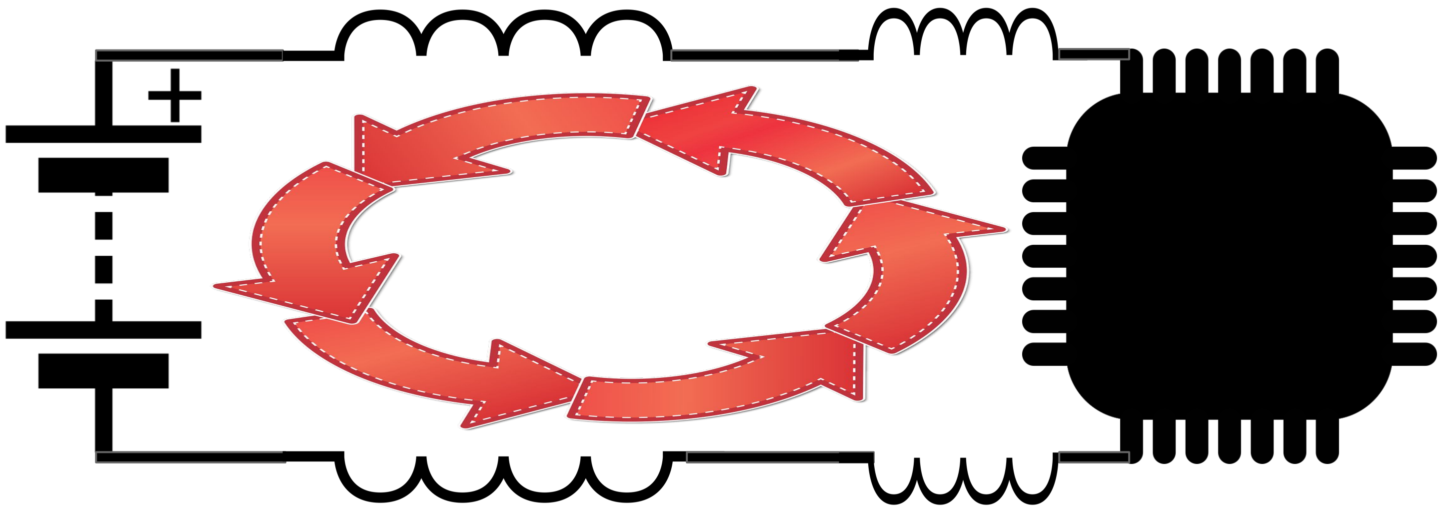
Removing decoupling capacitors.... why?

Parasitic inductance



Removing decoupling capacitors.... why?

Removing capacitors tries to force the high frequency current through the wires

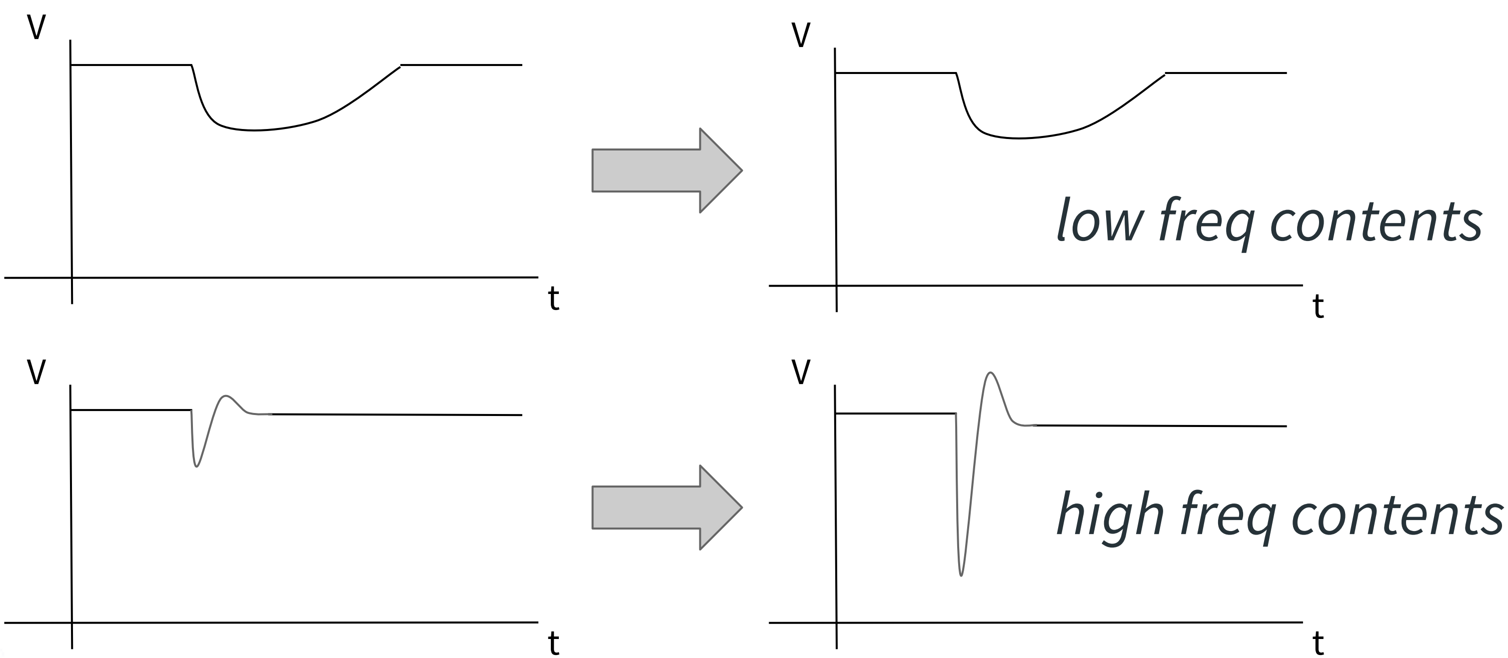


… but the inductance is still there and

$$v = L\frac{di}{dt}$$

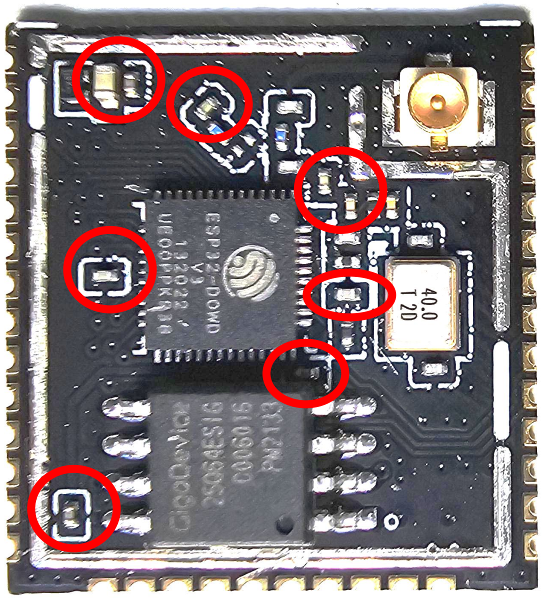
Any downside removing capacitors?

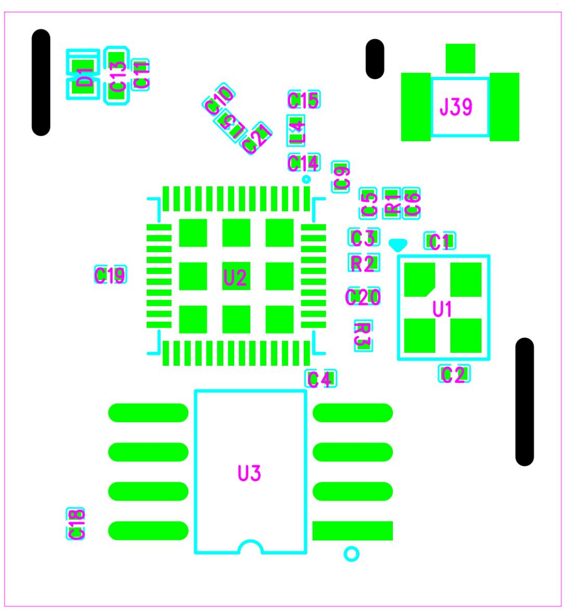
with decoupling caps | without decoupling caps

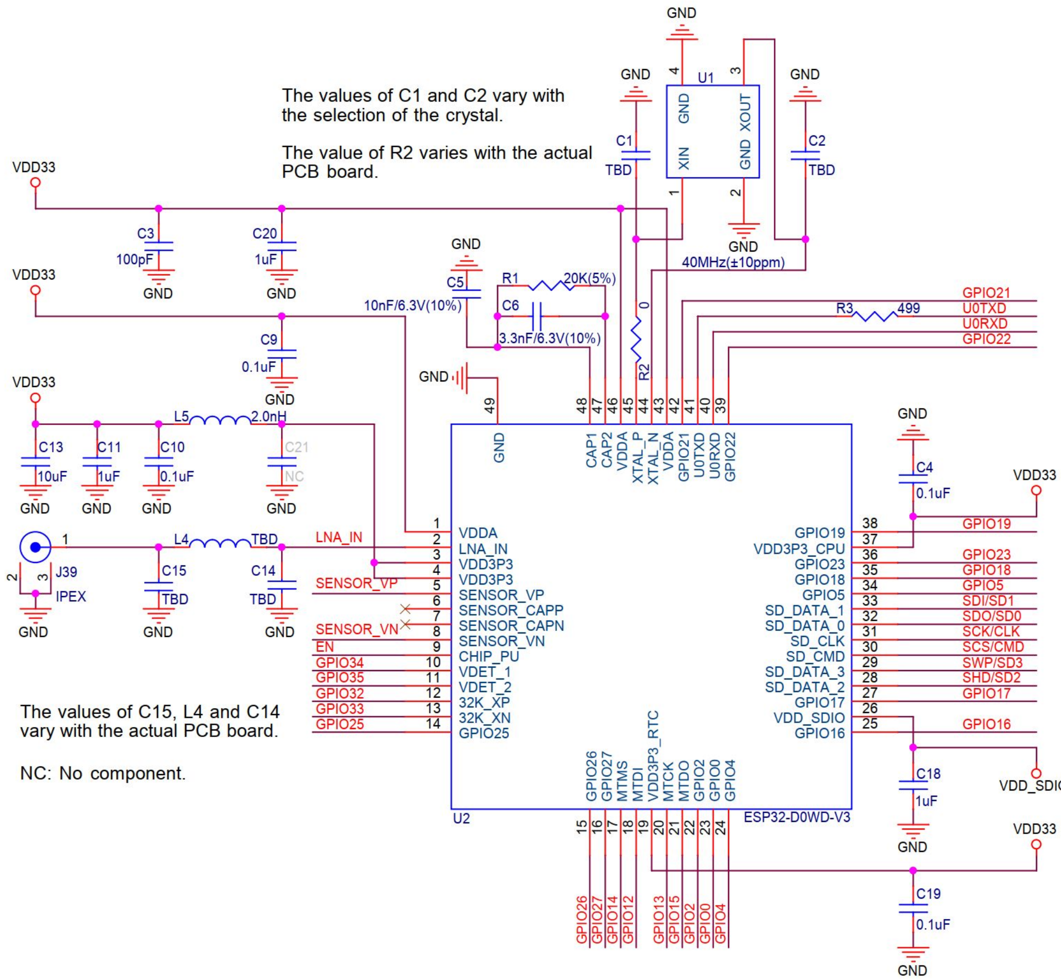


→ for a big enough dip, MCU resets occurs

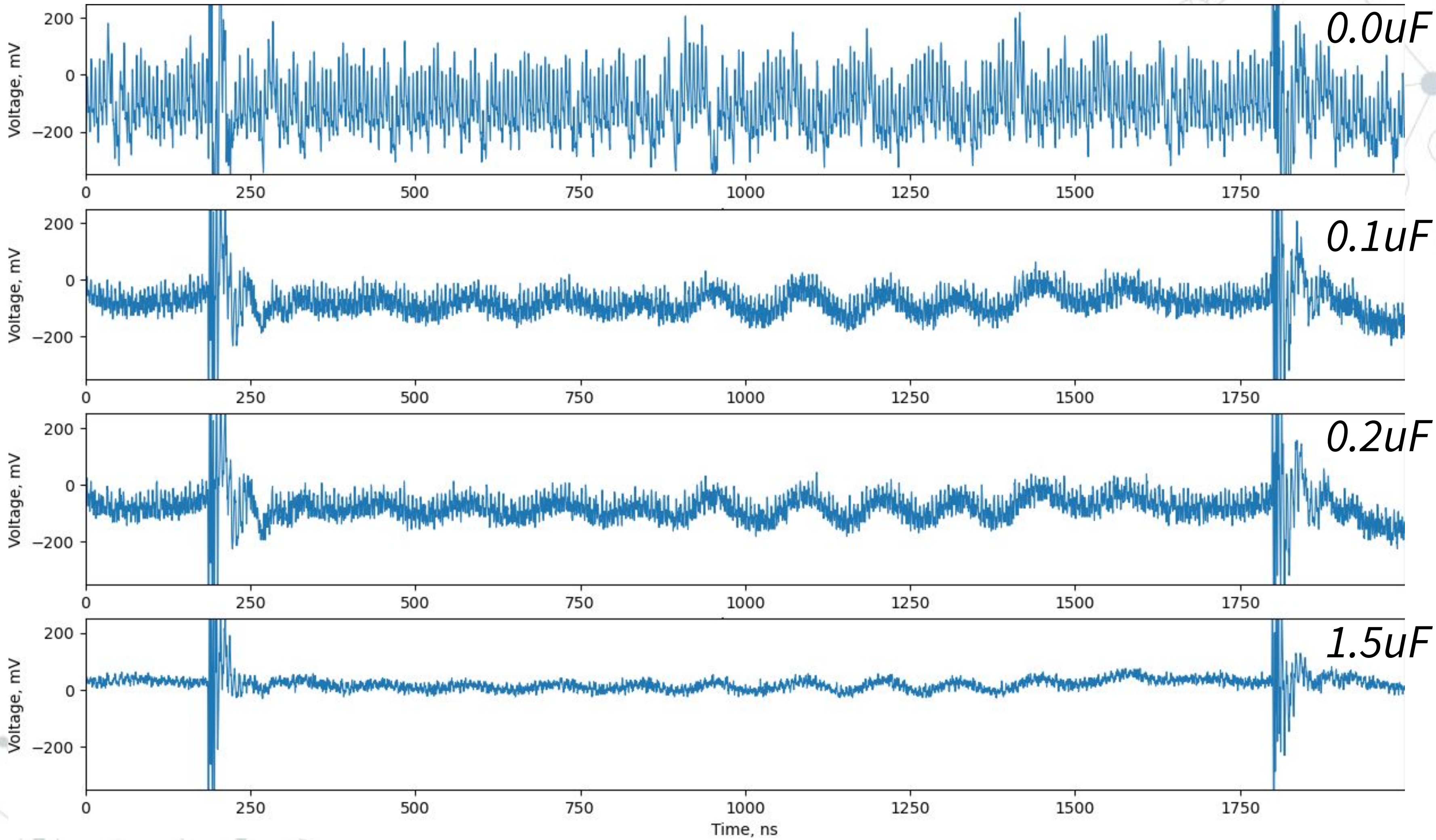
Removing caps on our DUT...





