SIDE CHANNEL ANALYSIS FOR CHEAPSKATES

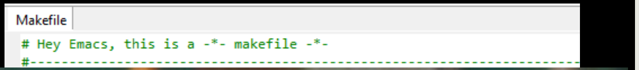
AKA: REAL Hardware Hacking

COLIN O'FLYNN

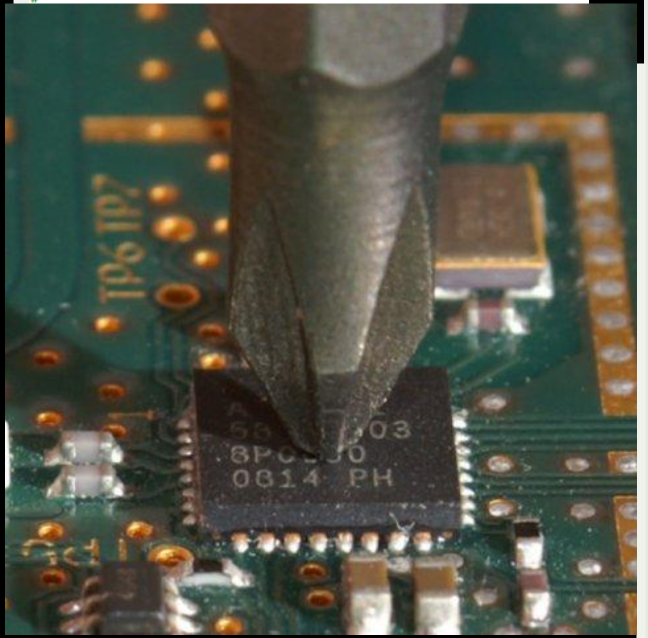
My Funding Provided By:

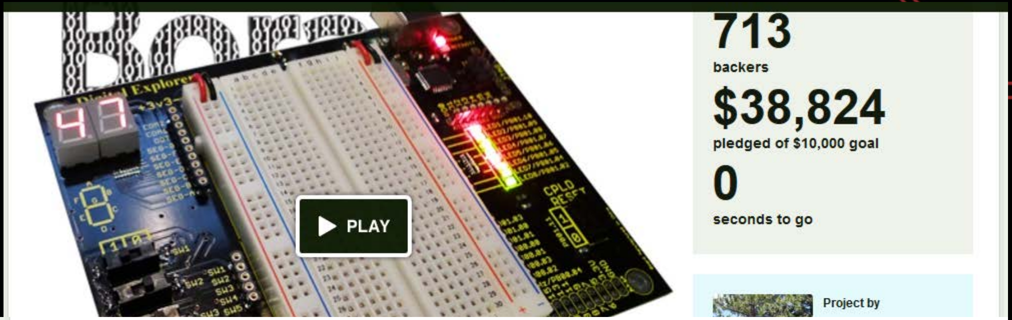
DALHOUSIE UNIVERSITY *Inspiring Minds*

NSERC CRSNG


Makefile

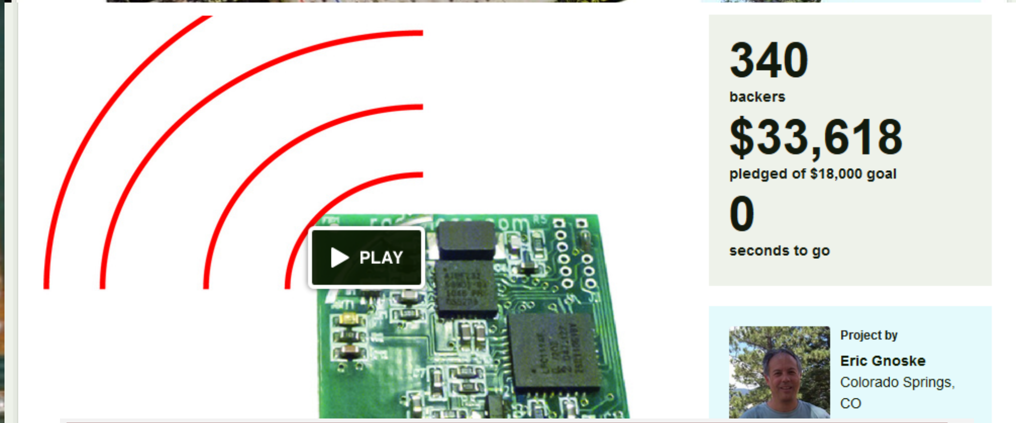
```
# Hey Emacs, this is a -*- makefile -*-
#----------------------------------------------------------------------------
```





713
backers
$38,824
pledged of $10,000 goal
0
seconds to go

Project by



340
backers
$33,618
pledged of $18,000 goal
0
seconds to go

Project by
Eric Gnoske
Colorado Springs, CO

Design a FIR Filter in an FPGA in 30 mins using High Level Synthesis

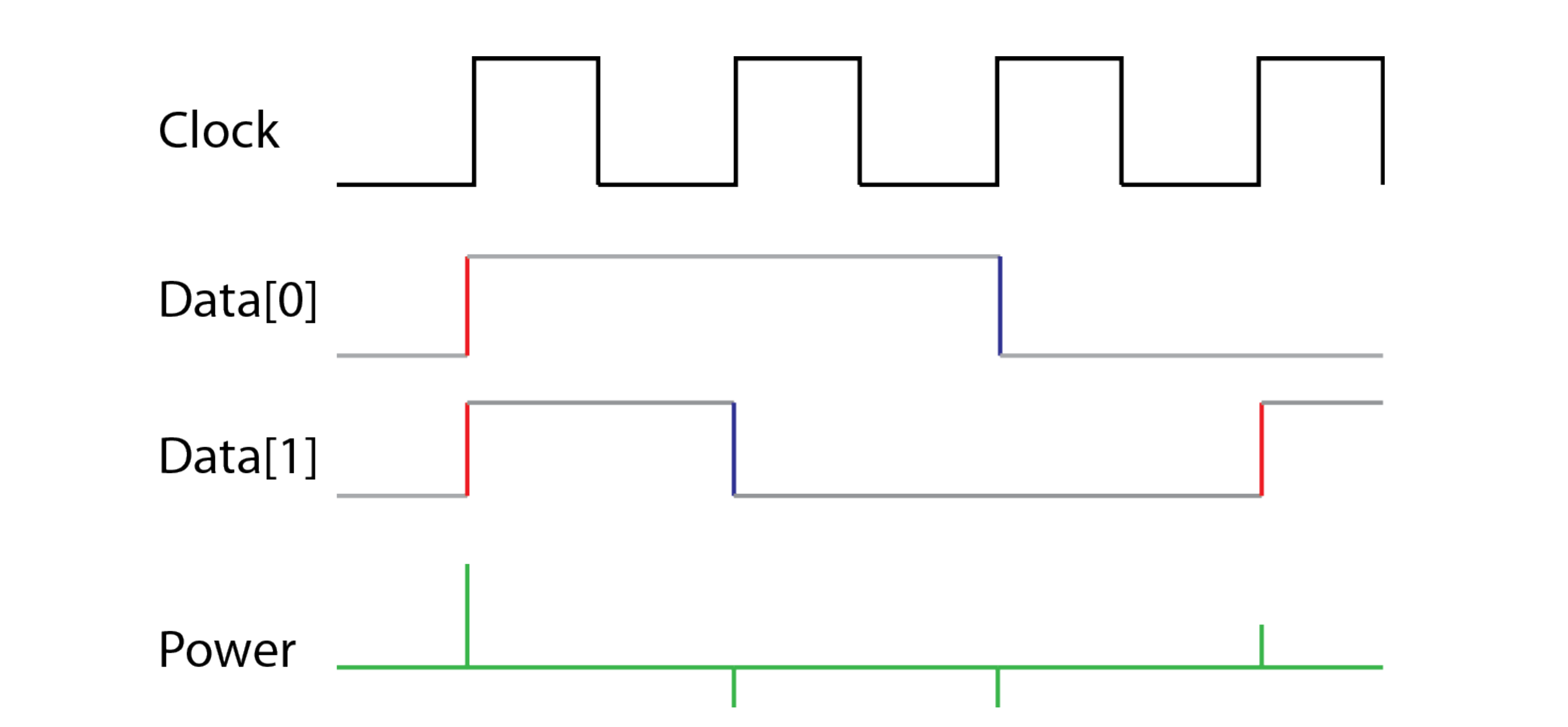
FIR Filter Design with HLS
Abusing Xilinx's Tools for Fun & Profit

I've been working with Xilinx's new High Level Synthesis tools built into Vivado. I'm slowly working on posting some more complete tutorials. In the mean-time **here** is a simple tutorial about making **a Finite Impulse Response Filter** on a real ADC/DAC board .

