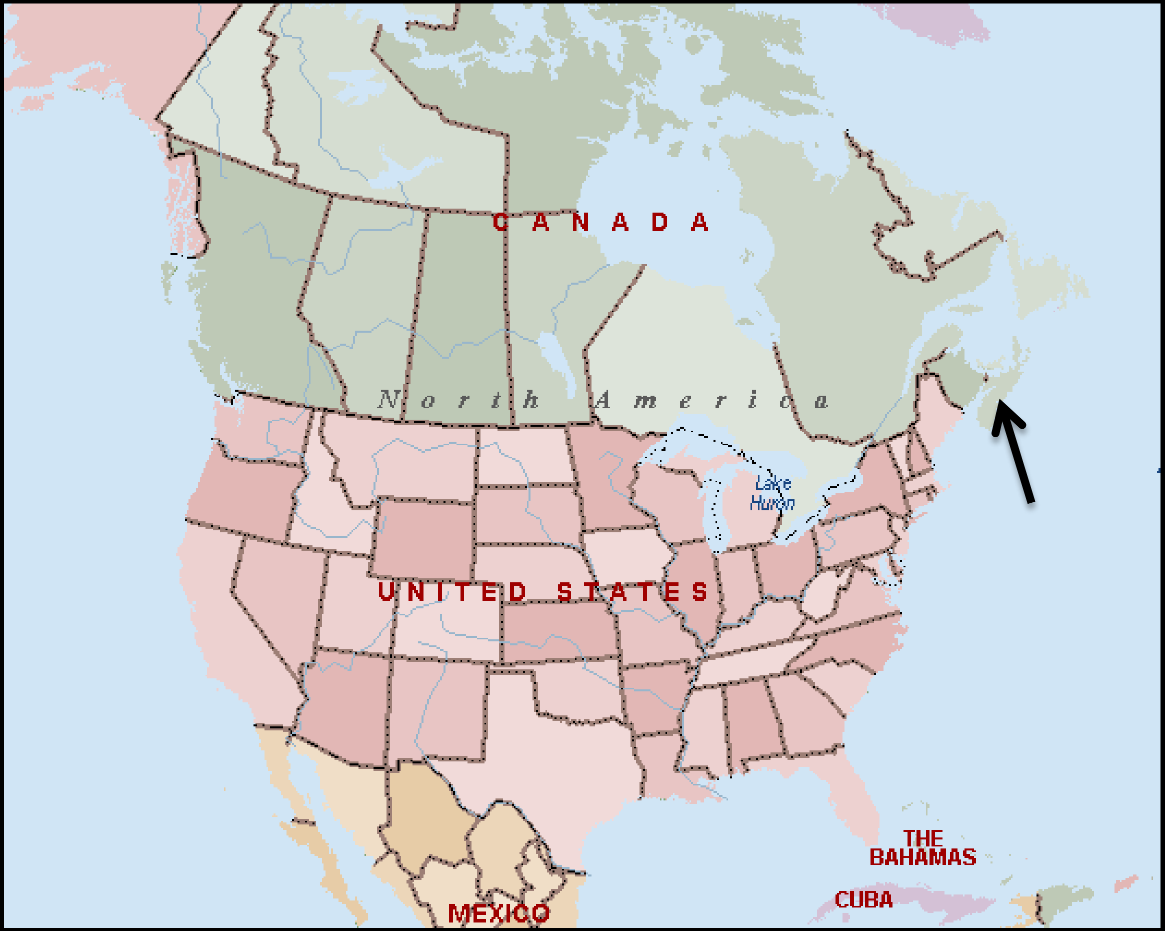
black hat EU 2013

SIDE CHANNEL ANALYSIS FOR CHEAPSKATES

BLACKHAT PRESENTATION

COLIN O'FLYNN

Colin O'Flynn



My Funding Provided By:

OZ Optics
Global Leader In Fiber Optic Products Since 1985
www.ozoptics.com

DALHOUSIE UNIVERSITY
Inspiring Minds

Special Thanks:

Cryptography Research Inc

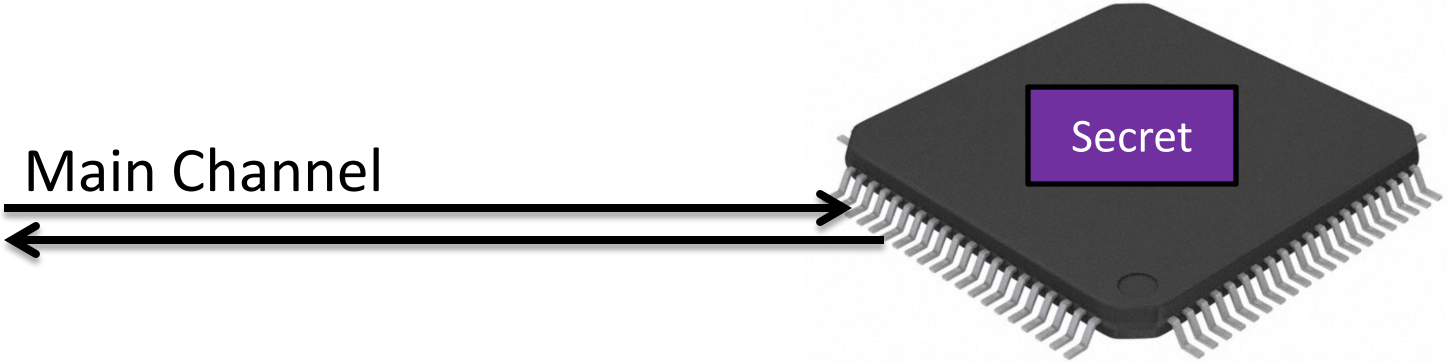
Blackhat Organizers & Sponsors

The Way Forward

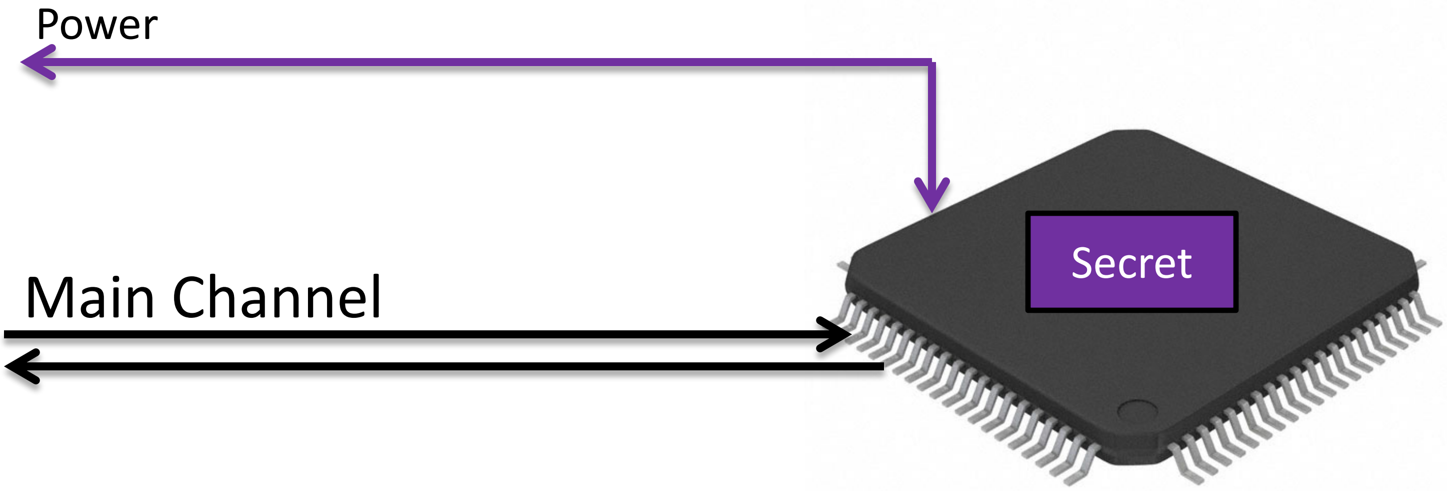
- What is Side Channel Analysis (SCA) – 15 mins
- Your First Attack! – 10 mins
- *ChipWhisperer* Software – 10 mins
- Waveform Acquisition – 5 mins
- Amplifiers/Front-End Stuff – 5 mins
- Measuring Current in Real Devices? – 5 mins
- Where to go from Here? – 5 mins

The Side Channel

Side Channel?



Side Channel?



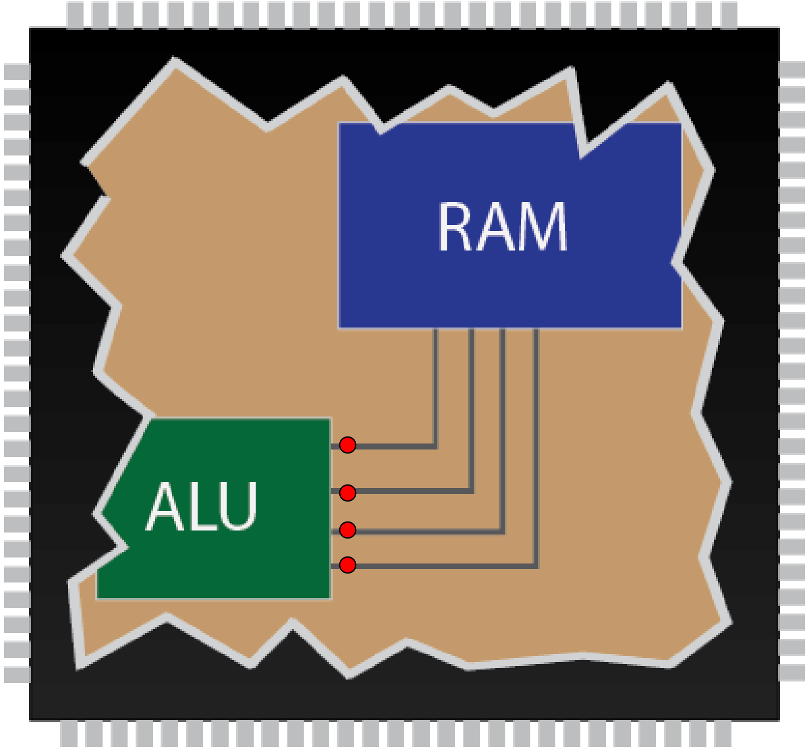
Power

Main Channel

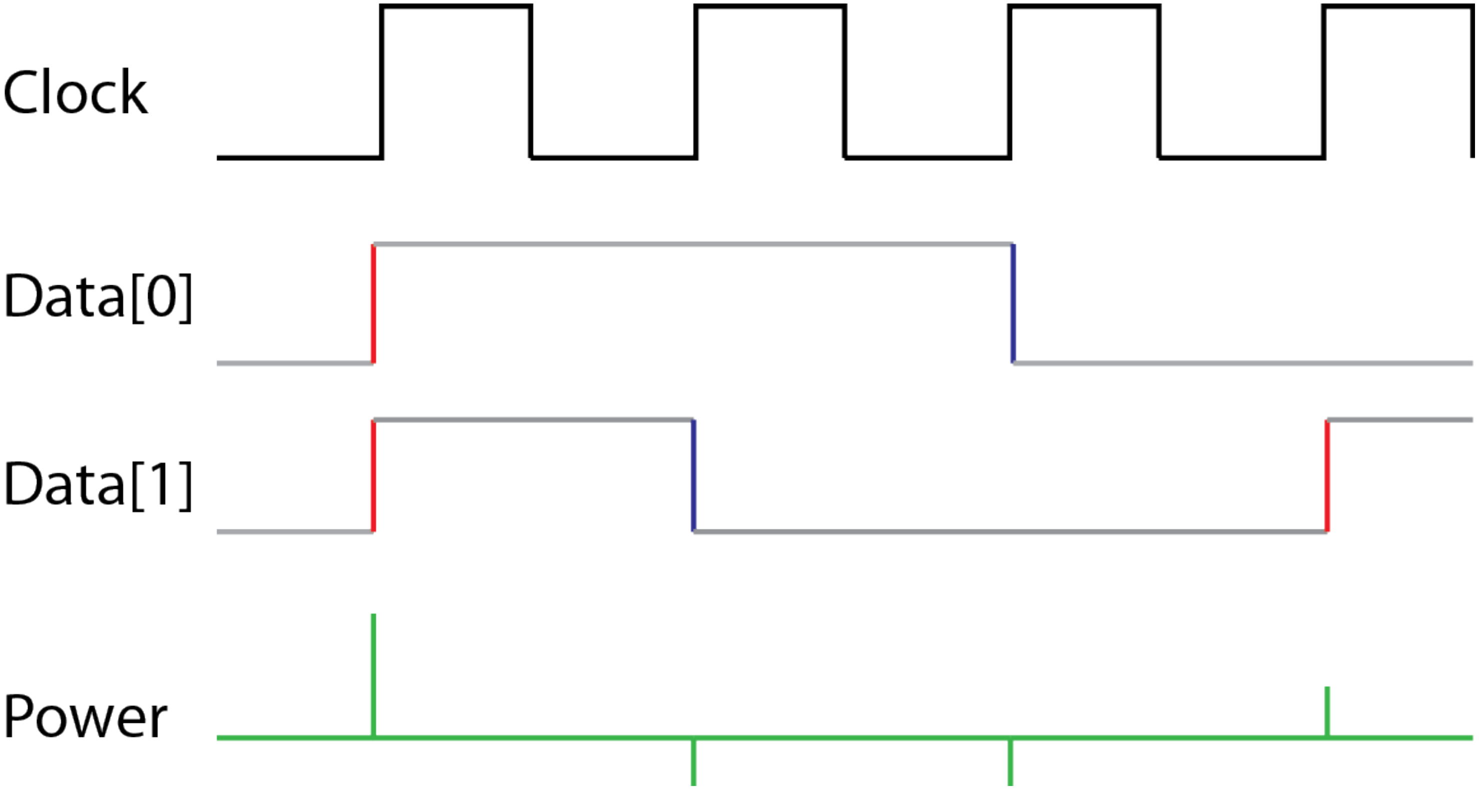
Secret

Power Channel.

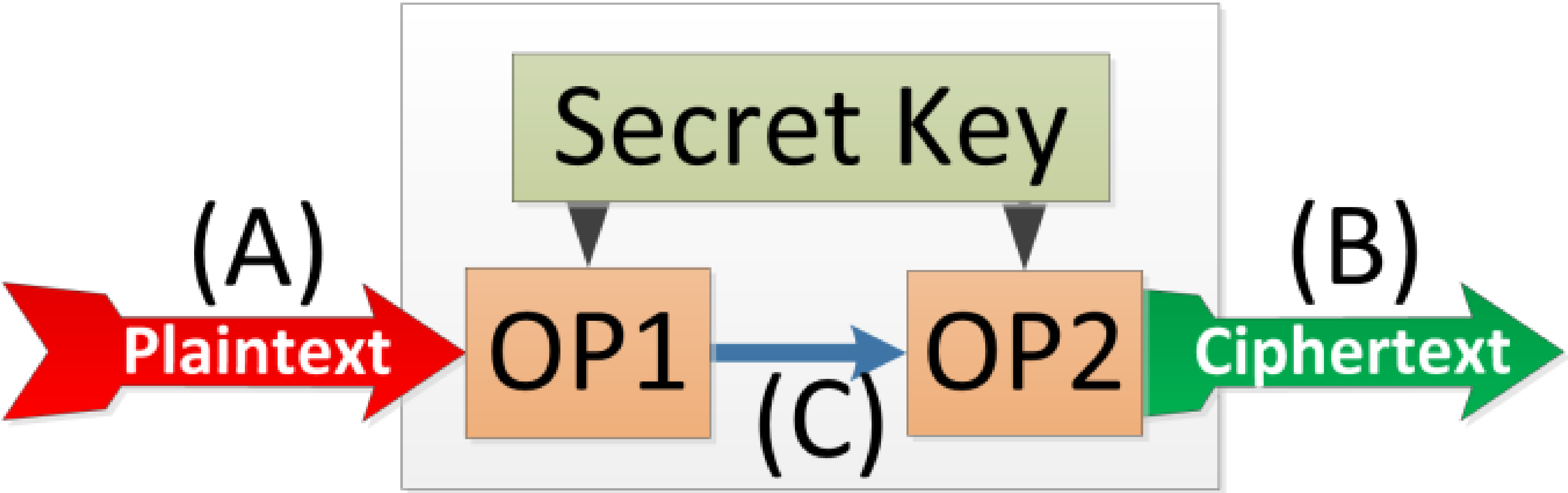
Power Channel.



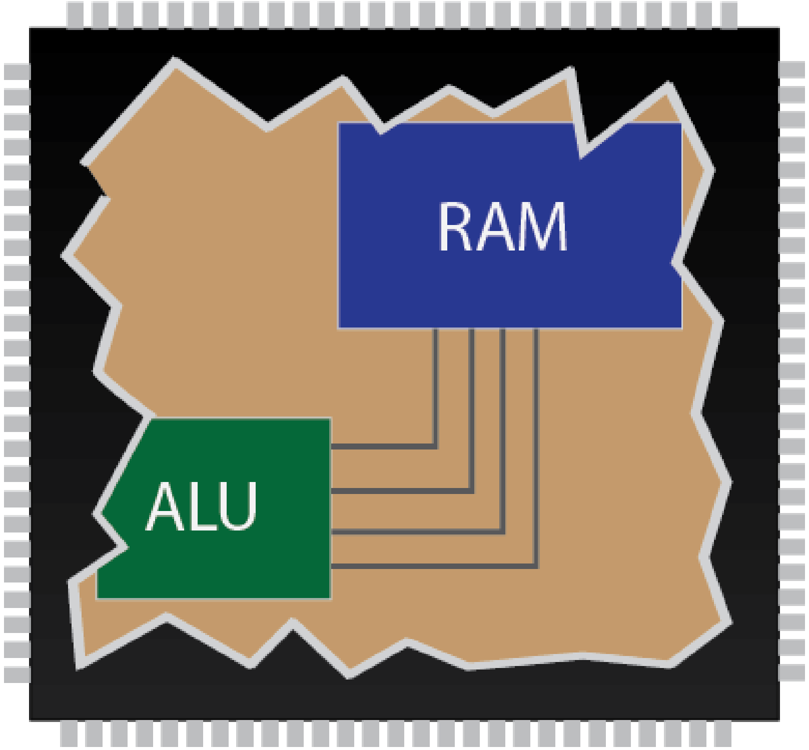
Power Channel.



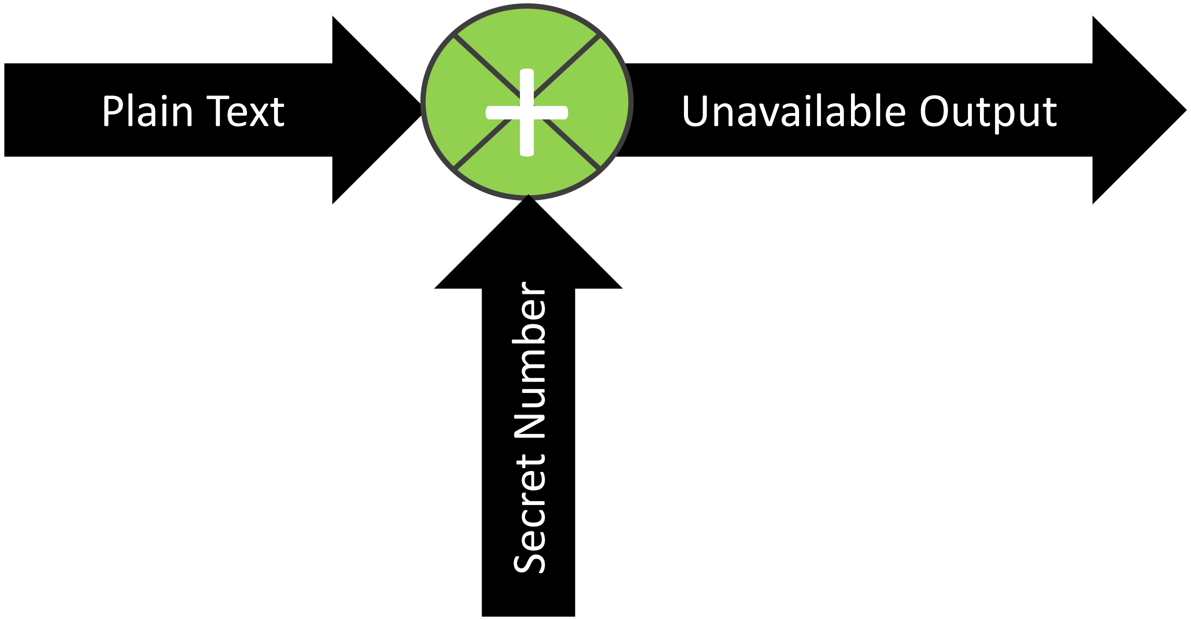
Side Channel.



Simple 4-Bit Example



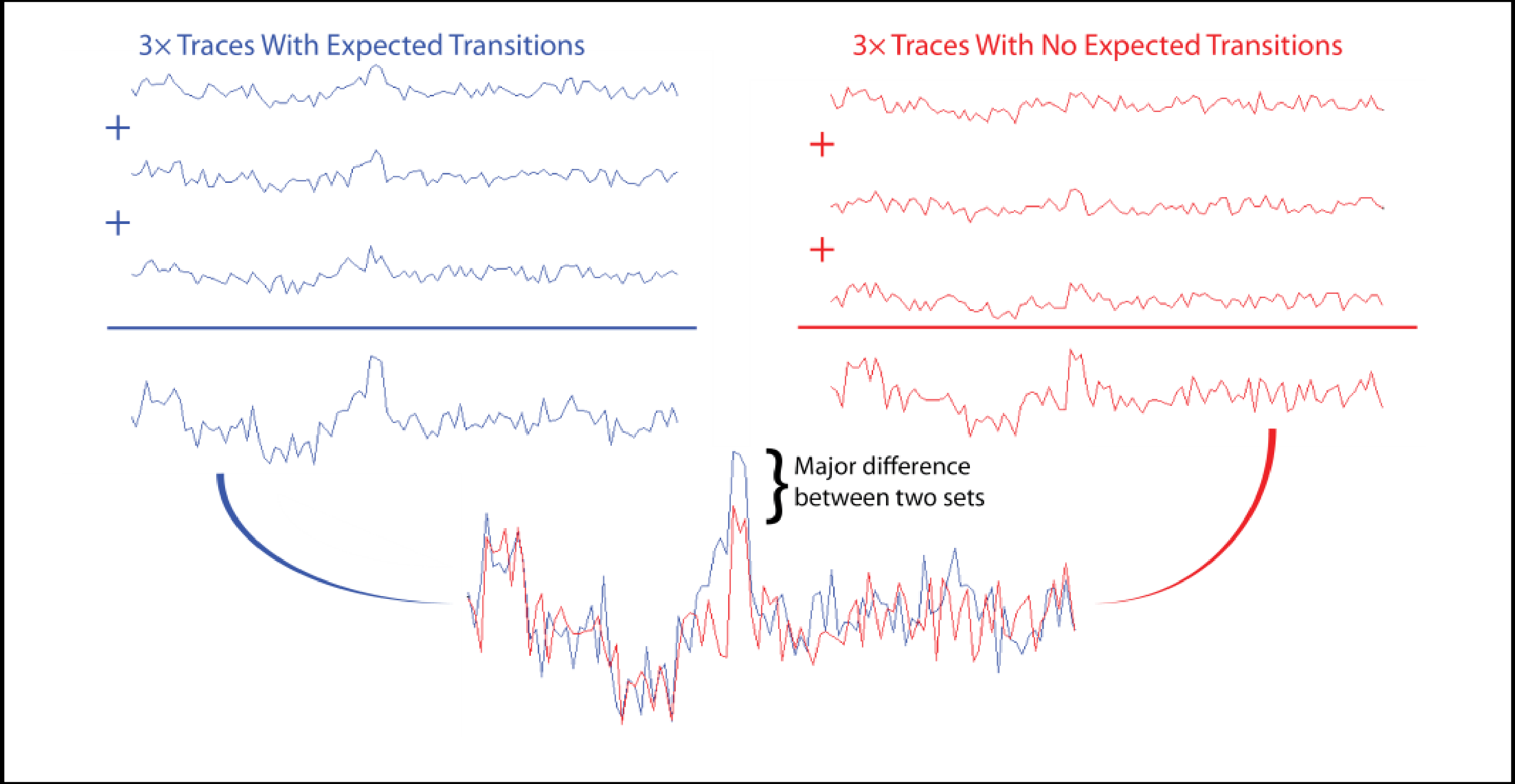
Simple 4-Bit Example



Simple 4-Bit Example

Input Plaintext	Hyp. Secret Number	Hyp. Bit 0 Value
4	2	0
7	2	1
2	2	0
1	2	1
0	2	0
6	2	0
5	2	1

Differential Power Analysis


3× Traces With Expected Transitions
+
+
3× Traces With No Expected Transitions
+
+
Major difference between two sets

Differential Power Analysis

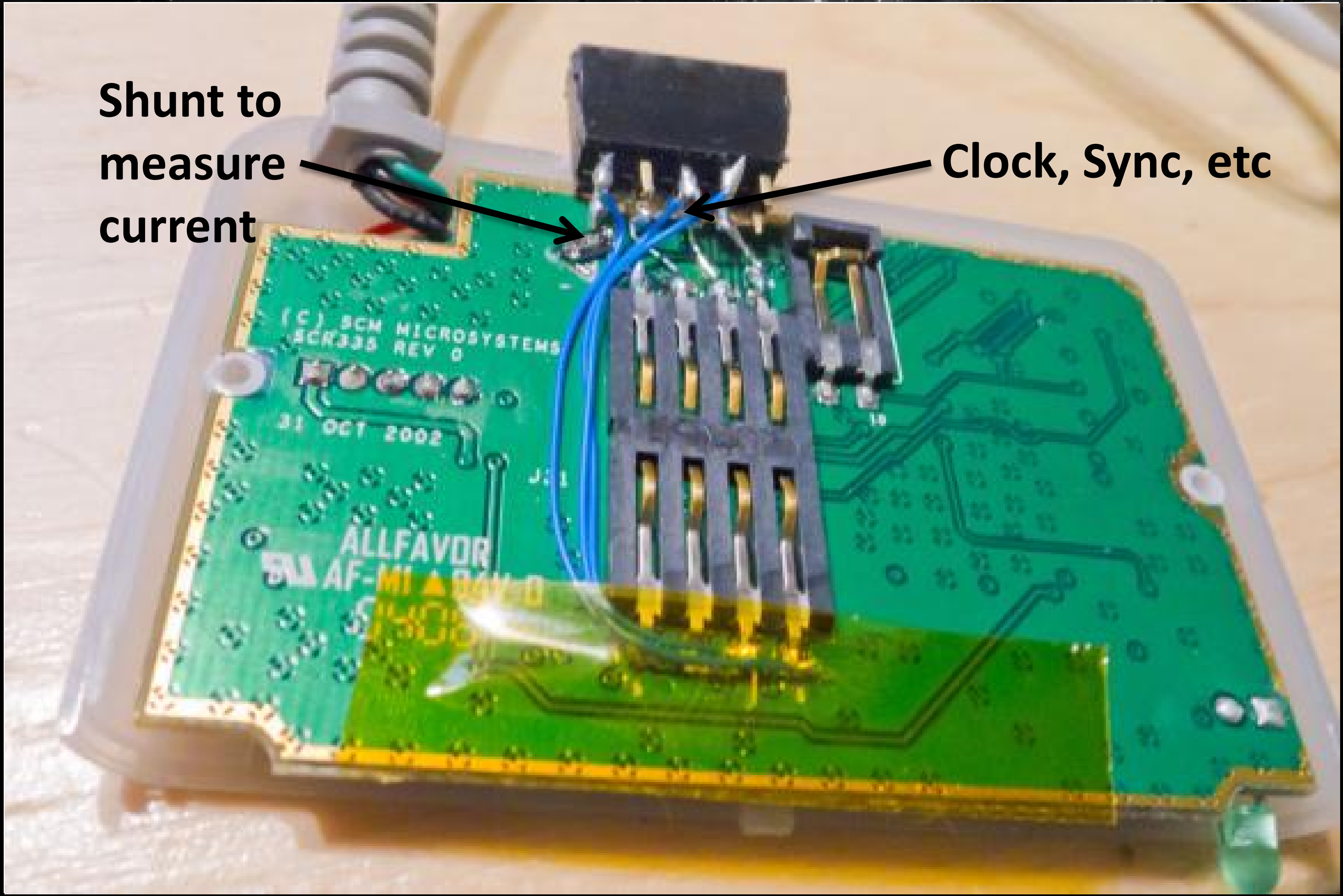
1. Input many plaintexts & measure power
2. Target a single bit in each byte.
3. Make a guess of what key byte is. For each power trace, is this bit now a 1 or 0?
4. Split traces into two groups based on that bit
5. Find mean of each group, subtract
6. If guess is correct, we should see a big peak
7. Repeat 3-6 for all 256 possible bytes

```python
#For all 16 bytes of key
for bnum in range(0, 16):
    diffs = [0]*256
    #For each 0..0xFF possible value of the key byte
    for key in range(0, 256):
        #Initialize arrays & variables to zero
        mean1 = numpy.zeros(len(traces[0,pointstart:pointend]))
        mean0 = numpy.zeros(len(traces[0,pointstart:pointend]))
        num1 = 0
        num0 = 0

        #For each trace, do the following
        for tnum in range(len(traces)):
            #Generate the output of the SBOX
            Hyp = SBOX[int(plaintexts[tnum, bnum], 16) ^ key]

            #Is target bit 1 or target bit 0?
            if (Hyp & (1 << targetbit)) != 0:
                #Bit is 1, so add this trace to the 1 partition
                mean1 = numpy.add(mean1, traces[tnum,pointstart:pointend])
                num1 = num1 + 1
            else:
                #Bit is 0, so add this trace to the 0 partition
                mean0 = numpy.add(mean0, traces[tnum,pointstart:pointend])
                num0 = num0 + 1

        #Average
        mean1 = mean1 / num1
        mean0 = mean0 / num0

        #Find the difference between the two means
        diff = numpy.subtract(mean1, mean0)
        #Find the biggest difference for this specific key & store
        diffs[key] = max(numpy.fabs(diff))
    #From all the key candidates, select the largest difference as most likely
    print "%2x "%diffs.index(max(diffs)),
```