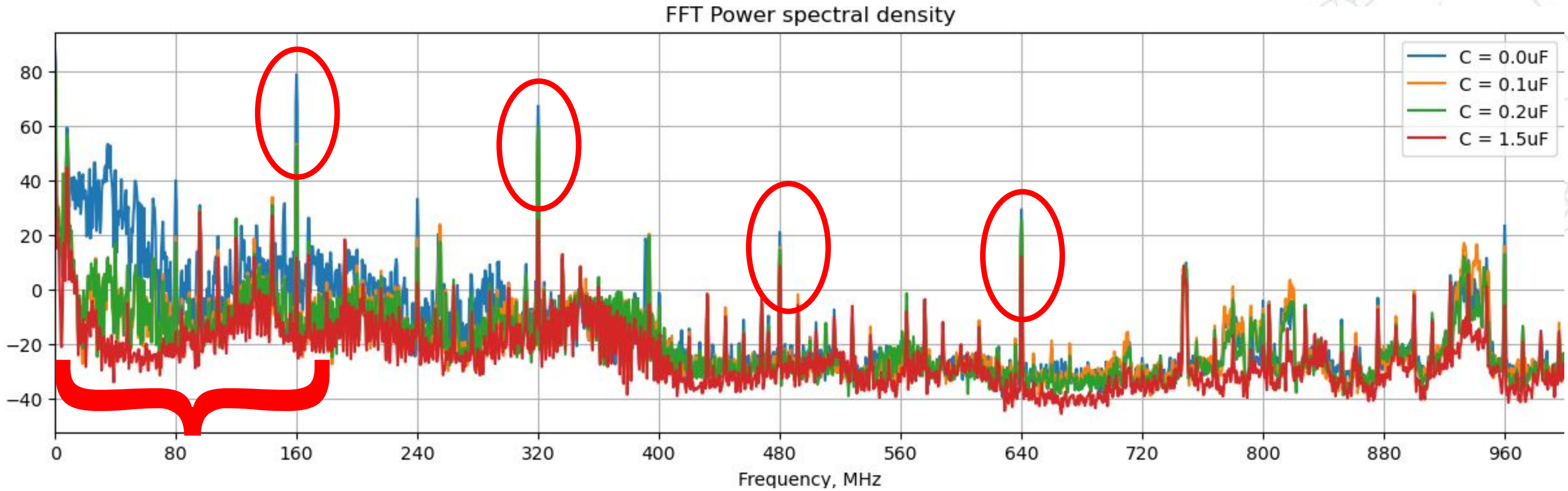


Time domain vs onboard capacitance



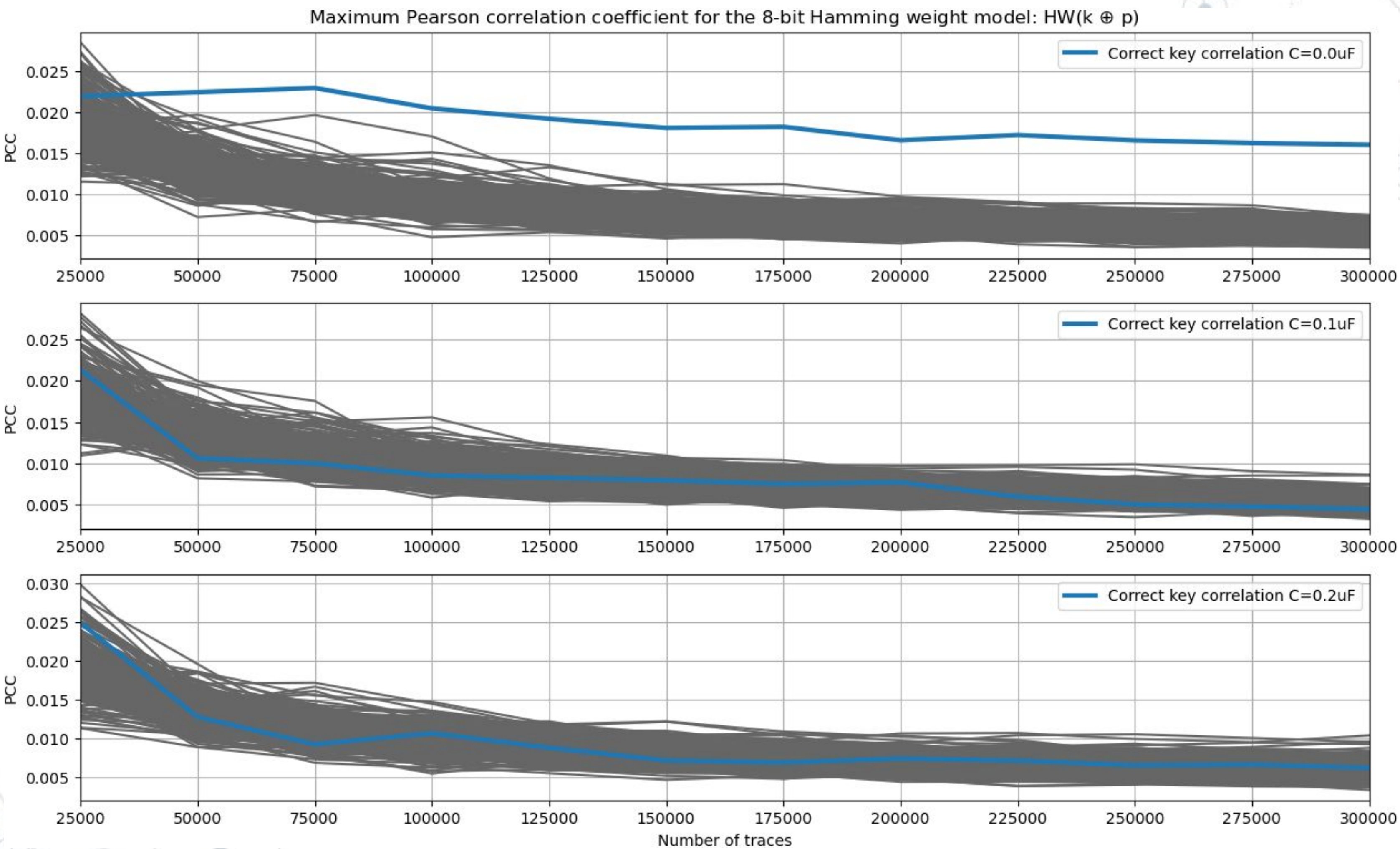
more capacitance → less high frequencies

Frequency contents vs onboard capacitance



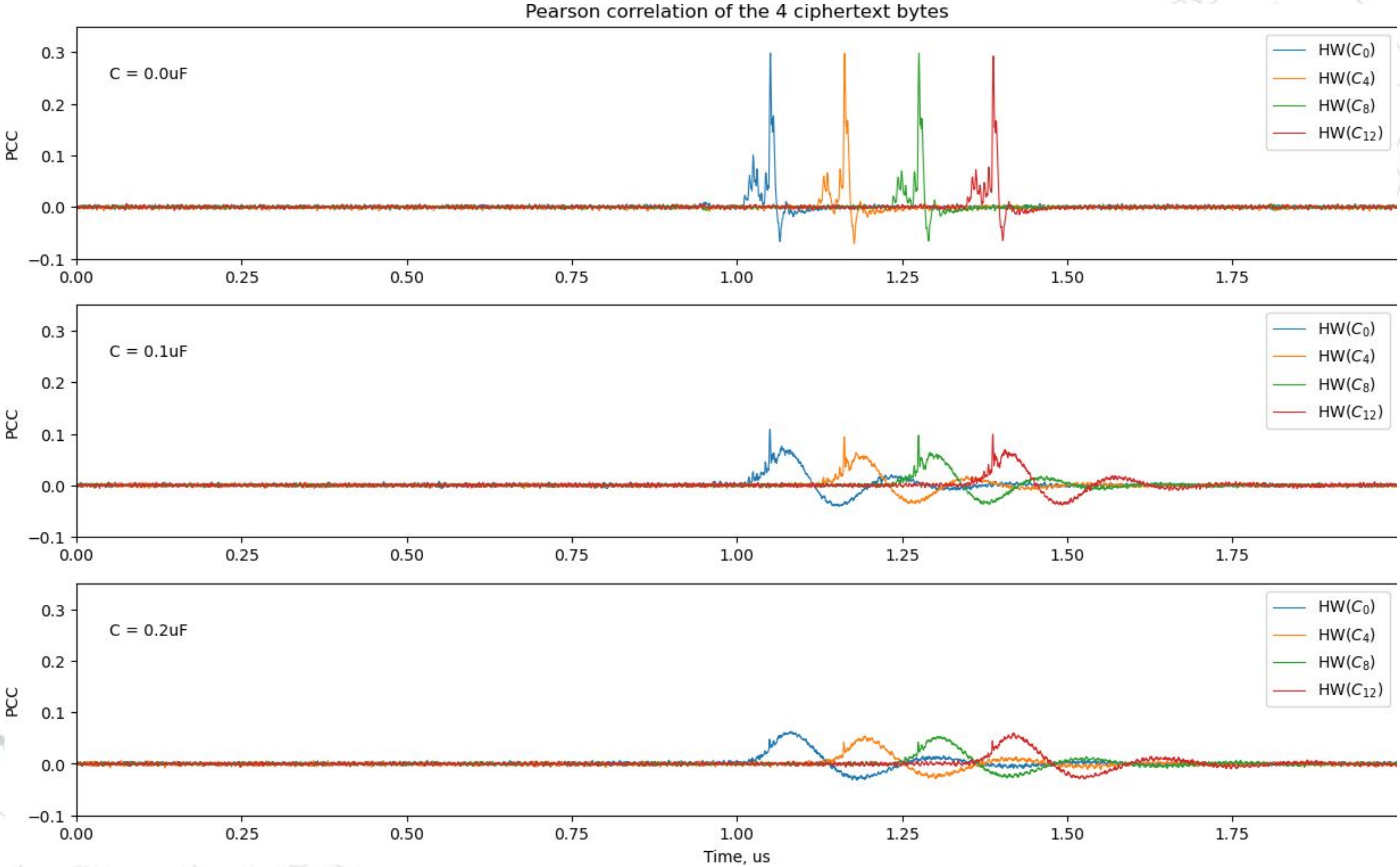
Freq.	0uF	0.1uF	0.2uF	1.5uF
160MHz	78.7	53.1	52.4	11.4
320MHz	67.2	58.4	59.2	25.2
480MHz	20.9	15.4	14.5	8.5
640MHz	29.2	23.8	25.5	12.0

Performing the attack…



No attack possible with capacitors on the board !

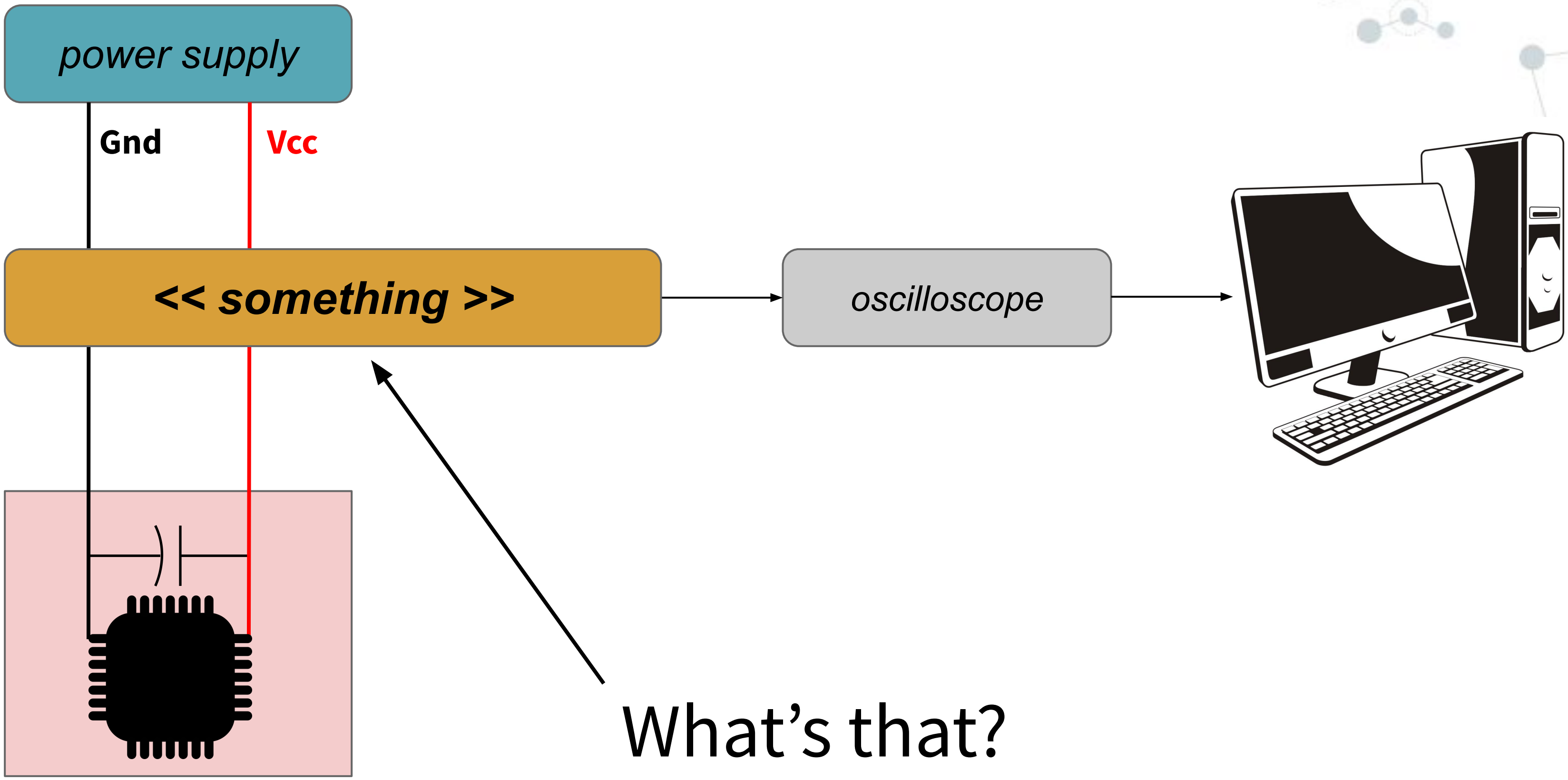
Performing the attack… other correlation



Conclusion?