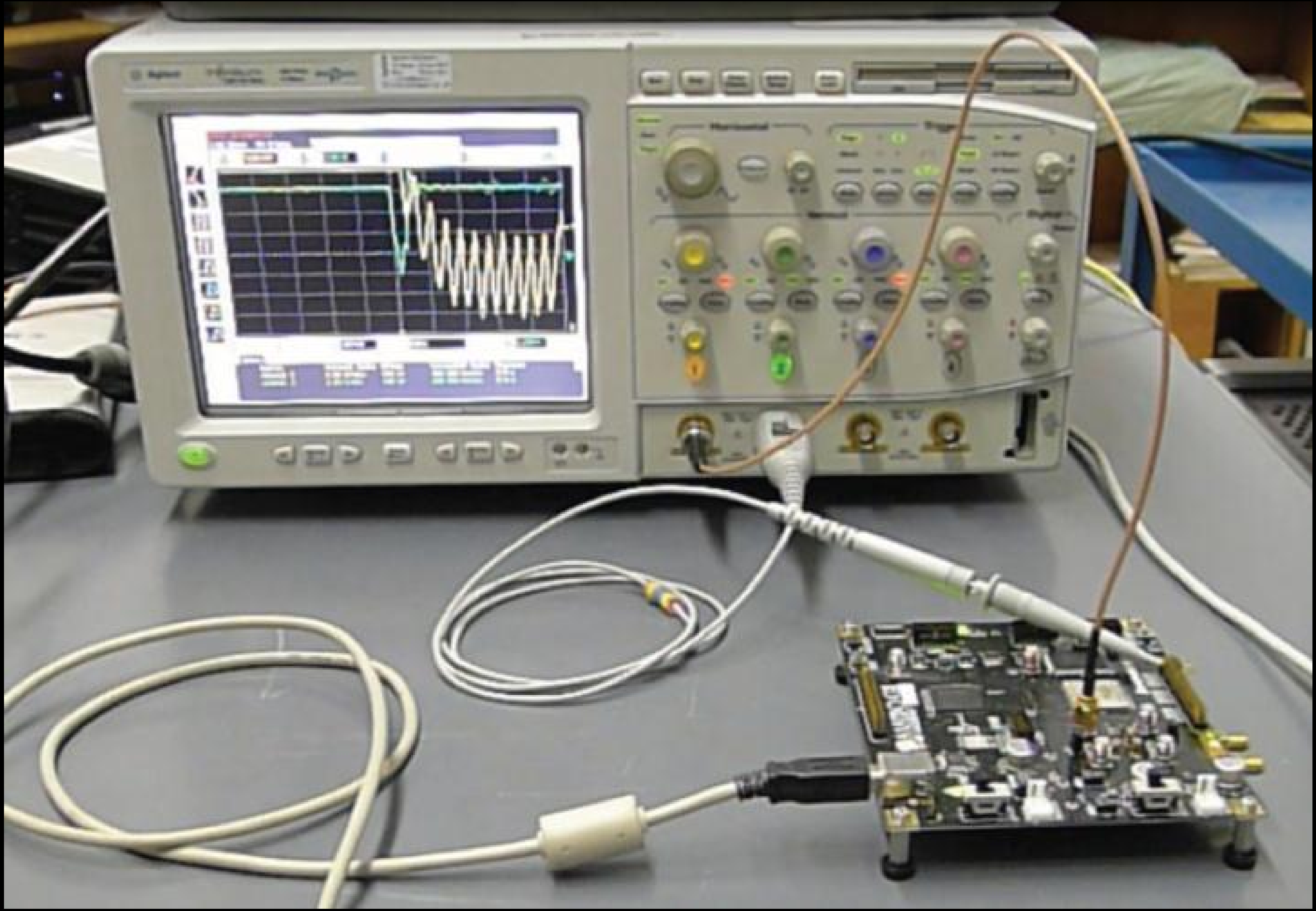
Permalink | **Leave a comment**

60-Second Version

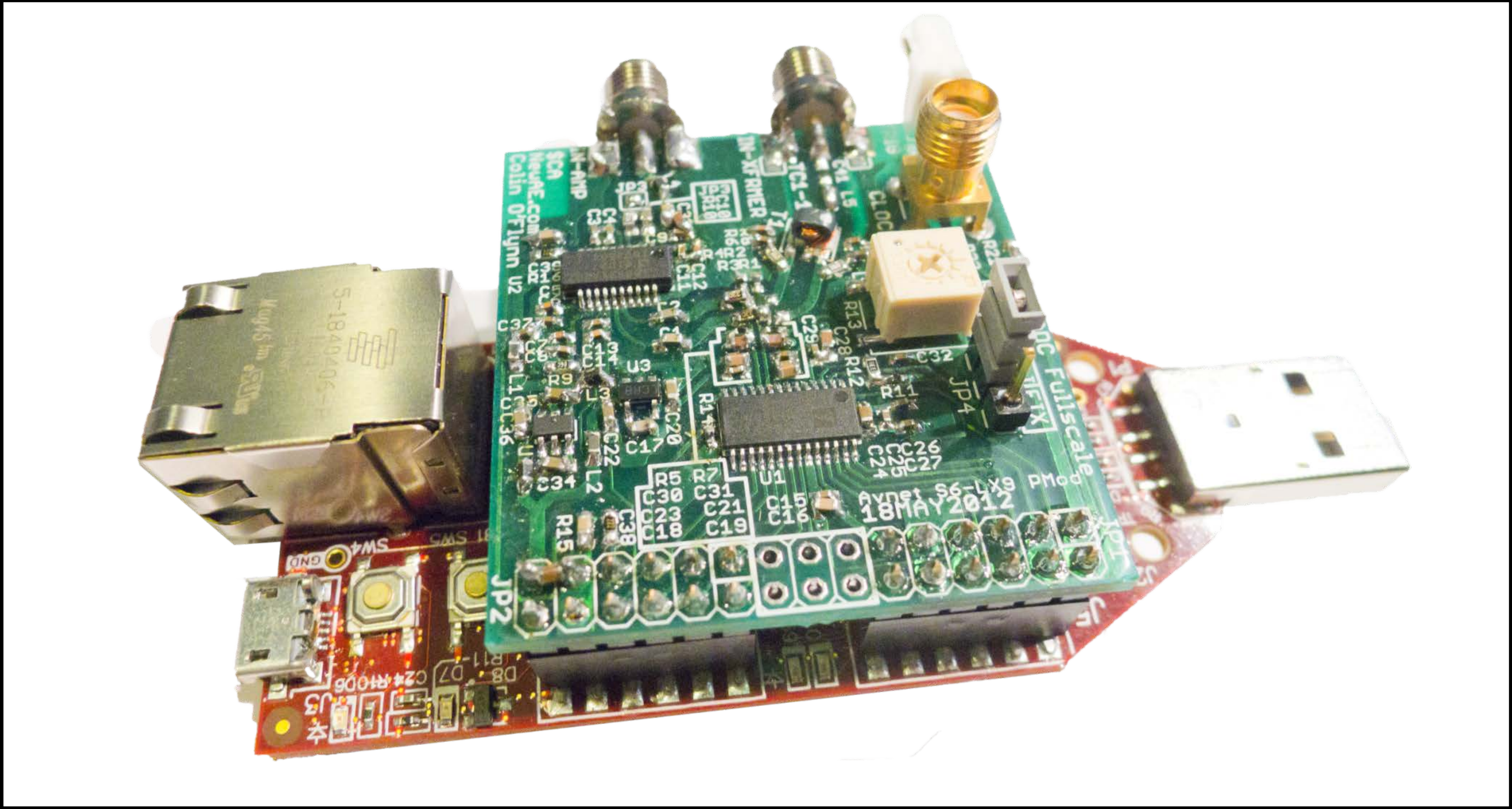
60-Second Version



60-Second Version



60-Second Version

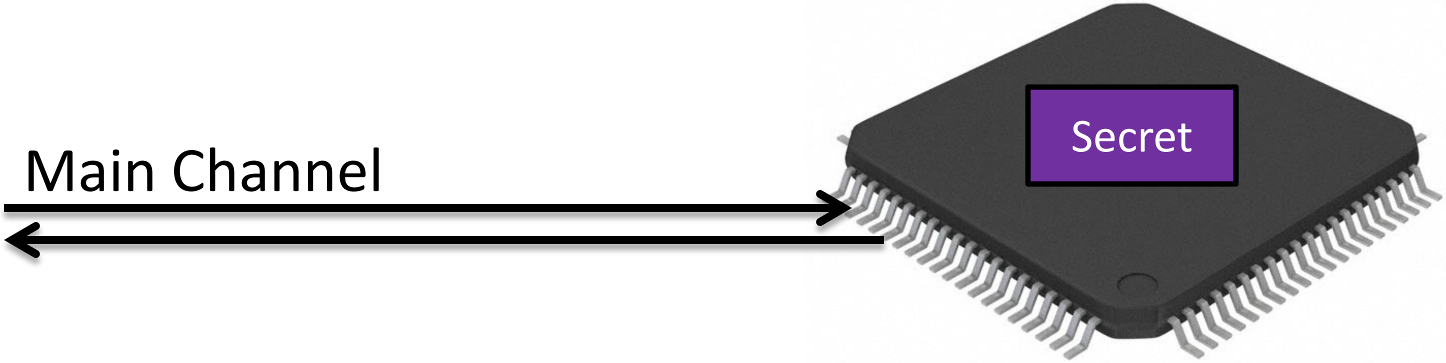


Motivation

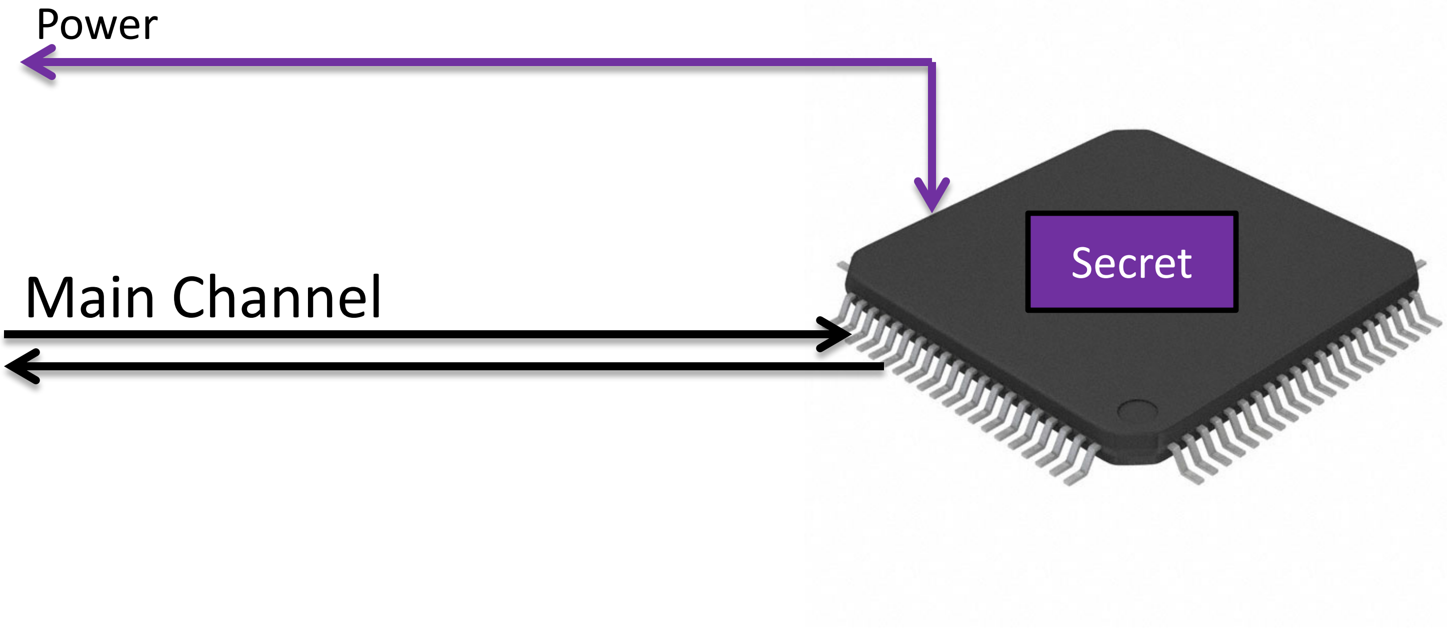
- **Not** for 1337 H4X0|25
- You WILL have to learn how the attacks work, understand the (fairly small) amount of math