Your First Attack

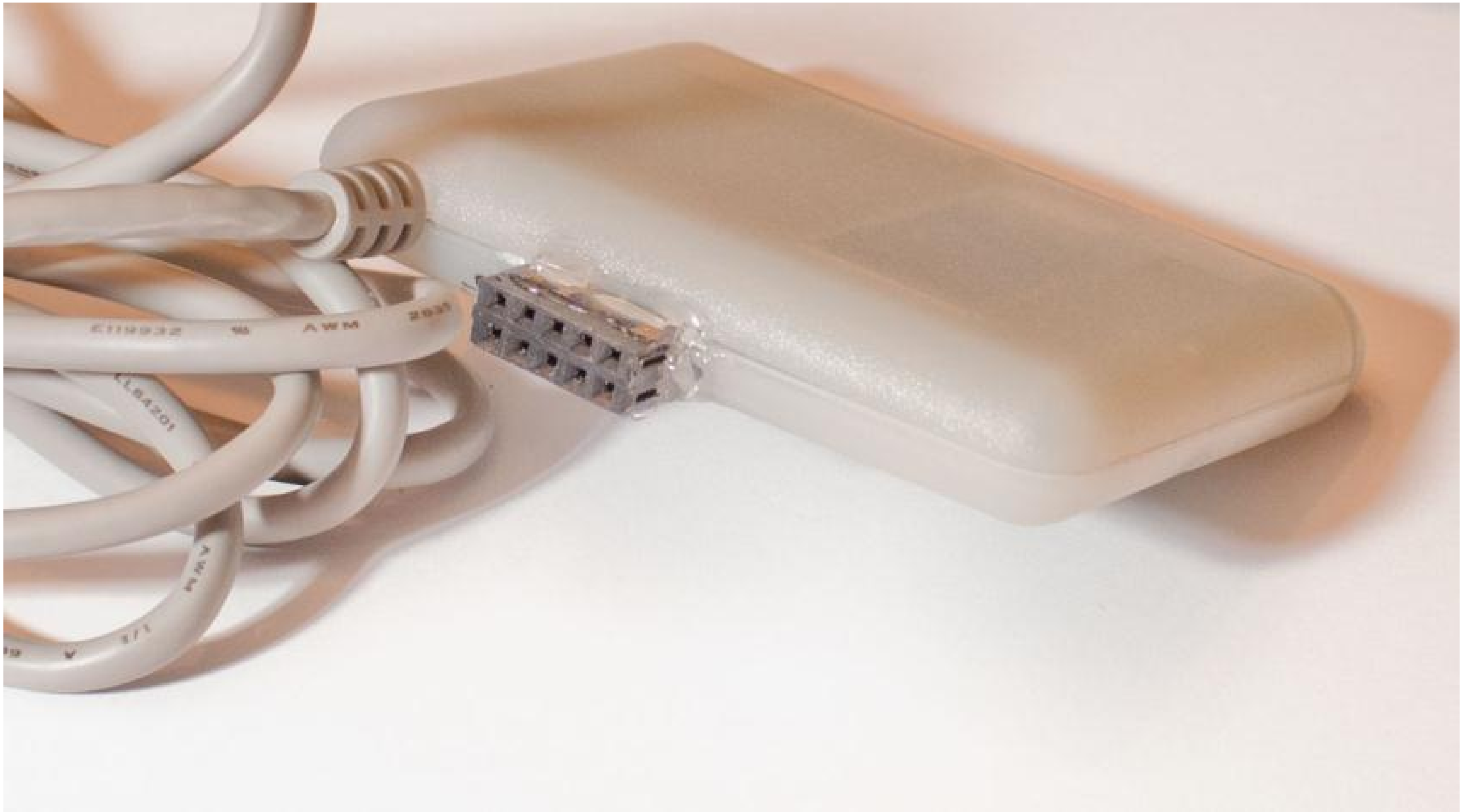
Should I Attack a Smartcard?

Attacks against Smart Card

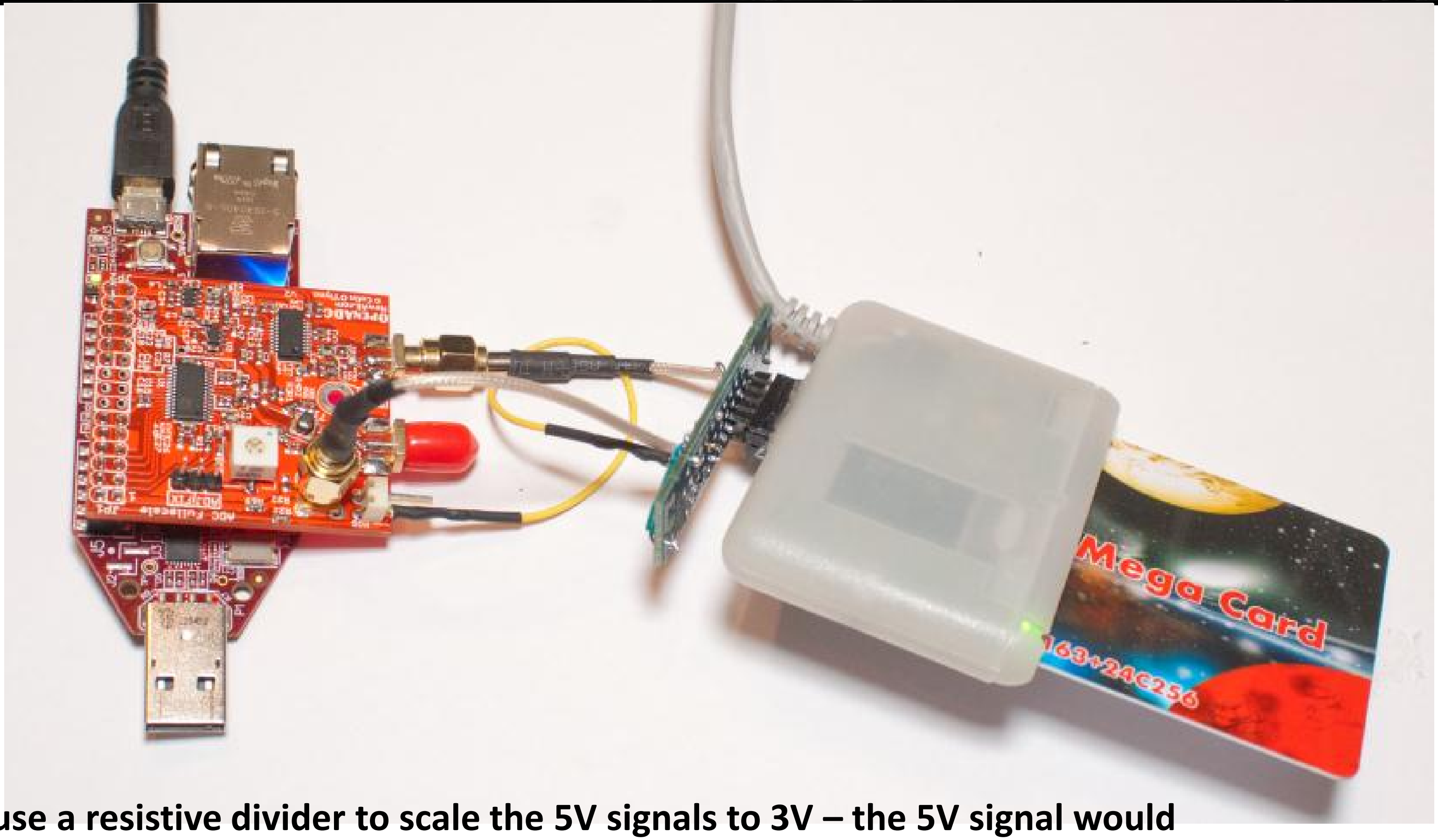


Shunt to measure current

Clock, Sync, etc

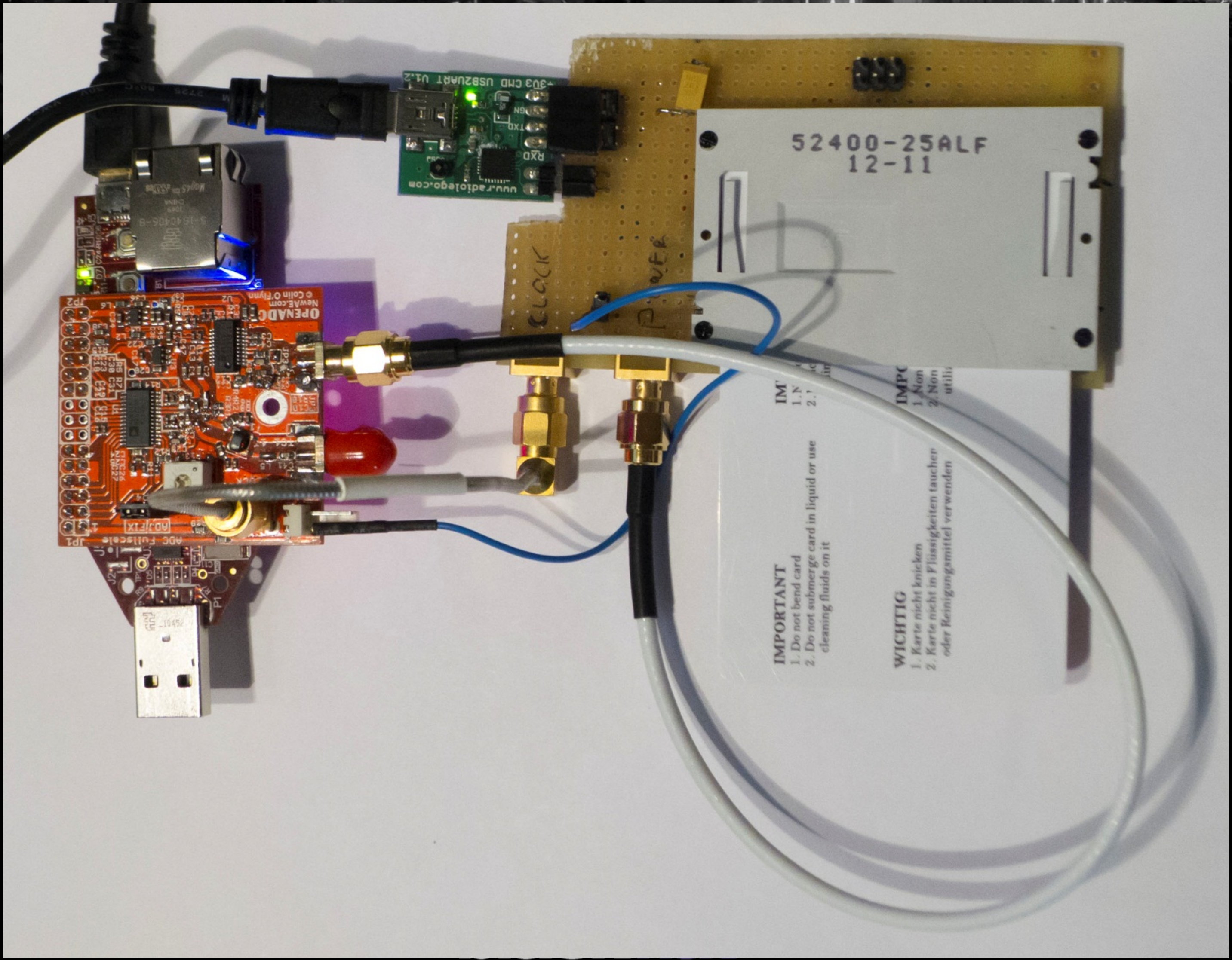

E119932
AWM
2835
LL84201
AWM
1/1

SmartCard Capture

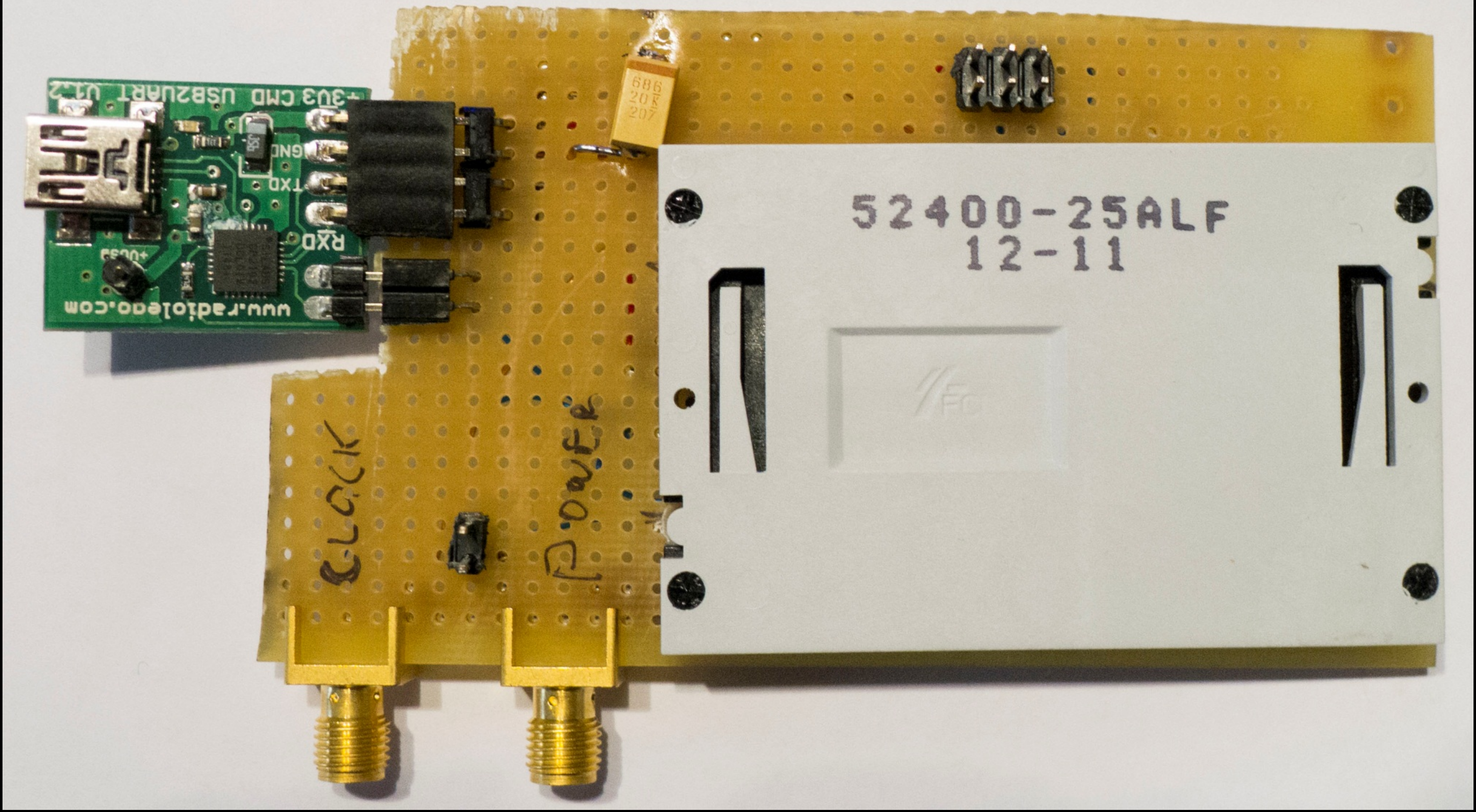


Note we use a resistive divider to scale the 5V signals to 3V – the 5V signal would immediately destroy the FPGA board!

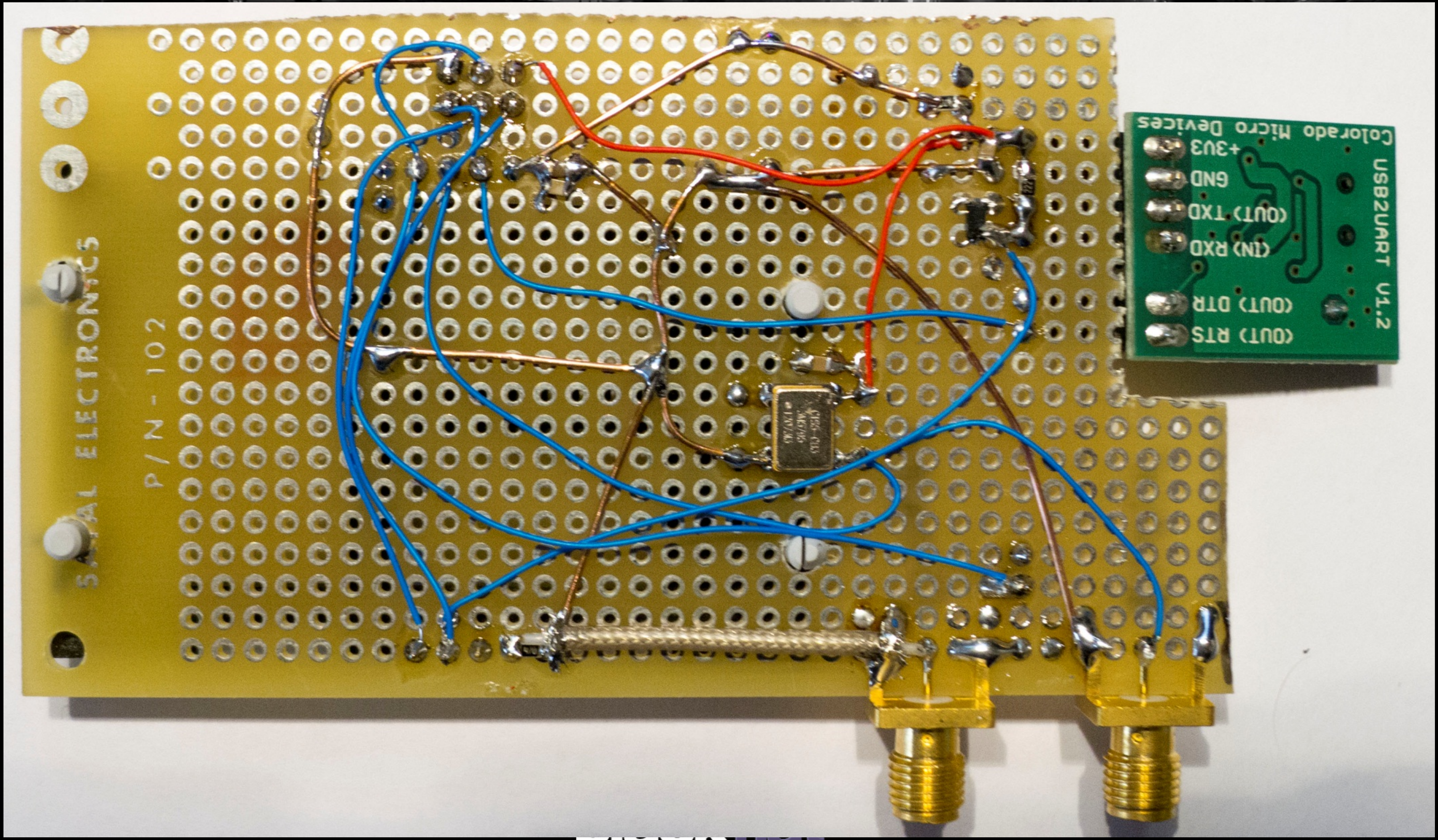
SmartCard Capture - Cheap



SmartCard Capture - Cheap



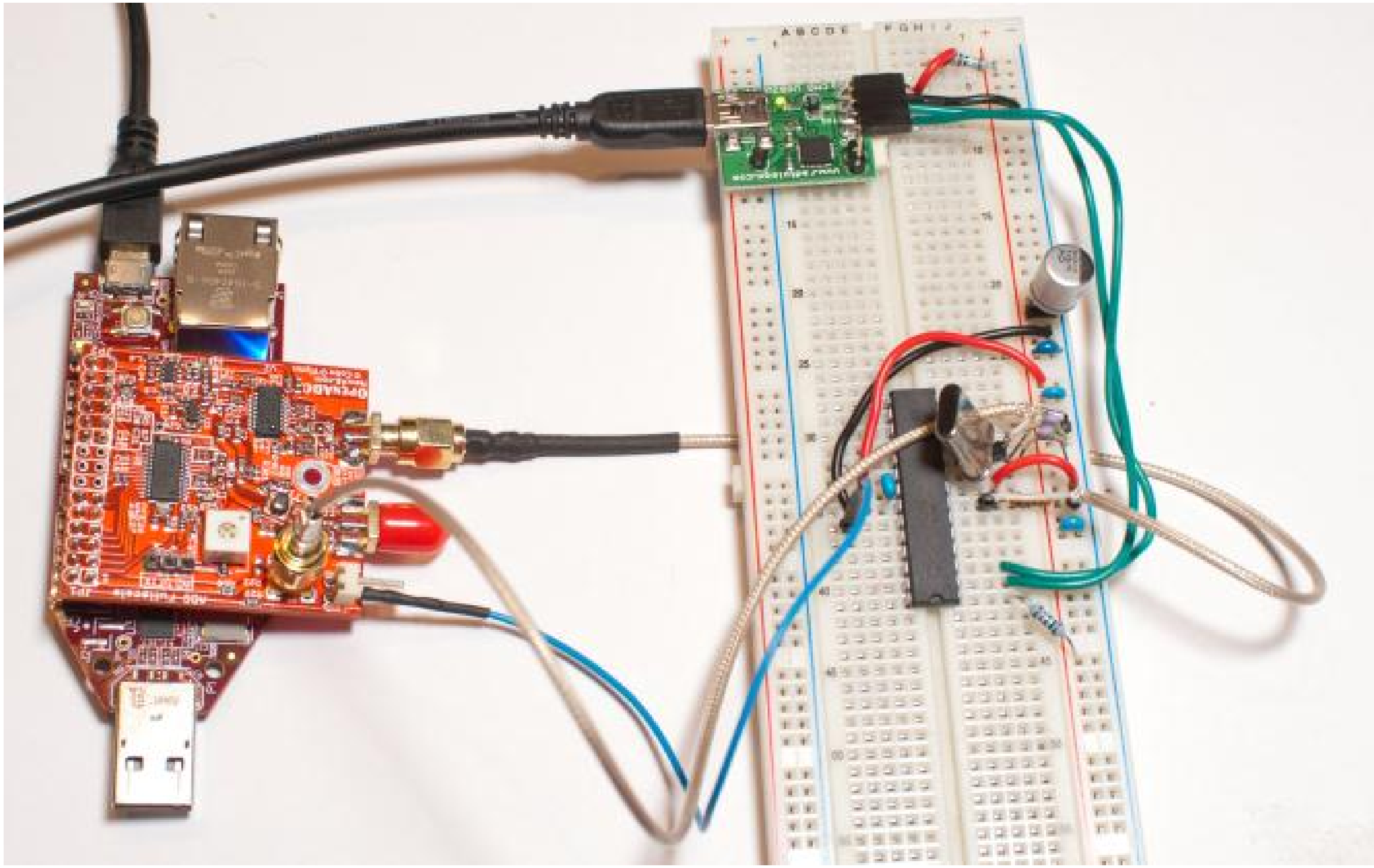
SmartCard Capture - Cheap



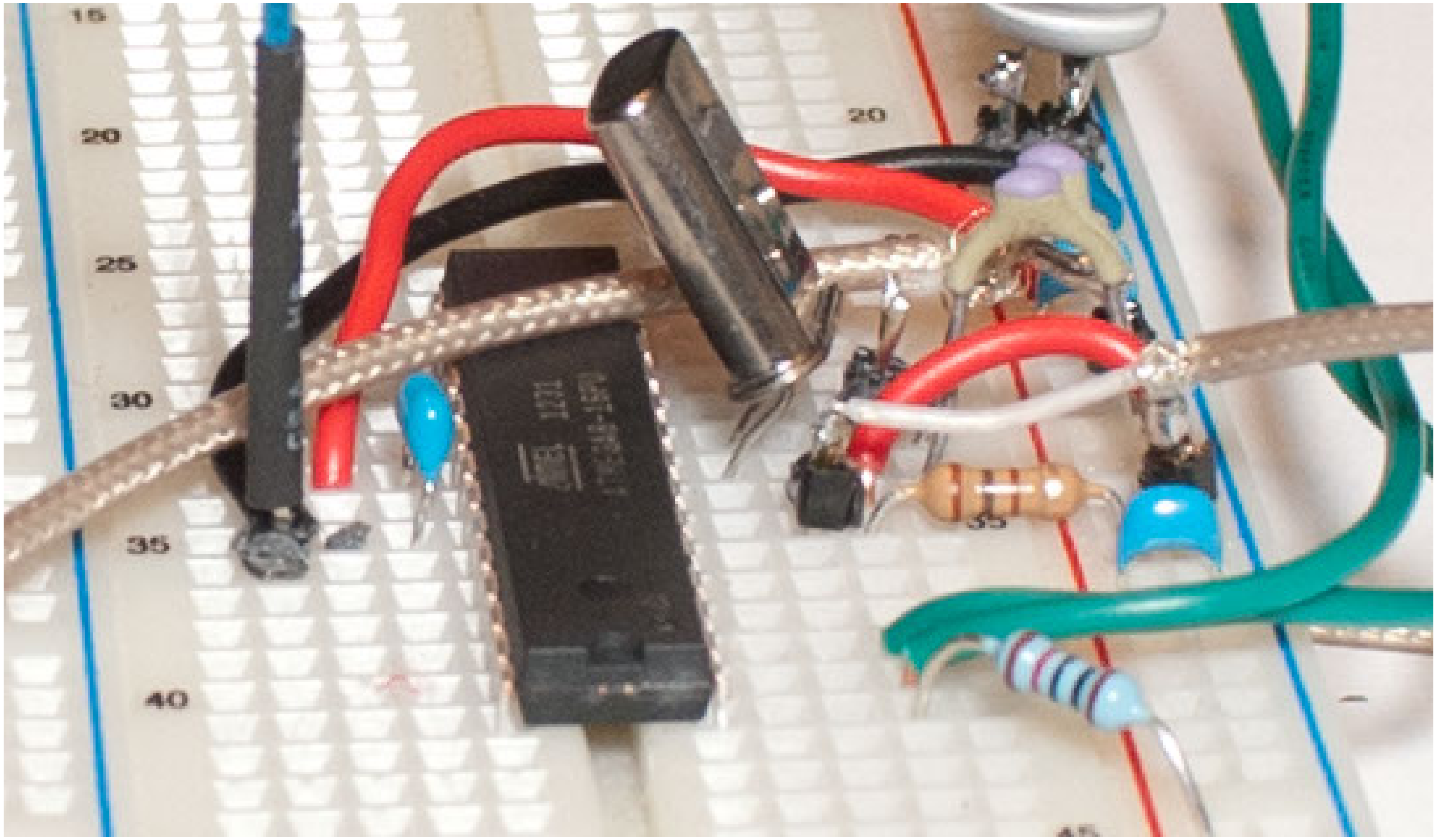
So What do you Do?