No capacitors (except if it reboots)

Your typical measurement setup

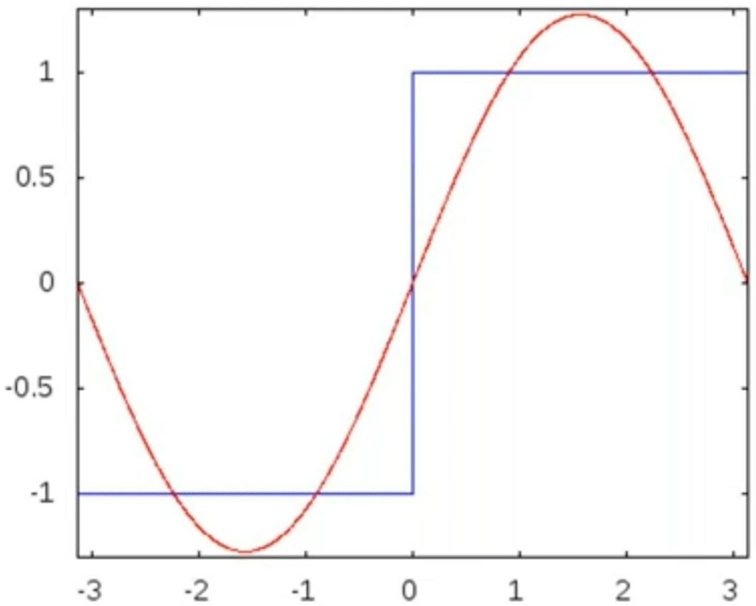


Different tools, different bandwidths

Different tools:

- Differential probe
- Current probe
- Shunt resistor
- LISN

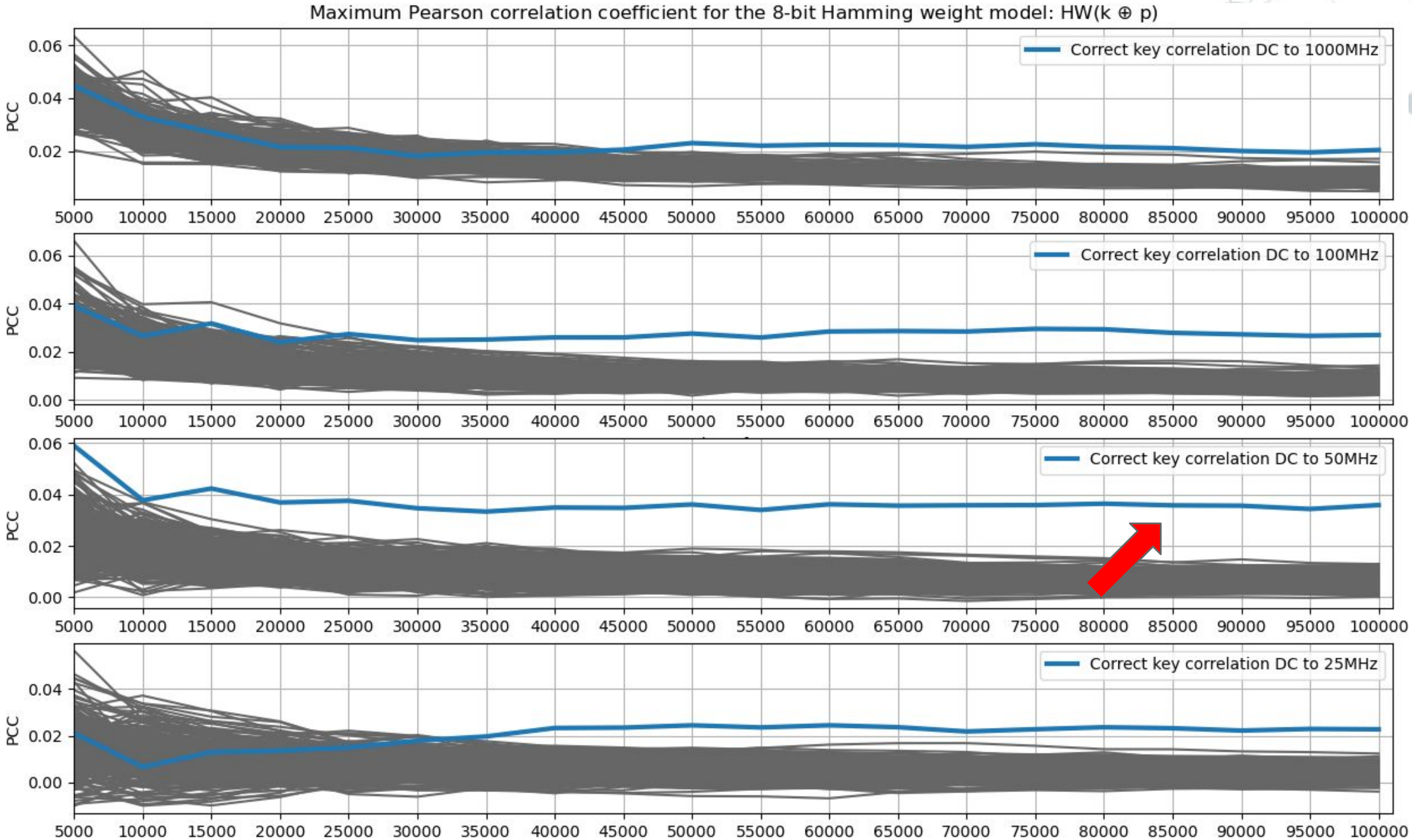
With different bandwidths



Don't forget about the harmonics!

$$x(t) = sin\omega_0 t \; + \frac{1}{3} sin3\omega_0 t \; + \frac{1}{5} sin5\omega_0 t \; + \cdots$$

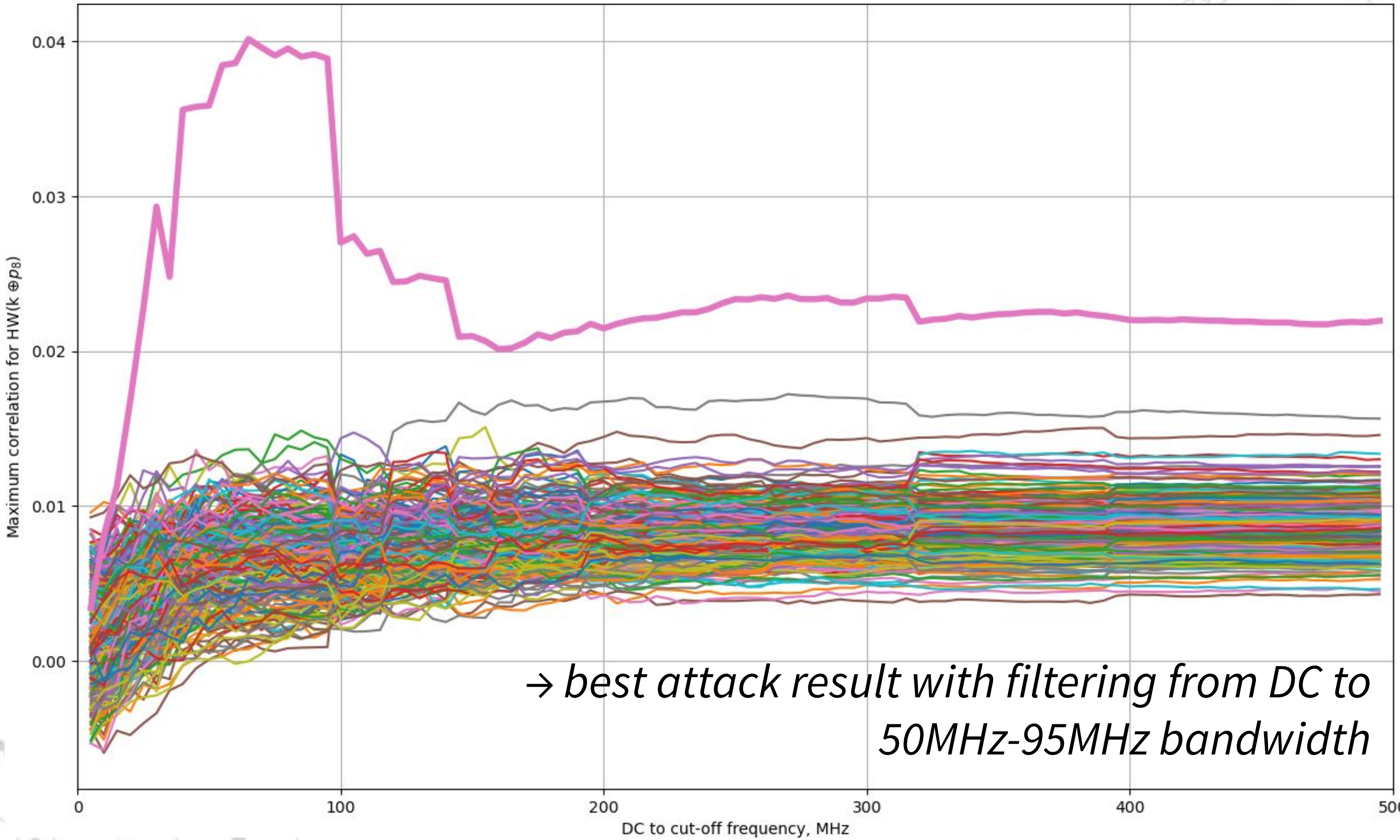
Attack success vs frequency contents



→ best attack result with a 50MHz bandwidth

→ too much noise present in high freqs ?