- You WILL have to learn about hardware design, software programming of both target & software, etc
- You WILL get frustrated, run into bugs with my tools, and have to fix/debug them yourself

THE SIDE CHANNEL

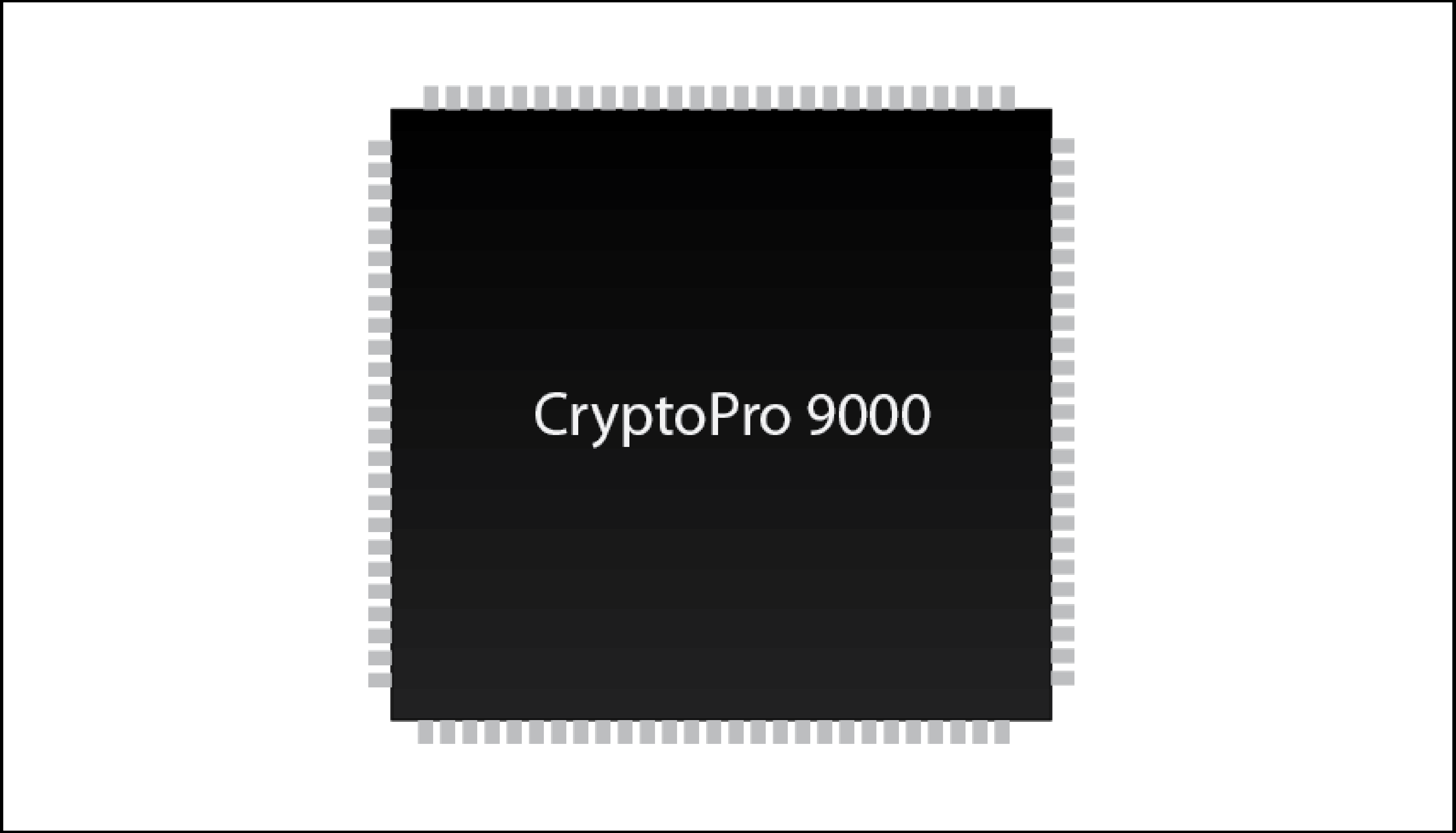
Side Channel?



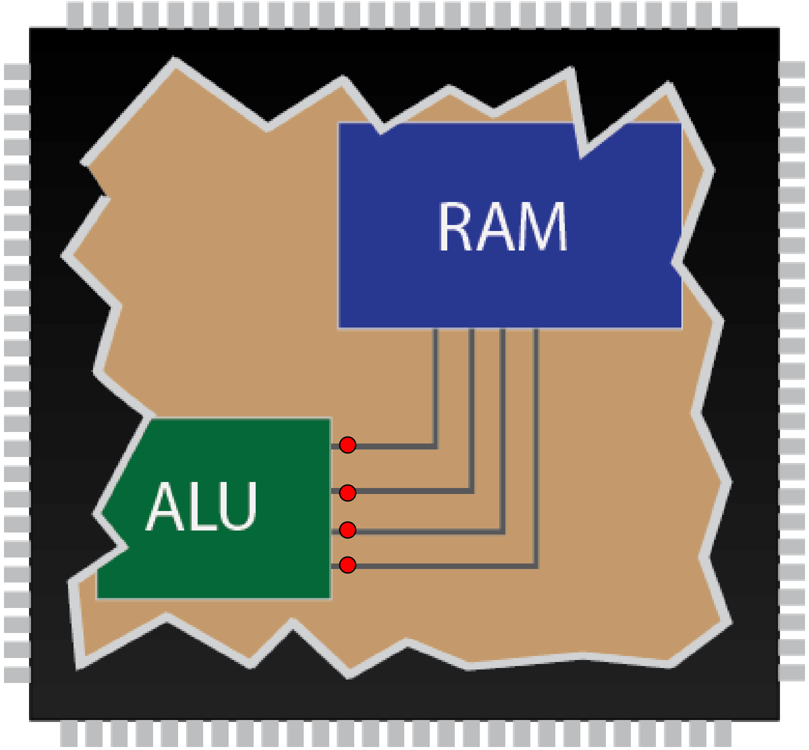
Side Channel?