=

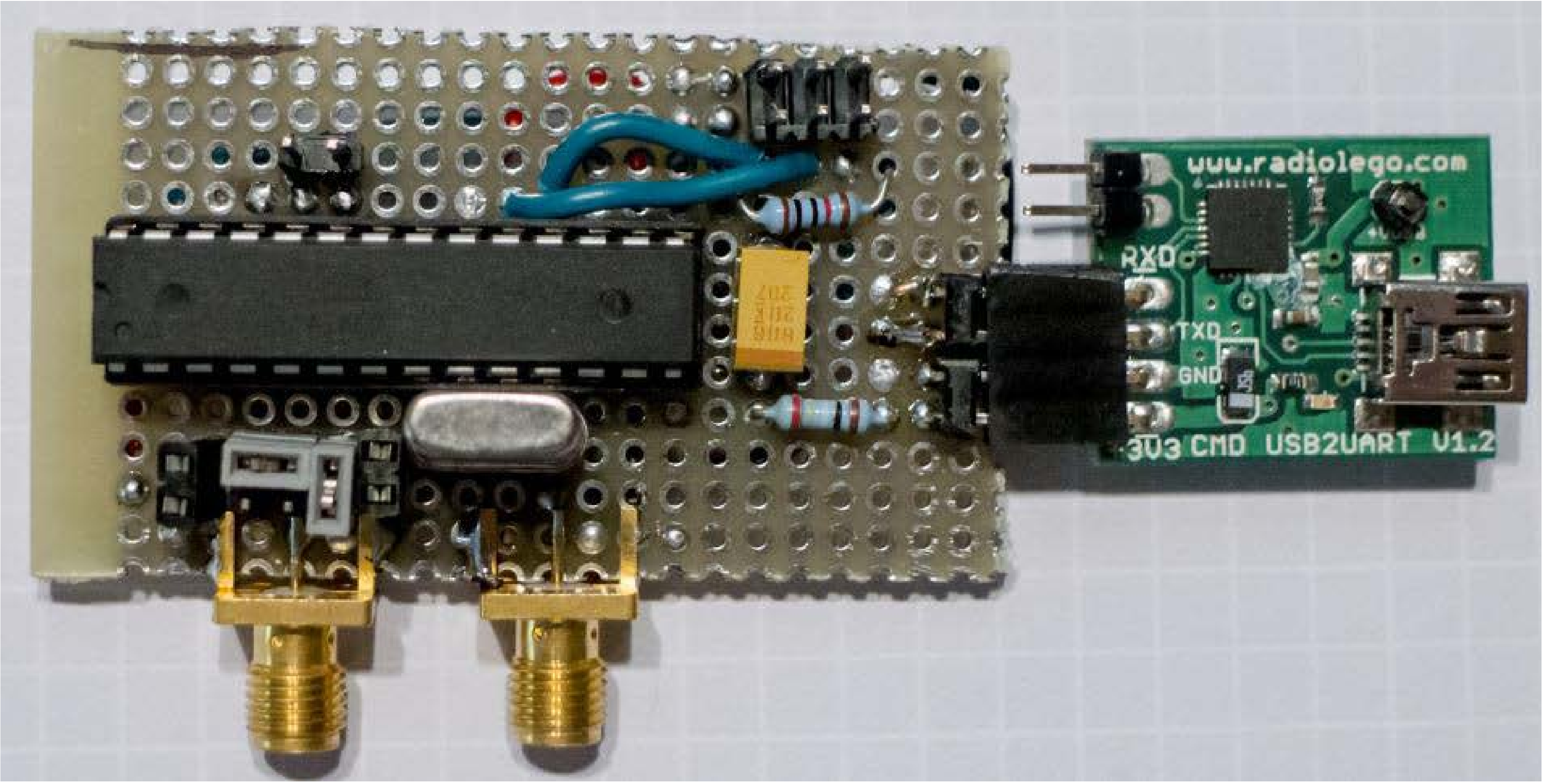
What does this Look Like?



What does this Look Like?



A PCB Version



Let’s Do This: Shopping List

- AtMega8-16PU
- 7.37 MHz Crystal
- 22pF Capacitors
- 100 ohm resistors
- 680uF (or bigger) capacitor
- 1uF Ceramic Capacitor
- 0.1uF Ceramic Capacitor
- Cables/Connectors
- Breadboard
- Capture HW
- Serial-USB Adapter
- Power?
- AVR Programmer

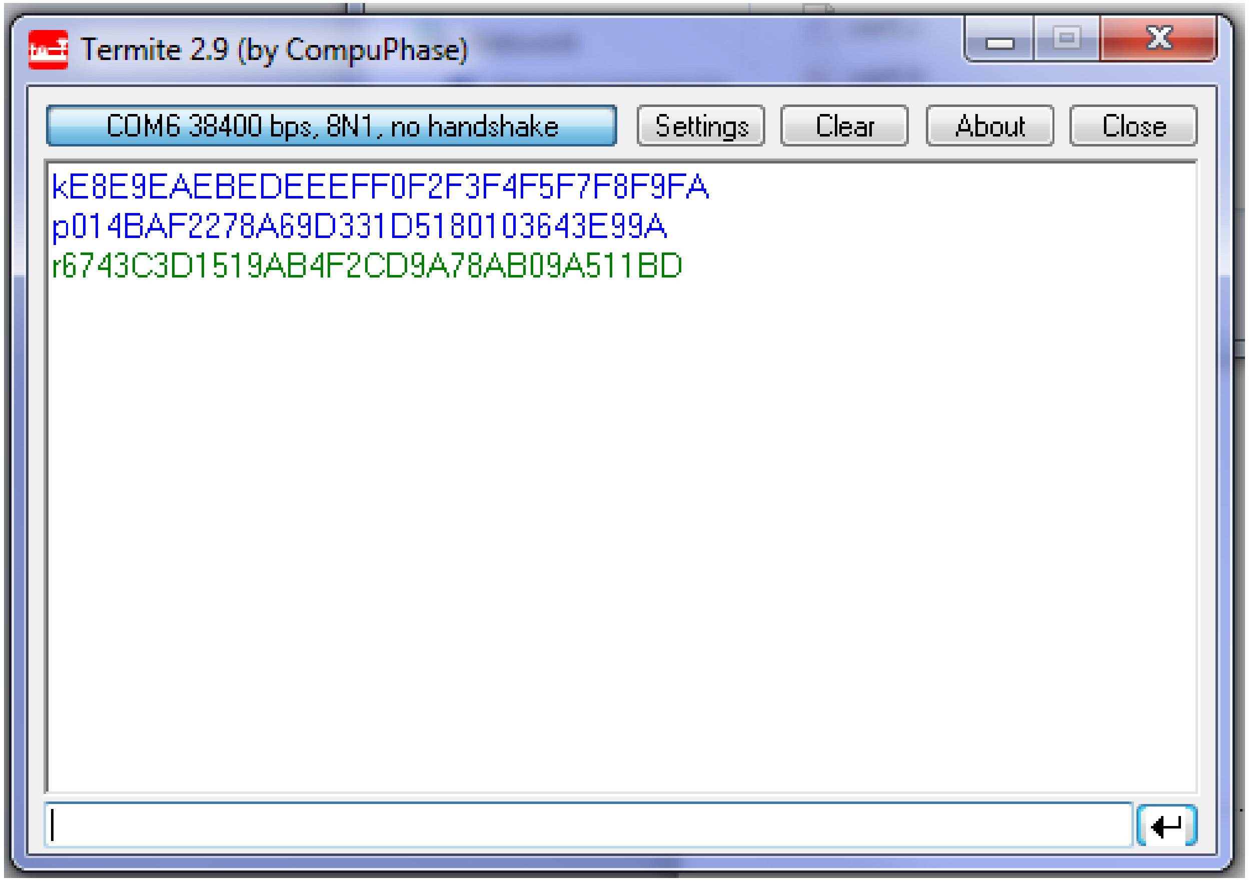
Notes on Step 1

- Ideally Get ATMega8-16PU
- Crystal not 100% needed but makes life easier
- Example here uses Colorado Micro Devices USB2UART, many other manufactures of USB/Serial Cables
- Need Capture HW too – OpenADC used here, can use general purpose scope (Tiepie suggested as Differential versions, Picoscope popular too)

Step 2: Build your Target HW

- See schematic in ref material
- Insert resistor in power line
- Need AVR programmer. Can use:
  - AVR-ISP MK-II
  - Arduino setup as programmer
  - Lots of other cheap AVR programmers (see EBay)

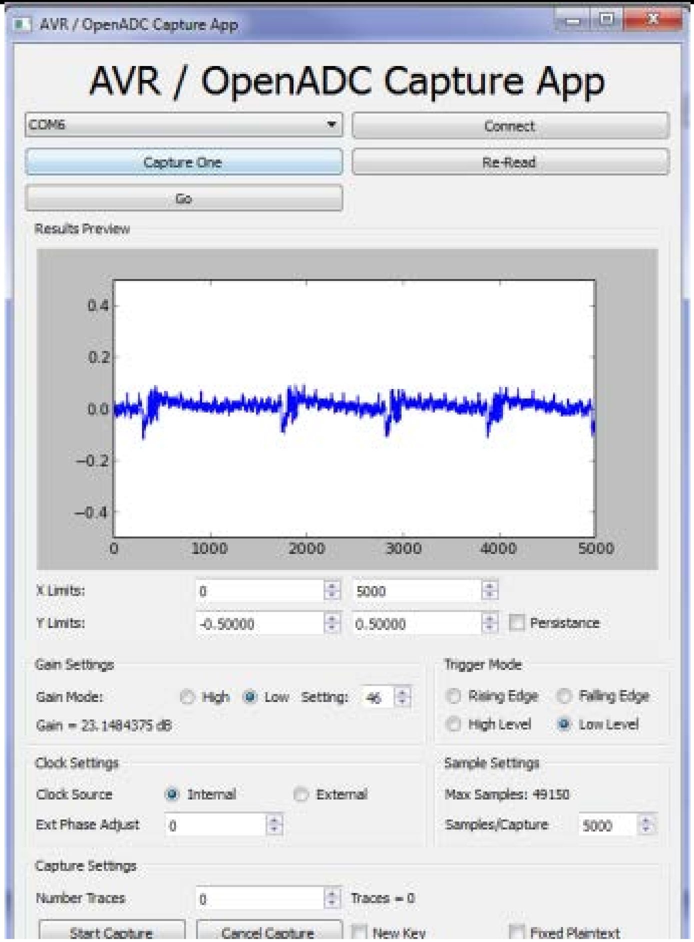
Step 2: Continued (Testing)


Termite 2.9 (by CompuPhase)
COM6 38400 bps, 8N1, no handshake
Settings
Clear
About
Close

```
kE8E9EAEBEDEEEFF0F2F3F4F5F7F8F9FA
p014BAF2278A69D331D5180103643E99A
r6743C3D1519AB4F2CD9A78AB09A511BD
```

Use serial port to confirm working

Step 3: Characterize



AVR / OpenADC Capture App

COM6

X Limits: 0 5000

Y Limits: -0.50000 0.50000 □ Persistance

Gain Settings

Gain Mode: ○ High ● Low Setting: 46

Gain = 23.1484375 dB

Trigger Mode

○ Rising Edge ○ Falling Edge

○ High Level ● Low Level

Clock Settings

Clock Source ● Internal ○ External

Ext Phase Adjust 0

Sample Settings

Max Samples: 49150

Samples/Capture 5000

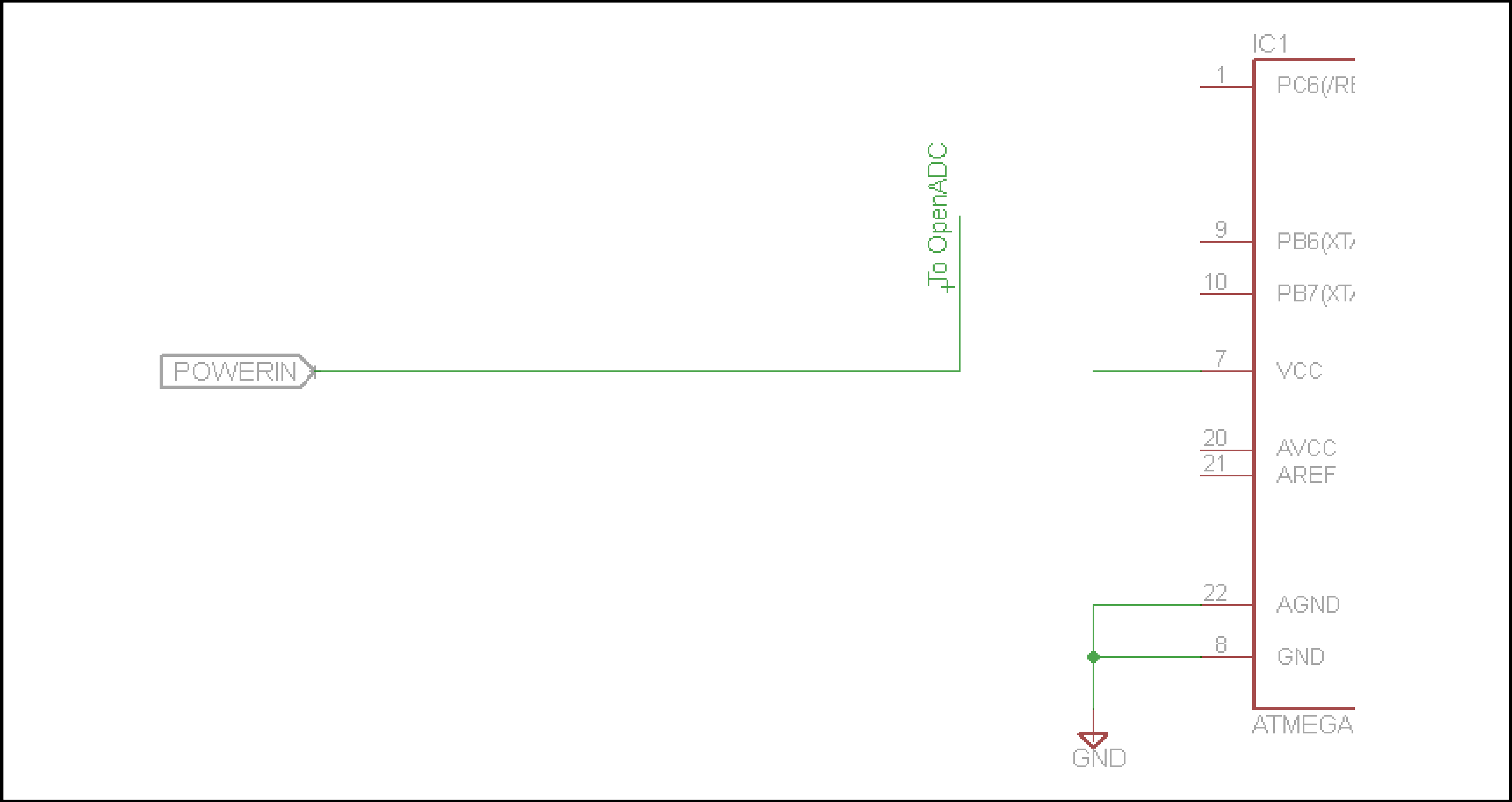
Capture Settings

Number Traces 0 Traces = 0

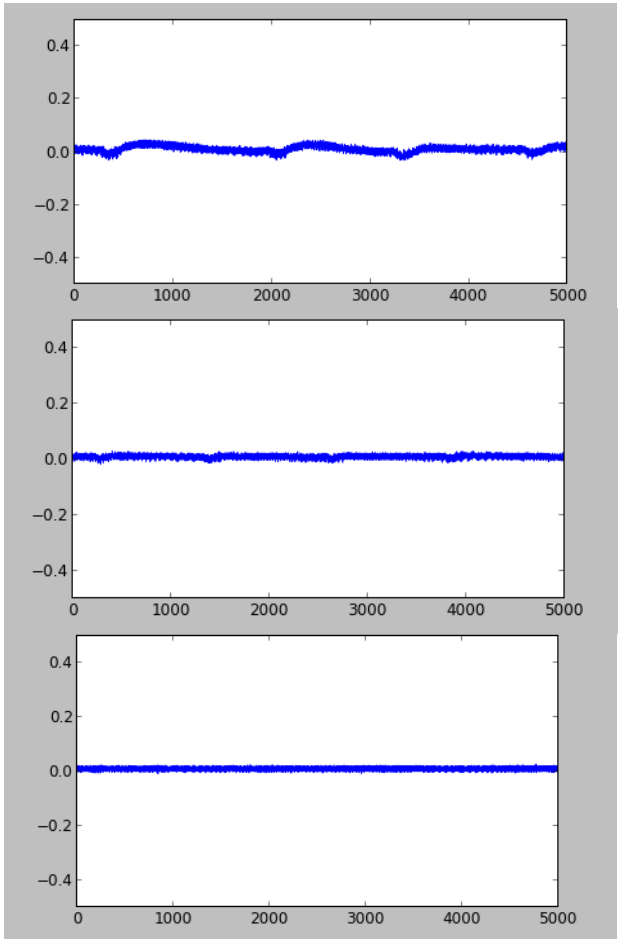
□ New Key □ Fixed Plaintext

- Probe connected to VCC rail, not across shunt

Step 3: Characterize



Step 3: Characterize

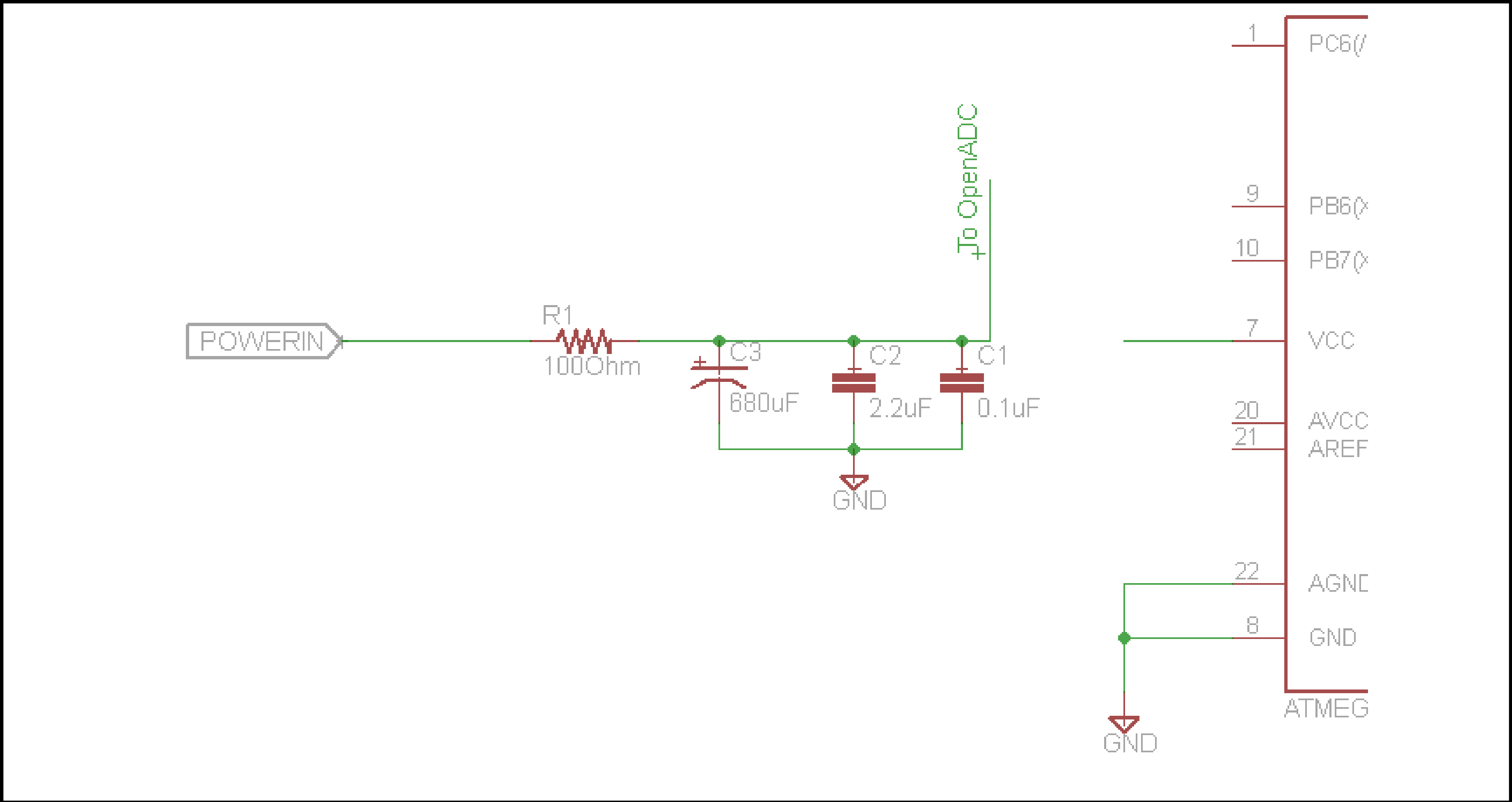


2.2uF Ceramic Capacitor

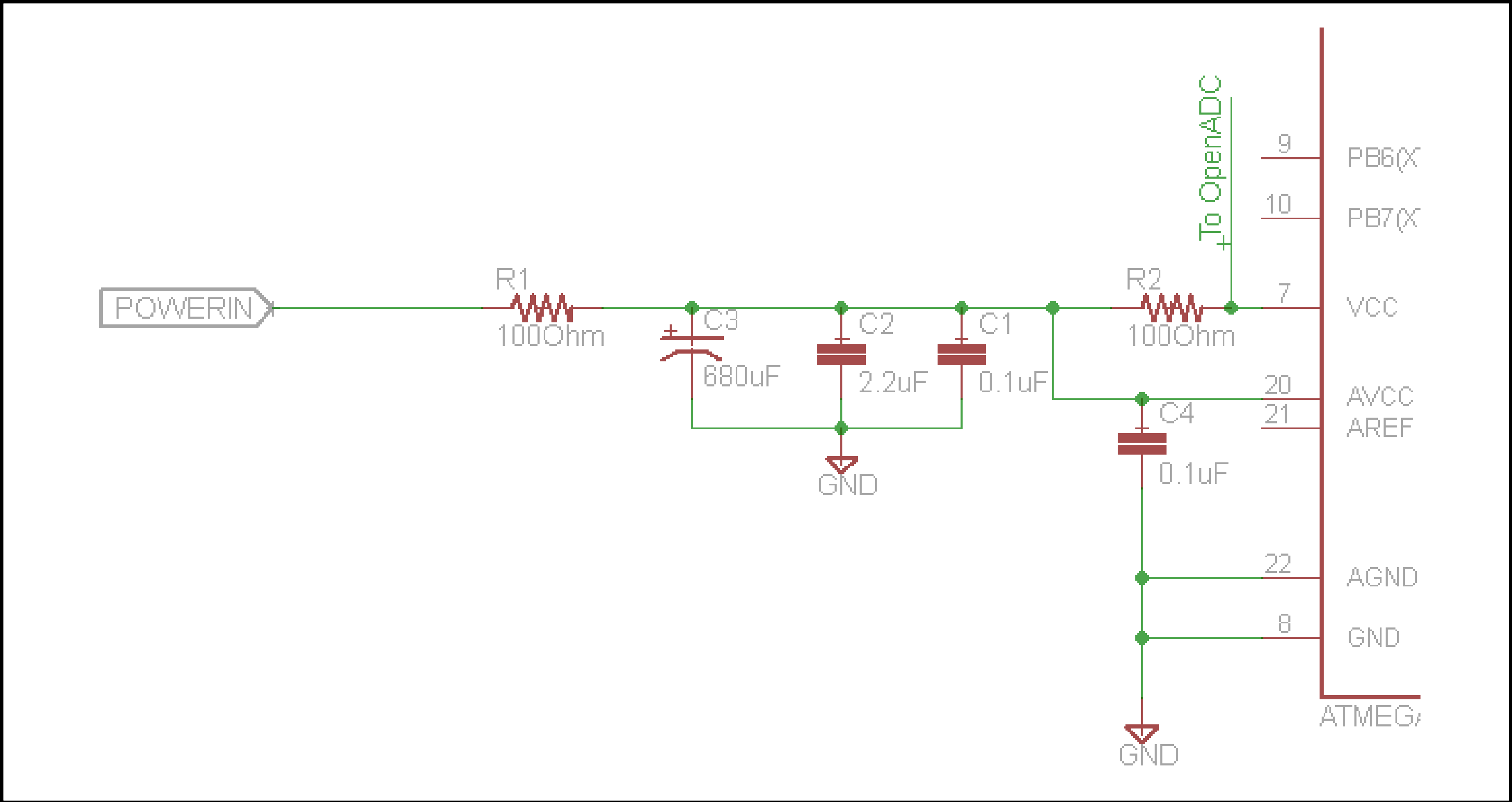
+680uF Electrolyctic

+100 ohm series resistor

Step 3: Characterize

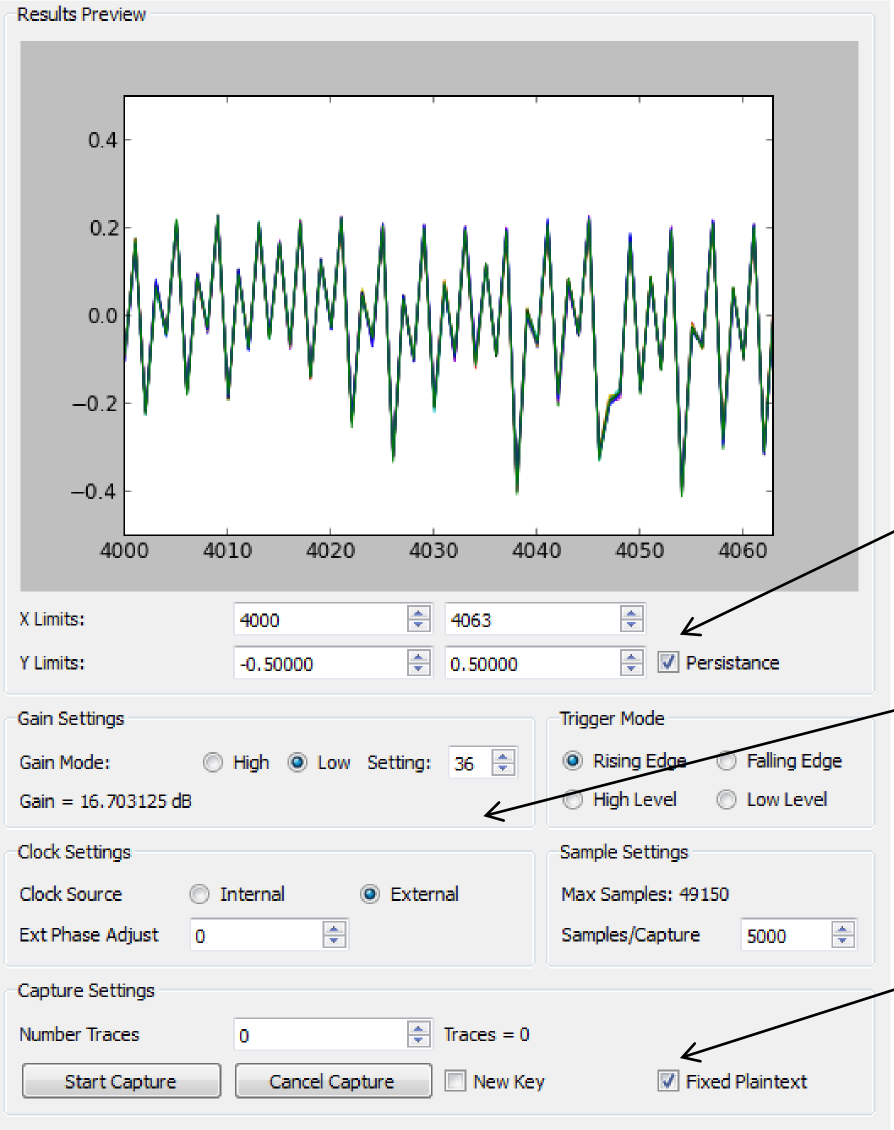


Step 3: Shunt



To OpenADC
+
POWERIN
R1
100Ohm
C3
+
680uF
C2
2.2uF
C1
0.1uF
GND
R2
100Ohm
C4
0.1uF
GND
9
PB6(X
10
PB7(X
7
VCC
20
AVCC
21
AREF
22
AGND
8
GND
ATMEGA