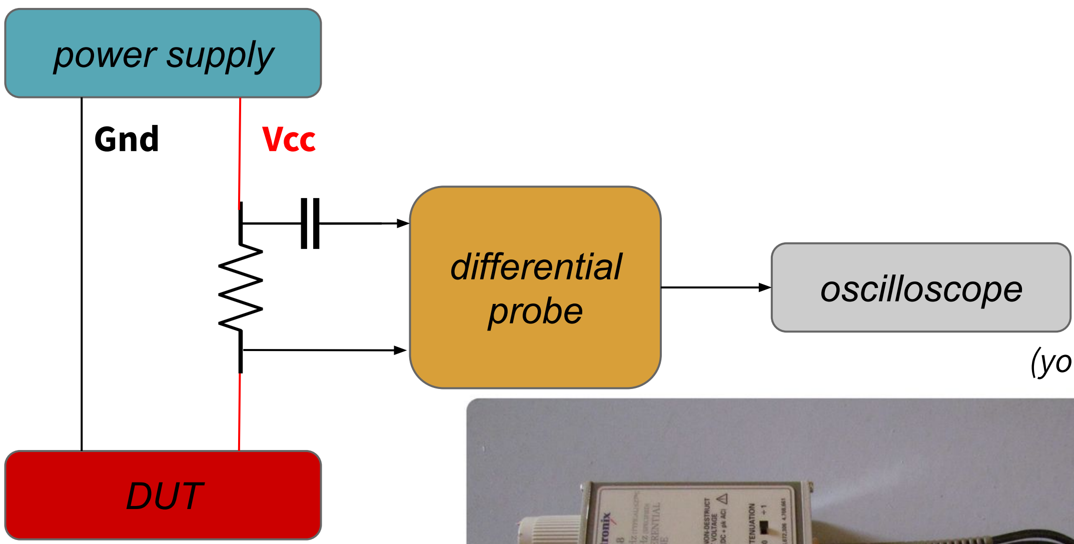
Attack success vs frequency contents



→ *best attack result with filtering from DC to 50MHz-95MHz bandwidth*

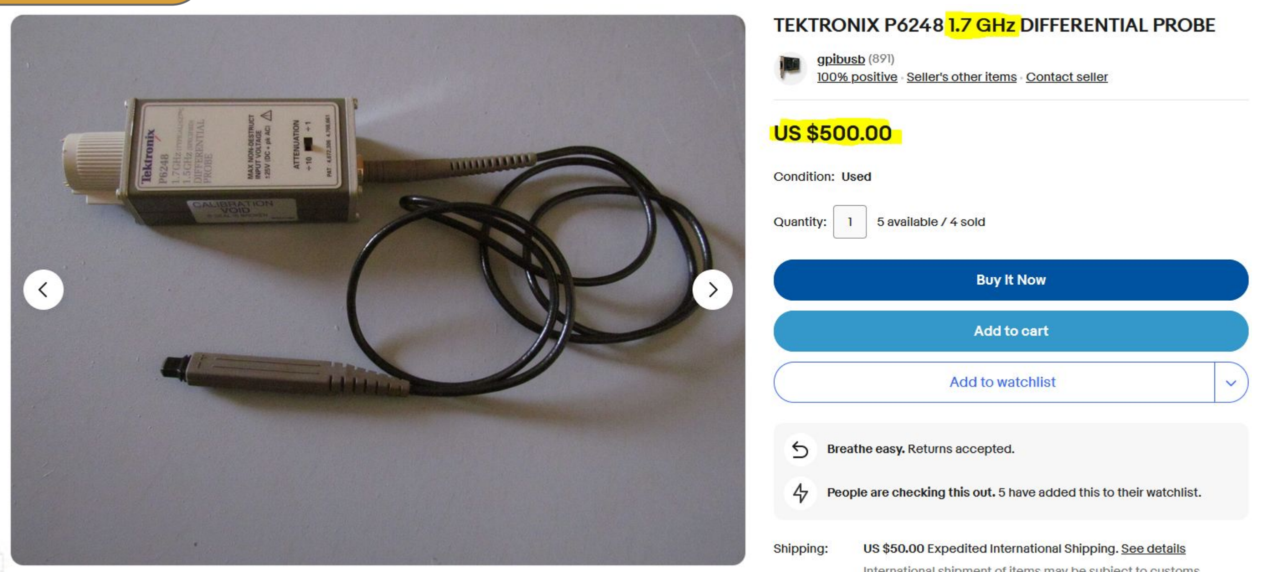
1) Differential probe

Measures the voltage across a shunt resistor



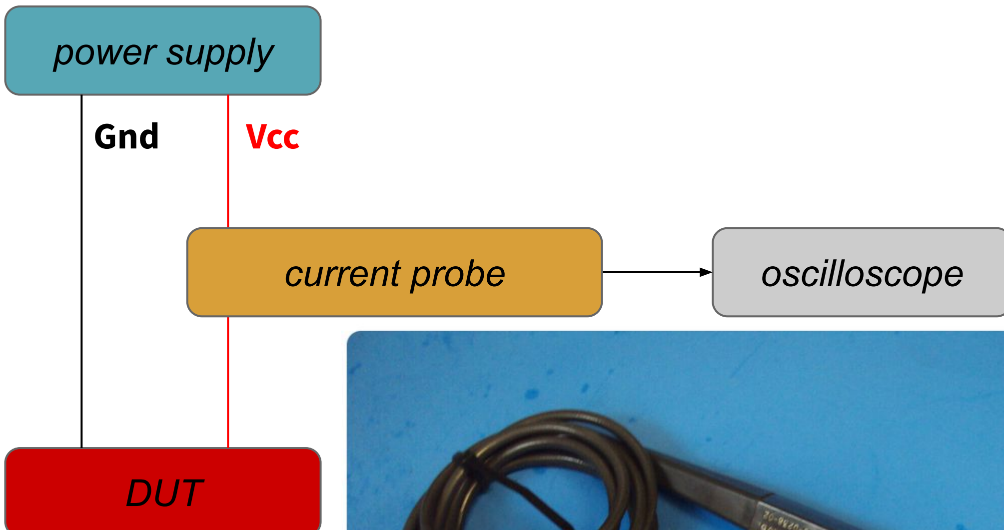
up to 1.7GHz

(you do need to buy the scope that supports it)

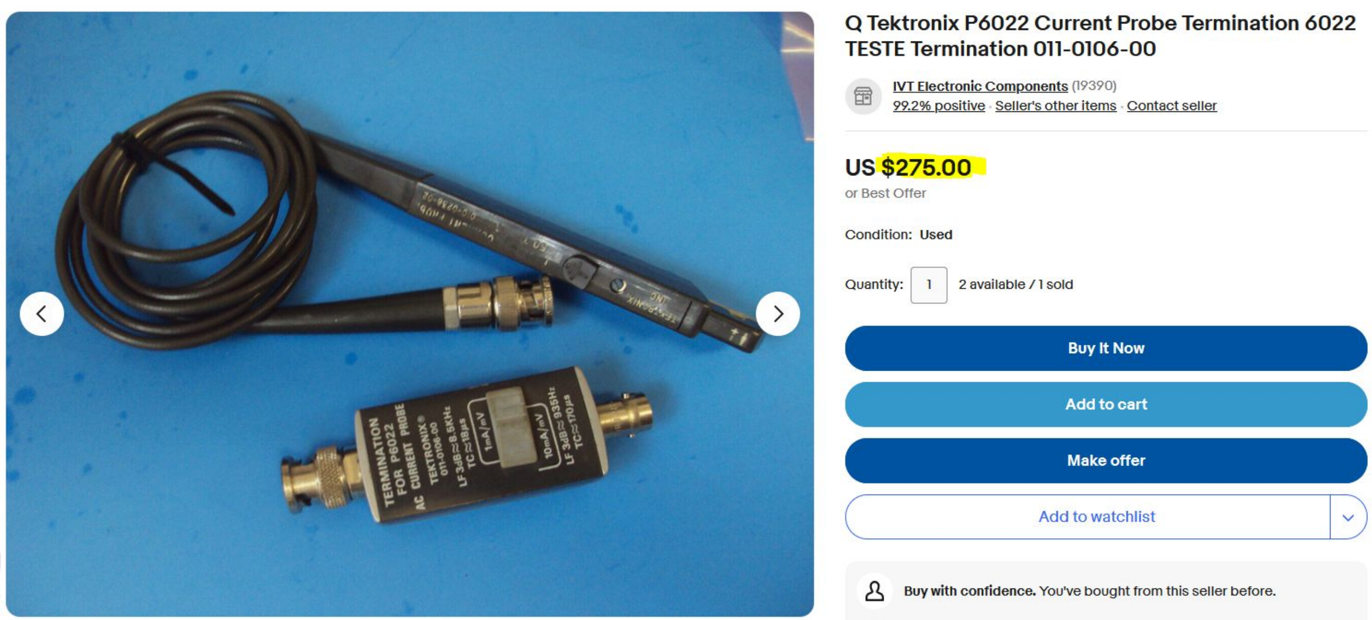


2) Current probe

Clips around a **wire** to measure current

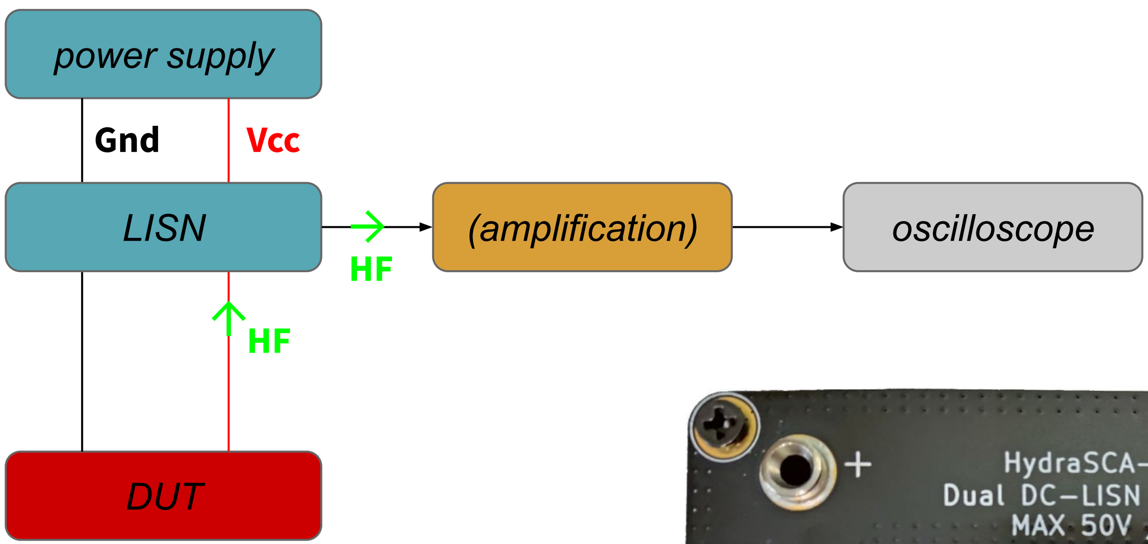


up to 100MHz



3) LISN

Works by ‘isolating’ the supply from the load

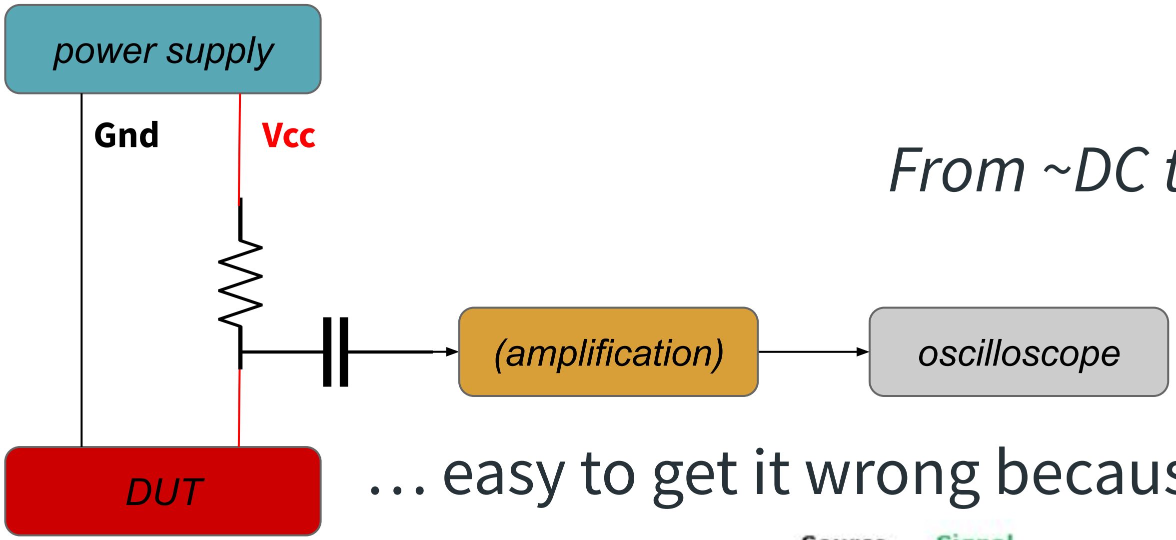


up to 430MHz

~250USD

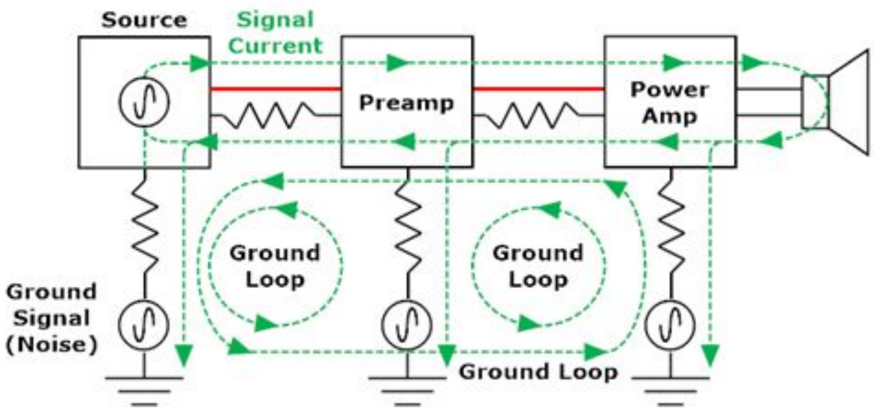
4) Shunt resistor

The simplest setup by far



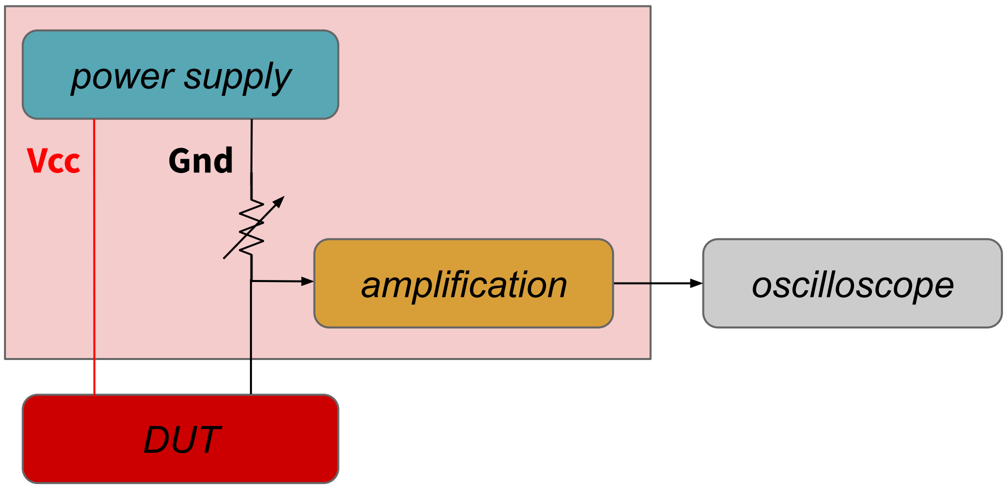
From ~DC to xGHz, for free!