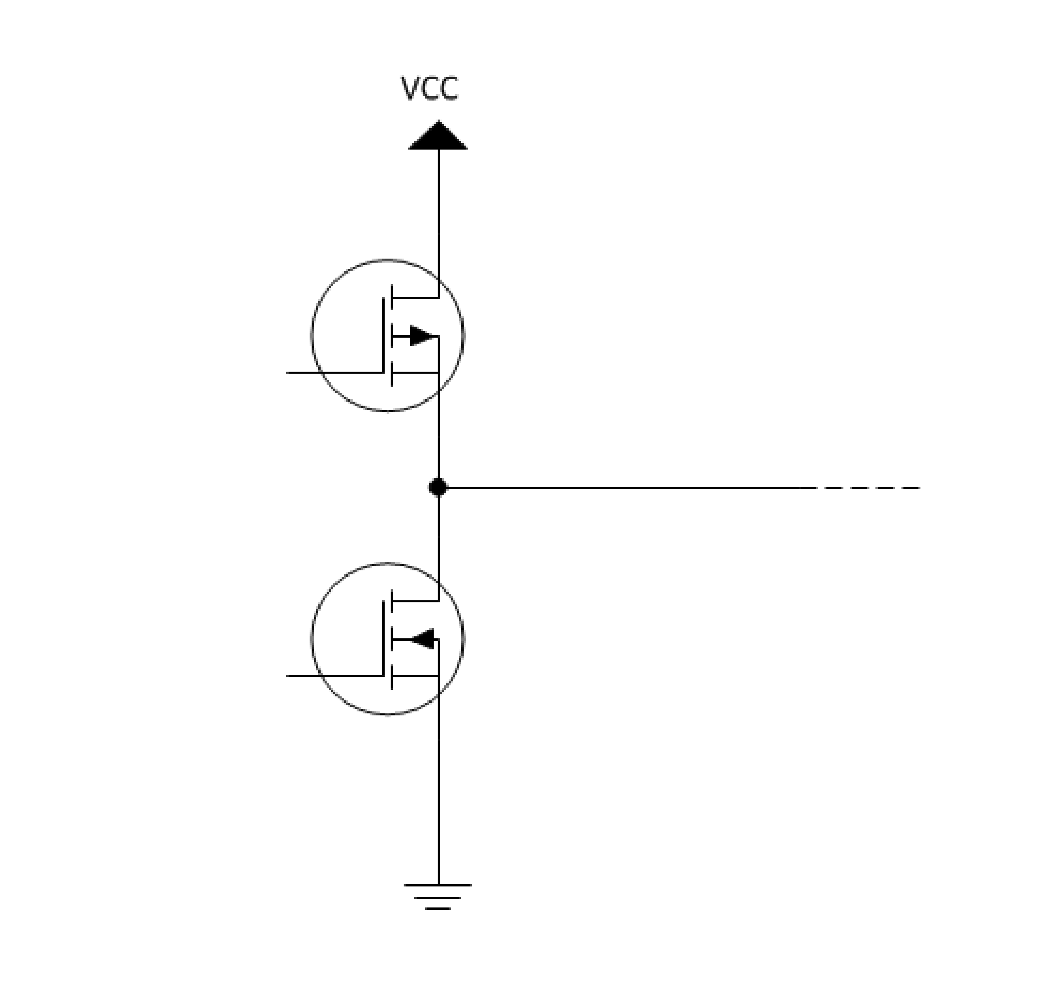
Power Channel.



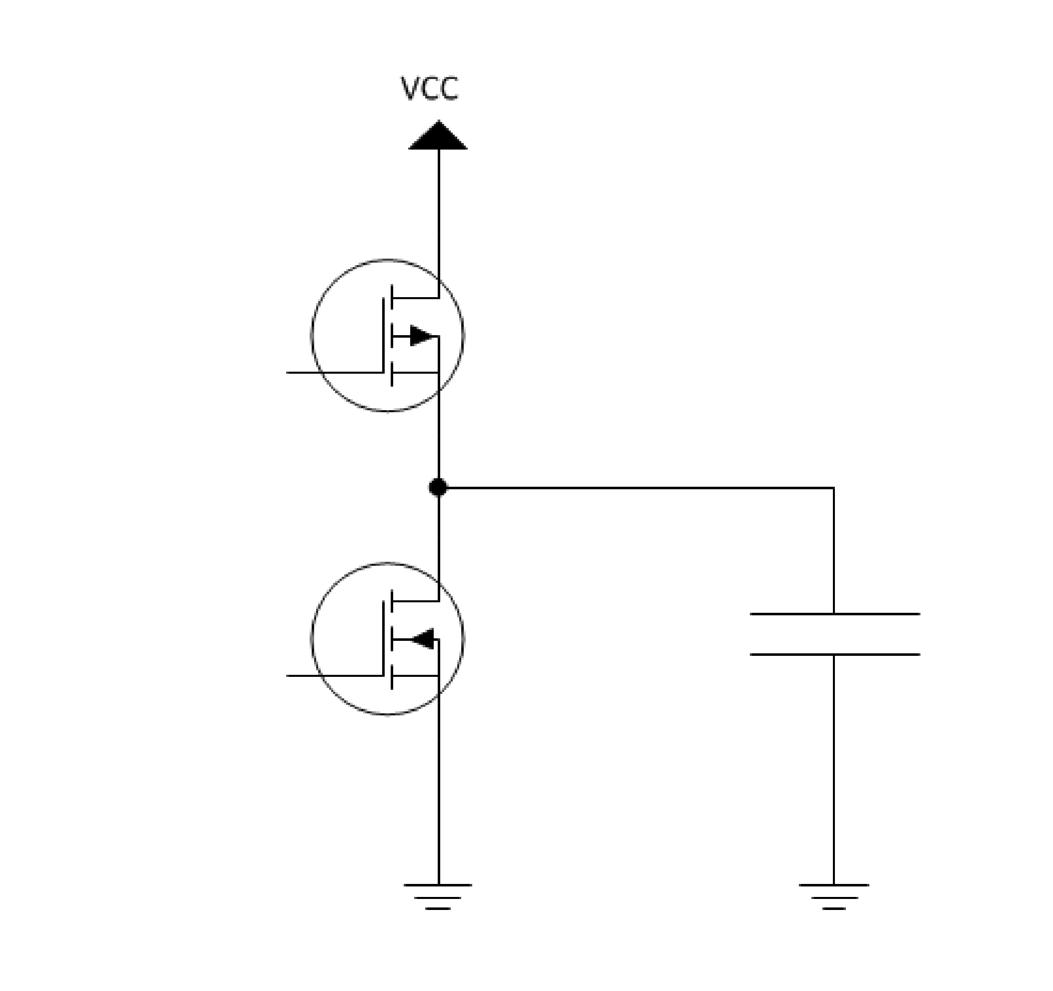
Power Channel.