Step 3: Characterization Cont'd



Results Preview

X Limits: 4000 4063

Y Limits: -0.50000 0.50000 ☑ Persistance

Gain Settings

Gain Mode: ○ High ● Low Setting: 36

Gain = 16.703125 dB

Trigger Mode

● Rising Edge ○ Falling Edge

○ High Level ○ Low Level

Clock Settings

Clock Source ○ Internal ● External

Ext Phase Adjust 0

Sample Settings

Max Samples: 49150

Samples/Capture 5000

Capture Settings

Number Traces 0 Traces = 0

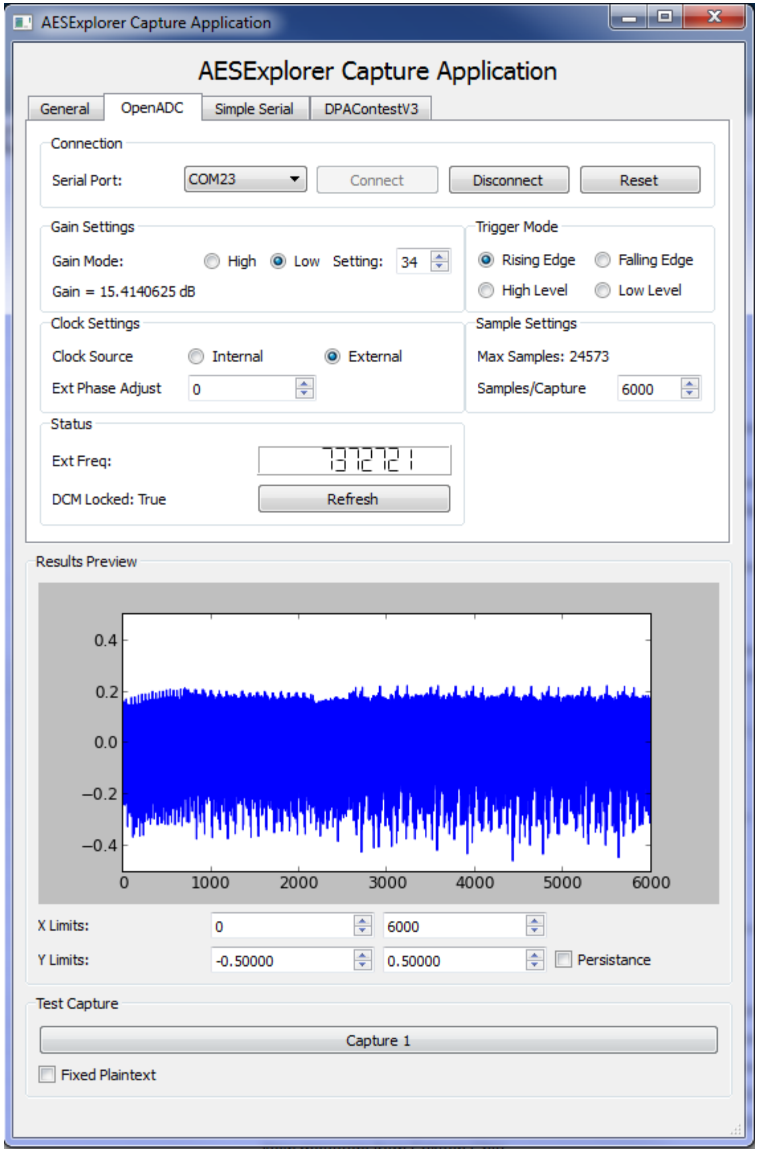
Start Capture Cancel Capture □ New Key ☑ Fixed Plaintext

Persistence Mode in Scope

Adjust gain, trigger, etc to get reliable signal

Fixed Plaintext

Step 4: Acquire


AESExplorer Capture Application

AESExplorer Capture Application

Connection

Serial Port: COM23

Gain Settings

Gain Mode: ○ High ● Low Setting: 34

Gain = 15.4140625 dB

Trigger Mode

● Rising Edge ○ Falling Edge

○ High Level ○ Low Level

Clock Settings

Clock Source ○ Internal ● External

Ext Phase Adjust 0

Sample Settings

Max Samples: 24573

Samples/Capture 6000

Status

Ext Freq: 7372721

DCM Locked: True

Results Preview

X Limits: 0 6000

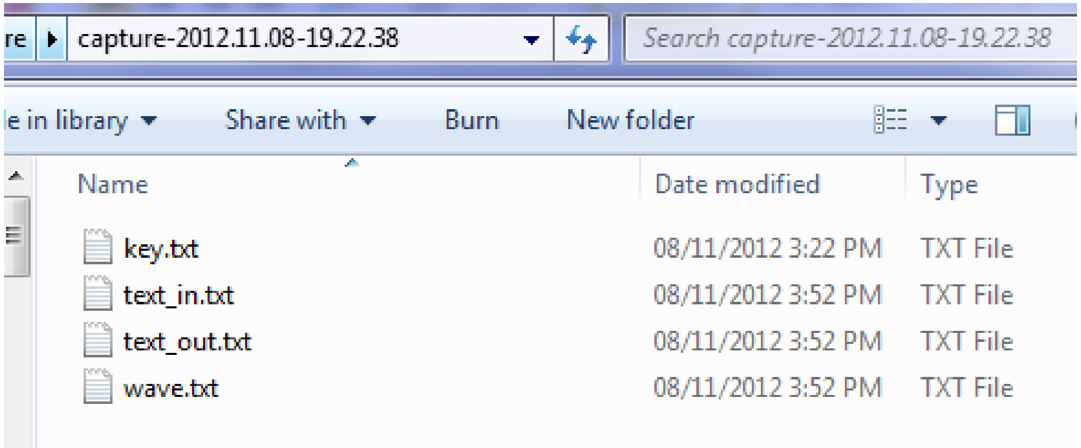
Y Limits: -0.50000 0.50000 □ Persistance

Test Capture

□ Fixed Plaintext

- Use AESExplorer ‘Capture’ application, written in Python with PySide
  - Included on Blackhat CD
- Capture ~2500 traces, 6000 samples/capture

Step 4: Acquire



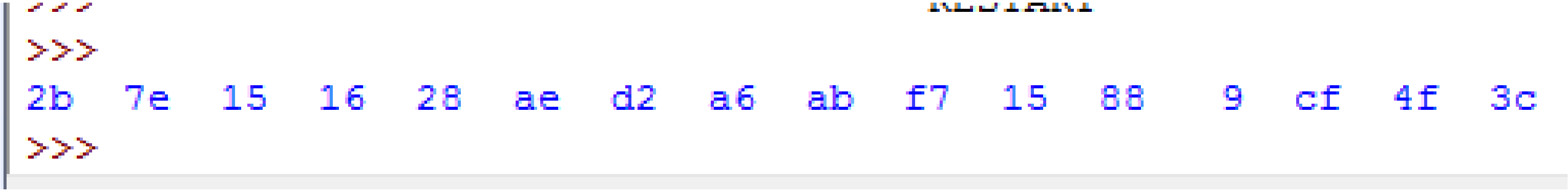
re ▸ capture-2012.11.08-19.22.38
Search capture-2012.11.08-19.22.38
e in library ▾
Share with ▾
Burn
New folder

Name	Date modified	Type
key.txt	08/11/2012 3:22 PM	TXT File
text_in.txt	08/11/2012 3:52 PM	TXT File
text_out.txt	08/11/2012 3:52 PM	TXT File
wave.txt	08/11/2012 3:52 PM	TXT File

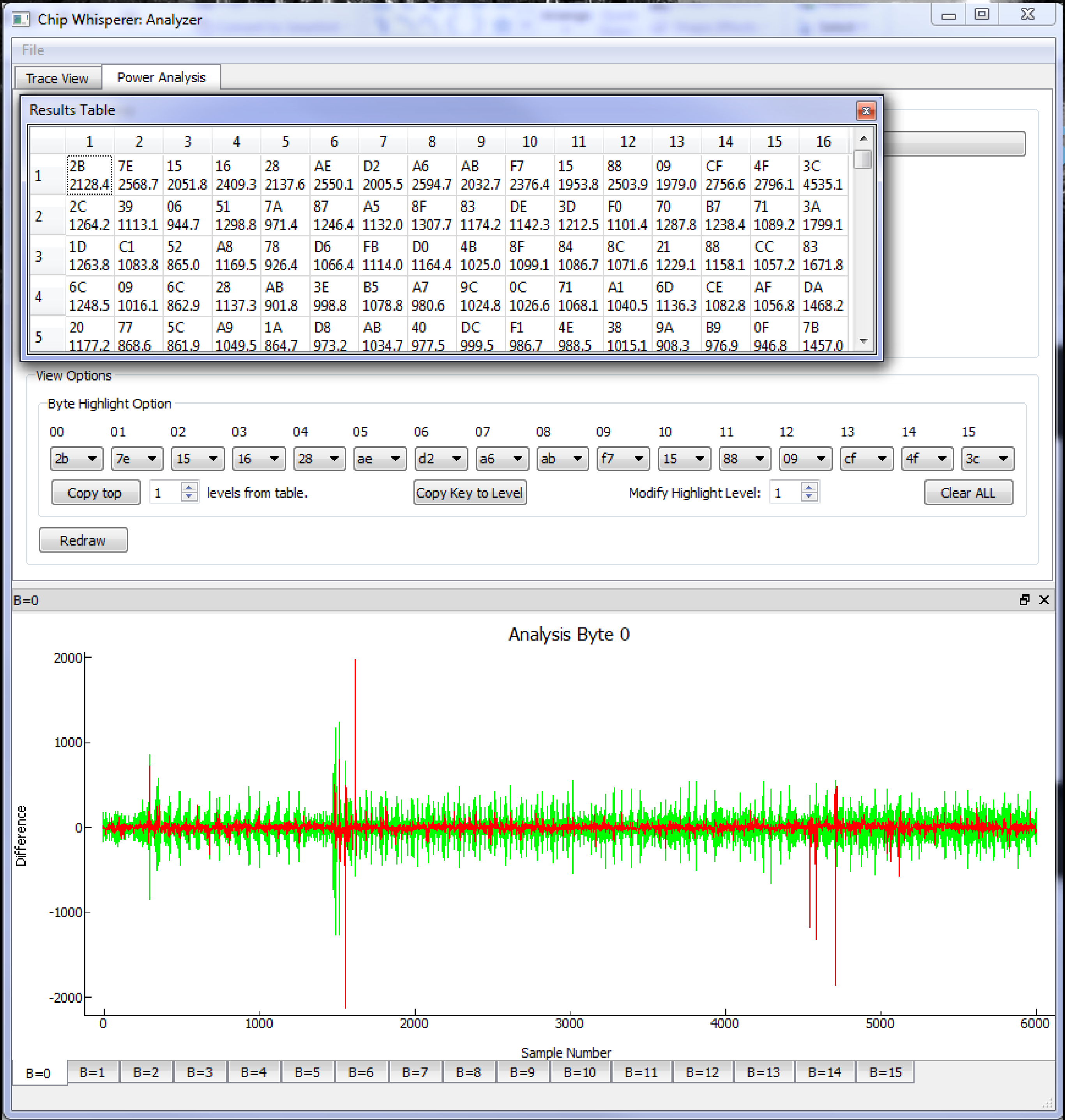
text_in.txt & wave.txt are the needed files

Step 5: Break It

Copy wave.txt & text_in.txt to same directory as dpa_attack.py, run:



```
>>>                                              RESTART
>>>
2b   7e   15   16   28   ae   d2   a6   ab   f7   15   88    9   cf   4f   3c
>>>
```



Results Table

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2B 2128.4	7E 2568.7	15 2051.8	16 2409.3	28 2137.6	AE 2550.1	D2 2005.5	A6 2594.7	AB 2032.7	F7 2376.4	15 1953.8	88 2503.9	09 1979.0	CF 2756.6	4F 2796.1	3C 4535.1
2	2C 1264.2	39 1113.1	06 944.7	51 1298.8	7A 971.4	87 1246.4	A5 1132.0	8F 1307.7	83 1174.2	DE 1142.3	3D 1212.5	F0 1101.4	70 1287.8	B7 1238.4	71 1089.2	3A 1799.1
3	1D 1263.8	C1 1083.8	52 865.0	A8 1169.5	78 926.4	D6 1066.4	FB 1114.0	D0 1164.4	4B 1025.0	8F 1099.1	84 1086.7	8C 1071.6	21 1229.1	88 1158.1	CC 1057.2	83 1671.8
4	6C 1248.5	09 1016.1	6C 862.9	28 1137.3	AB 901.8	3E 998.8	B5 1078.8	A7 980.6	9C 1024.8	0C 1026.6	71 1068.1	A1 1040.5	6D 1136.3	CE 1082.8	AF 1056.8	DA 1468.2
5	20 1177.2	77 868.6	5C 861.9	A9 1049.5	1A 864.7	D8 973.2	AB 1034.7	40 977.5	DC 999.5	F1 986.7	4E 988.5	38 1015.1	9A 908.3	B9 976.9	0F 946.8	7B 1457.0

Byte Highlight Option

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
2b	7e	15	16	28	ae	d2	a6	ab	f7	15	88	09	cf	4f	3c

Copy top 1 levels from table.

Modify Highlight Level: 1

ChipWhisperer

www.ChipWhisperer.com

- GIT Repository for tools demoed here
- GIT Repository for hardware designs
- Mailing List for discussion
- Wiki for Documentation

Current Software Tools

ChipWhisperer-Capture

- Capture tools, interfaces to OpenADC + target boards
- Records traces

ChipWhisperer-Analyzer

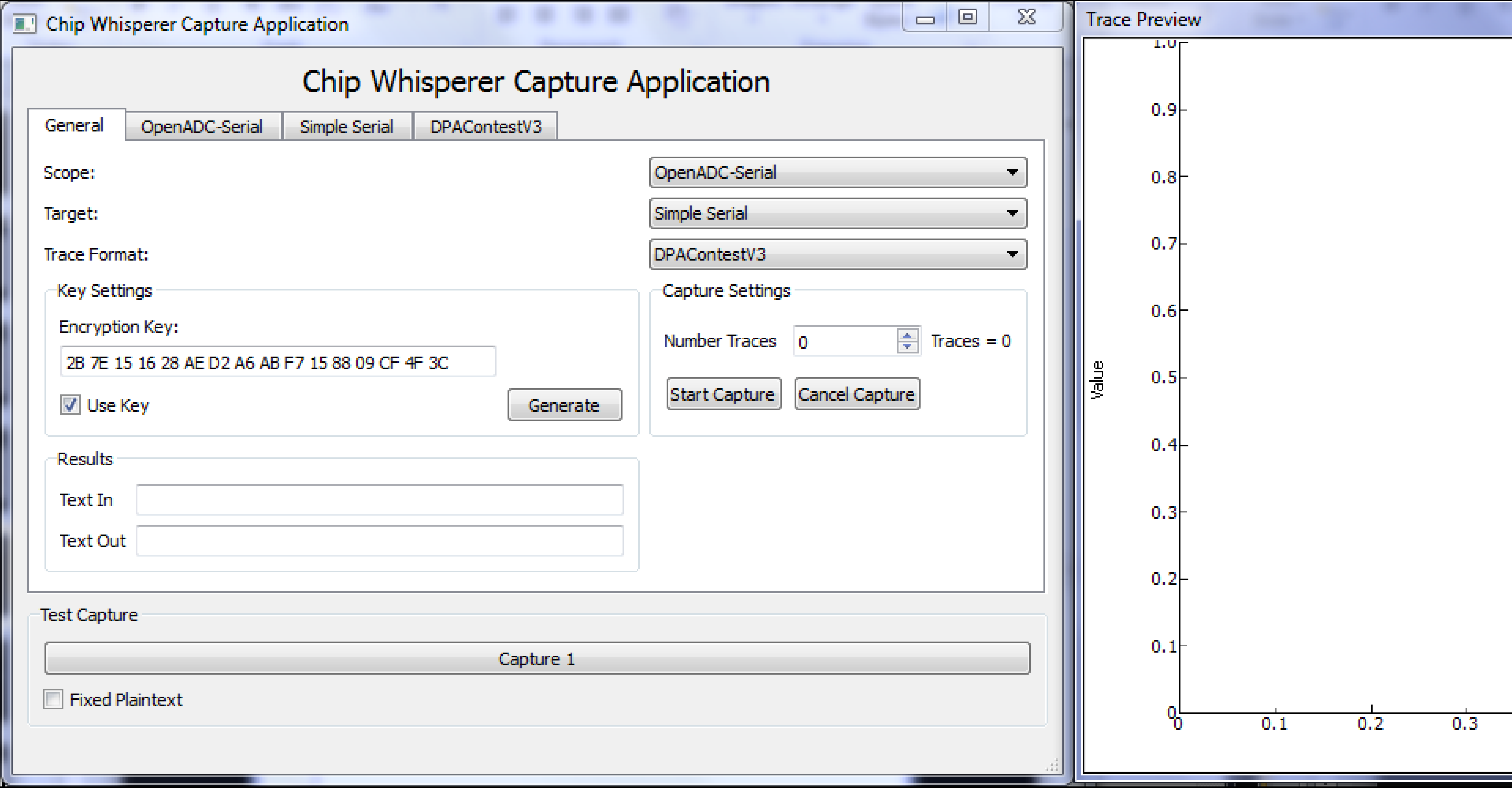
- Applies attacks to power traces

About the Tools

- All tools *Open Source* (LGPL License)

- Written in Python using PySide for GUI

- Uses trace file format from DPA Contest V3, which publishes some example captures



Chip Whisperer Capture Application

Scope: OpenADC-Serial

Target: Simple Serial

Trace Format: DPAContestV3

Key Settings

Encryption Key: 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C

☑ Use Key

Capture Settings

Number Traces 0 Traces = 0

Results

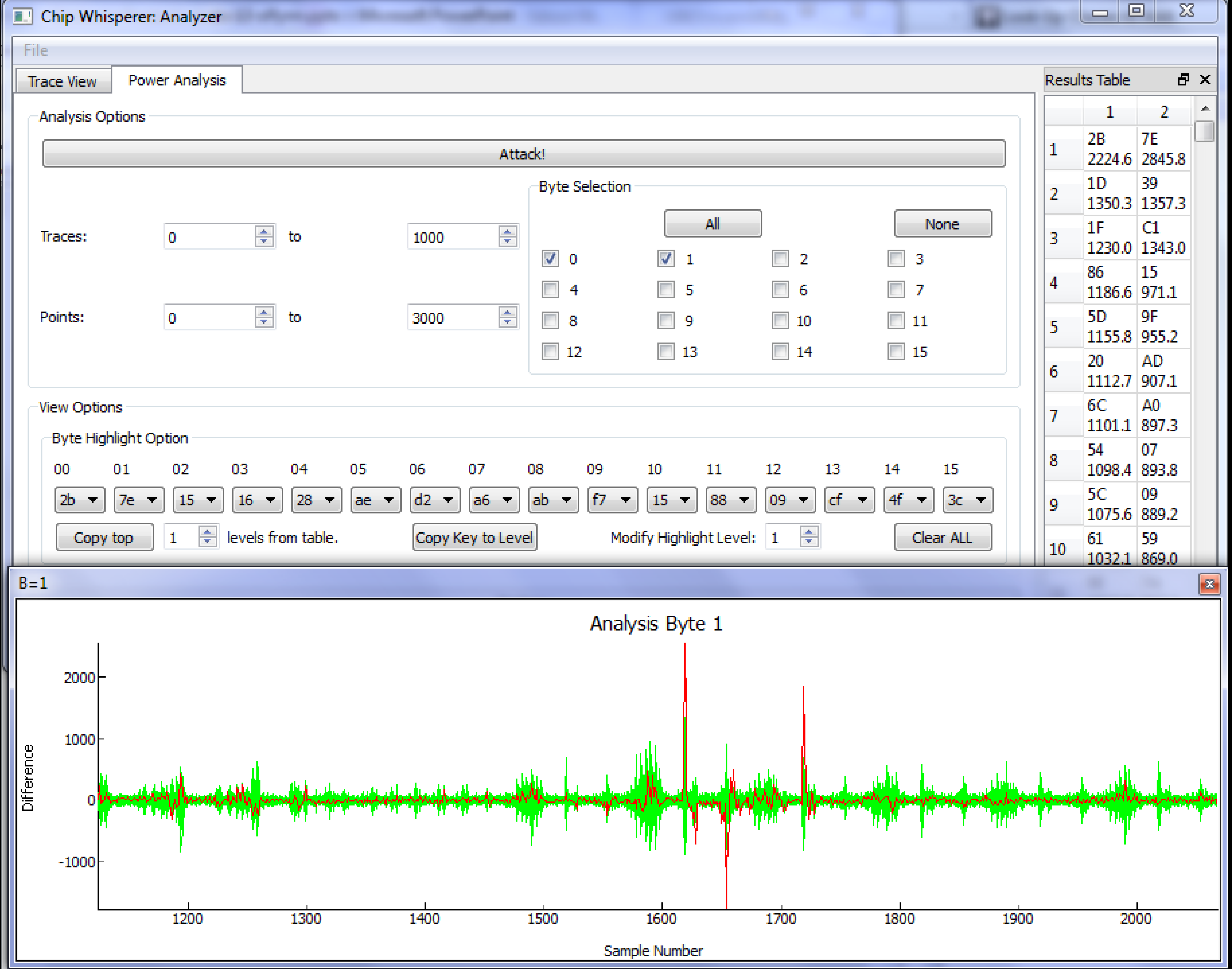
Text In

Text Out

Test Capture

☐ Fixed Plaintext

- Runs on Windows/Linux/Mac
- Supports multiple different targets
- Dockable preview window (to right) shows power as measurements occuring



Chip Whisperer: Analyzer

File

Trace View | Power Analysis

Analysis Options

Attack!

Traces: 0 to 1000

Points: 0 to 3000

Byte Selection

All | None

☑ 0 ☑ 1 □ 2 □ 3
□ 4 □ 5 □ 6 □ 7
□ 8 □ 9 □ 10 □ 11
□ 12 □ 13 □ 14 □ 15

View Options

Byte Highlight Option

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
2b	7e	15	16	28	ae	d2	a6	ab	f7	15	88	09	cf	4f	3c

Copy top 1 levels from table. | Copy Key to Level | Modify Highlight Level: 1 | Clear ALL

Results Table

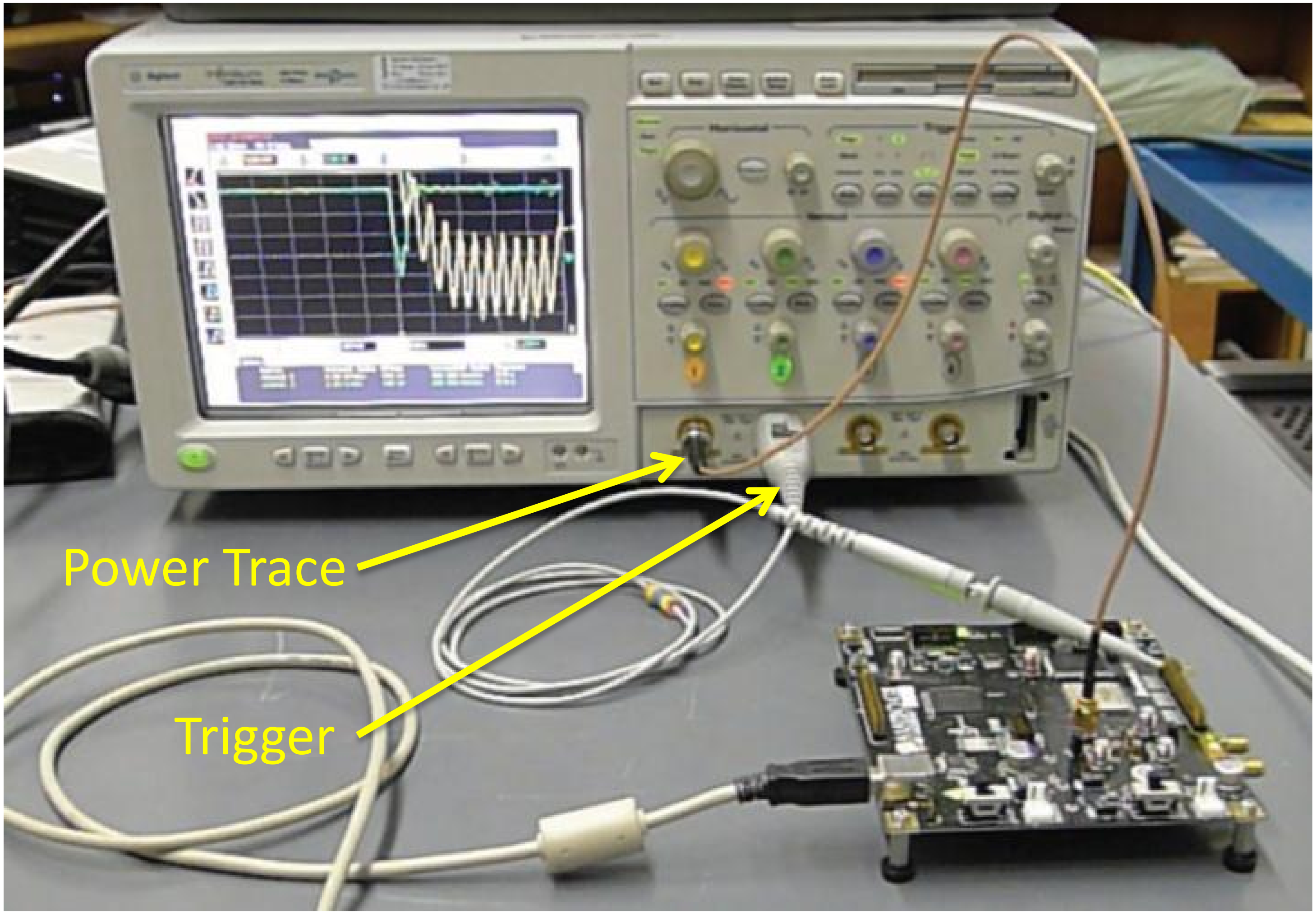
	1	2
1	2B 2224.6	7E 2845.8
2	1D 1350.3	39 1357.3
3	1F 1230.0	C1 1343.0
4	86 1186.6	15 971.1
5	5D 1155.8	9F 955.2
6	20 1112.7	AD 907.1
7	6C 1101.1	A0 897.3
8	54 1098.4	07 893.8
9	5C 1075.6	09 889.2
10	61 1032.1	59 869.0

B=1

Analysis Byte 1

Waveform Acquisition & Low-Cost Alternatives

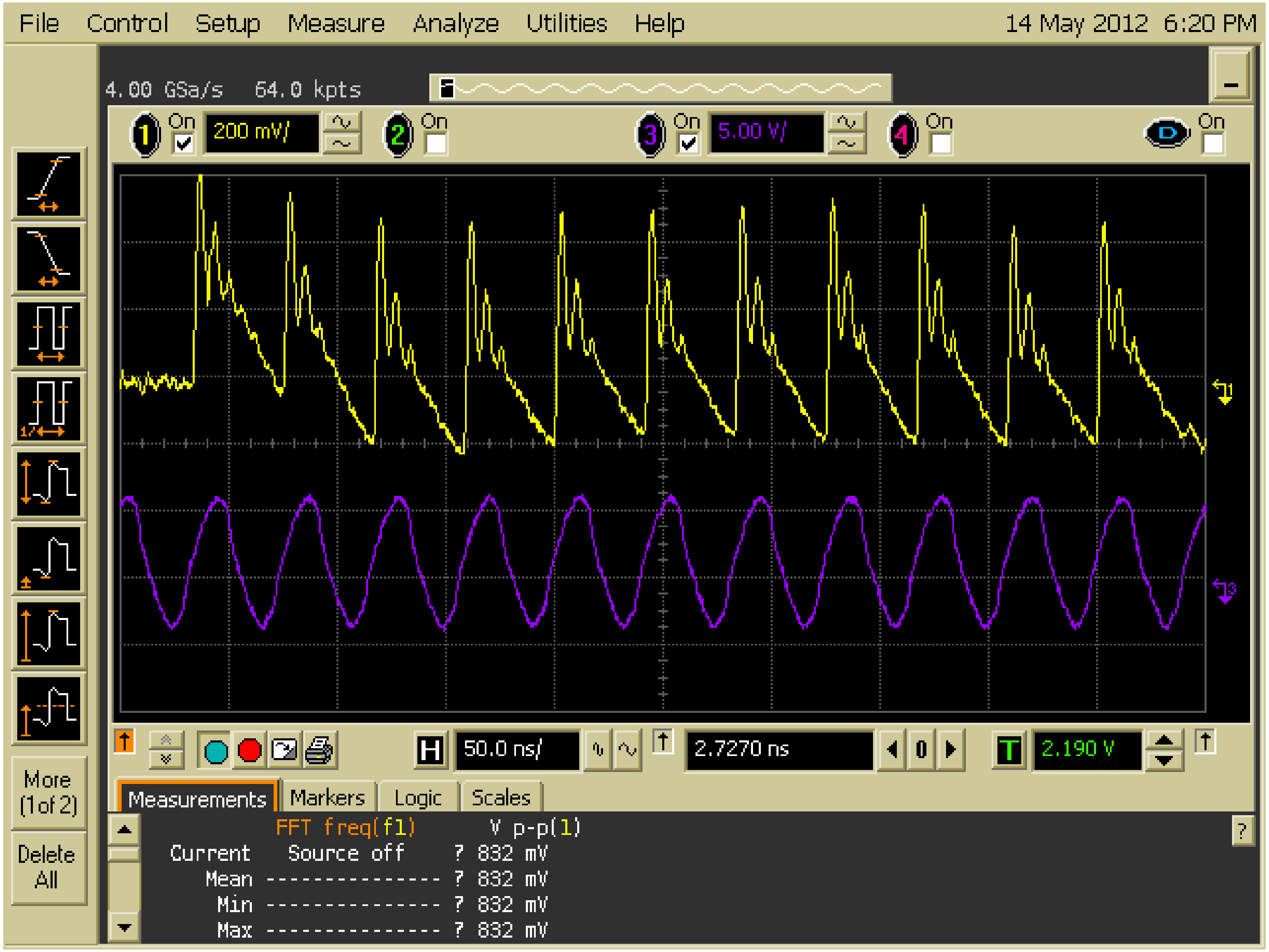
What's a 'Normal' Setup look like?



Is this Really Typical?