… easy to get it wrong because of ground loops

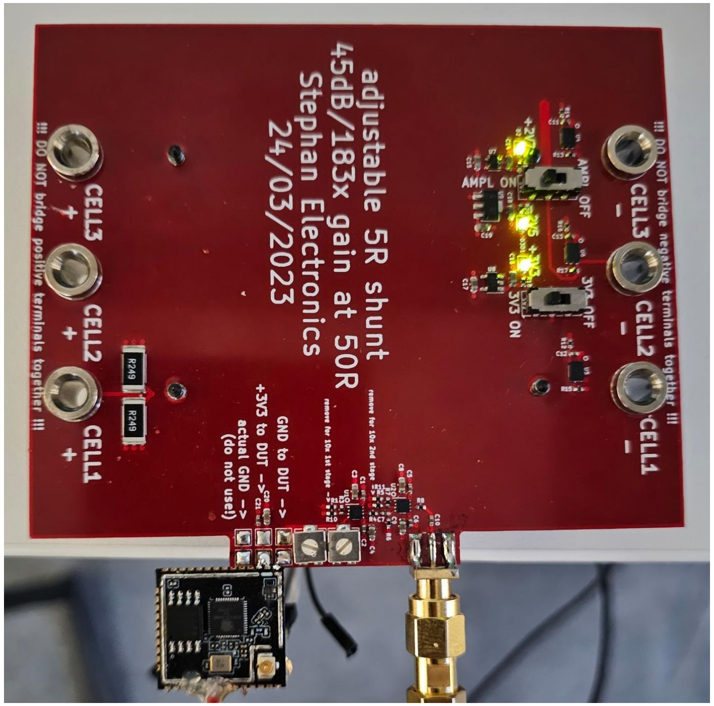


5) Our new approach #1

A shunt resistor without the ground loop issues:



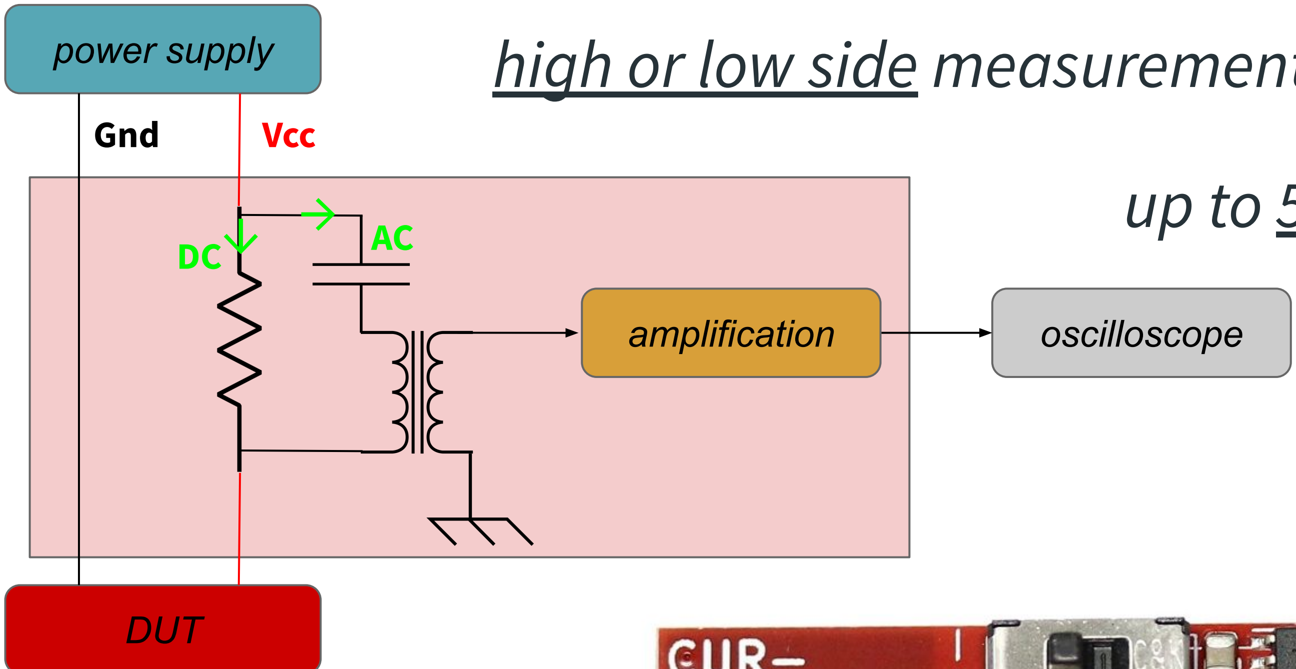
up to 1GHz for $125



low side measurement

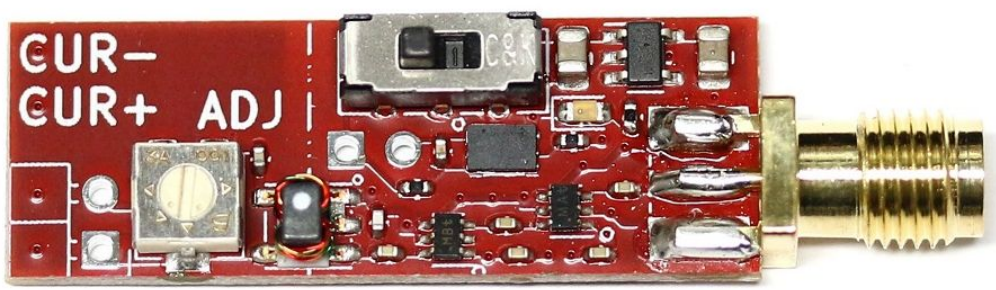
5) Our new approach #2

An isolated ‘shunt resistor’ :



high or low side measurement

up to 500MHz for $25



Summarizing

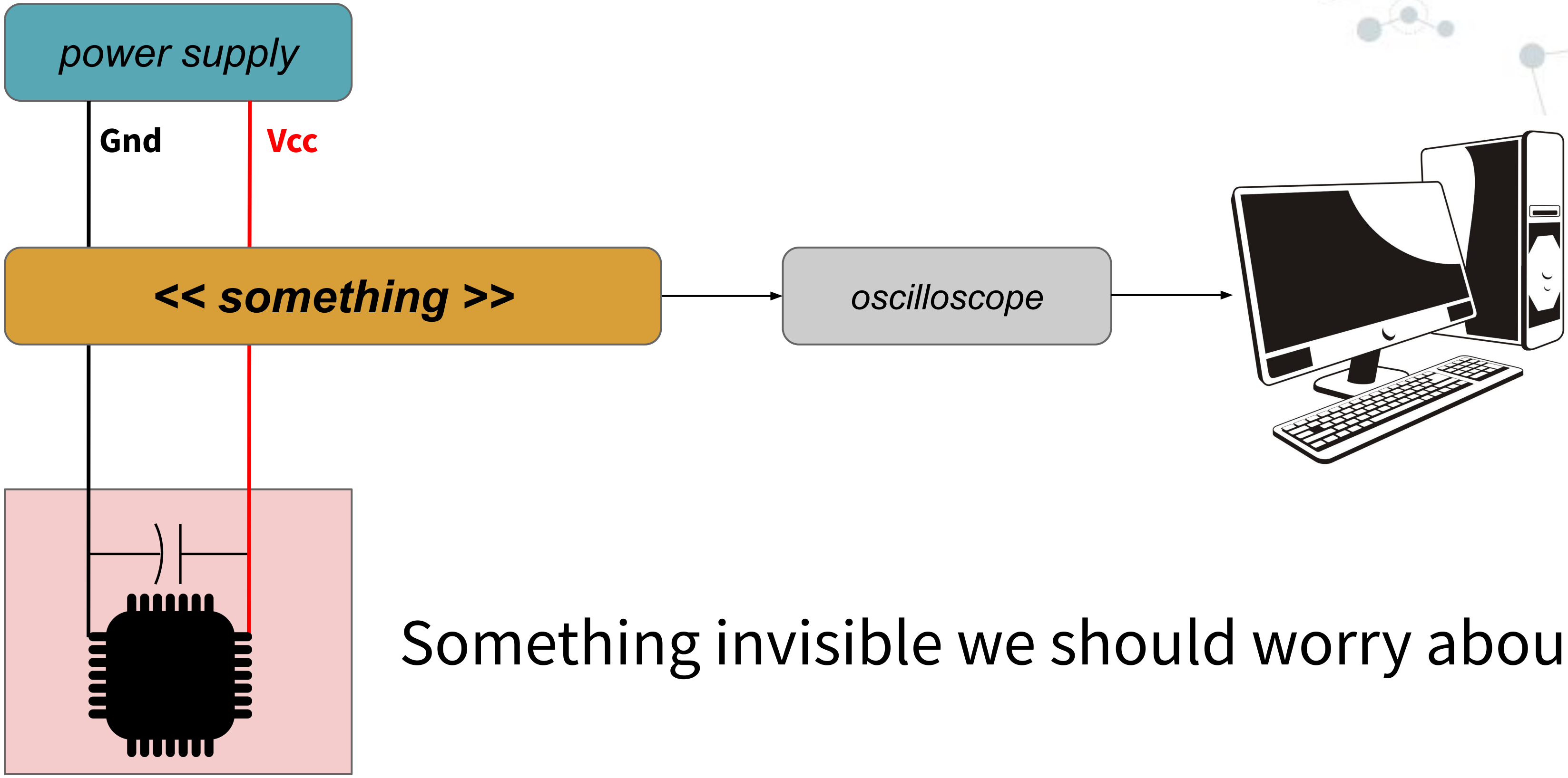
Which one should you pick?

Solution	Frequency	Complexity	Sense Side	Price
differential probe :	DC - 1.7GHz	relatively easy	low & high	~$500
current probe :	DC - 100MHz	easy	low & high	~$300
LISN :	‘DC’ - 430MHz	easy	N/A	~$250
shunt resistor :	‘unlimited’	‘impossible’	low & high	free
‘good shunt resistor’:	2MHz - 1GHz	easy	low	~$100
isolated shunt :	2MHz - 500MHz	relatively easy	low & high	~$25

Only taking into account these criterias…

the cheapest, really.

What else?

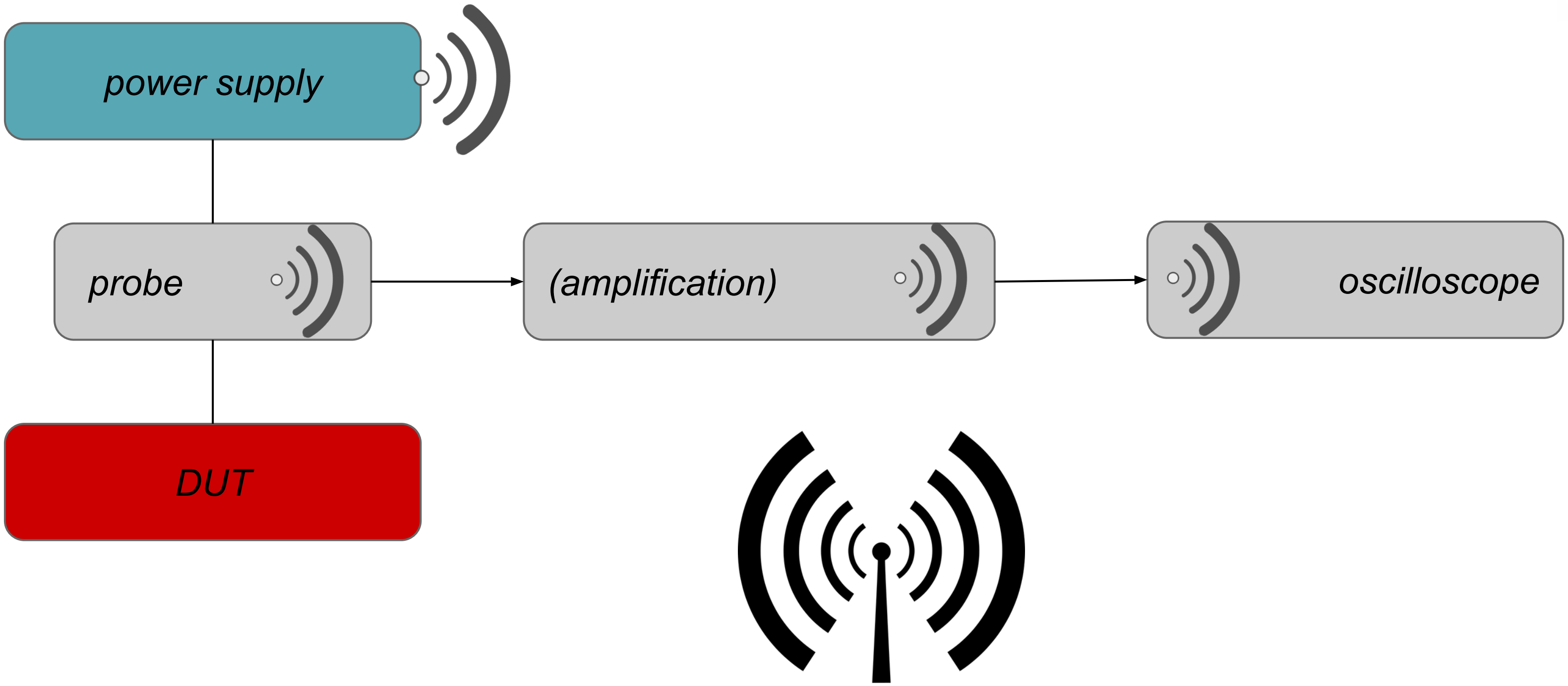


Something invisible we should worry about ?

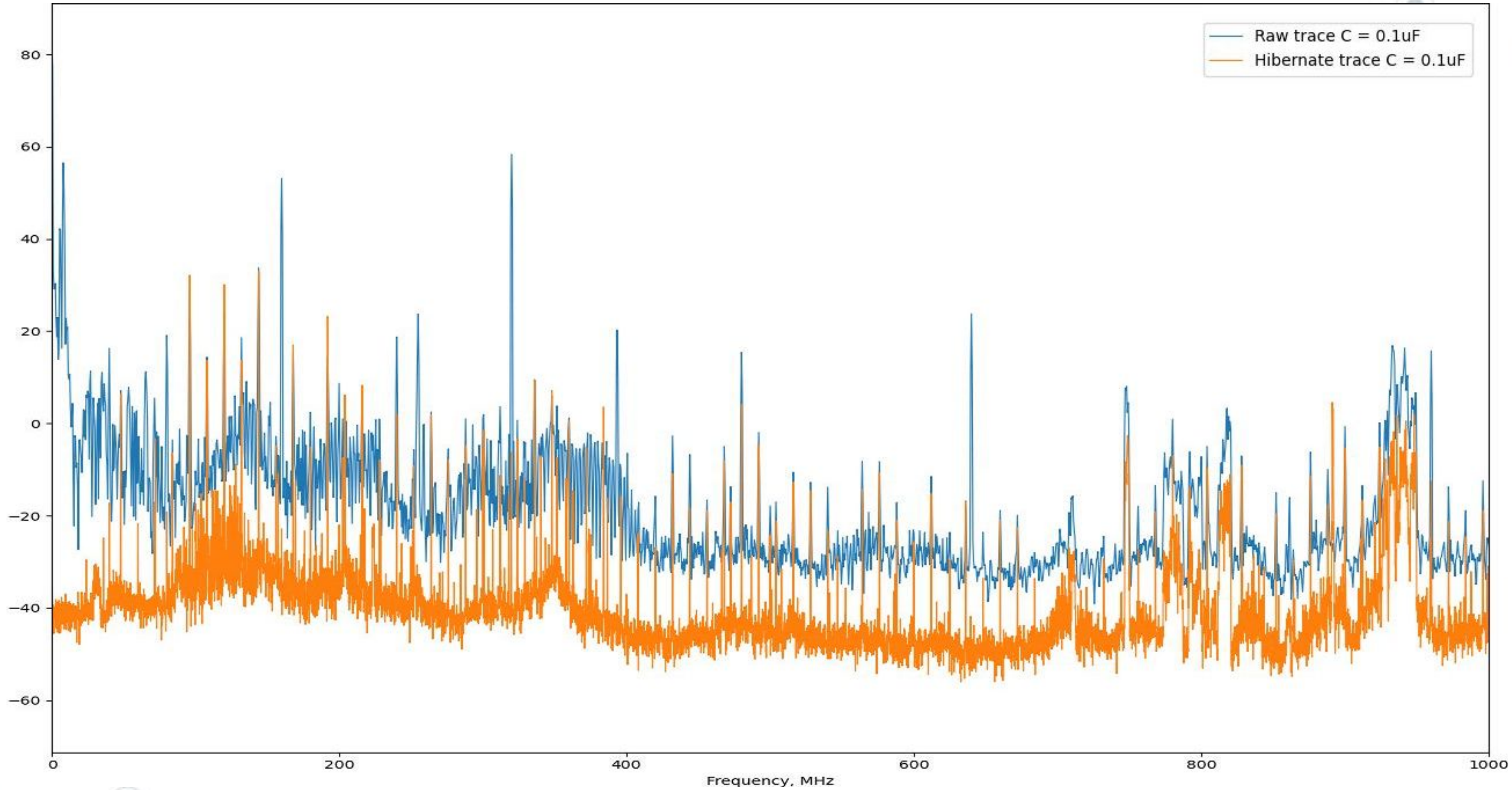
"Electrical noise is the static that disrupts the melody of clean signals."