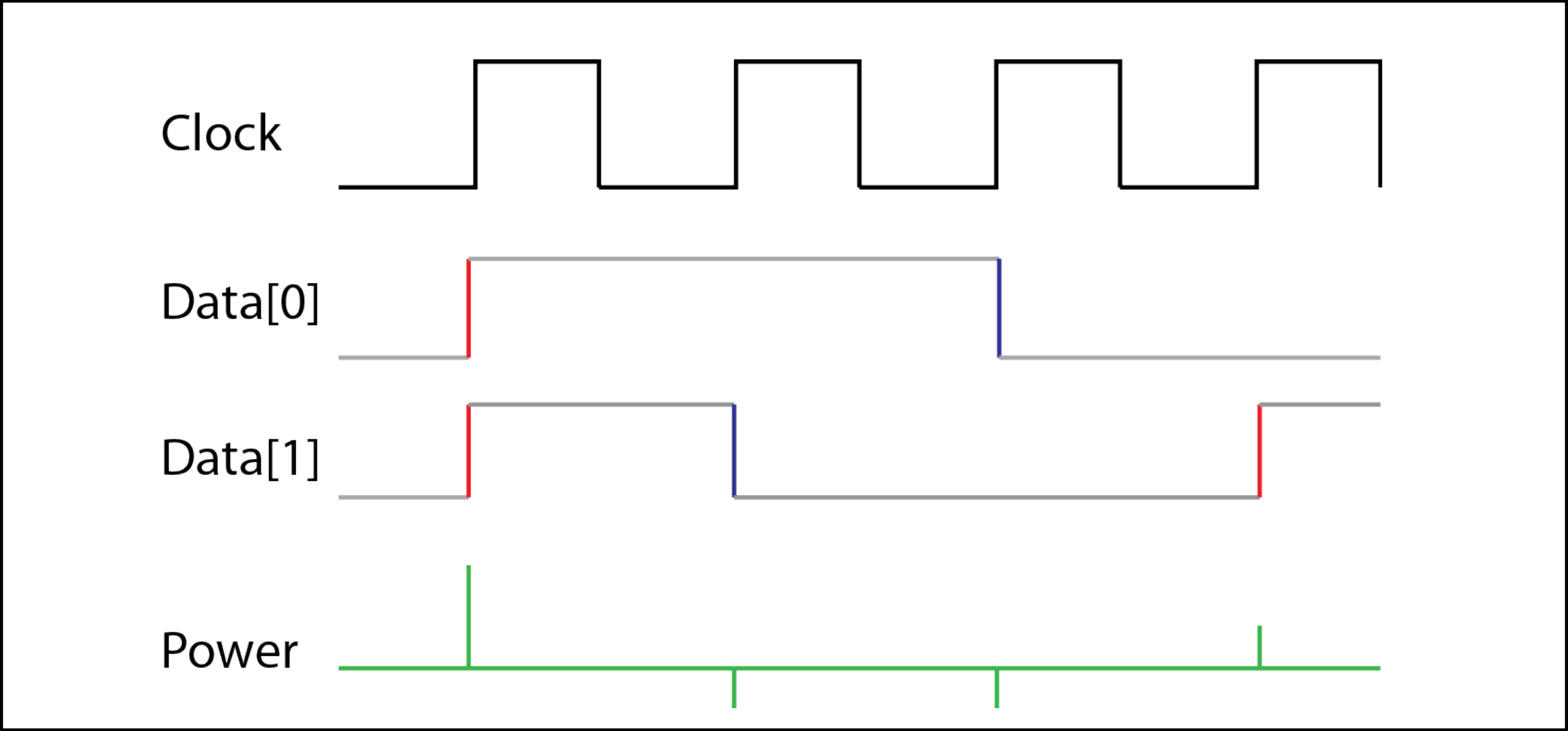
Data Bus Line



Data Bus Line



Power Channel.

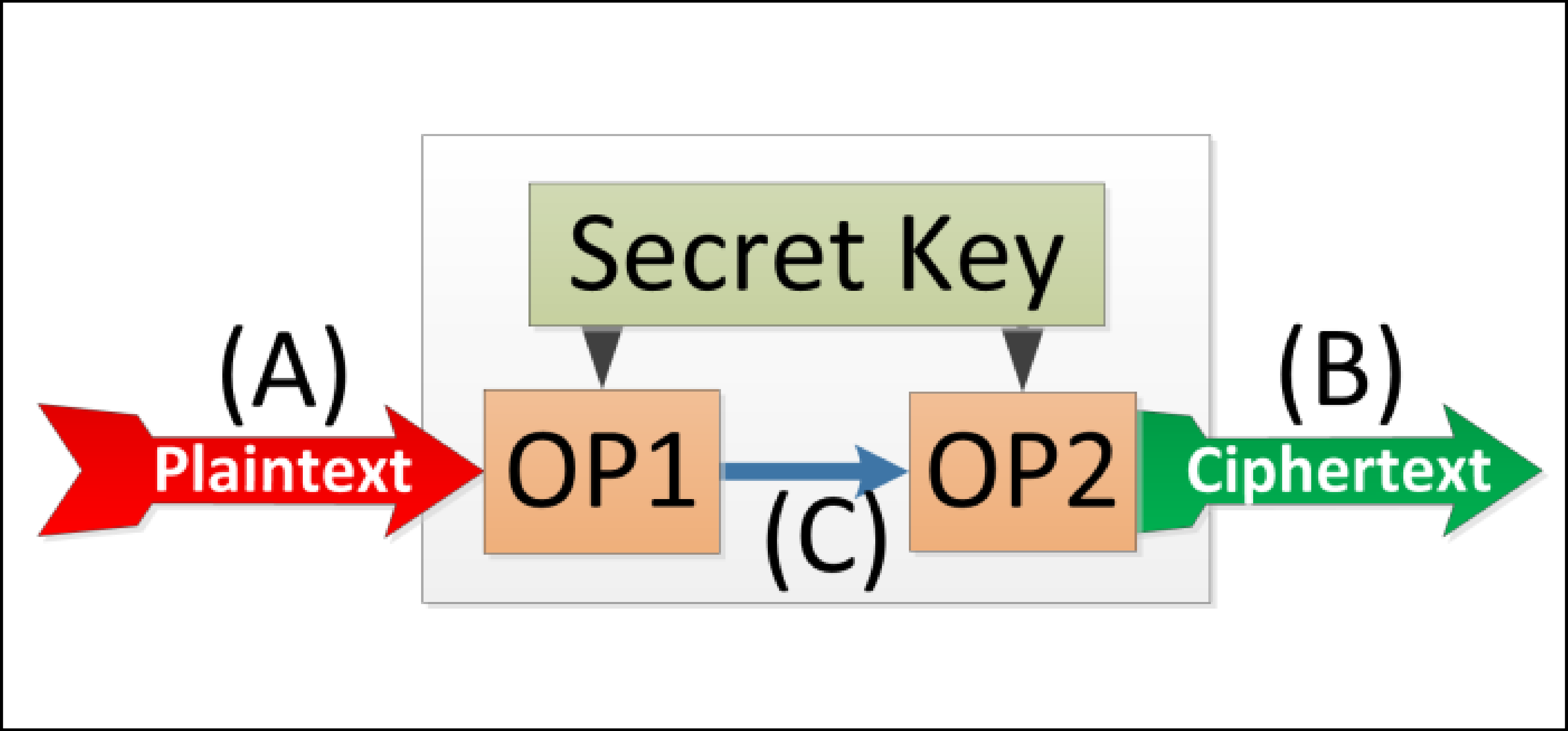


Power Model?