Author	Work	Year	Scope	Cost
Dario Carluccio	Electromagnetic Side Channel Analysis Embedded Crypto Devices	2005	Infiniium 5432D MSO	$8000
Youssef Souissi et al.	Embedded systems security: An evaluation methodology against Side Channel Attacks	2011	Infiniium 54855	$20 000
Dakshi Agrawal et al.	The EM Side–Channel(s)	2003	100 MHz, 12 bit	$1000
F.X. Standaert et al.	Using subspace-based template attacks to compare and combine power and electromagnetic information leakages	2008	1 GHz bandwidth	$7500

Can We Do Better?

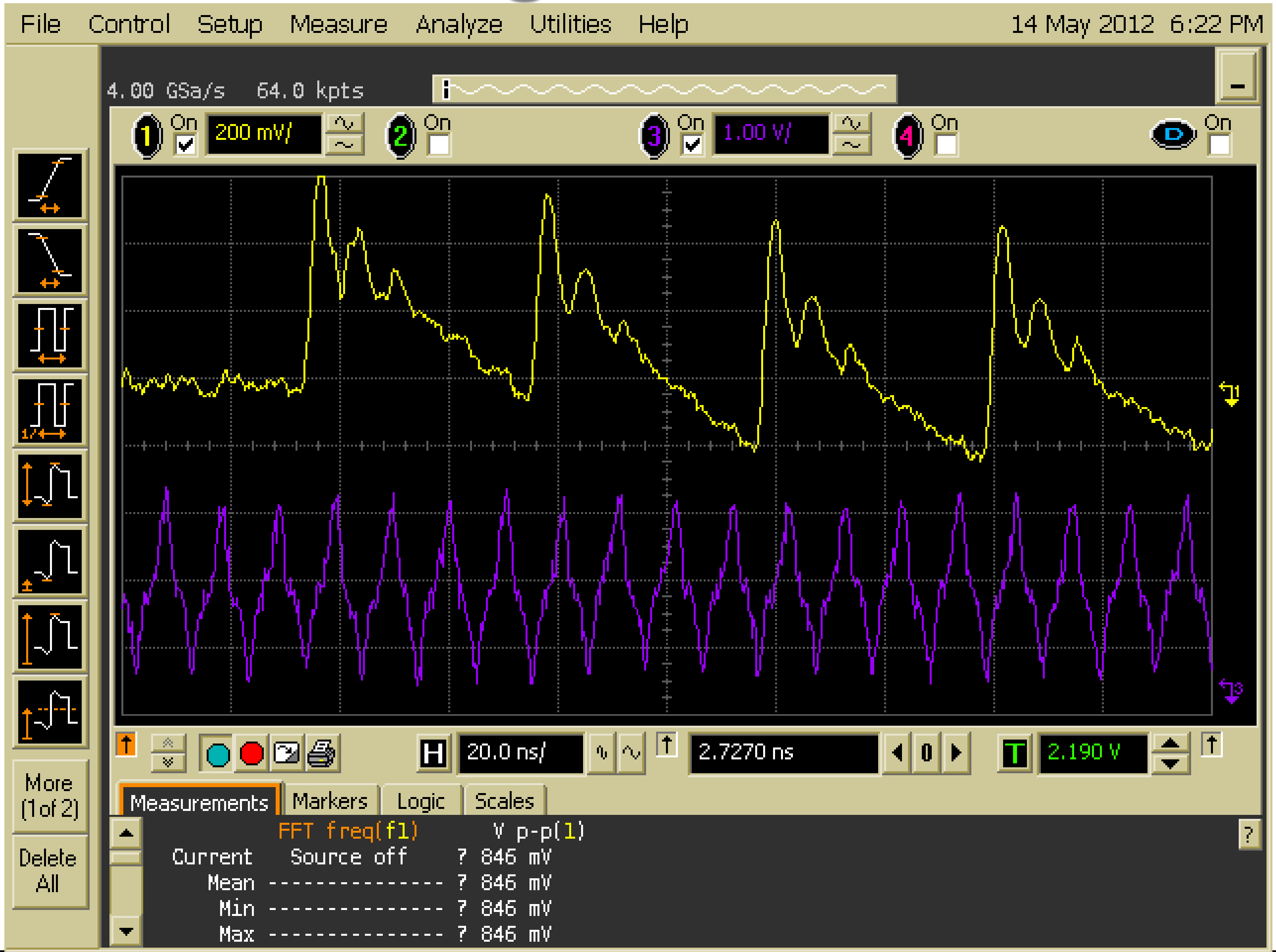


```
         FFT freq(f1)       V p-p(1)
Current   Source off       ? 832 mV
   Mean ---------------- ? 832 mV
    Min ---------------- ? 832 mV
    Max ---------------- ? 832 mV
```

Power

Clock

Using 4x Source Clock



14 May 2012 6:22 PM

4.00 GSa/s 64.0 kpts

200 mV/

1.00 V/

20.0 ns/

2.7270 ns

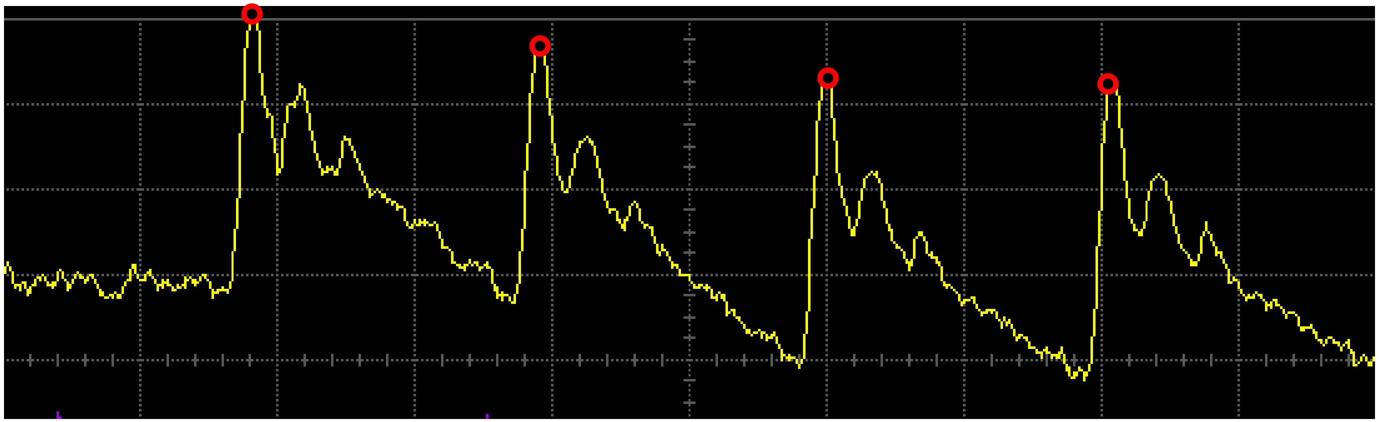
2.190 V

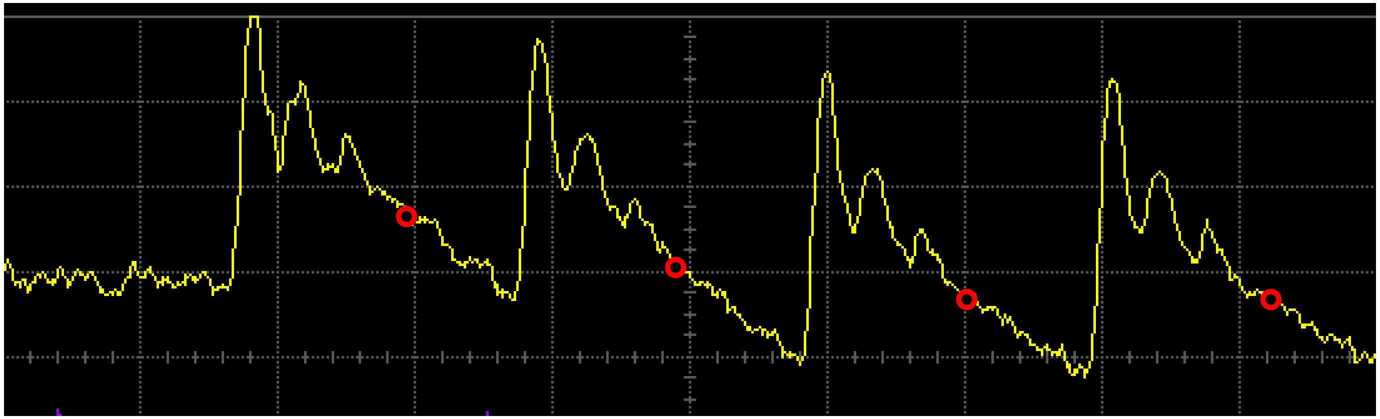
```
              FFT freq(f1)       V p-p(1)
  Current   Source off     ? 846 mV
     Mean --------------- ? 846 mV
      Min --------------- ? 846 mV
      Max --------------- ? 846 mV
```

Power

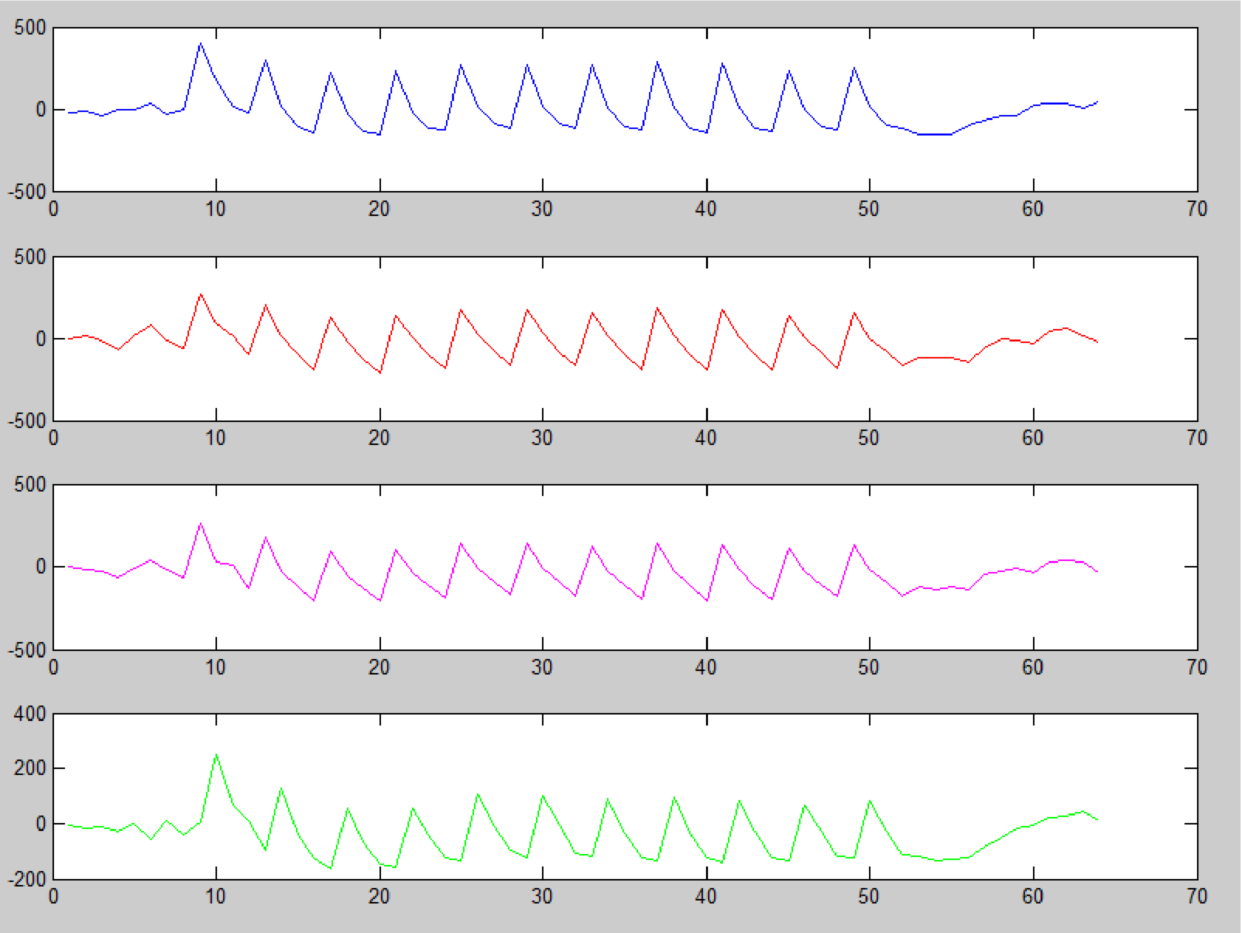
Clock

What about Phase Shift?

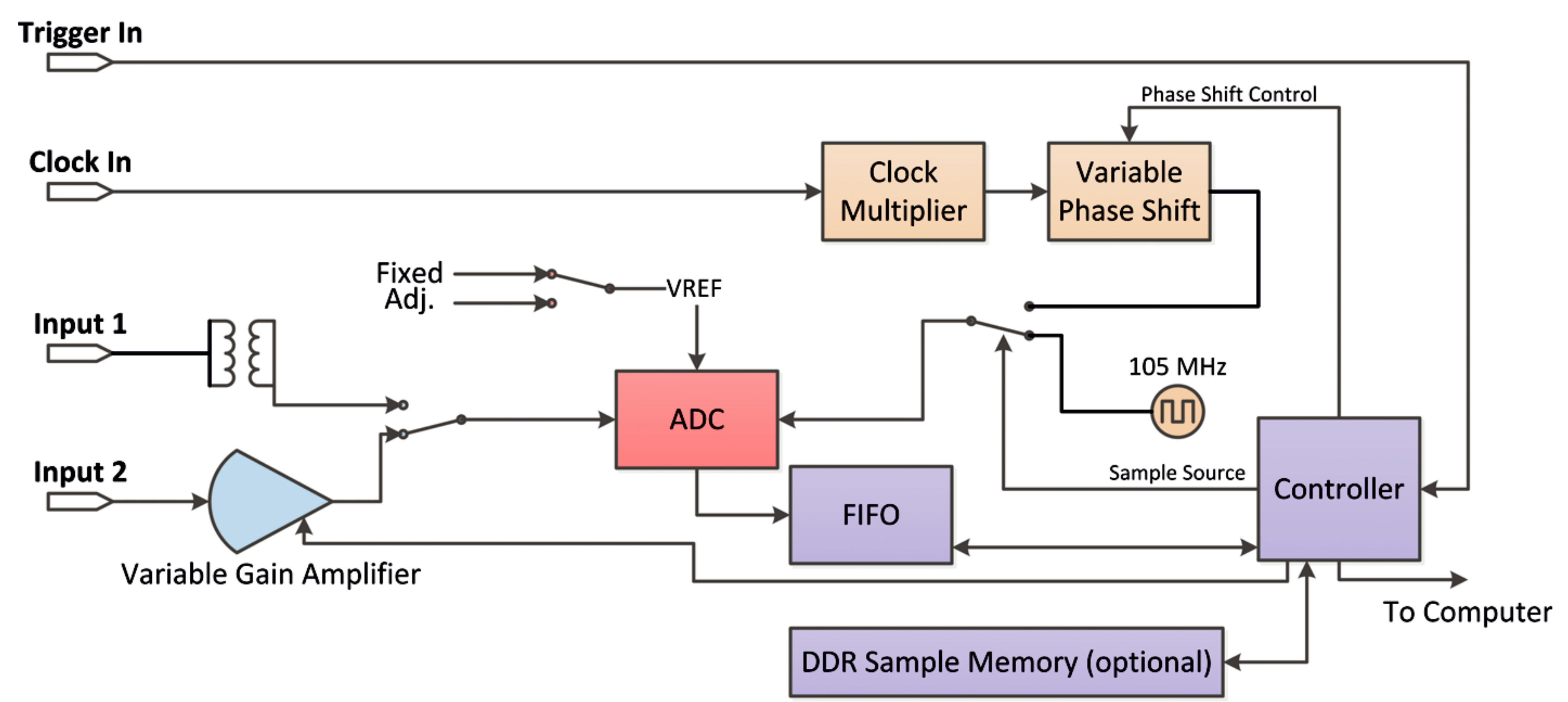




4x Sample Clock with Different Phases

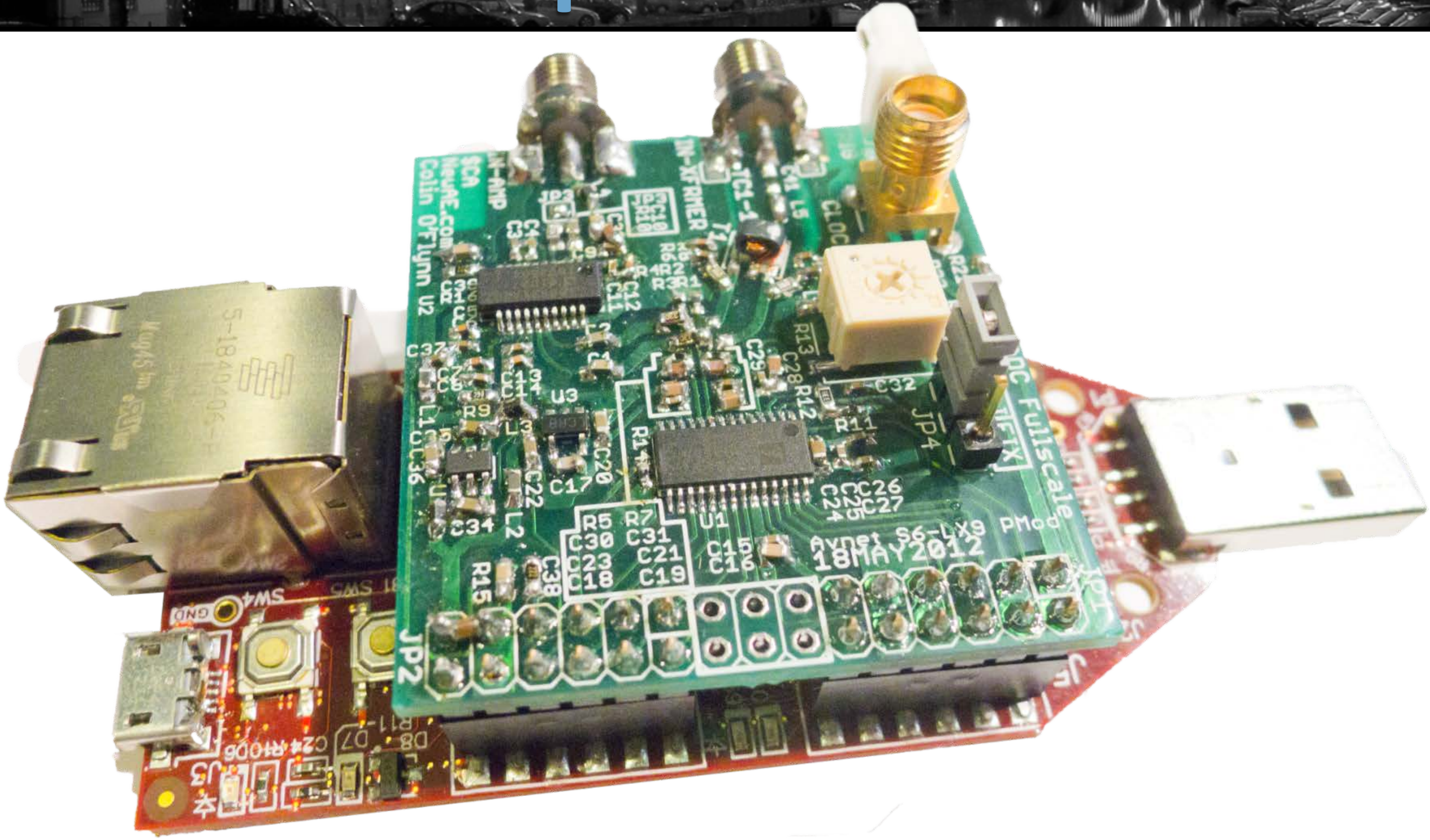


Desired Capture HW



See “*A Case Study of Side-Channel Analysis using Decoupling Capacitor Power Measurement with the OpenADC*” by Colin O’Flynn & Zhizhang Chen

OpenADC


SCA
NewAE.com
Colin O'Flynn
Avnet S6-LX9 PMod
18MAY2012
JP2
JP4

OpenADC

- Can use up to 105 MSPS in oscilloscope-like mode
- Supports synchronizing to sample clock of device, so can attack high-speed targets
- Built-in amplifier
- Open Source design!

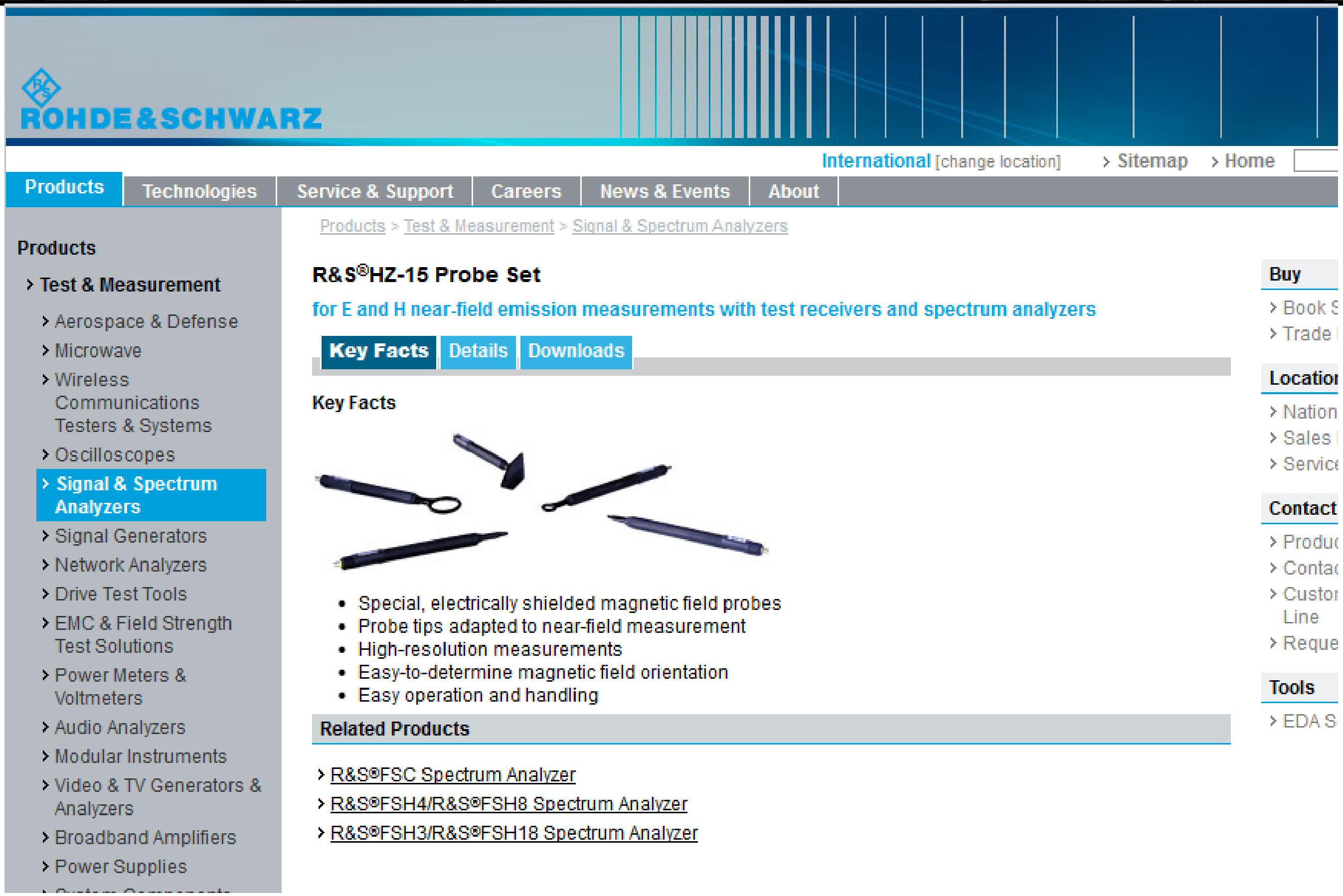
Synchronous Sampling Scope

e.g.:

- CleverScope with CS810 Option
- PicoScope PS6000

Magnetic Field Probes

Rohde & Schwarz



R&S®HZ-15 Probe Set

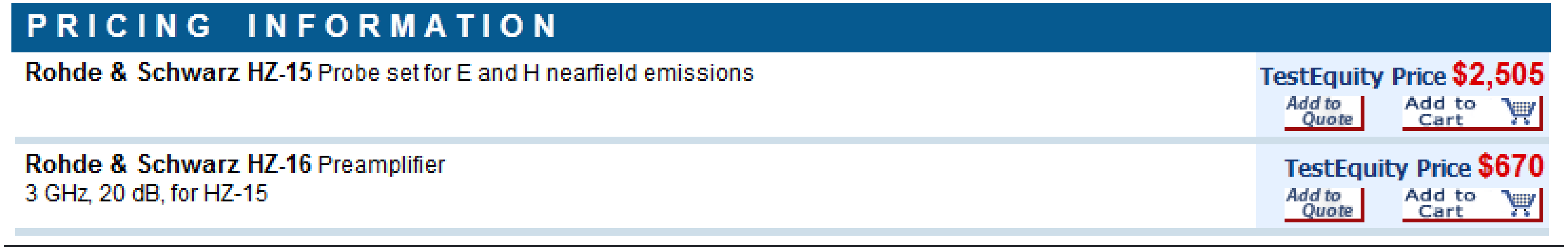
for E and H near-field emission measurements with test receivers and spectrum analyzers

Key Facts

- Special, electrically shielded magnetic field probes
- Probe tips adapted to near-field measurement
- High-resolution measurements
- Easy-to-determine magnetic field orientation
- Easy operation and handling

Related Products

- R&S®FSC Spectrum Analyzer
- R&S®FSH4/R&S®FSH8 Spectrum Analyzer
- R&S®FSH3/R&S®FSH18 Spectrum Analyzer