- Unknown

Where does the noise come from?



Noise from the environment



shared peaks = environmental noise

Noise coming from oscilloscopes

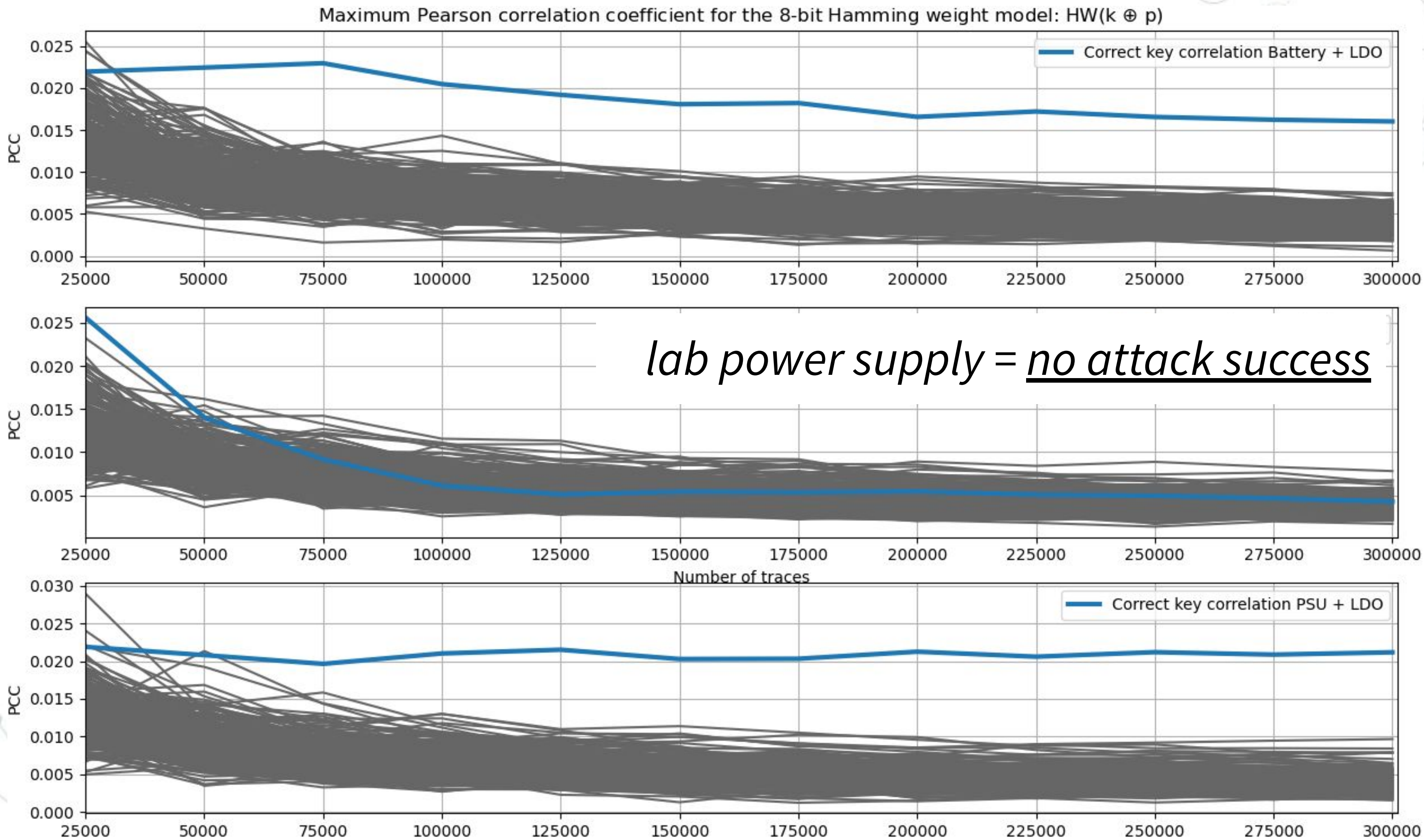
~ 4.7k USD

- Brand-new chipset "Centaurus" developed by RIGOL
- Ultra-low noise floor at 18 μVrms in minimum
- 12-bit vertical resolution[1]
- 200/400/800 MHz analog bandwidth (selectable), 4 analog channels, and 1 EXT channel
- Up to 4 GSa/s real-time sample rate
- Max. memory depth: 500 Mpts (optional)
- Min. vertical sensitivity: 100 μV/div
- Up to 1,500,000 wfms/s waveform capture rate with the UltraAcquire mode
- 10.1'' 1280*800 HD touch display

Typical trick used (if you have the time) :

Signal-to-noise ratio improvement: $\sqrt{\#\text{ of averaged waveforms}}$ dB

Noise from the power supplies



Noise from current probes

CURRENT PROBE CT6711

Frequency bandwidth	DC to 120 MHz (-3 dB)
Rise time	2.9 ns or shorter
Delay time (Typical)	30 A range: 12 ns, 5 A range: 12 ns, 0.5 A range: 13 ns (Delay time relative to rising waveform of input signal 1 ns)
Noise level	75 µA rms max (at 0.5 A range, using 20 MHz band measuring instrument)

~ 6k USD

that noise spec. is confusing: noise is integrated over bandwidth !

$$\mu\mathrm{Vrms} = \mathrm{nV}/\sqrt{(\mathrm{Hz})} * \sqrt{(\mathrm{BW}_{\mathrm{kHz}} * 1.57)}$$

so you don’t know the noise at a given frequency

Noise from differential probes

TEKTRONIX P6248 1.7 GHz DIFFERENTIAL PROBE

gpibusb (891)
100% positive · Seller's other items · Contact seller

US $500.00

Condition: Used

Quantity: 1 5 available / 4 sold

Buy It Now

Add to cart

Add to watchlist

Breathe easy. Returns accepted.

People are checking this out. 5 have added this to their watchlist.

Shipping: US $50.00 Expedited International Shipping. See details

Typical characteristics

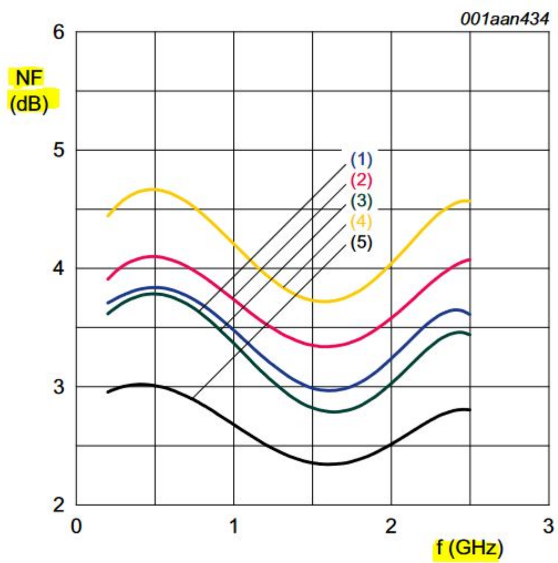
Input capacitance	
Differential mode	<1 pF
Common mode	<2 pF
Input resistance	
Differential mode	200 kΩ
Common mode	100 kΩ
Linearity	±2%
Noise	<50 nV/squareroot Hz

Using the same 20MHz BW as before and a 1R shunt: 280uA rms

You can 'cheat' by using a 10R shunt to get 28uA rms

… but you still need to buy the compatible scope

Noise from amplification chains



P_{drive} = –39 dBm; Z_0 = 50 Ω.

(1) V_{CC} = 2.7 V; T_{amb} = 85 °C; I_{CC} = 4.90 mA

(2) V_{CC} = 2.7 V; T_{amb} = –40 °C; I_{CC} = 4.70 mA

(3) V_{CC} = 3.0 V; T_{amb} = 25 °C; I_{CC} = 5.70 mA

(4) V_{CC} = 3.3 V; T_{amb} = 85 °C; I_{CC} = 6.70 mA

(5) V_{CC} = 3.3 V; T_{amb} = –40 °C; I_{CC} = 6.60 mA

Fig 11. Noise figure as function of frequency; typical values

‘Noise Figure’, yet another unit…

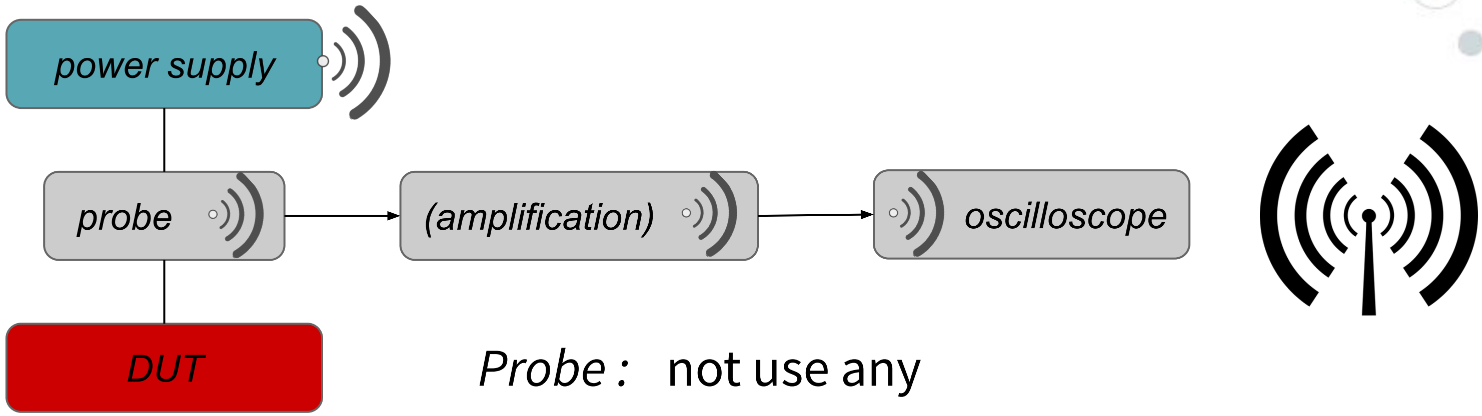
TLDR: how much noise an amplifier adds, compared to an ideal one

> for a 3.6dB NF amplifier, 20MHz BW

→ 2.81uV rms (2.81uA rms for a 1R shunt)

10x better than our probes (and for $0.3)

So how to optimize for noise ?



Probe :	not use any
Environment :	tin foil (hat)
Power Supply :	batteries or heavy filtering
Amplification Chain :	amplifiers with low noise figure
Measurement Instrument :	amplify enough so the input noise doesn’t matter

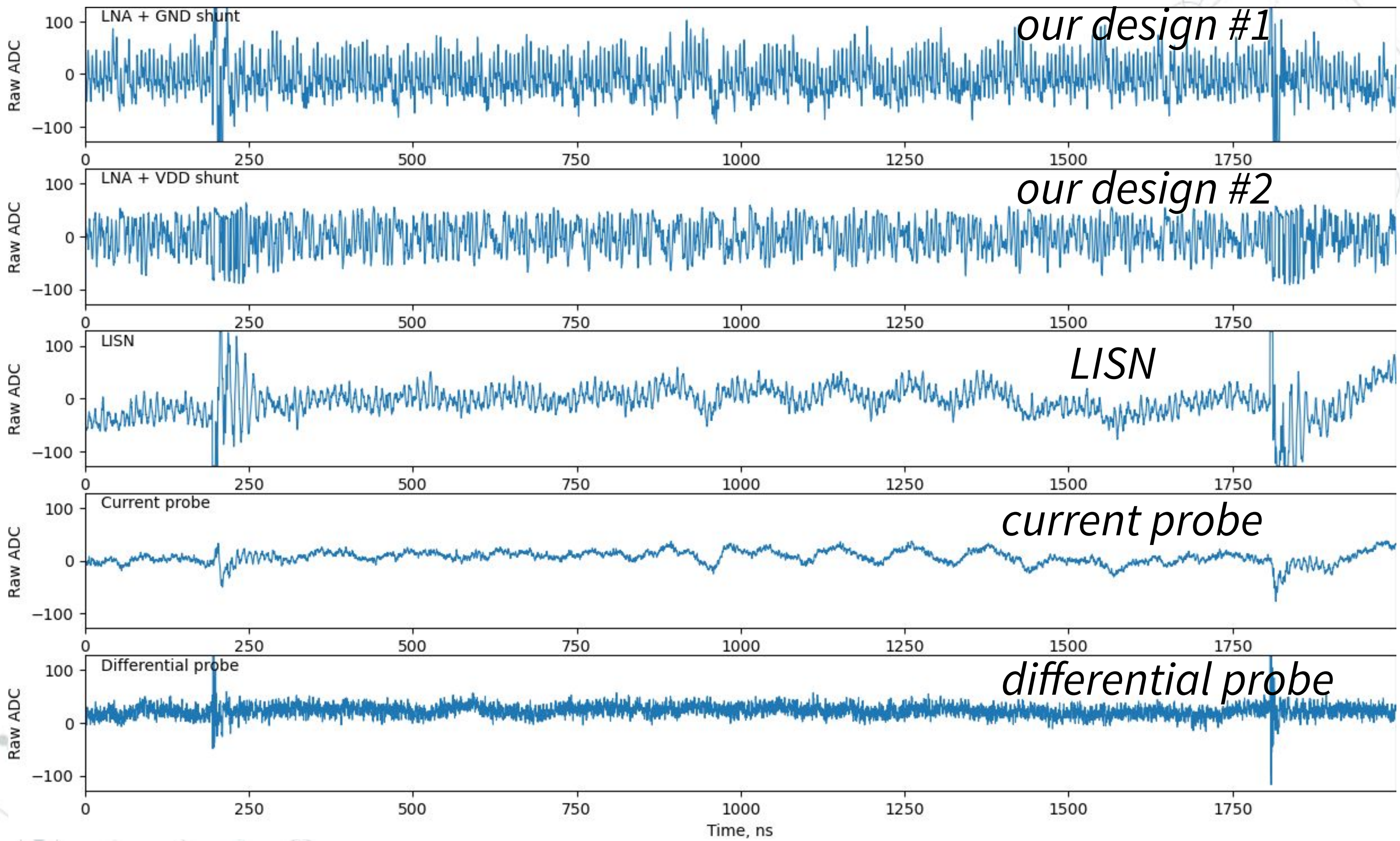
→ essentially doing the same as any RF receiver before digitization !