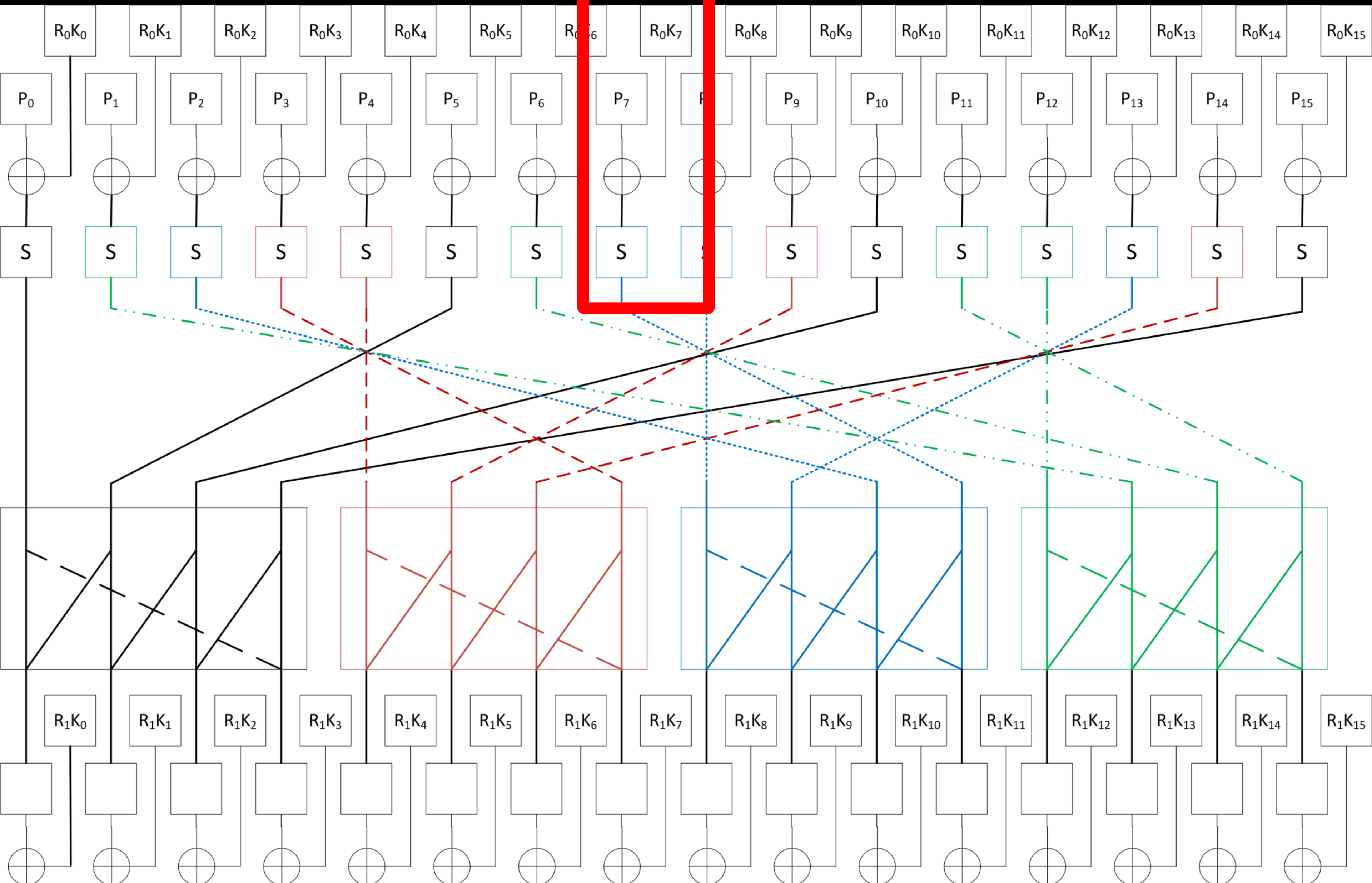
1. Hamming Distance

2. Hamming Weight

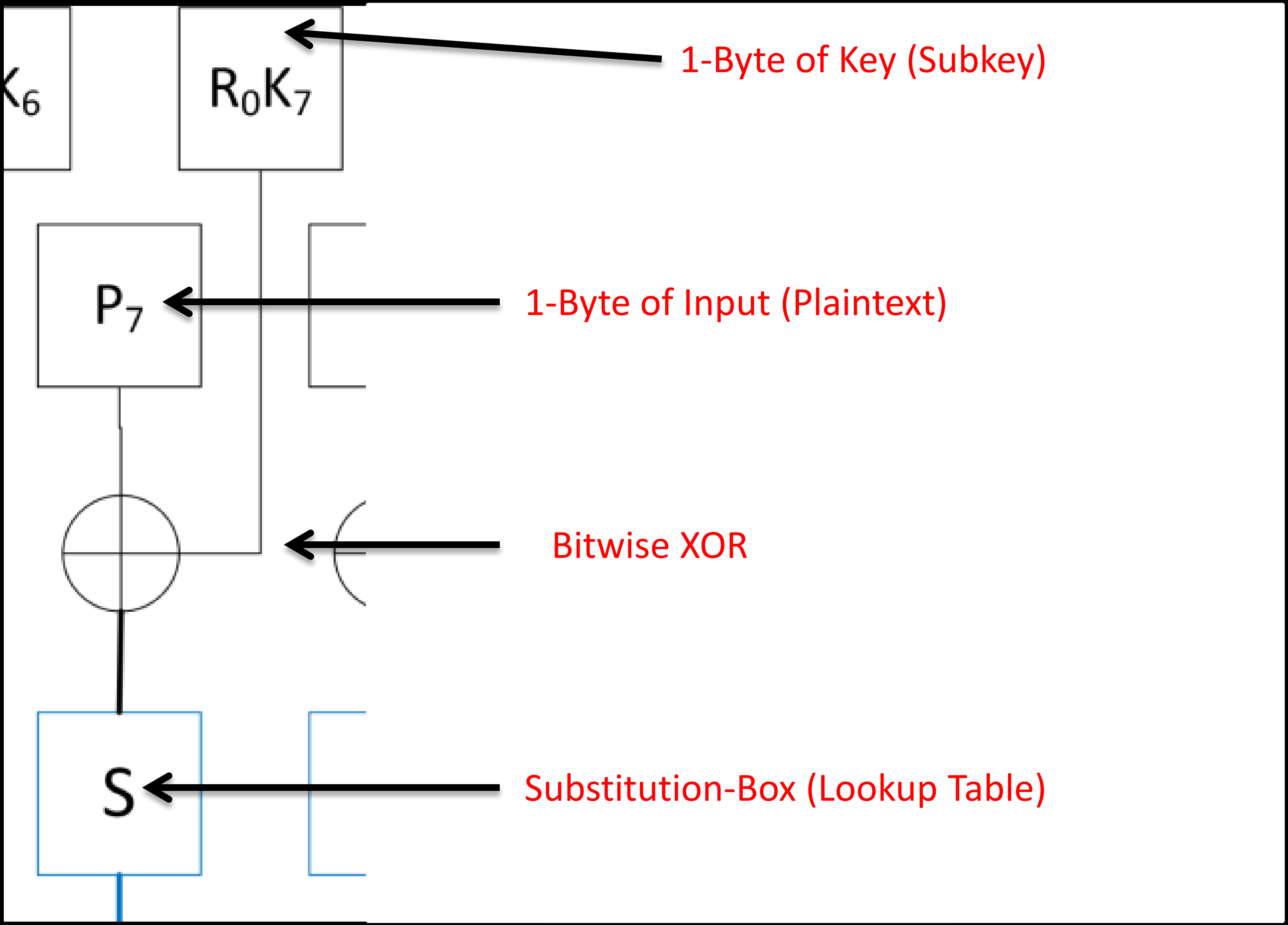
Side Channel.



Looking at AES-128



More Detail of AES



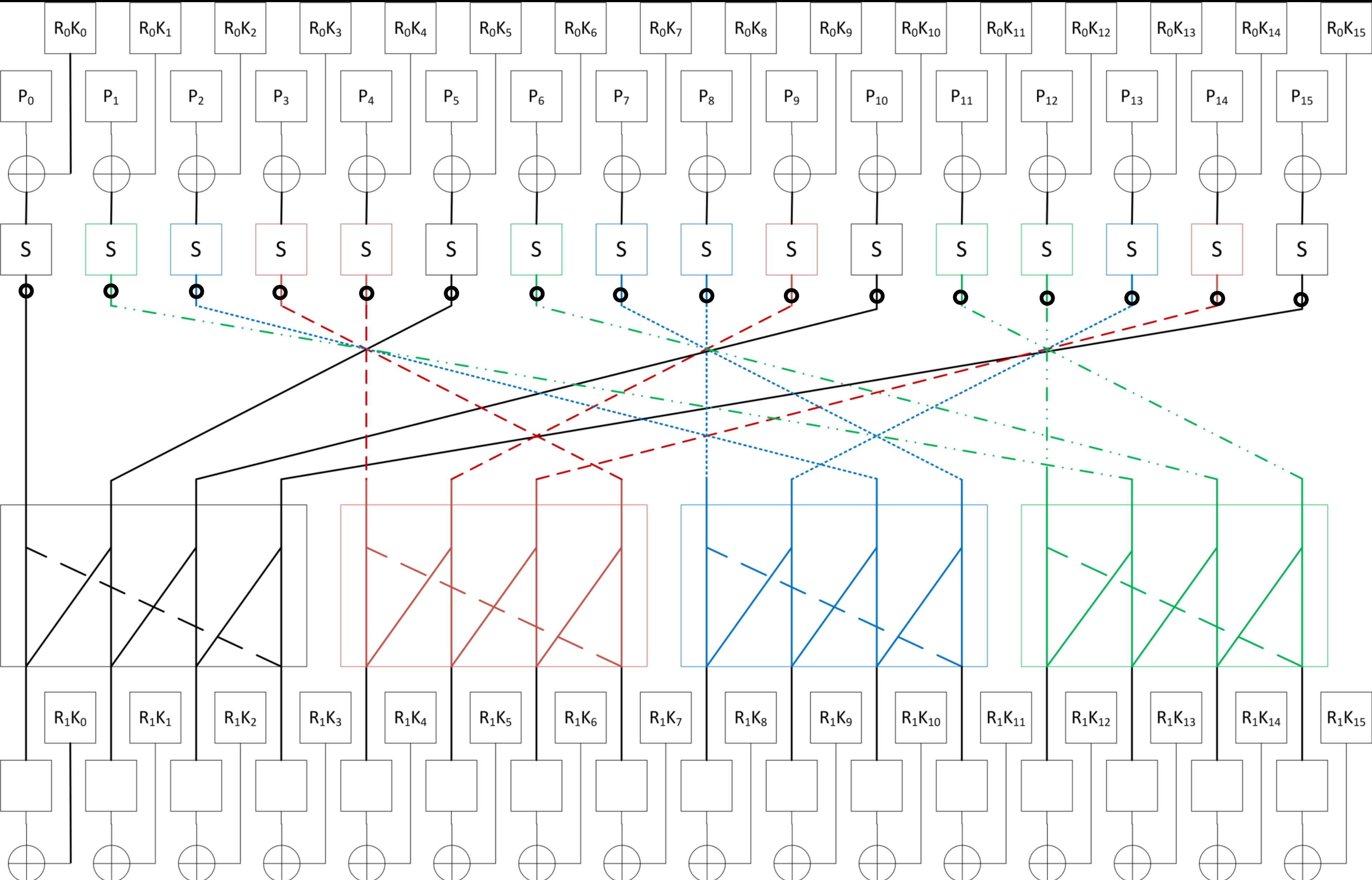
1-Byte of Key (Subkey)

1-Byte of Input (Plaintext)