PRICING INFORMATION

Rohde & Schwarz HZ-15 Probe set for E and H nearfield emissions

TestEquity Price **$2,505**

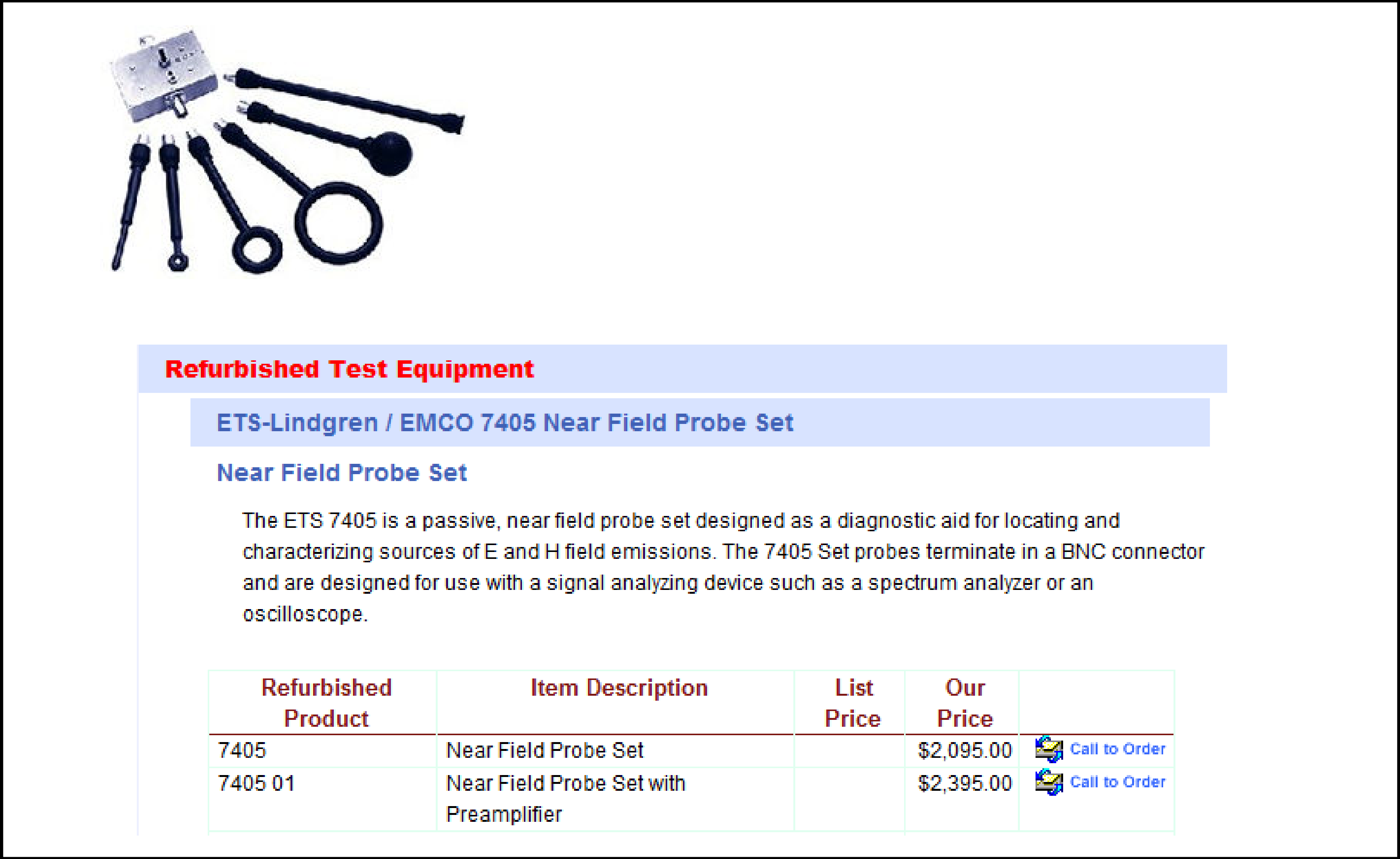
Add to Quote | Add to Cart

Rohde & Schwarz HZ-16 Preamplifier
3 GHz, 20 dB, for HZ-15

TestEquity Price **$670**

Add to Quote | Add to Cart

ETS-Lindgren



Refurbished Test Equipment

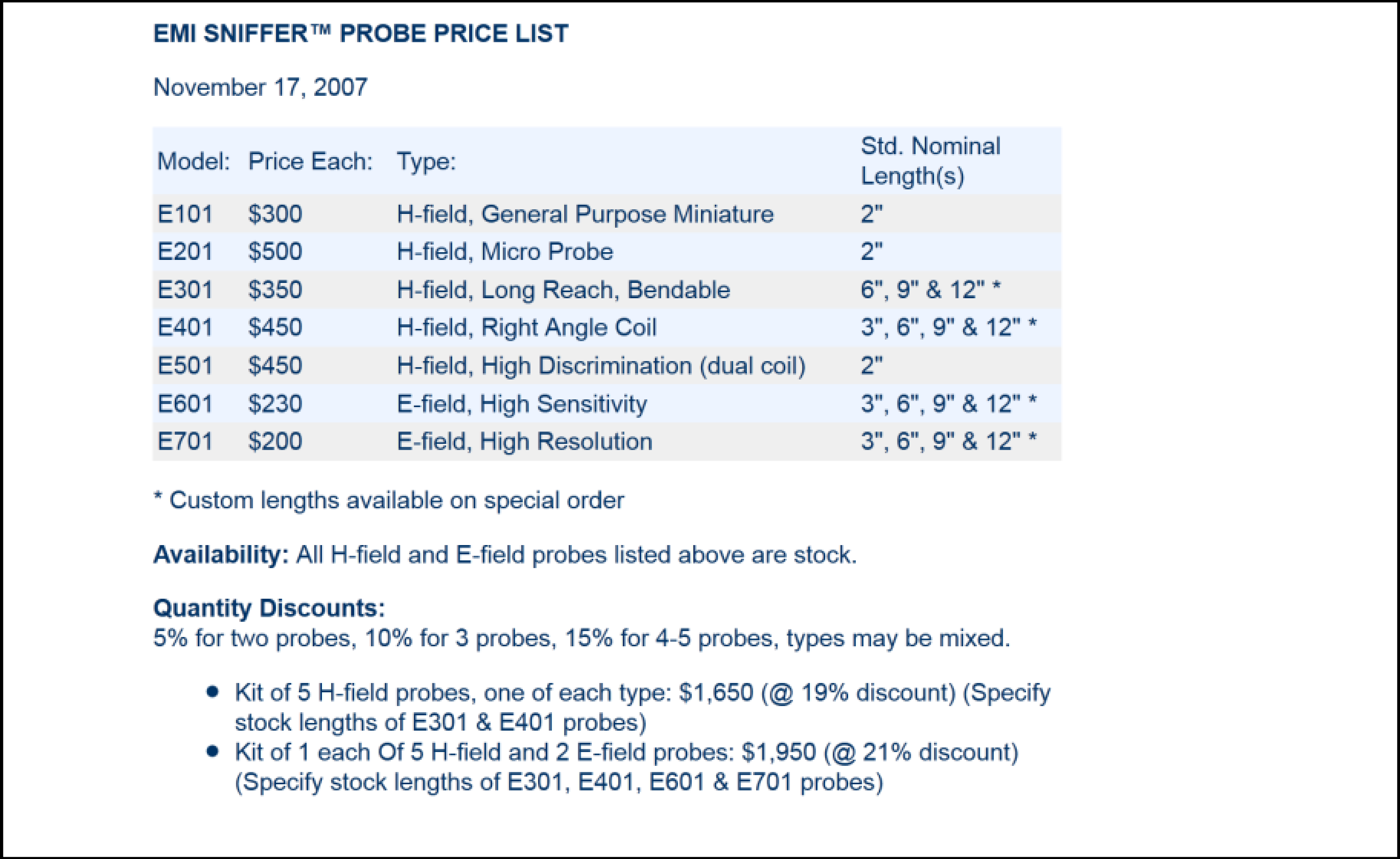
ETS-Lindgren / EMCO 7405 Near Field Probe Set

Near Field Probe Set

The ETS 7405 is a passive, near field probe set designed as a diagnostic aid for locating and characterizing sources of E and H field emissions. The 7405 Set probes terminate in a BNC connector and are designed for use with a signal analyzing device such as a spectrum analyzer or an oscilloscope.

Refurbished Product	Item Description	List Price	Our Price	
7405	Near Field Probe Set		$2,095.00	☎ Call to Order
7405 01	Near Field Probe Set with Preamplifier		$2,395.00	☎ Call to Order

Bruce Carsten Associates, Inc.



EMI SNIFFER™ PROBE PRICE LIST

November 17, 2007

Model:	Price Each:	Type:	Std. Nominal Length(s)
E101	$300	H-field, General Purpose Miniature	2"
E201	$500	H-field, Micro Probe	2"
E301	$350	H-field, Long Reach, Bendable	6", 9" & 12" *
E401	$450	H-field, Right Angle Coil	3", 6", 9" & 12" *
E501	$450	H-field, High Discrimination (dual coil)	2"
E601	$230	E-field, High Sensitivity	3", 6", 9" & 12" *
E701	$200	E-field, High Resolution	3", 6", 9" & 12" *

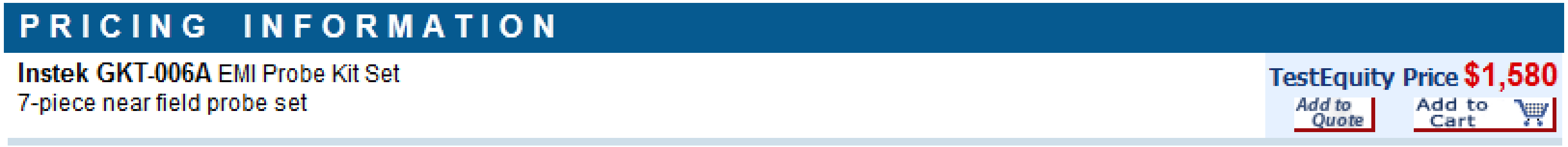
* Custom lengths available on special order

Availability: All H-field and E-field probes listed above are stock.

Quantity Discounts:
5% for two probes, 10% for 3 probes, 15% for 4-5 probes, types may be mixed.

- Kit of 5 H-field probes, one of each type: $1,650 (@ 19% discount) (Specify stock lengths of E301 & E401 probes)
- Kit of 1 each Of 5 H-field and 2 E-field probes: $1,950 (@ 21% discount) (Specify stock lengths of E301, E401, E601 & E701 probes)

Instek



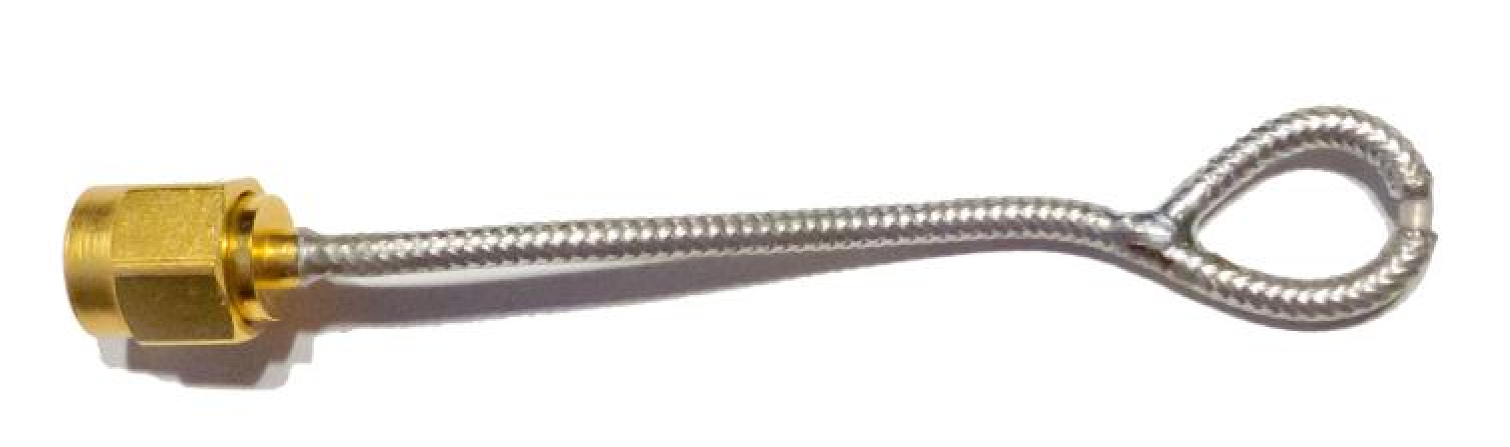
PRICING INFORMATION

Instek GKT-006A EMI Probe Kit Set
7-piece near field probe set

TestEquity Price $1,580

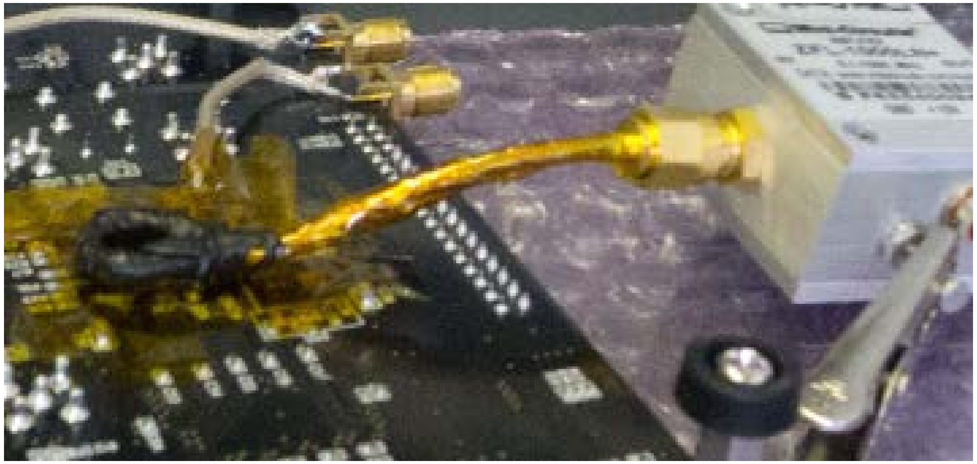
DIY: Example

Length of Semi-Rigid cable with SMA Connectors ($3 surplus) can be turned into a simple magnetic loop:

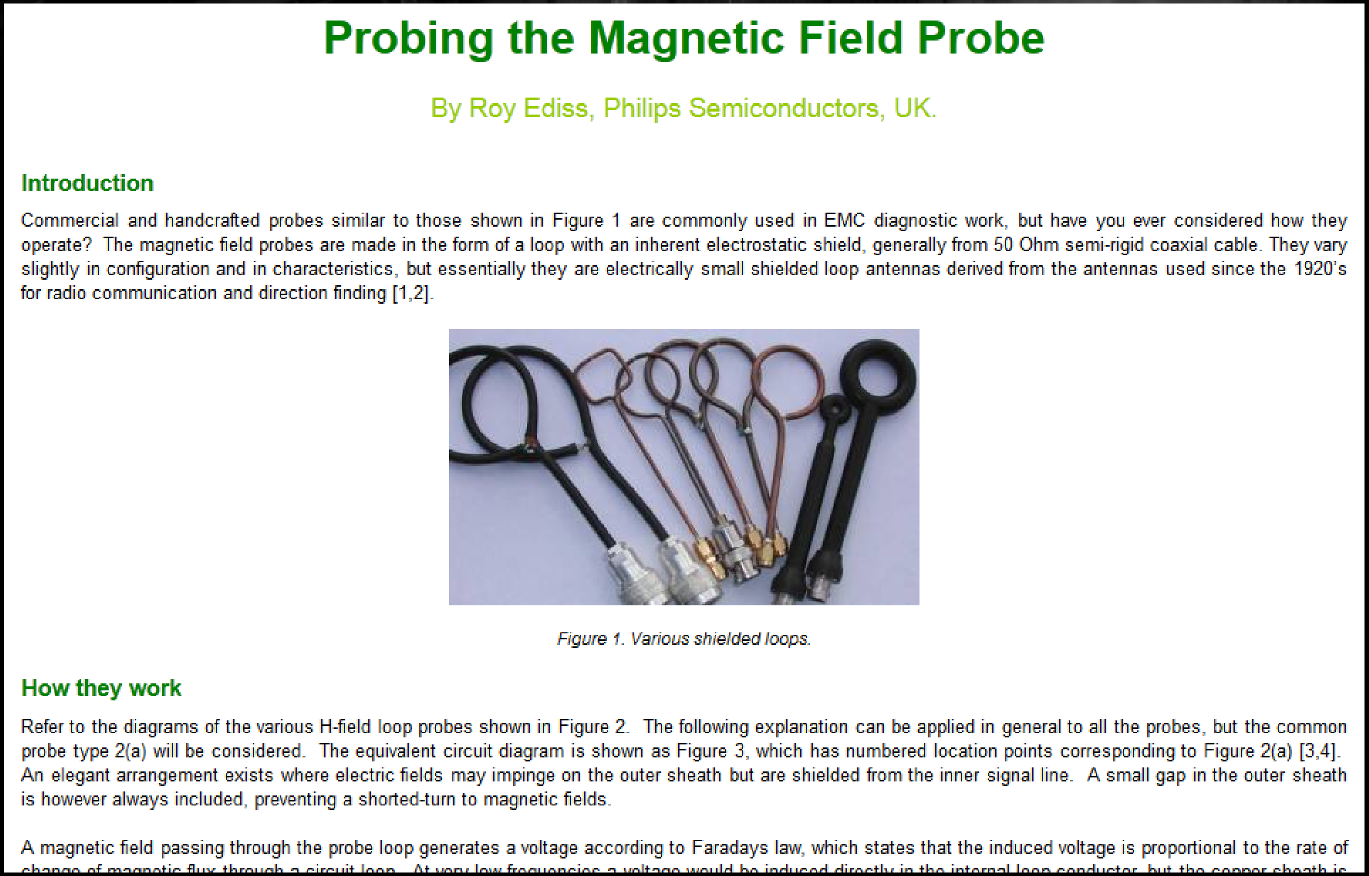


DIY: Example

Wrap entire thing in non-conductive tape (here I used self-fusing + polyimide) to avoid shorting out anything:



DIY: Some Useful References



Probing the Magnetic Field Probe

By Roy Ediss, Philips Semiconductors, UK.

Introduction

Commercial and handcrafted probes similar to those shown in Figure 1 are commonly used in EMC diagnostic work, but have you ever considered how they operate? The magnetic field probes are made in the form of a loop with an inherent electrostatic shield, generally from 50 Ohm semi-rigid coaxial cable. They vary slightly in configuration and in characteristics, but essentially they are electrically small shielded loop antennas derived from the antennas used since the 1920's for radio communication and direction finding [1,2].

Figure 1. Various shielded loops.

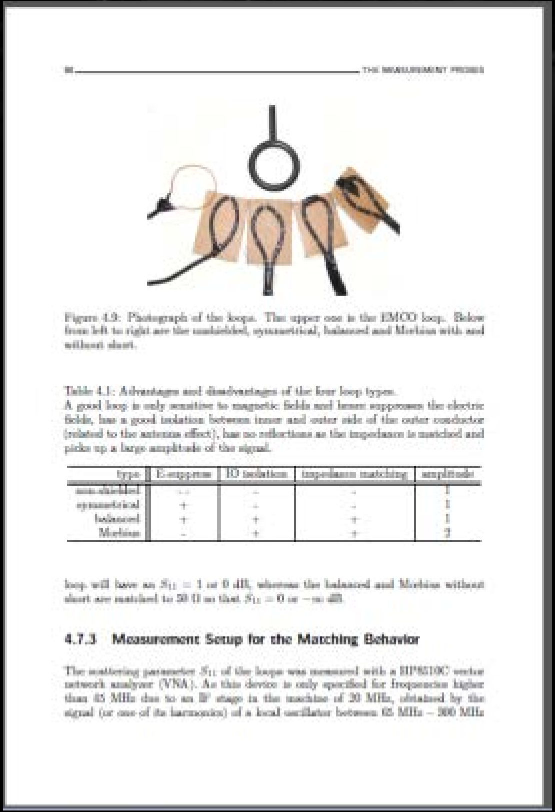
How they work

Refer to the diagrams of the various H-field loop probes shown in Figure 2. The following explanation can be applied in general to all the probes, but the common probe type 2(a) will be considered. The equivalent circuit diagram is shown as Figure 3, which has numbered location points corresponding to Figure 2(a) [3,4]. An elegant arrangement exists where electric fields may impinge on the outer sheath but are shielded from the inner signal line. A small gap in the outer sheath is however always included, preventing a shorted-turn to magnetic fields.

A magnetic field passing through the probe loop generates a voltage according to Faradays law, which states that the induced voltage is proportional to the rate of change of magnetic flux through a circuit loop. At very low frequencies a voltage would be induced directly in the internal loop conductor, but the copper sheath is

http://www.compliance-club.com/archive/old_archive/030718.htm

DIY: Some Useful References



88 THE MEASUREMENT PROBES

Figure 4.9: Photograph of the loops. The upper one is the EMCO loop. Below from left to right are the unshielded, symmetrical, balanced and Moebius with and without short.

Table 4.1: Advantages and disadvantages of the four loop types.
A good loop is only sensitive to magnetic fields and hence suppresses the electric fields, has a good isolation between inner and outer side of the outer conductor (related to the antenna effect), has no reflections as the impedance is matched and picks up a large amplitude of the signal.

type	E-suppress	IO isolation	impedance matching	amplitude
non-shielded	--	-	-	1
symmetrical	+	-	-	1
balanced	+	+	+	1
Moebius	-	+	+	2

loop will have an $S_{11} = 1$ or 0 dB, whereas the balanced and Moebius without short are matched to 50 Ω so that $S_{11} = 0$ or $-\infty$ dB.

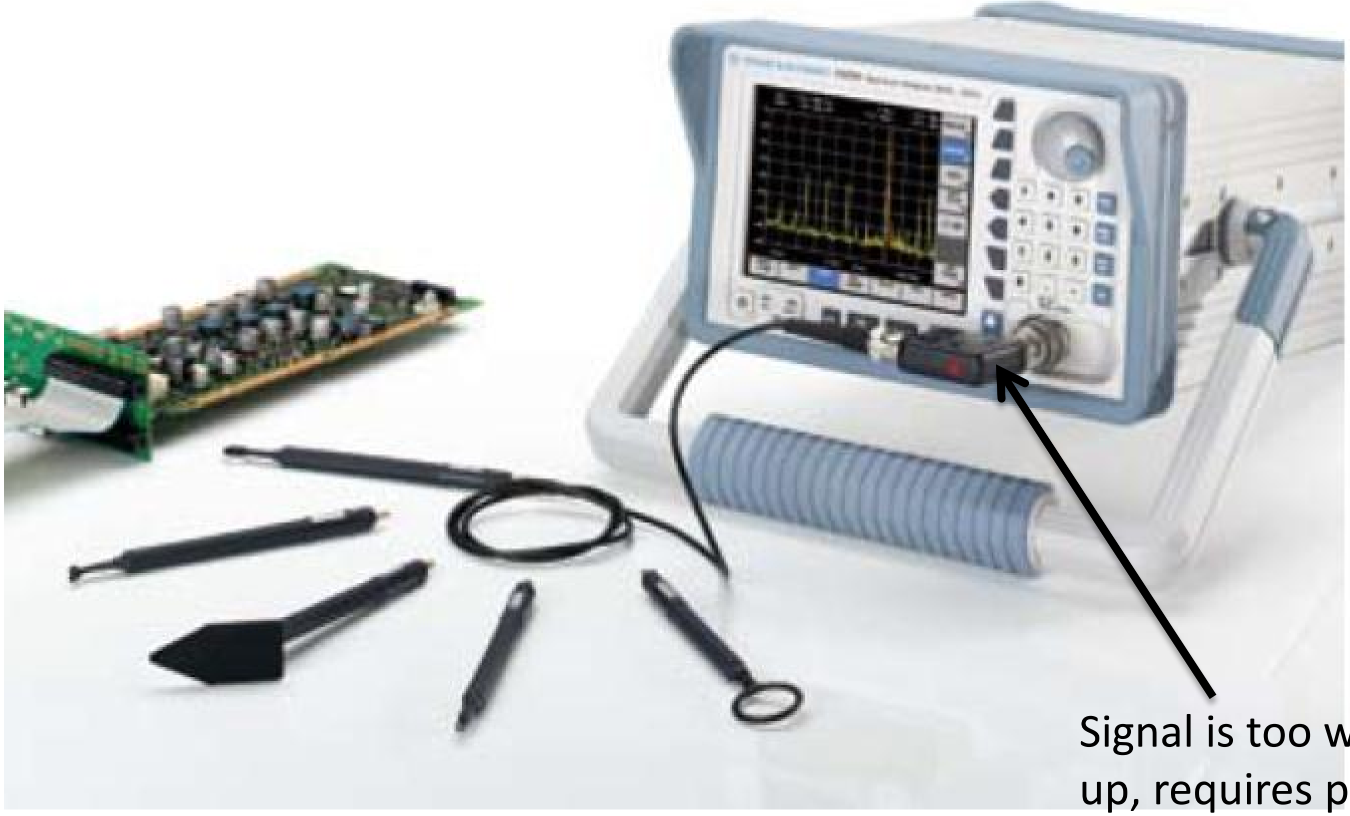
4.7.3 Measurement Setup for the Matching Behavior

The scattering parameter S_{11} of the loops was measured with a HP8510C vector network analyzer (VNA). As this device is only specified for frequencies higher than 45 MHz due to an IF stage in the machine of 20 MHz, obtained by the signal (or one of its harmonics) of a local oscillator between 65 MHz – 300 MHz

Elke De Mulder: Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices
http://www.cosic.esat.kuleuven.be/publications/thesis-182.pdf

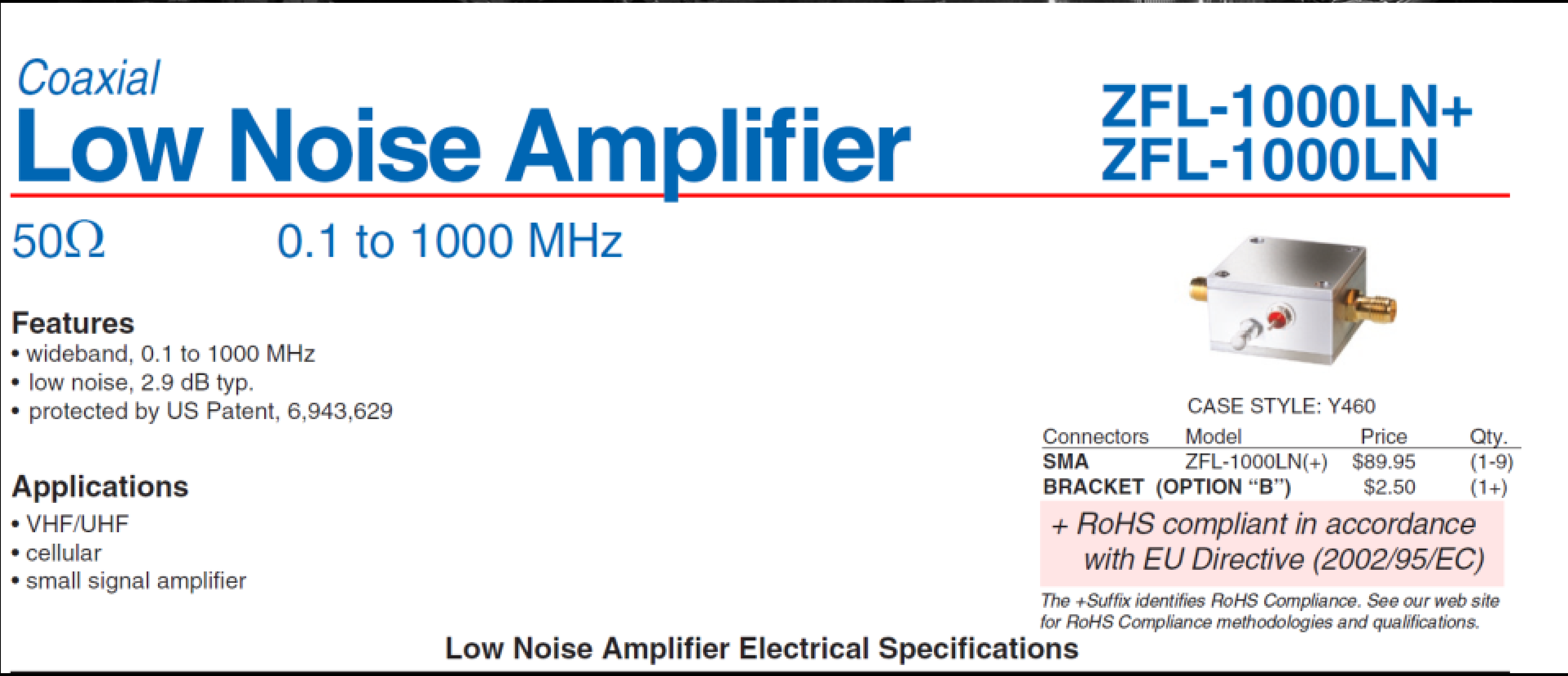
Pre-Amplifier (Probe or Other)

Pre-amplifier



Signal is too weak to be picked up, requires pre-amplifier in addition to probe.

Pre-amplifier: Buying One



Coaxial

Low Noise Amplifier

ZFL-1000LN+
ZFL-1000LN

50Ω 0.1 to 1000 MHz

Features

- wideband, 0.1 to 1000 MHz
- low noise, 2.9 dB typ.
- protected by US Patent, 6,943,629

Applications

- VHF/UHF
- cellular
- small signal amplifier

CASE STYLE: Y460

Connectors	Model	Price	Qty.
SMA	ZFL-1000LN(+)	$89.95	(1-9)
BRACKET (OPTION "B")		$2.50	(1+)

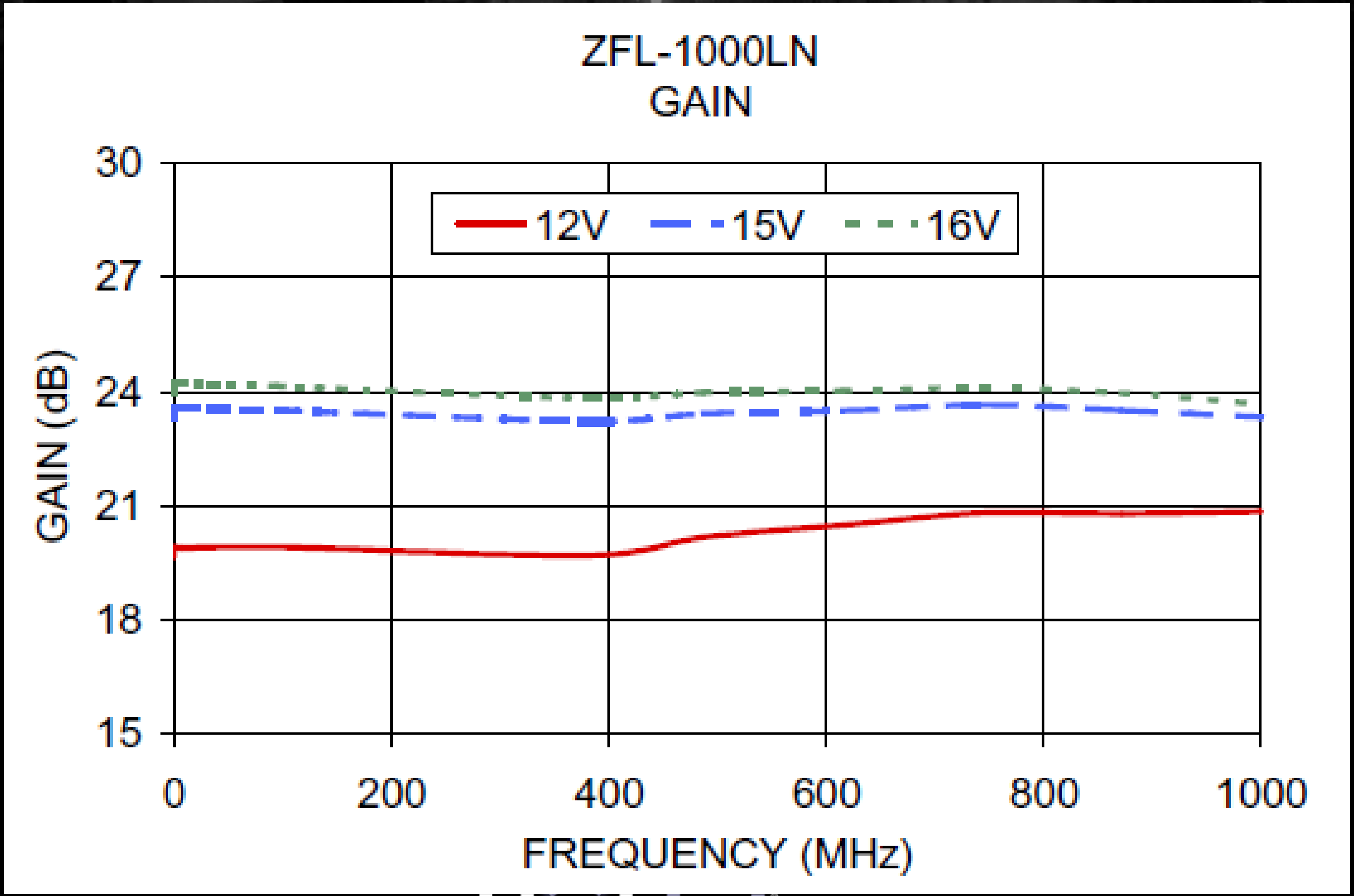
+ RoHS compliant in accordance with EU Directive (2002/95/EC)

The +Suffix identifies RoHS Compliance. See our web site for RoHS Compliance methodologies and qualifications.