→ allowing you to use a cheap second hand scope

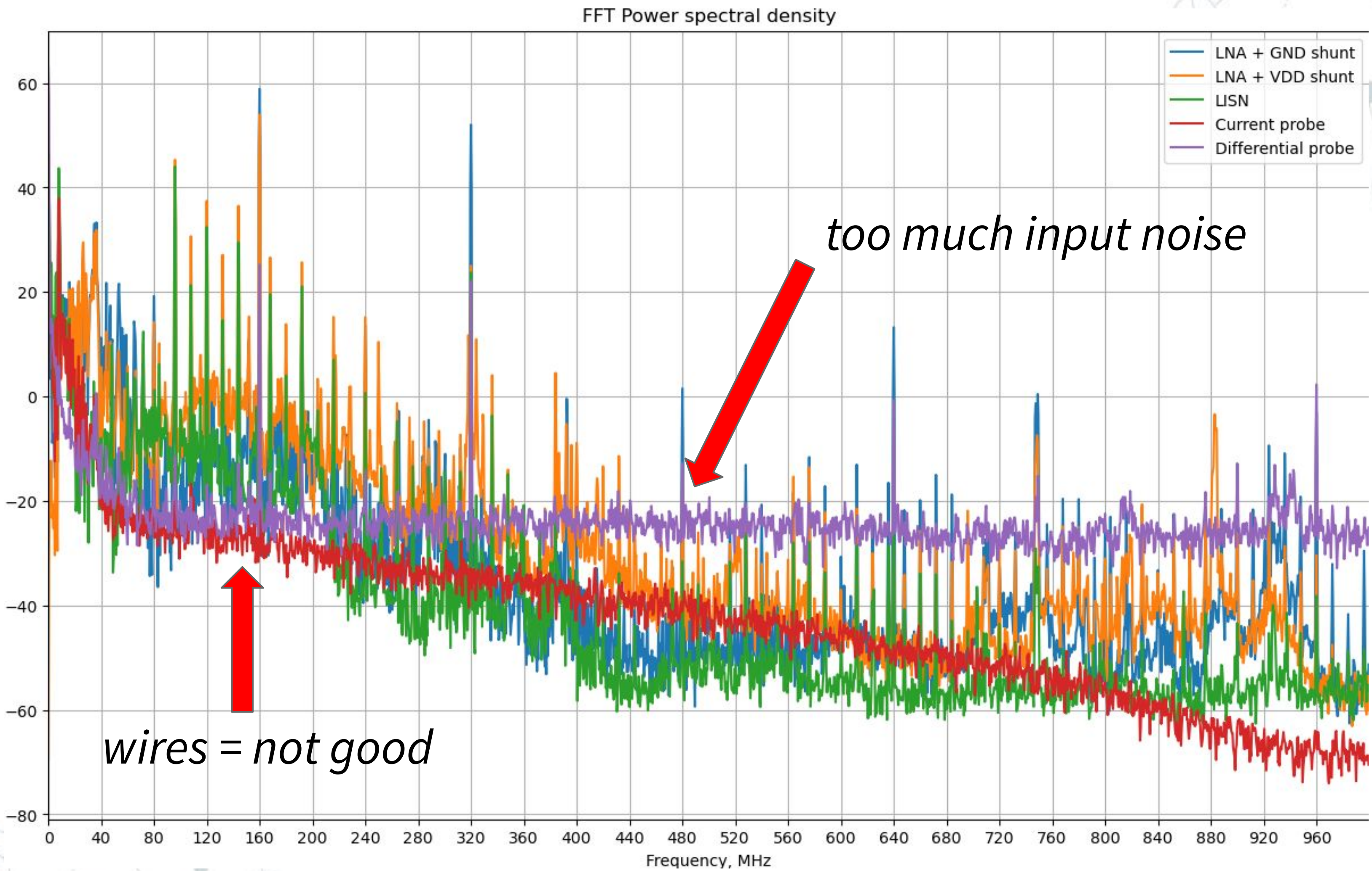
Bandwidth, gain, input noise…

Let’s confirm our analysis by comparing measurement methods on an ideal setup

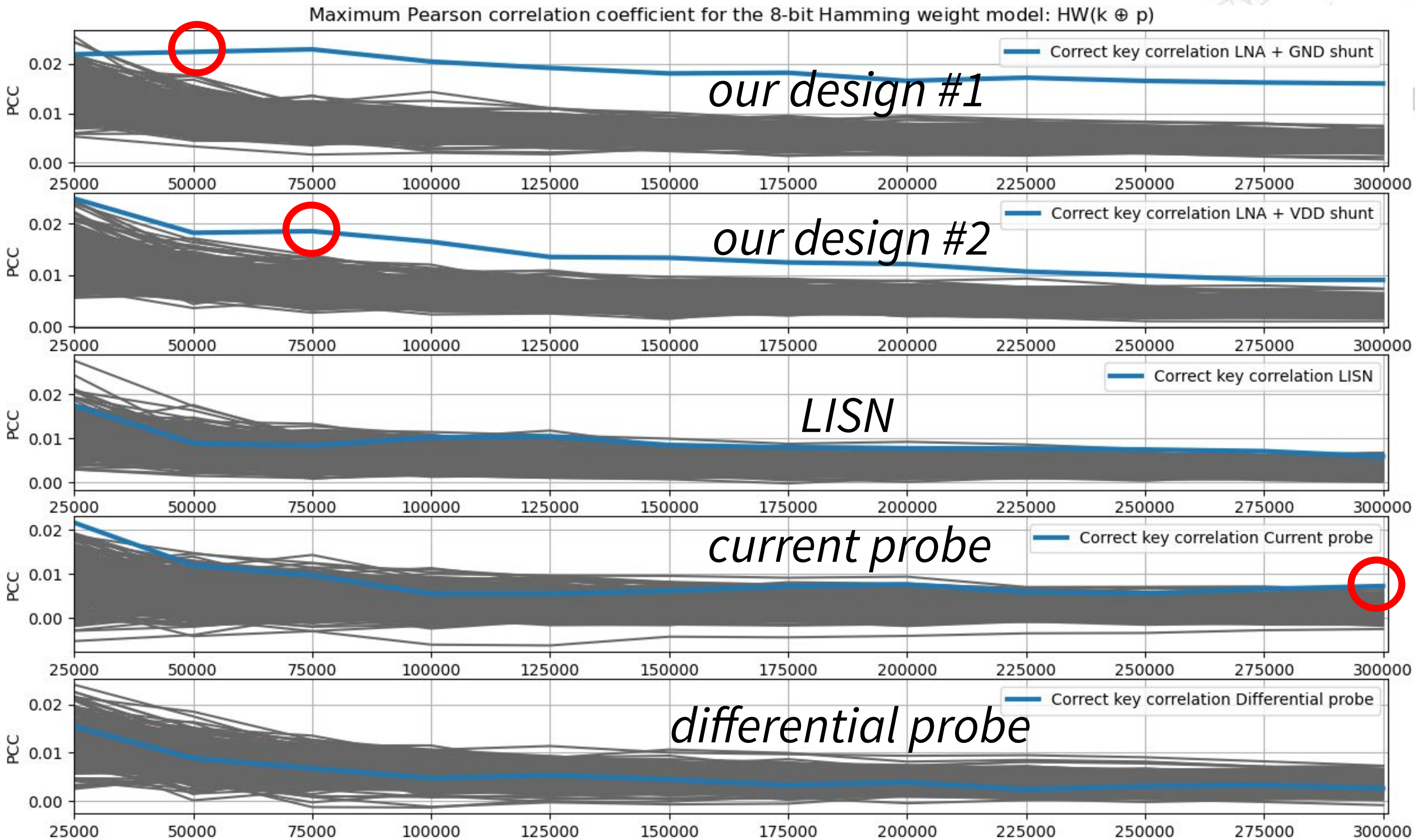
Comparing probes - time domain



Comparing probes - frequency domain



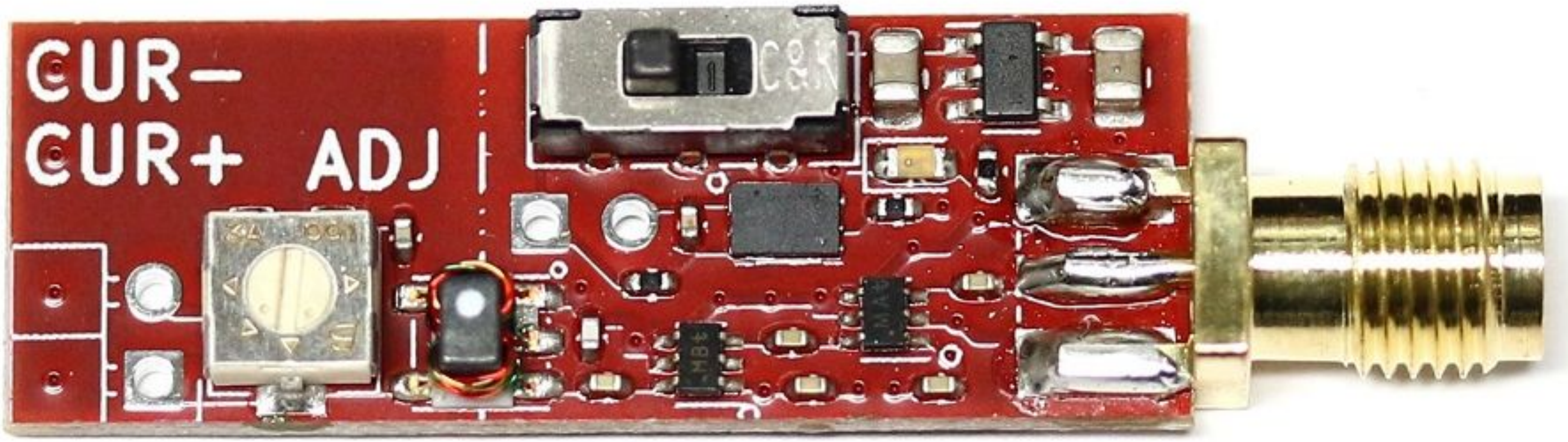
Comparing probes - actual attack



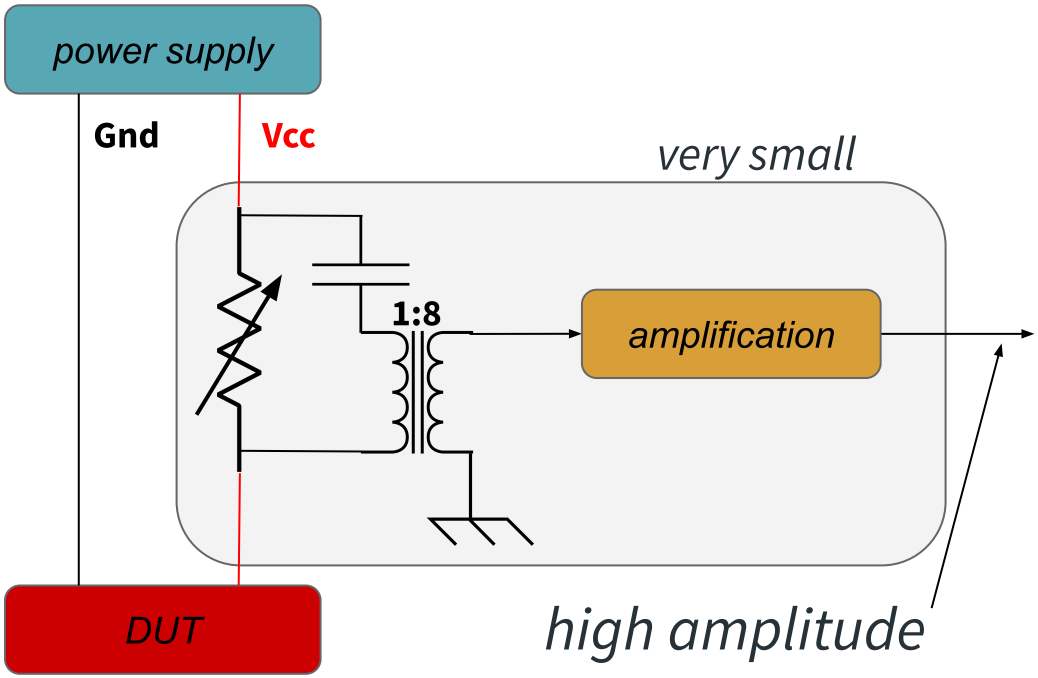
→ *less than 100k traces needed for our platforms !*

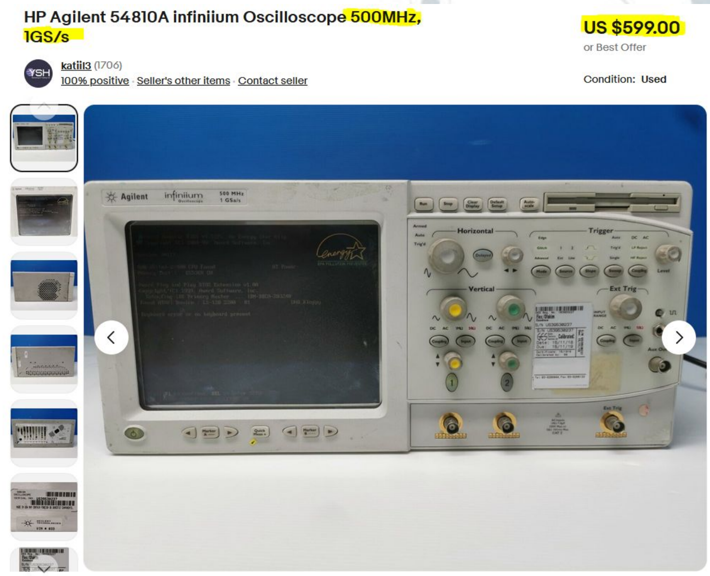
So how did we do it?