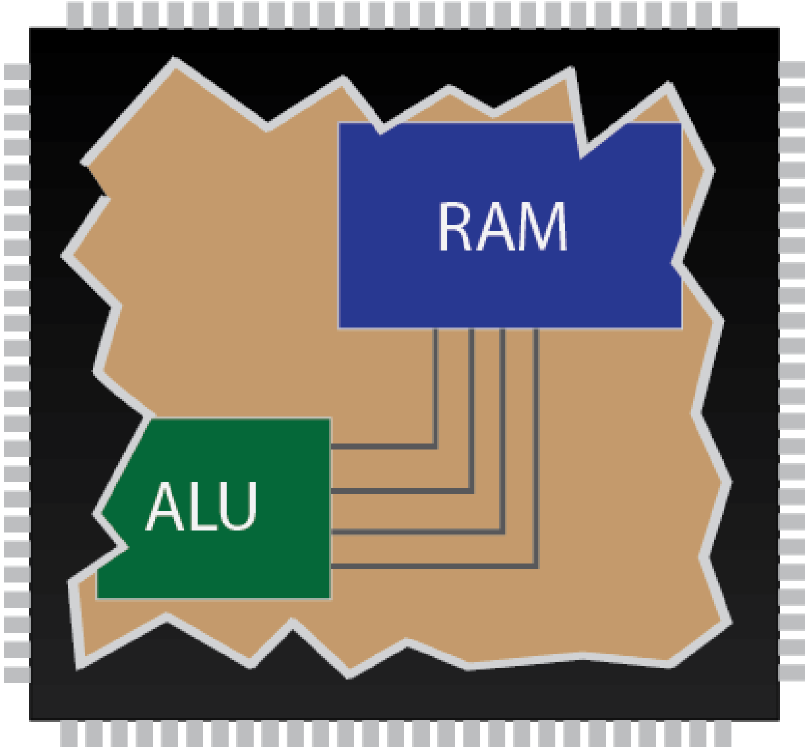
Bitwise XOR

Substitution-Box (Lookup Table)

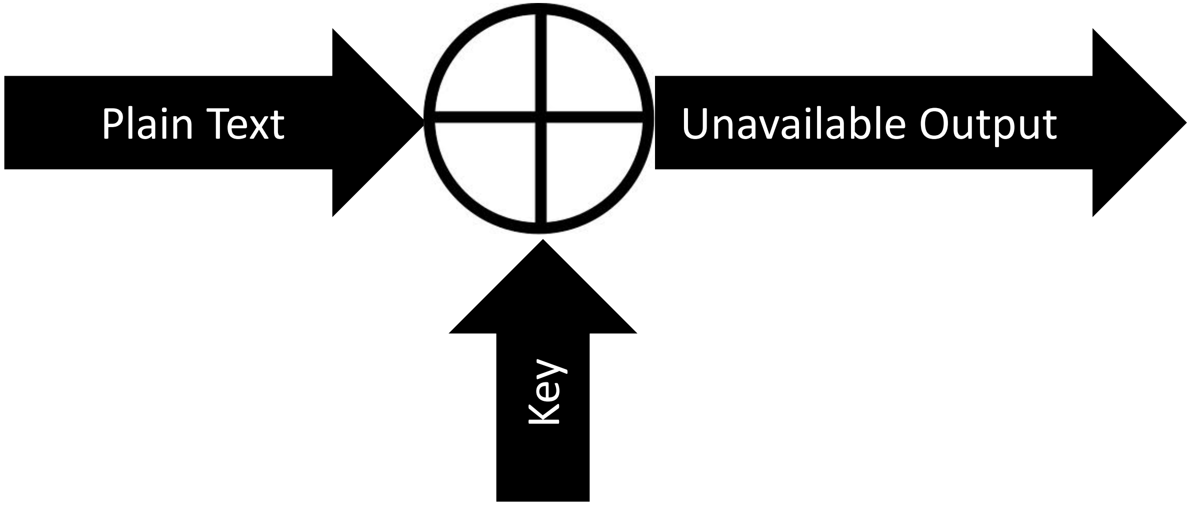
Looking at AES-128



Simple 4-Bit Example



Simple 4-Bit Example



Correlation Analysis

Input Plaintext	Hyp. Key	Hyp Result	Hyp HW
0100 (4)	0010 (2)	0110 (6)	2
0111 (7)	0010 (2)	0101 (5)	2
0010 (2)	0010 (2)	0000 (0)	0
0001 (1)	0010 (2)	0011 (3)	2
0000 (0)	0010 (2)	0010 (2)	1
0110 (6)	0010 (2)	0100 (4)	1
0101 (5)	0010 (2)	0111 (7)	3

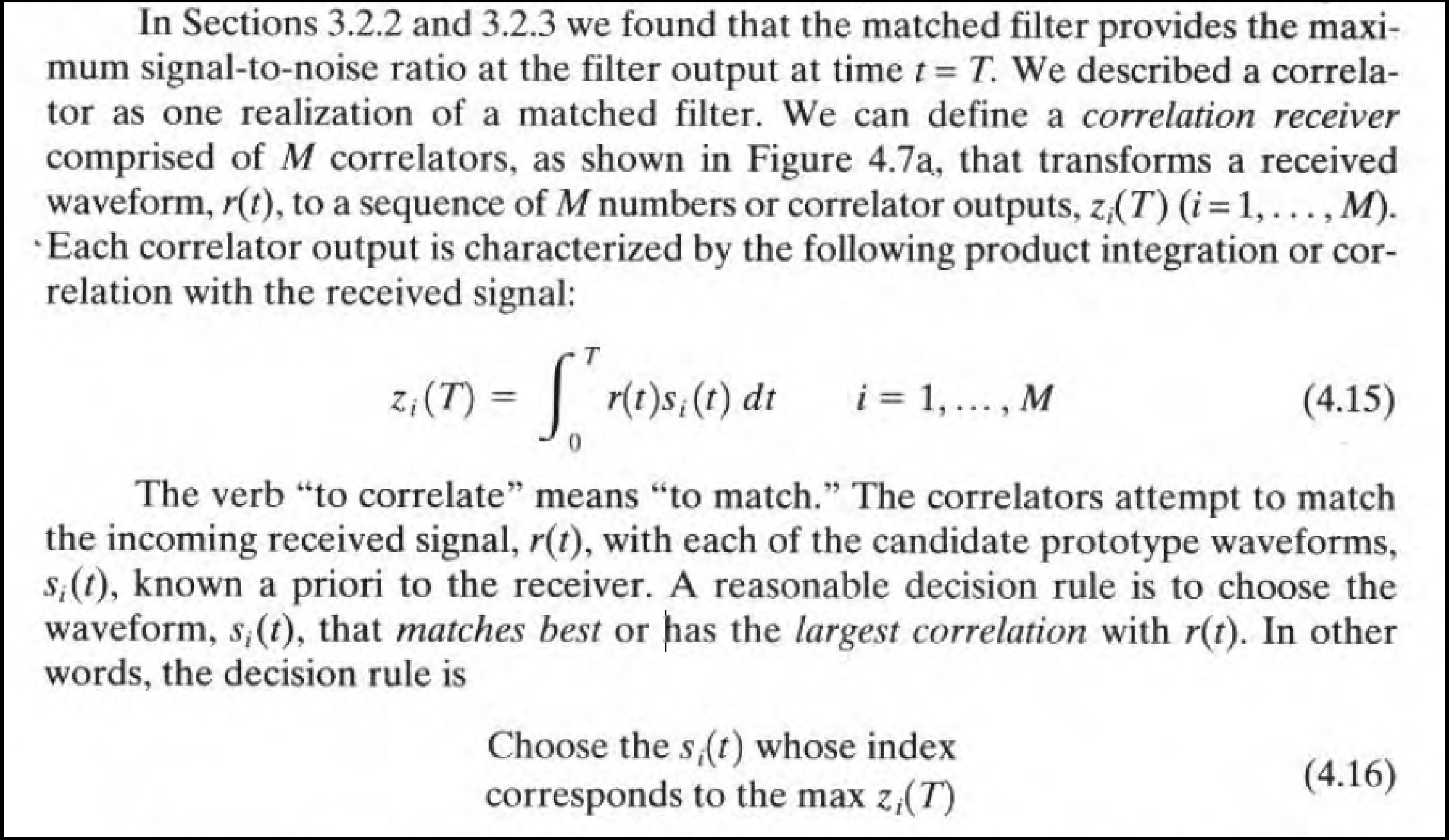
Simple Example Failings

- ‘Attacking’ XOR not ideal
- In real systems attack non-linear functions:
  - S-Box (original & most common)
  - MixCols (e.g. xtime())

Correlation Power Analysis

1. Input many plaintexts & measure power
2. For keyguess = 0,1,2,3,….,254,255:
    1. Based on known plaintext calculate S-Box output for each trace
    2. Use ‘power model’ to predict what power trace should look like
    3. Measure correlation between model & measured over all traces
3. Keyguess resulting in highest correlation is probably correct