Low Noise Amplifier Electrical Specifications

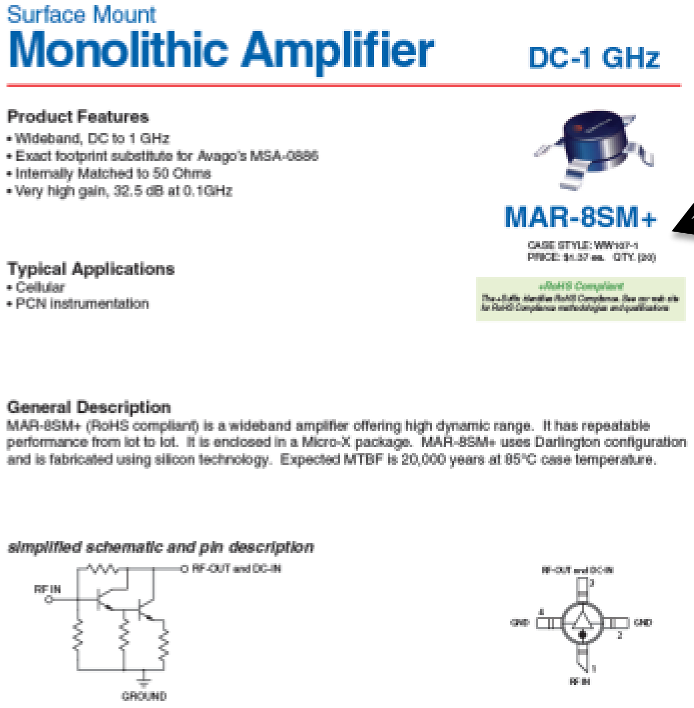
Assuming we are making a probe, there is no need to purchase the expensive pre-amplifier offered by that manufacture. Here is a 20 dB amplifier for $90, it was shown being used in another photo.

Pre-amplifier: Buying One



Pre-Amplifier: Making One

But we can get cheaper. We can make a pre-amplifier with similar characteristics for even less!



Surface Mount

Monolithic Amplifier DC-1 GHz

Product Features

- Wideband, DC to 1 GHz
- Exact footprint substitute for Avago's MSA-0886
- Internally Matched to 50 Ohms
- Very high gain, 32.5 dB at 0.1GHz

MAR-8SM+

CASE STYLE: WW107-1
PRICE: $1.37 ea. QTY. (20)

+RoHS Compliant
The +Suffix identifies RoHS Compliance. See our web site for RoHS Compliance methodologies and qualifications

Typical Applications

- Cellular
- PCN instrumentation

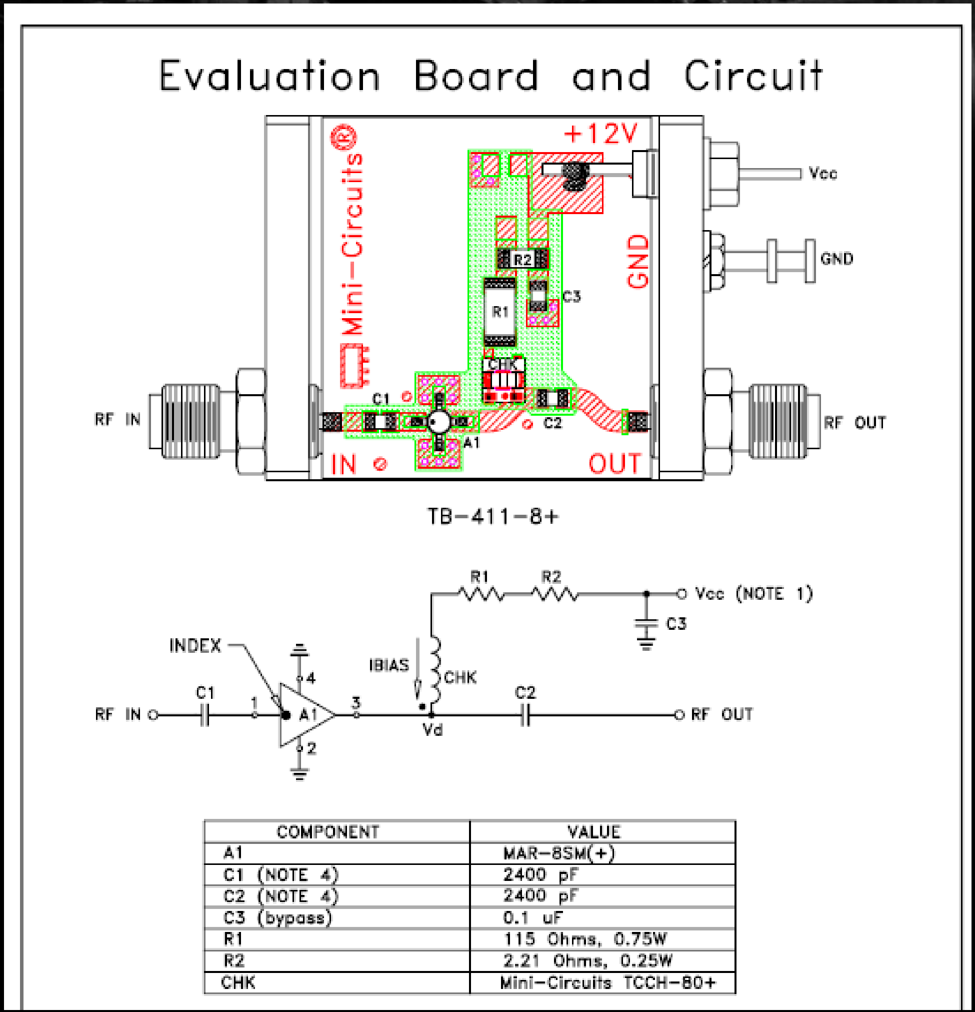
General Description

MAR-8SM+ (RoHS compliant) is a wideband amplifier offering high dynamic range. It has repeatable performance from lot to lot. It is enclosed in a Micro-X package. MAR-8SM+ uses Darlington configuration and is fabricated using silicon technology. Expected MTBF is 20,000 years at 85°C case temperature.

simplified schematic and pin description

Amplifier chip costs $2! Just needs a little support circuitry.

Pre-amplifier: Making One



Evaluation Board and Circuit

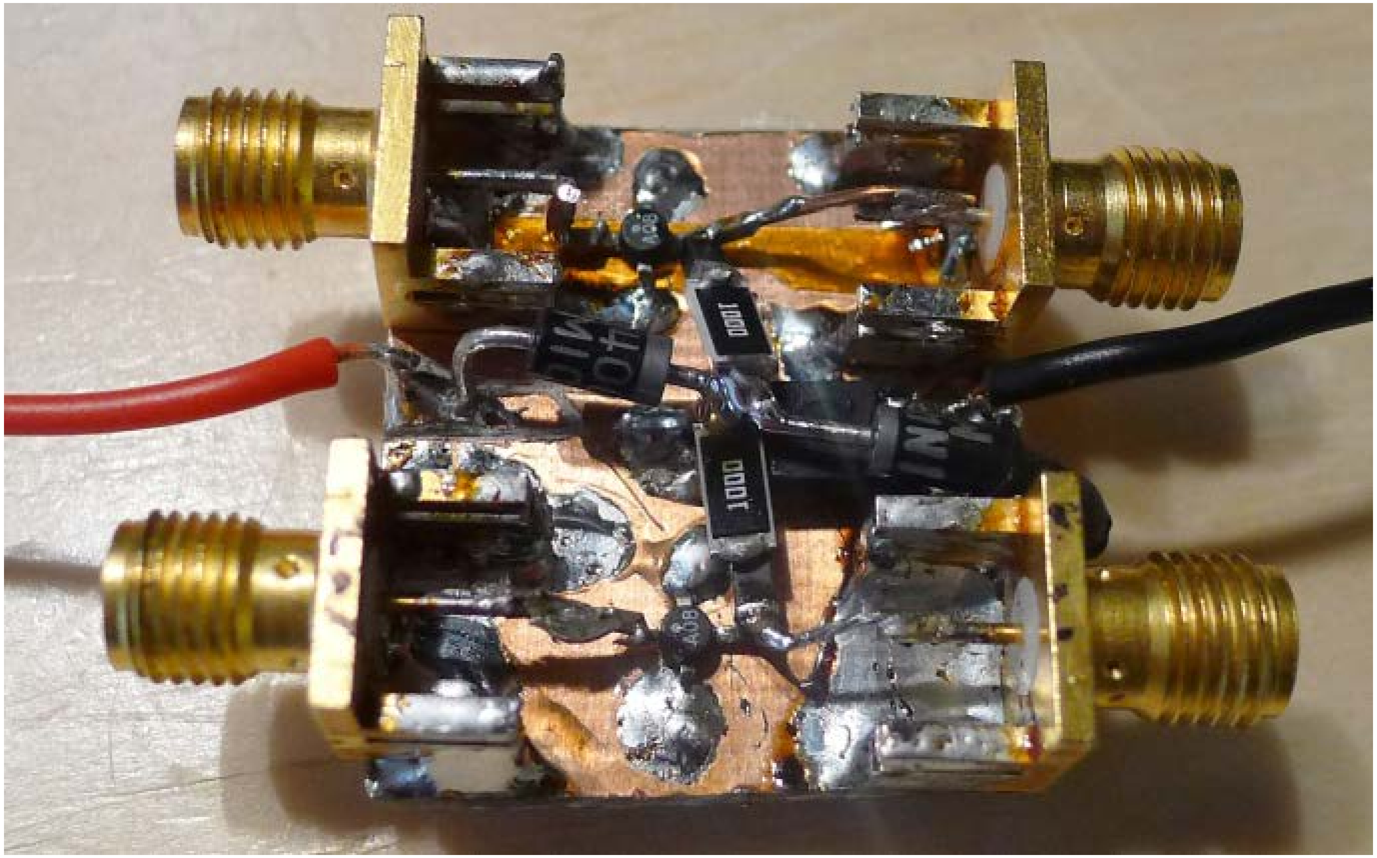
TB-411-8+

COMPONENT	VALUE
A1	MAR-8SM(+)
C1 (NOTE 4)	2400 pF
C2 (NOTE 4)	2400 pF
C3 (bypass)	0.1 uF
R1	115 Ohms, 0.75W
R2	2.21 Ohms, 0.25W
CHK	Mini-Circuits TCCH-80+

http://www.minicircuits.com/pcb/WTB-411-8+_P02.pdf

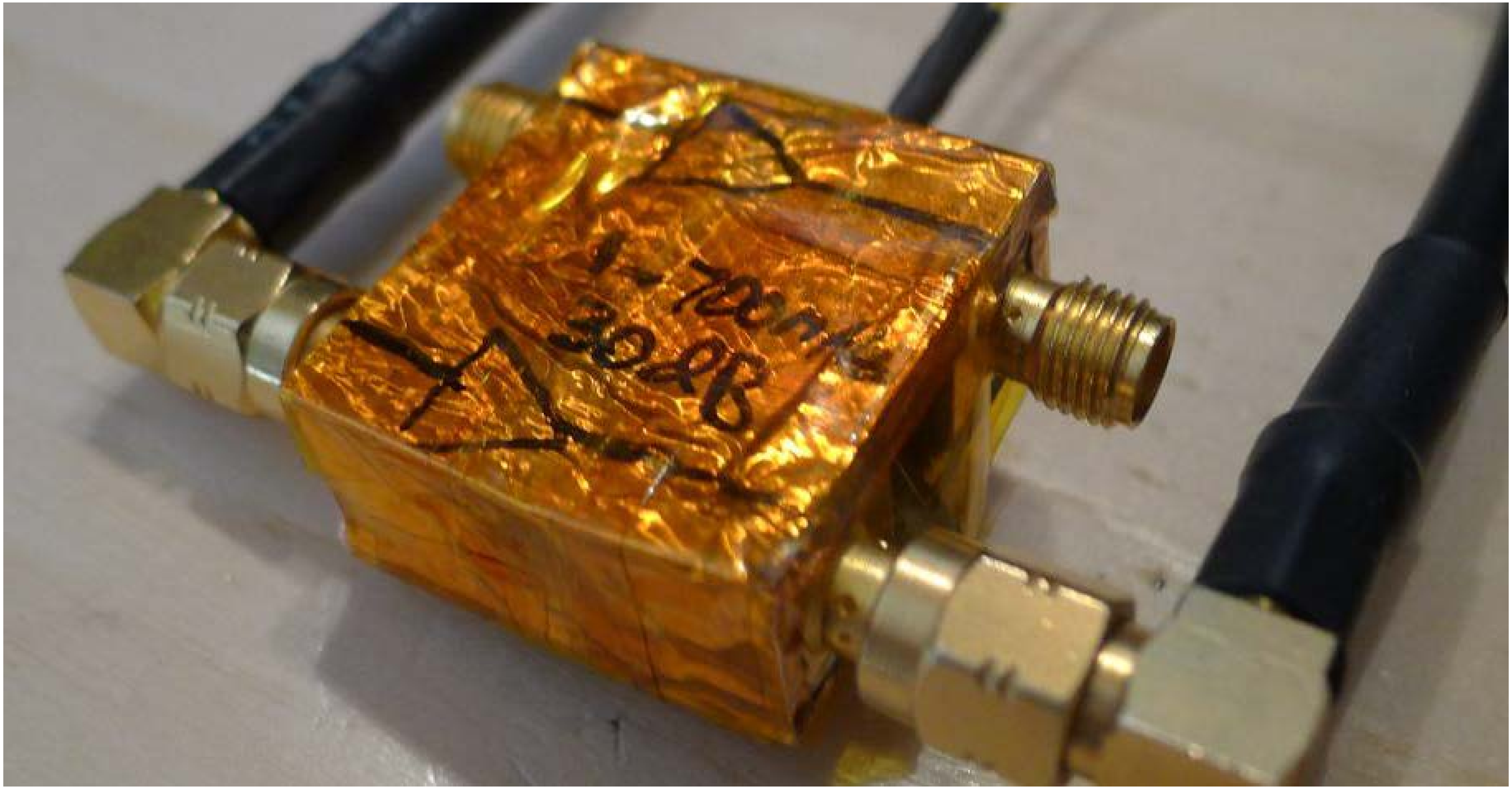
MiniCircuits lists full details of the required additional components

Building One: Even Cheaper



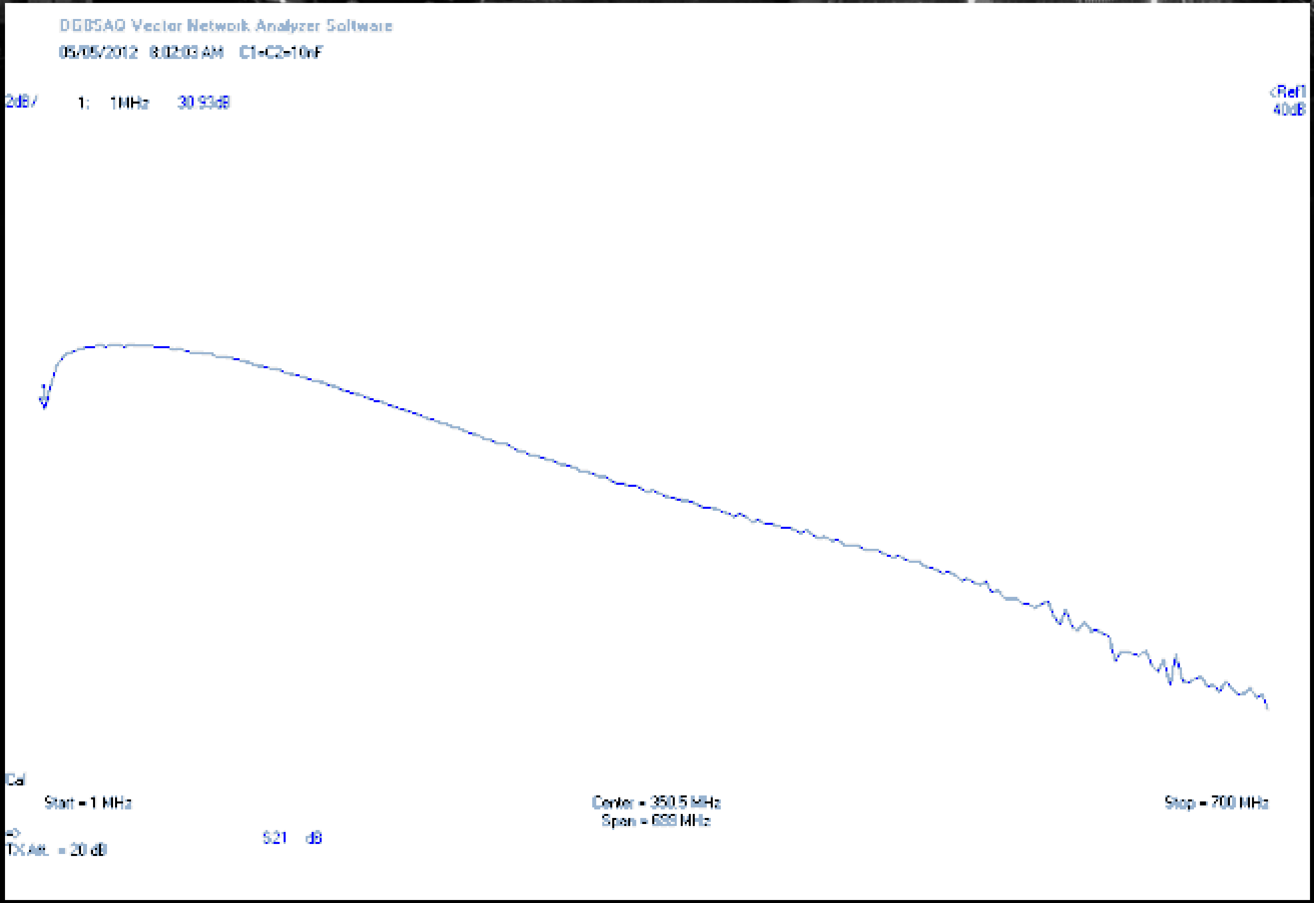
Here is an even cheaper version! Built on a piece of PCB, and has two channels to amplify different probes. This version has a voltage regulator on the bottom & protection diodes too, making it more robust than the basic schematic given.

Building One: Even Cheaper



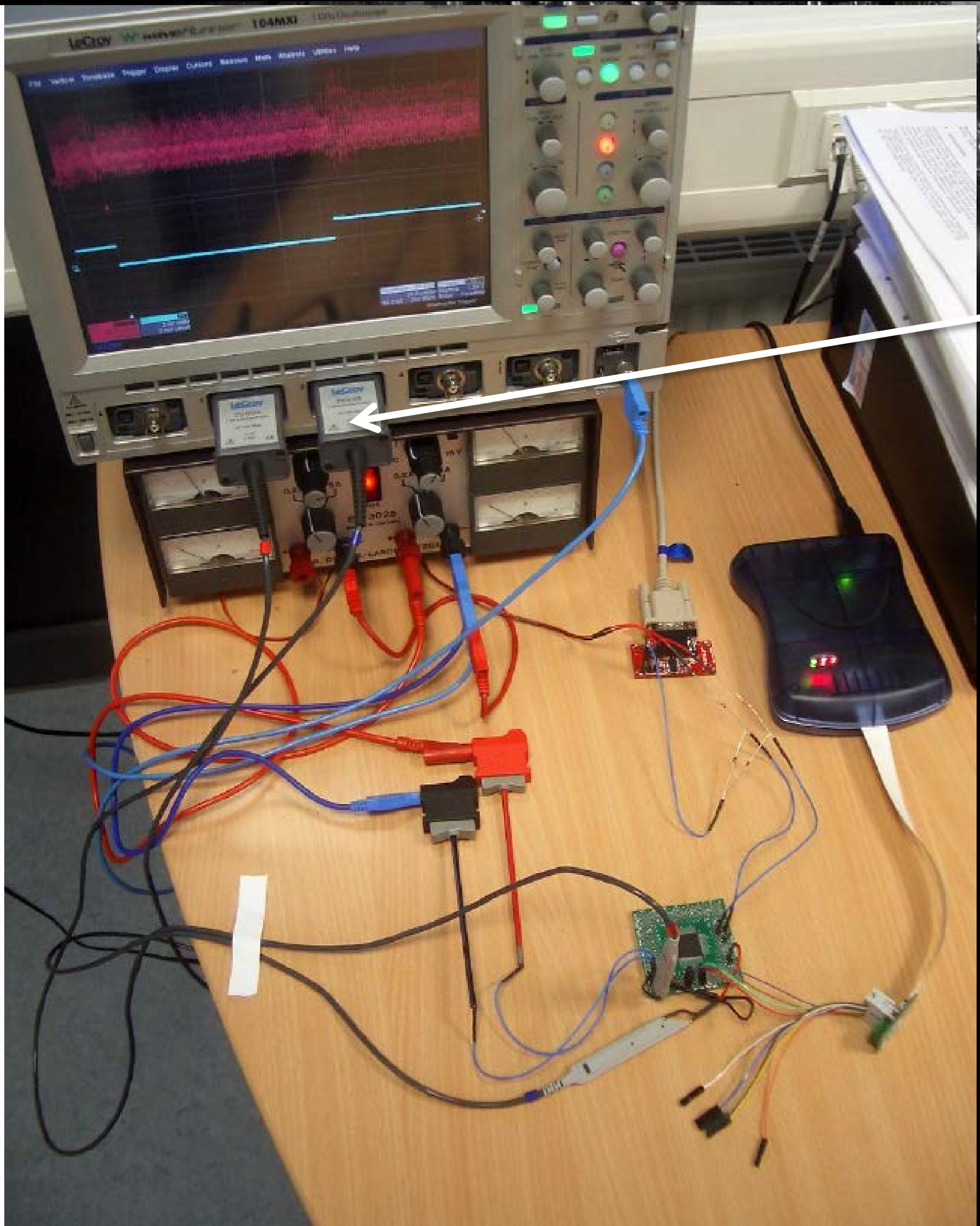
A PCB piece on top, some copper tape, and a final covering of non-conductive polyimide tape complete the amplifier. As a quick comparison to commercial ones let’s look at performance:

Building One: Results



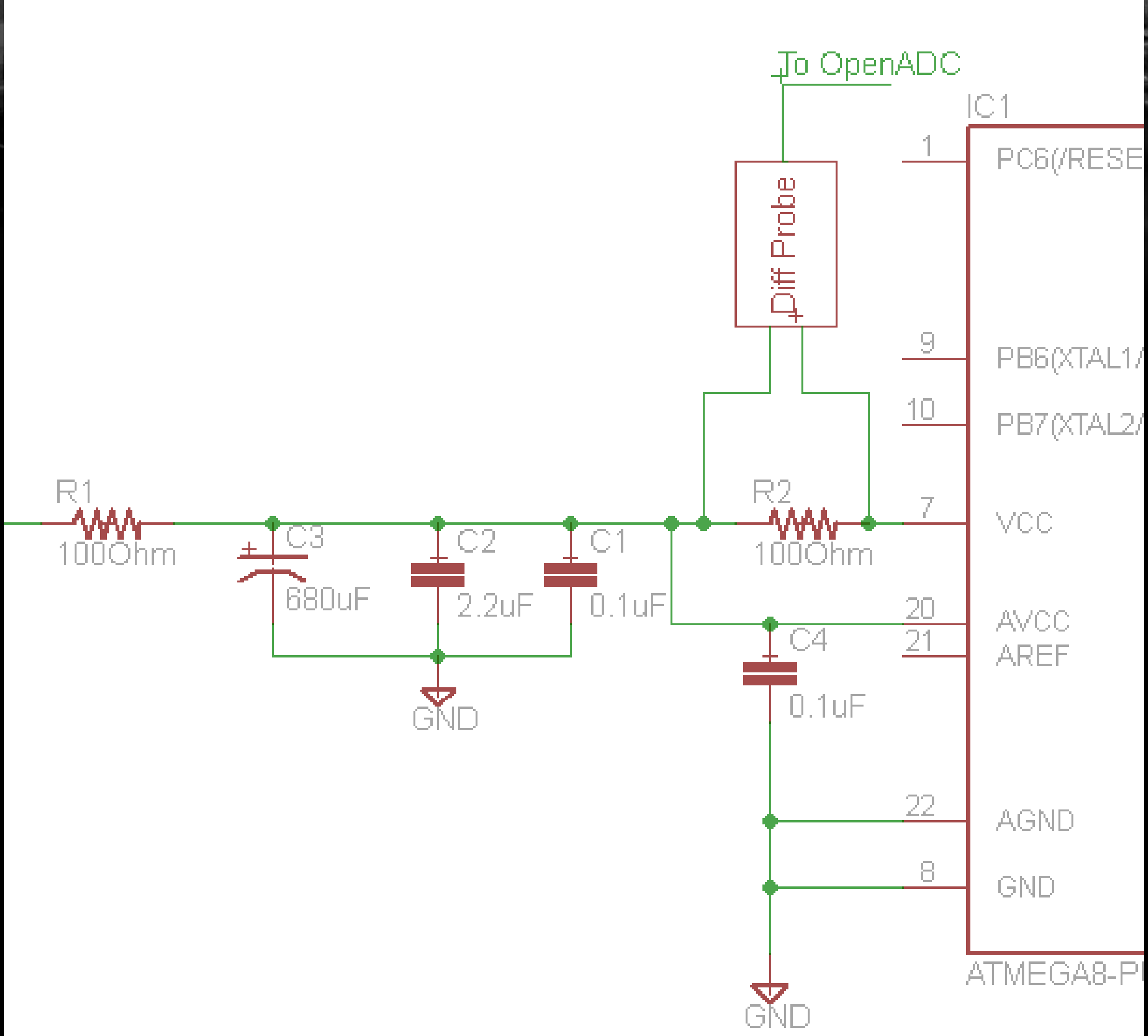
Here is the S21 measurement, showing amplifier gain. Gain varies from about 20-32 dB depending on frequency. The Noise Figure is below 3dB for this entire range.