Approach #2



Approach #2





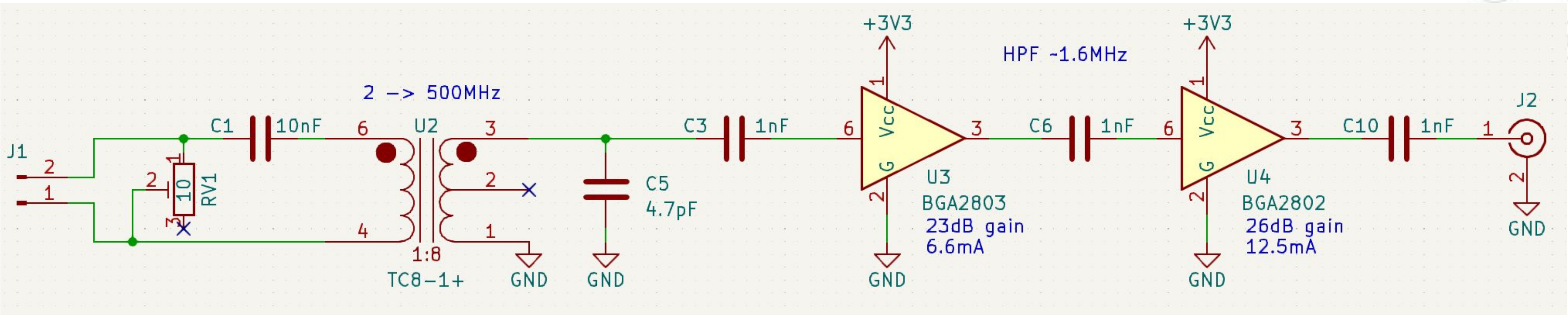
→ meant to be inserted into a DUT board (with its LDOs)

→ … or standalone if you provide clean power

→ isolated output = no ground loops !

→ $25, we have some with us!

Approach #2

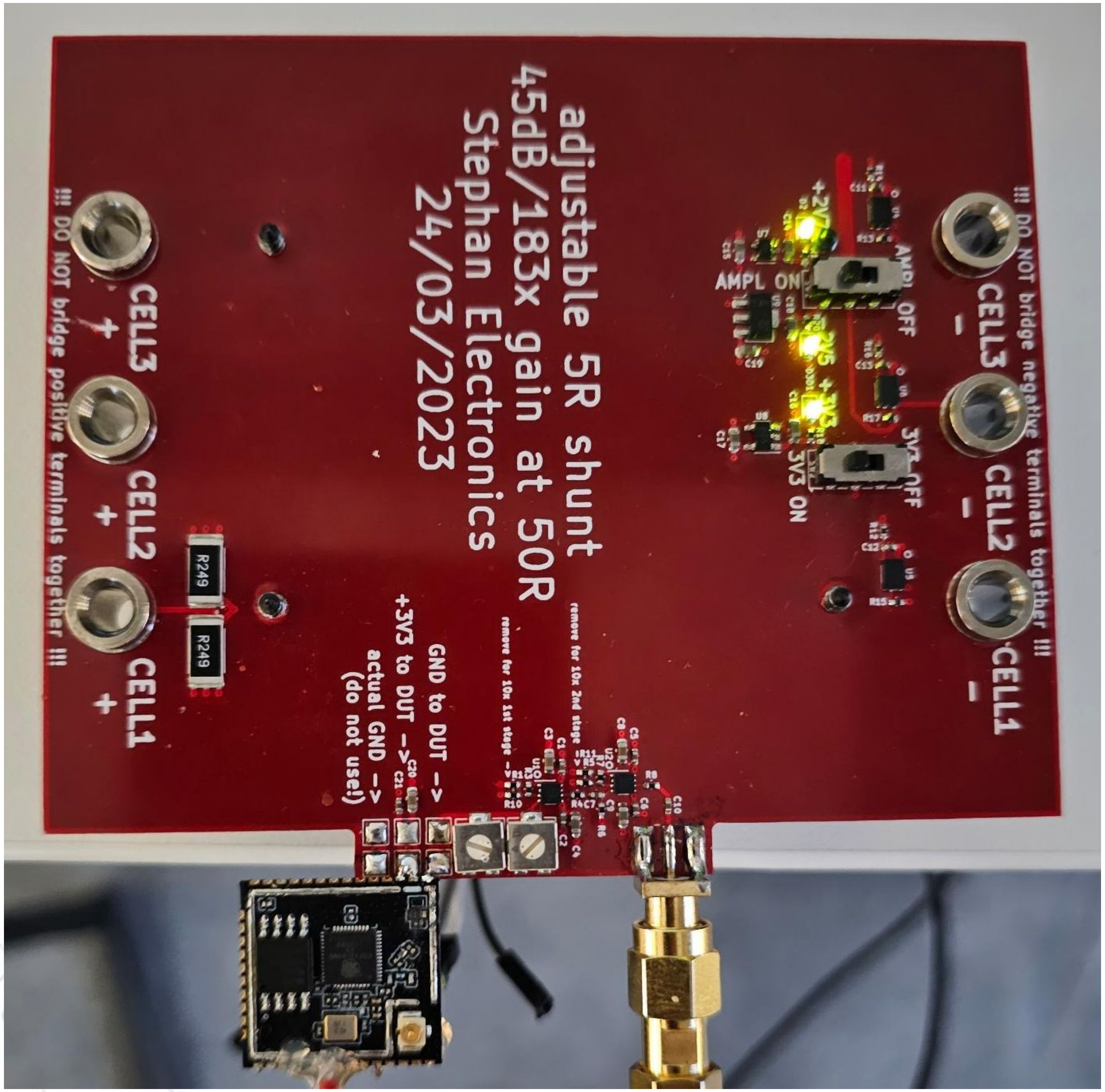


→ 1:8 balun to 'show' low impedance to the DUT

→ 2GHz low noise amplifiers

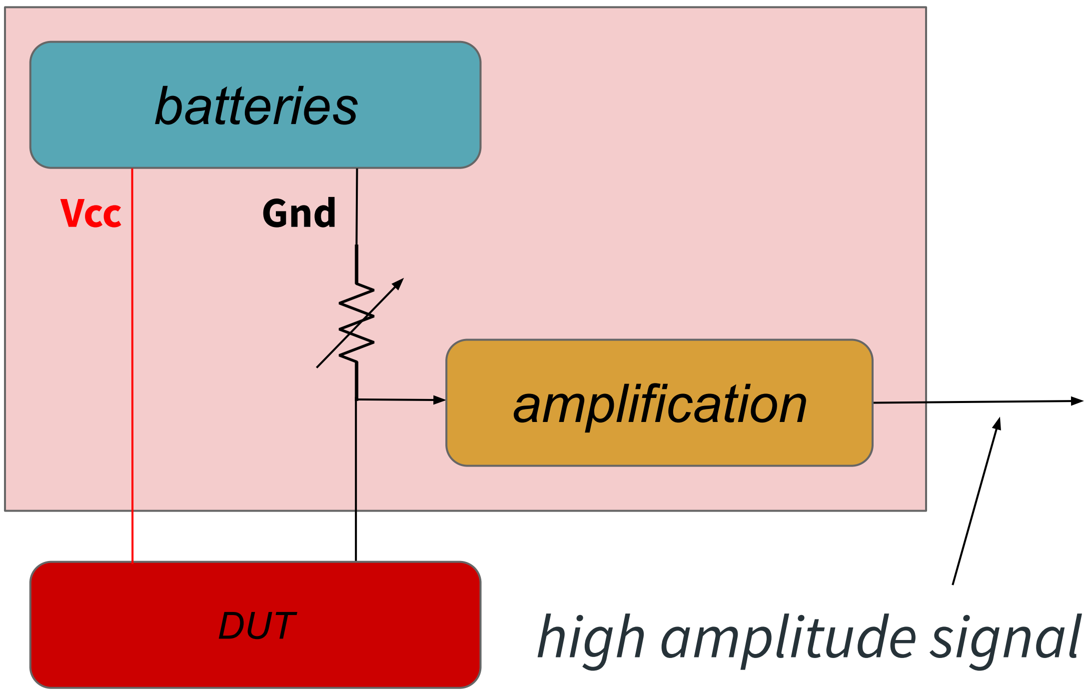
→ more details on www.limpkin.fr

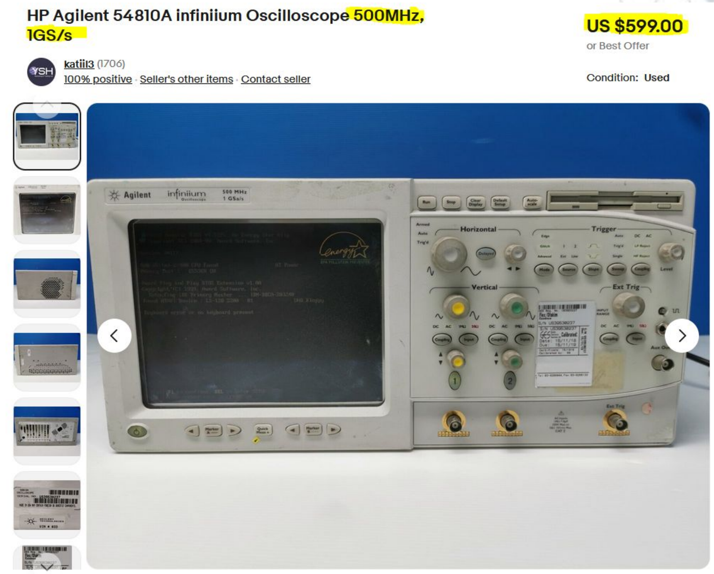
Approach #1



adjustable 5R shunt
45dB/183x gain at 50R
Stephan Electronics
24/03/2023
!!! DO NOT bridge positive terminals together !!!
!!! DO NOT bridge negative terminals together !!!
CELL3 +
CELL2 +
CELL1 +
CELL3 -
CELL2 -
CELL1 -
R249
R249
AMPL ON
AMPL OFF
3V3 ON
3V3 OFF
+2V7
GND to DUT -->
+3V3 to DUT -->
actual GND -->
(do not use!)

Approach #1



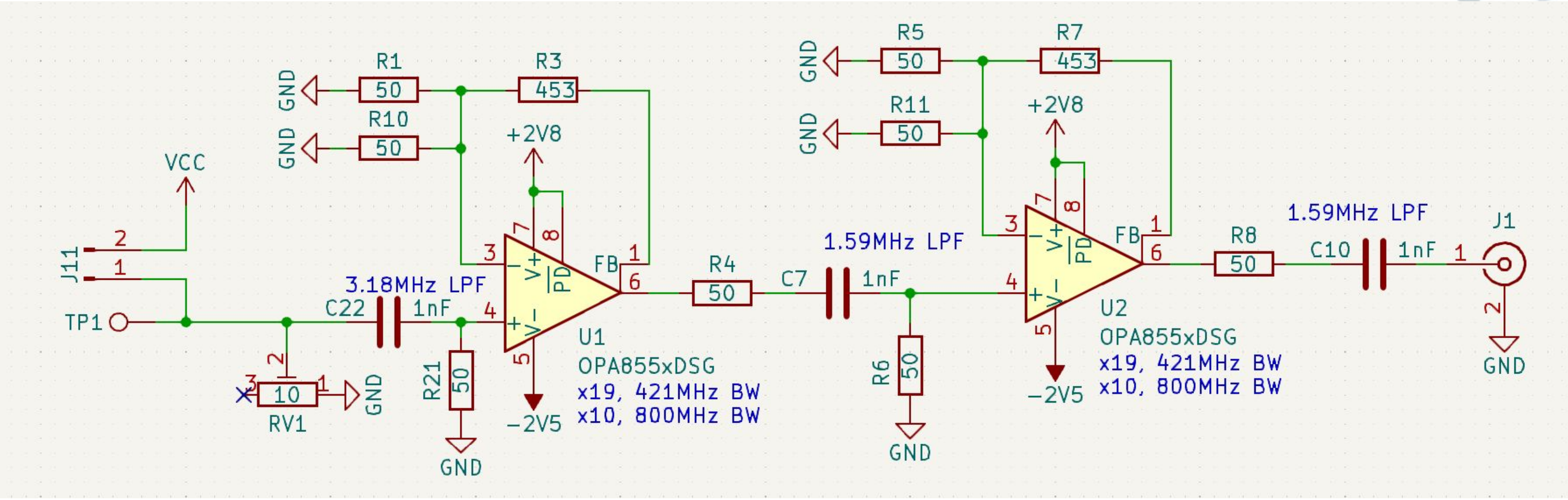


→ provides power to your attack target (1.2V/1.8V/3.3V)

→ will be released in a week or two

→ limpkin@limpkin.fr / www.limpkin.fr

Approach #1



→ low side shunt-based current sensing

→ 8GHz GBW low noise amplifiers

→ more details on www.limpkin.fr soon

In conclusion

To be the best side channel hacker out there:

- Do not use wires, probes, power supplies
- Remove decoupling capacitors
- Use a <u>cheap</u> scope
- … with our <u>cheap</u> boards

We have some $25 boards with us if you want !
… other boards to be released soon
www.limpkin.fr