Differential Probe

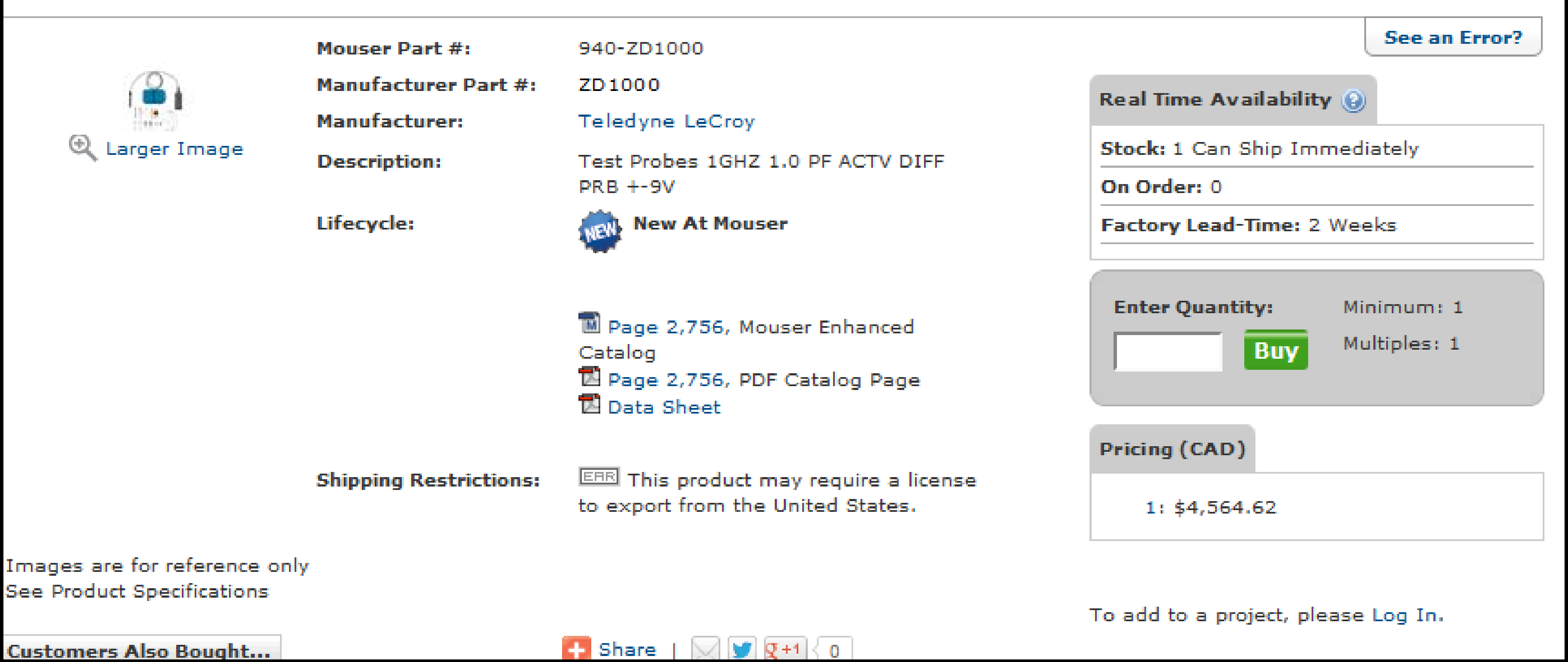


Differential Probe

From “**Side Channel Analysis of AVR XMEGA Crypto Engine”** by Ilya Kizhvatov


To OpenADC
IC1
Diff Probe
1
PC6(/RESE
9
PB6(XTAL1/
10
PB7(XTAL2/
R1
100Ohm
C3
680uF
C2
2.2uF
C1
0.1uF
R2
100Ohm
7
VCC
20
AVCC
21
AREF
C4
0.1uF
GND
22
AGND
8
GND
ATMEGA8-P
GND

What was that?



See an Error?

Mouser Part #:	940-ZD1000
Manufacturer Part #:	ZD1000
Manufacturer:	Teledyne LeCroy
Description:	Test Probes 1GHZ 1.0 PF ACTV DIFF PRB +-9V
Lifecycle:	NEW **New At Mouser**

Larger Image

Page 2,756, Mouser Enhanced Catalog

Page 2,756, PDF Catalog Page

Data Sheet

Shipping Restrictions: EAR This product may require a license to export from the United States.

Images are for reference only
See Product Specifications

Real Time Availability

Stock: 1 Can Ship Immediately

On Order: 0

Factory Lead-Time: 2 Weeks

Enter Quantity: Buy

Minimum: 1

Multiples: 1

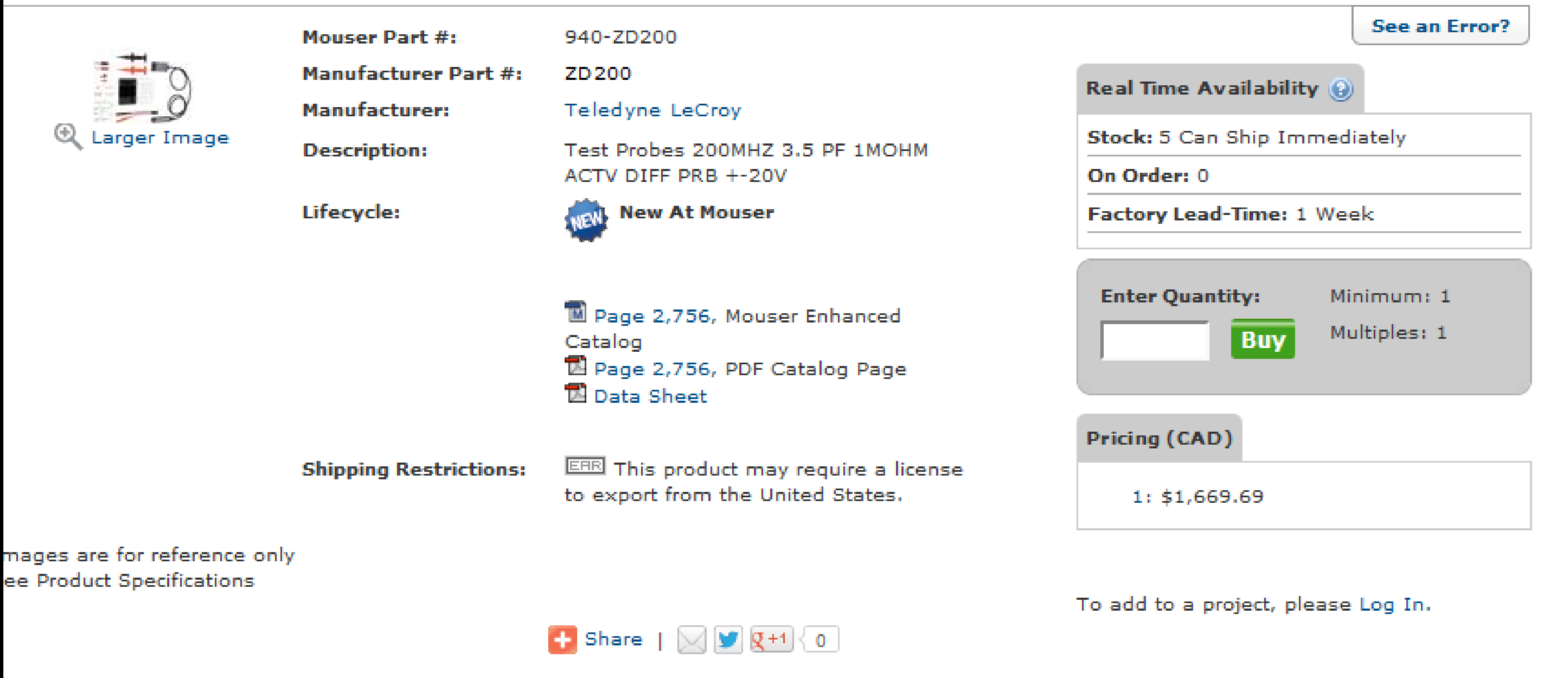
Pricing (CAD)

1: $4,564.62

To add to a project, please Log In.

Customers Also Bought...

We don't need 1000 MHz..



See an Error?

Mouser Part #: 940-ZD200

Manufacturer Part #: ZD200

Manufacturer: Teledyne LeCroy

Description: Test Probes 200MHZ 3.5 PF 1MOHM ACTV DIFF PRB +-20V

Lifecycle: NEW New At Mouser

Page 2,756, Mouser Enhanced Catalog

Page 2,756, PDF Catalog Page

Data Sheet

Shipping Restrictions: EAR This product may require a license to export from the United States.

mages are for reference only
ee Product Specifications

Real Time Availability

Stock: 5 Can Ship Immediately

On Order: 0

Factory Lead-Time: 1 Week

Enter Quantity: Minimum: 1

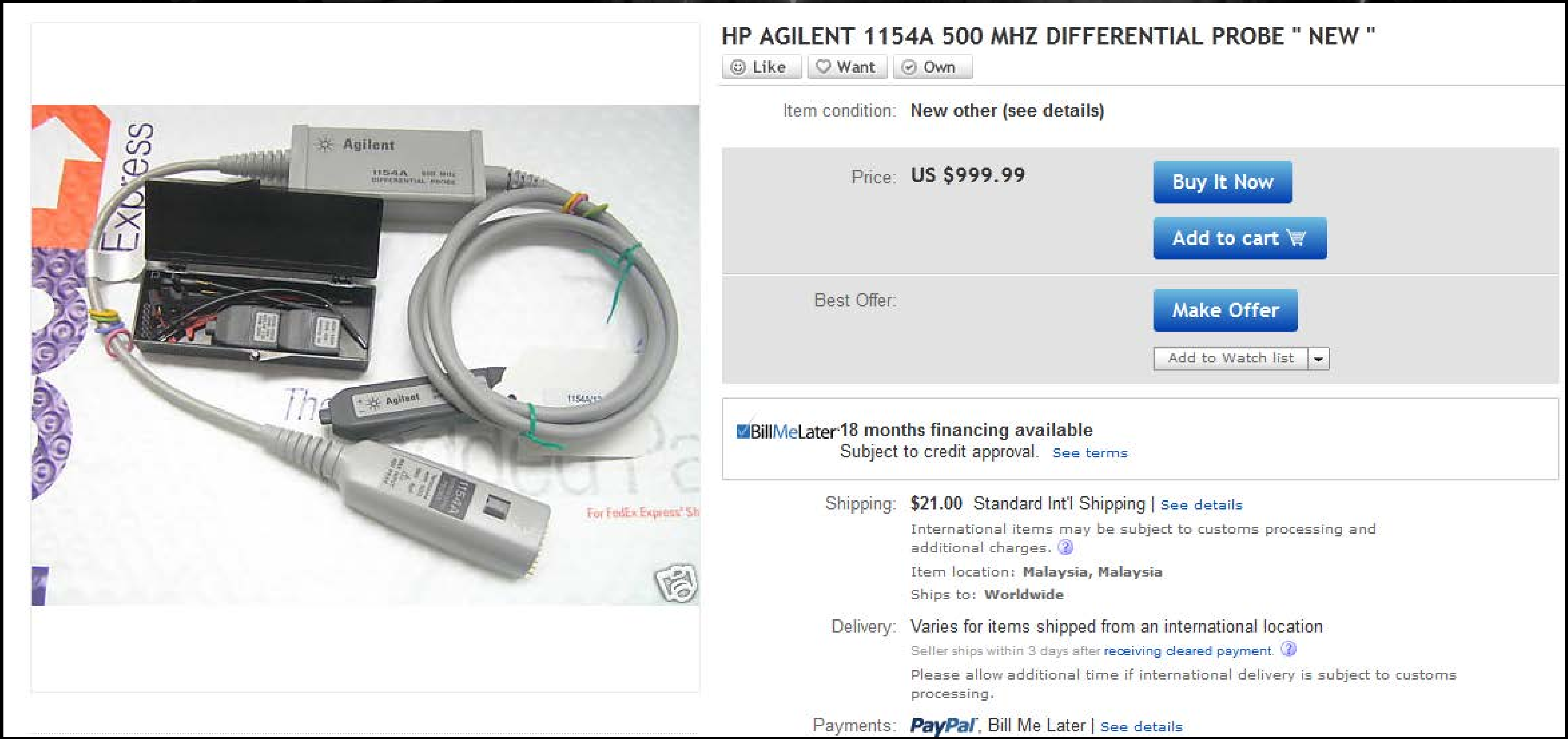
Multiples: 1

Pricing (CAD)

1: $1,669.69

To add to a project, please Log In.

Uh what about E-Bay?



HP AGILENT 1154A 500 MHZ DIFFERENTIAL PROBE " NEW "

Item condition: **New other (see details)**

Price: **US $999.99**

Best Offer:

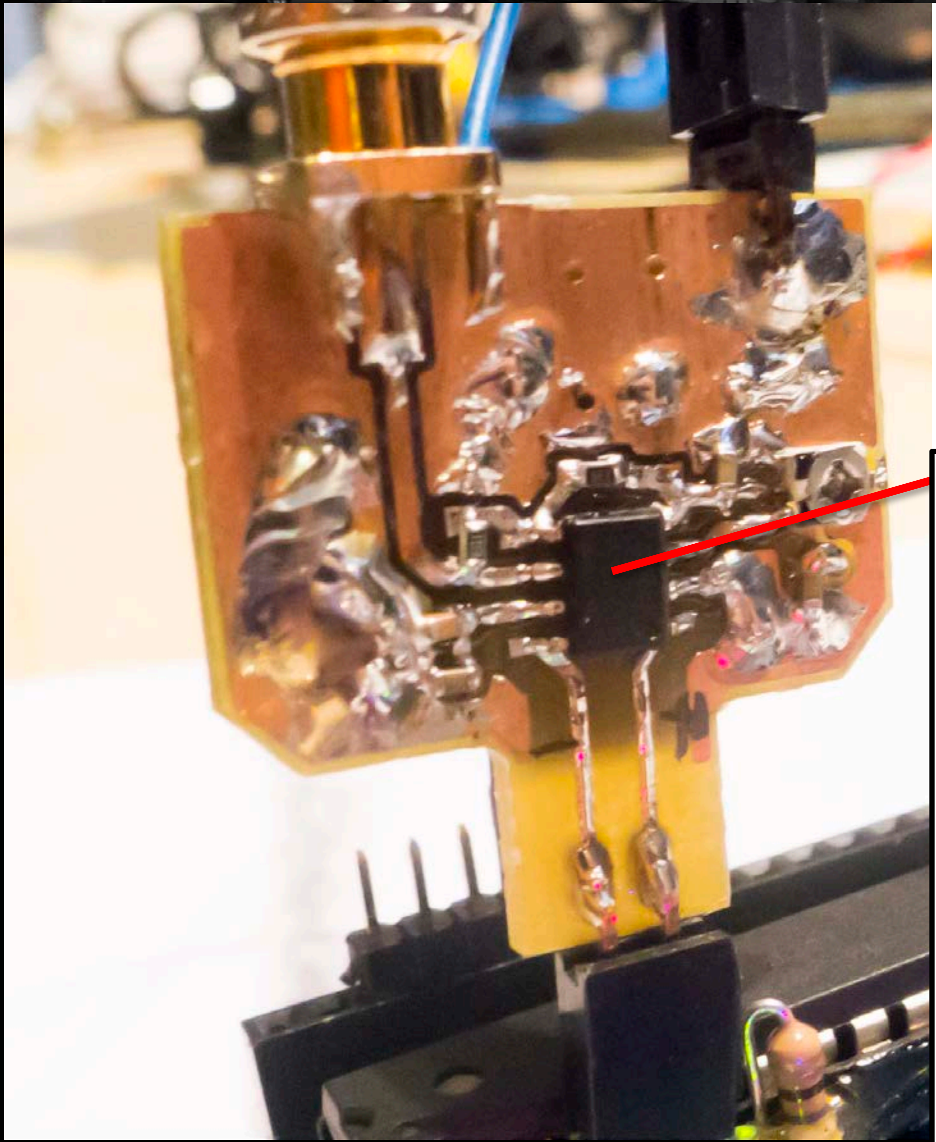
BillMeLater **18 months financing available**
Subject to credit approval. See terms

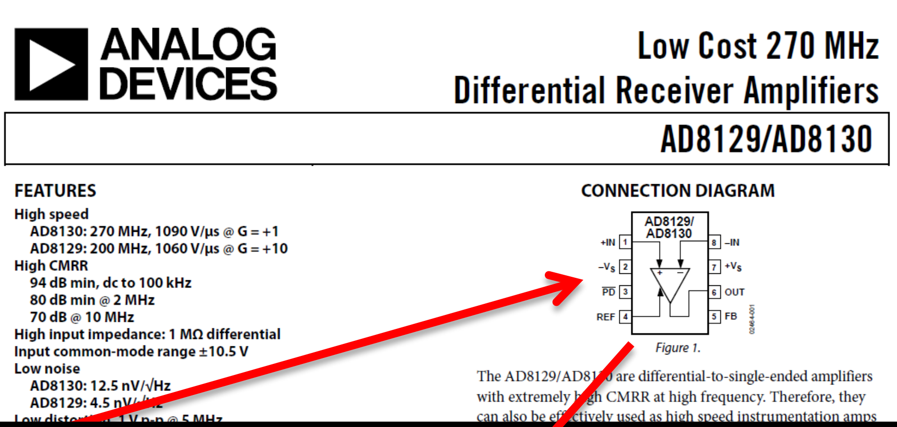
Shipping: $21.00 Standard Int'l Shipping | See details
International items may be subject to customs processing and additional charges.
Item location: **Malaysia, Malaysia**
Ships to: **Worldwide**

Delivery: Varies for items shipped from an international location
Seller ships within 3 days after receiving cleared payment.
Please allow additional time if international delivery is subject to customs processing.

Payments: PayPal, Bill Me Later | See details

How Cheap are you?





ANALOG DEVICES

Low Cost 270 MHz
Differential Receiver Amplifiers

AD8129/AD8130

FEATURES

High speed
- **AD8130: 270 MHz, 1090 V/μs @ G = +1**
- **AD8129: 200 MHz, 1060 V/μs @ G = +10**

High CMRR
- **94 dB min, dc to 100 kHz**
- **80 dB min @ 2 MHz**
- **70 dB @ 10 MHz**

High input impedance: 1 MΩ differential

Input common-mode range ±10.5 V

Low noise
- **AD8130: 12.5 nV/√Hz**
- **AD8129: 4.5 nV/√Hz**

Low distortion: 1 V p-p @ 5 MHz

CONNECTION DIAGRAM

Figure 1.

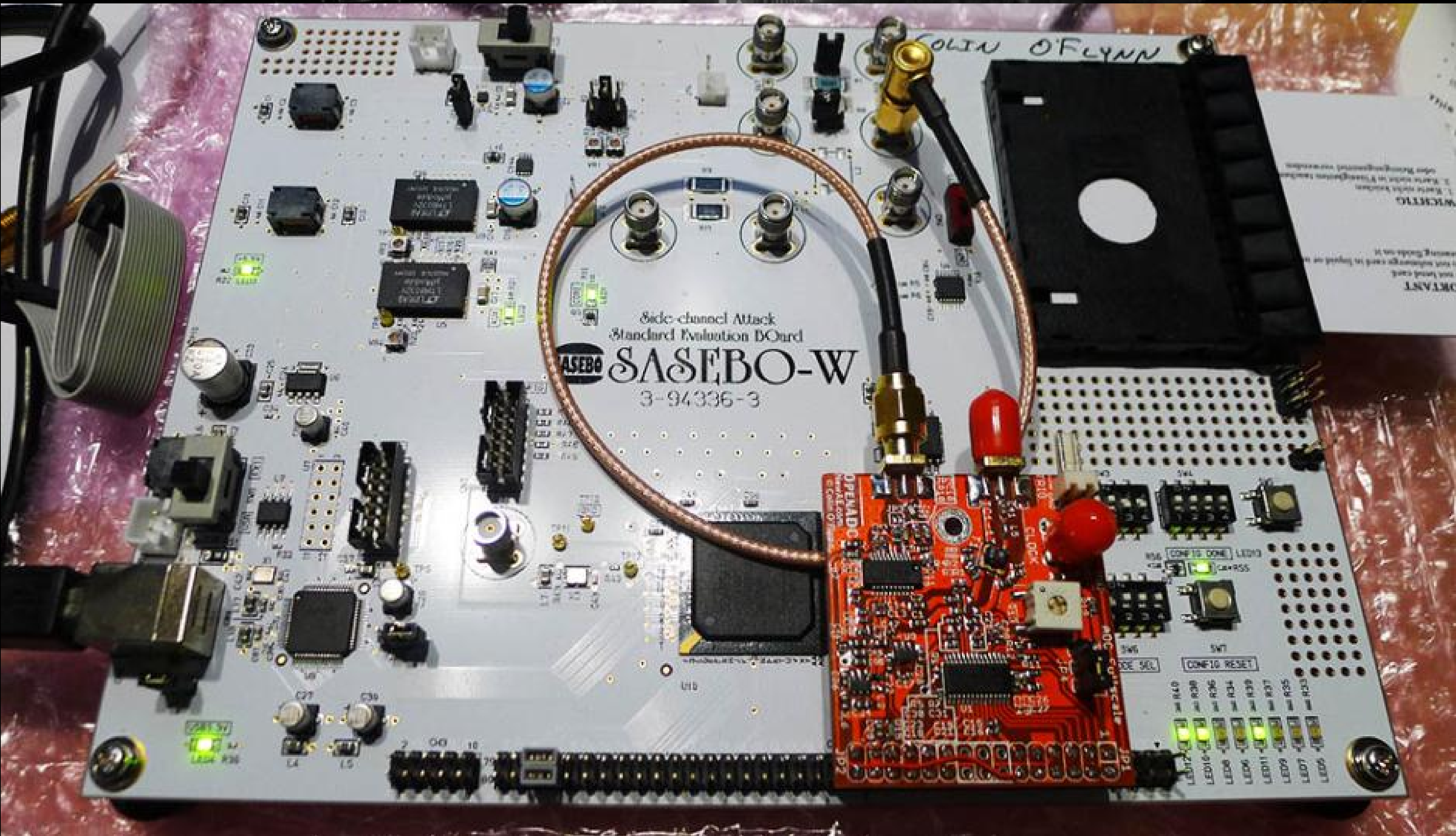
The AD8129/AD8130 are differential-to-single-ended amplifiers with extremely high CMRR at high frequency. Therefore, they can also be effectively used as high speed instrumentation amps

This chip is < $5 in single-unit quantities! Add a voltage supply & a few resistors/capacitors and you've got a pretty good probe.

Appendix: Targets

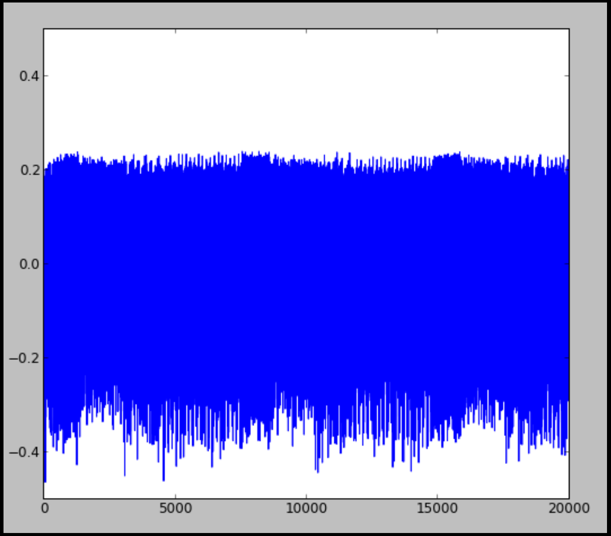
SASEBO-W Board

http://www.morita-tech.co.jp/SAKURA/en/hardware.html

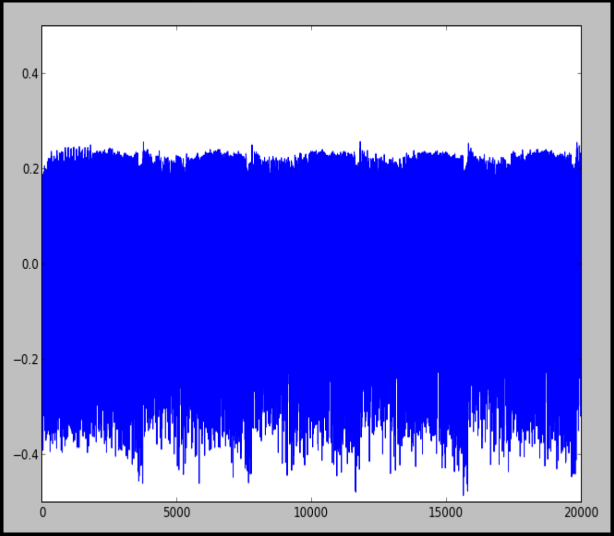


Example Results - AVR

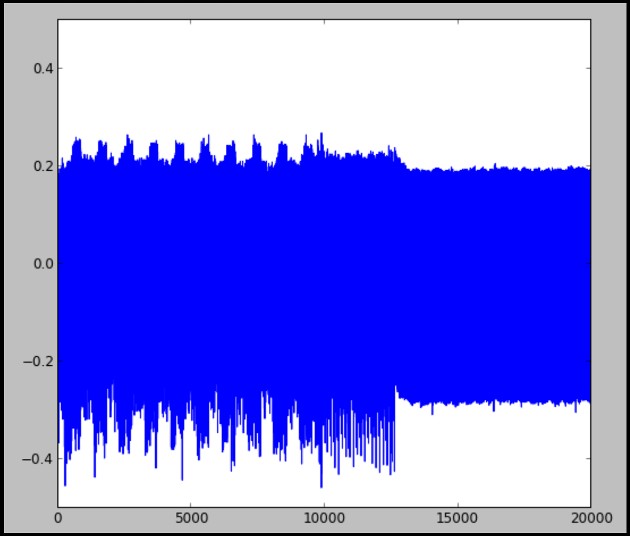
avr-crypto-lib in C



Straightforward C

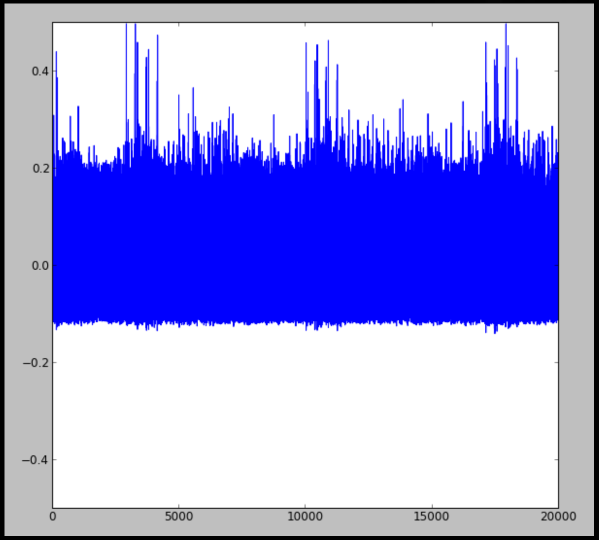


avr-crypto-lib in ASM

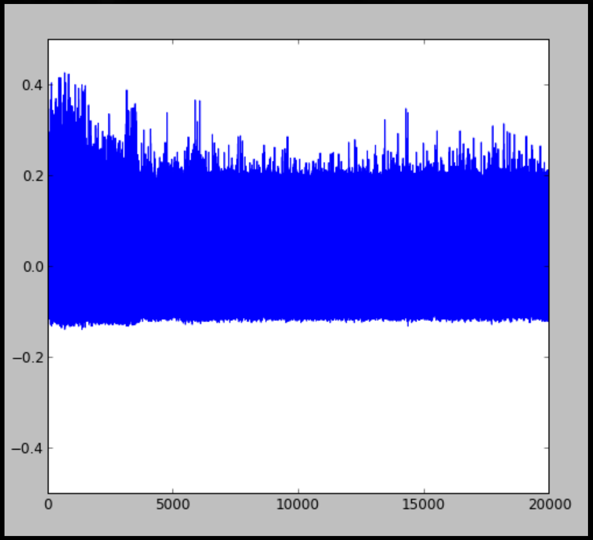


Example Results – XMega

avr-crypto-lib in C



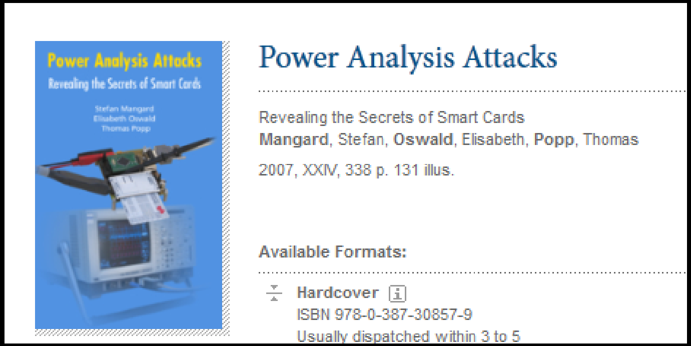
Hardware Implementation



Where to Go from Here?

Actions You Can Take

- Read the White Paper for more details including a 'Buying Guide' to start playing around – be SURE to check for updates to it on newae.com/blackhat
- There is a good book that covers a LOT:



Power Analysis Attacks

Revealing the Secrets of Smart Cards
Mangard, Stefan, **Oswald**, Elisabeth, **Popp**, Thomas

2007, XXIV, 338 p. 131 illus.

Available Formats:

Hardcover
ISBN 978-0-387-30857-9
Usually dispatched within 3 to 5

- Read original DPA Paper by Kocher, look at CHES & COSADE Proceedings
- **HINT**: Local universities often have access to all these, so use a computer on their network (e.g. from library)

Colin’s Blackhat Tour 2012/13

Blackhat Europe 2013 (You are Here)

- Introduction of open-source attack platform, better attacks
- Demo of other attacks

Blackhat Design West 2013:

- Introduction of open-source hardware targets
- Improvements to ChipWhisperer-Analyzer

Blackhat Las Vegas 2013 (Pending):

- Introduction of open-source complete HW package (targets, probes, etc)

Questions Etc.

Visit me on internet: newae.com/blackhat
chipwhisperer.com

E-mail me: coflynn@newae.com

Please complete the Speaker Feedback Surveys!

(Unless you didn’t like my presentation)