Correlation Power Analysis



In Sections 3.2.2 and 3.2.3 we found that the matched filter provides the maximum signal-to-noise ratio at the filter output at time $t = T$. We described a correlator as one realization of a matched filter. We can define a *correlation receiver* comprised of M correlators, as shown in Figure 4.7a, that transforms a received waveform, $r(t)$, to a sequence of M numbers or correlator outputs, $z_i(T)$ $(i = 1, \ldots, M)$. Each correlator output is characterized by the following product integration or correlation with the received signal:

$$z_i(T) = \int_0^T r(t)s_i(t)\,dt \qquad i = 1, \ldots, M \qquad (4.15)$$

The verb "to correlate" means "to match." The correlators attempt to match the incoming received signal, $r(t)$, with each of the candidate prototype waveforms, $s_i(t)$, known a priori to the receiver. A reasonable decision rule is to choose the waveform, $s_i(t)$, that *matches best* or has the *largest correlation* with $r(t)$. In other words, the decision rule is

$$\text{Choose the } s_i(t) \text{ whose index corresponds to the max } z_i(T) \qquad (4.16)$$

e.g. From "Digital Communications" by Bernard Sklar

ChipWhisperer

www.ChipWhisperer.com

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

Current Software Tools

ChipWhisperer-Capture

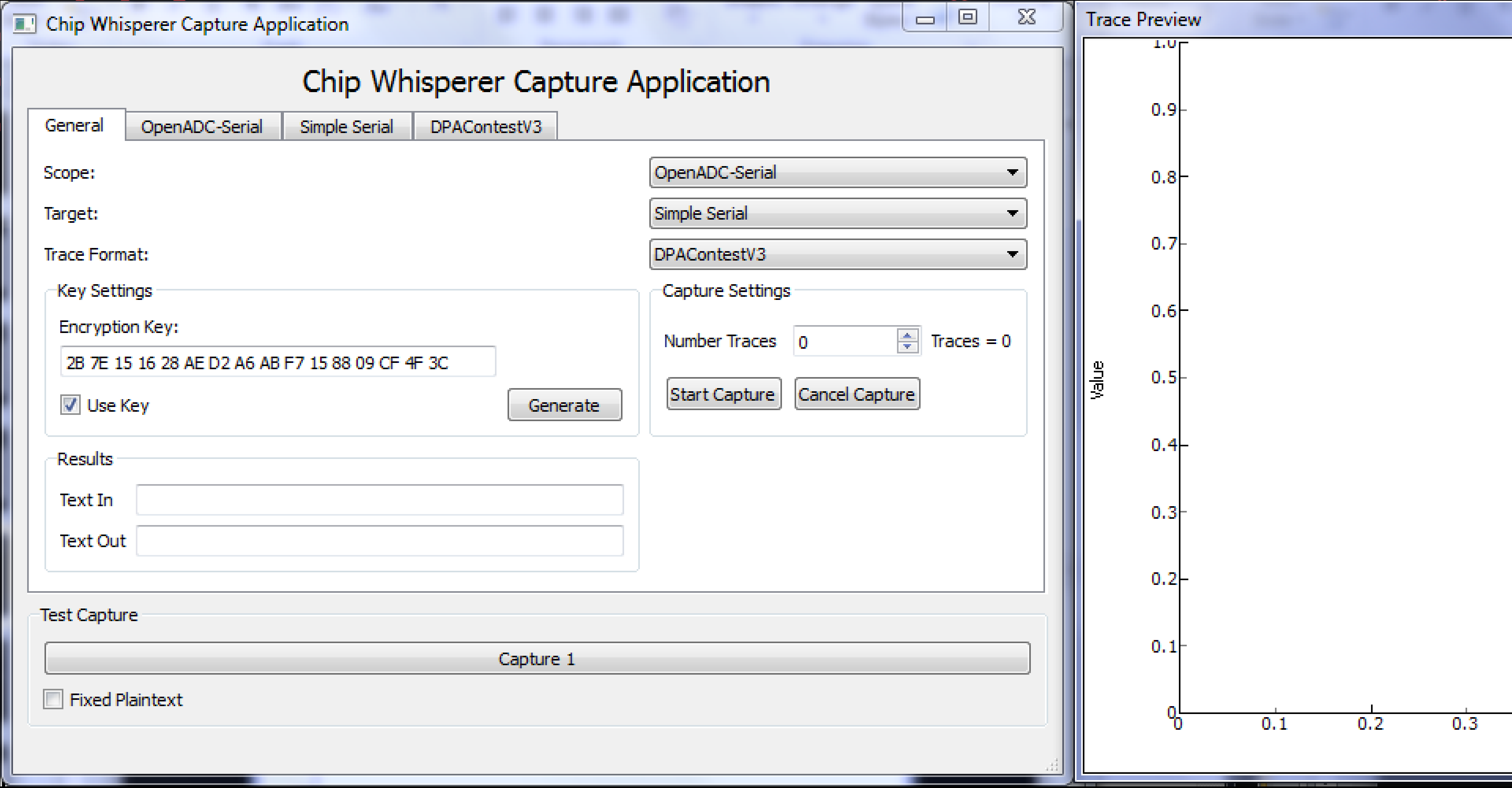
- Capture tools, interfaces to OpenADC + target boards
- Records traces

ChipWhisperer-Analyzer

- Applies attacks to power traces

About the Tools

- All tools *Open Source* (GPL License)
- Written in Python using PySide for GUI
- Uses trace file format from DPA Contest V3, which publishes some example captures, along with special project file format



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

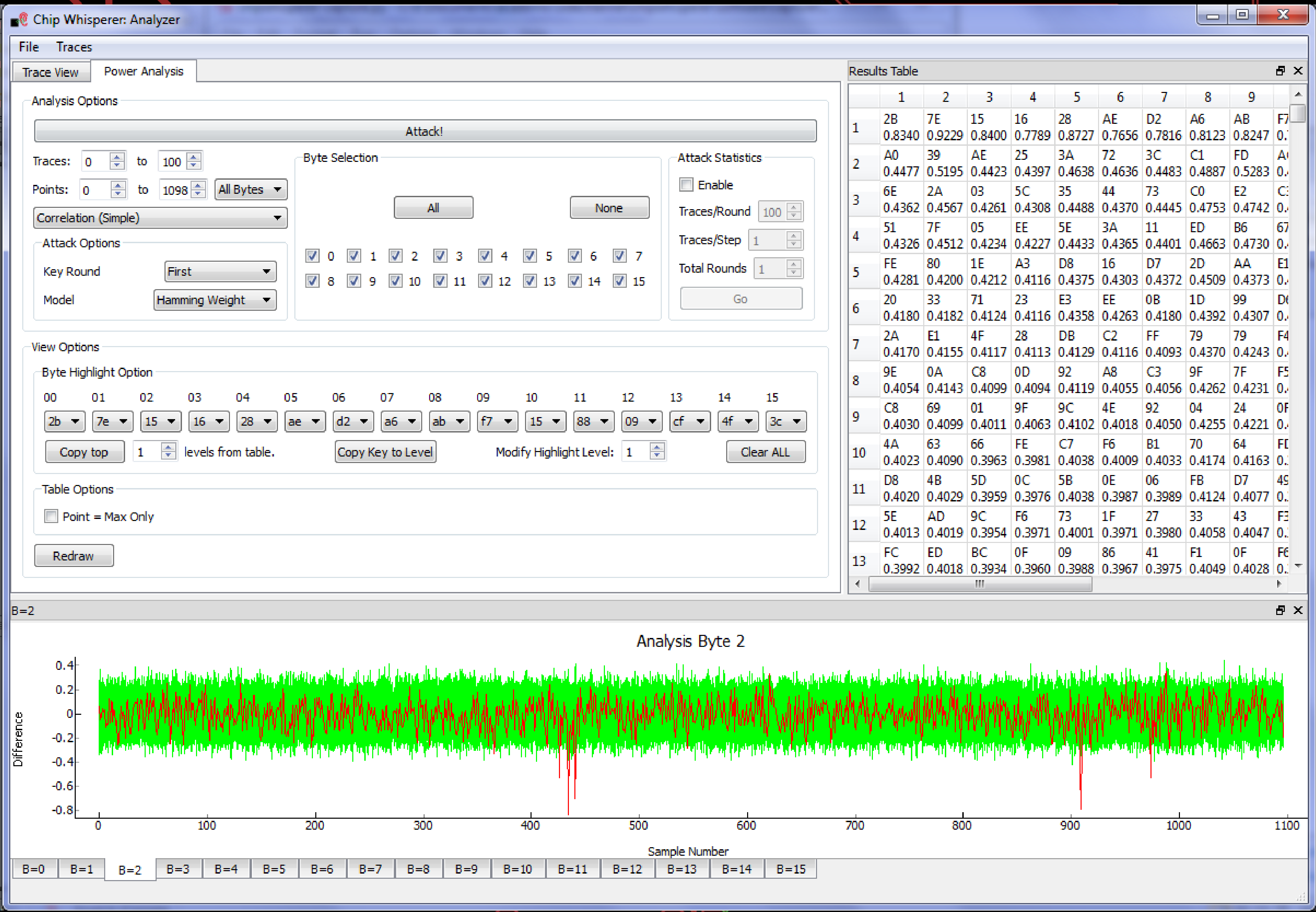
Results

Text In

Text Out

☐ Fixed Plaintext

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



Chip Whisperer: Analyzer

Analysis Options

Traces: 0 to 100

Points: 0 to 1098 All Bytes

Correlation (Simple)

Attack Options

Key Round: First

Model: Hamming Weight

Byte Selection

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

Attack Statistics

☐ Enable

Traces/Round: 100

Traces/Step: 1

Total Rounds: 1

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

1 levels from table.

Modify Highlight Level: 1

Table Options

☐ Point = Max Only

Results Table

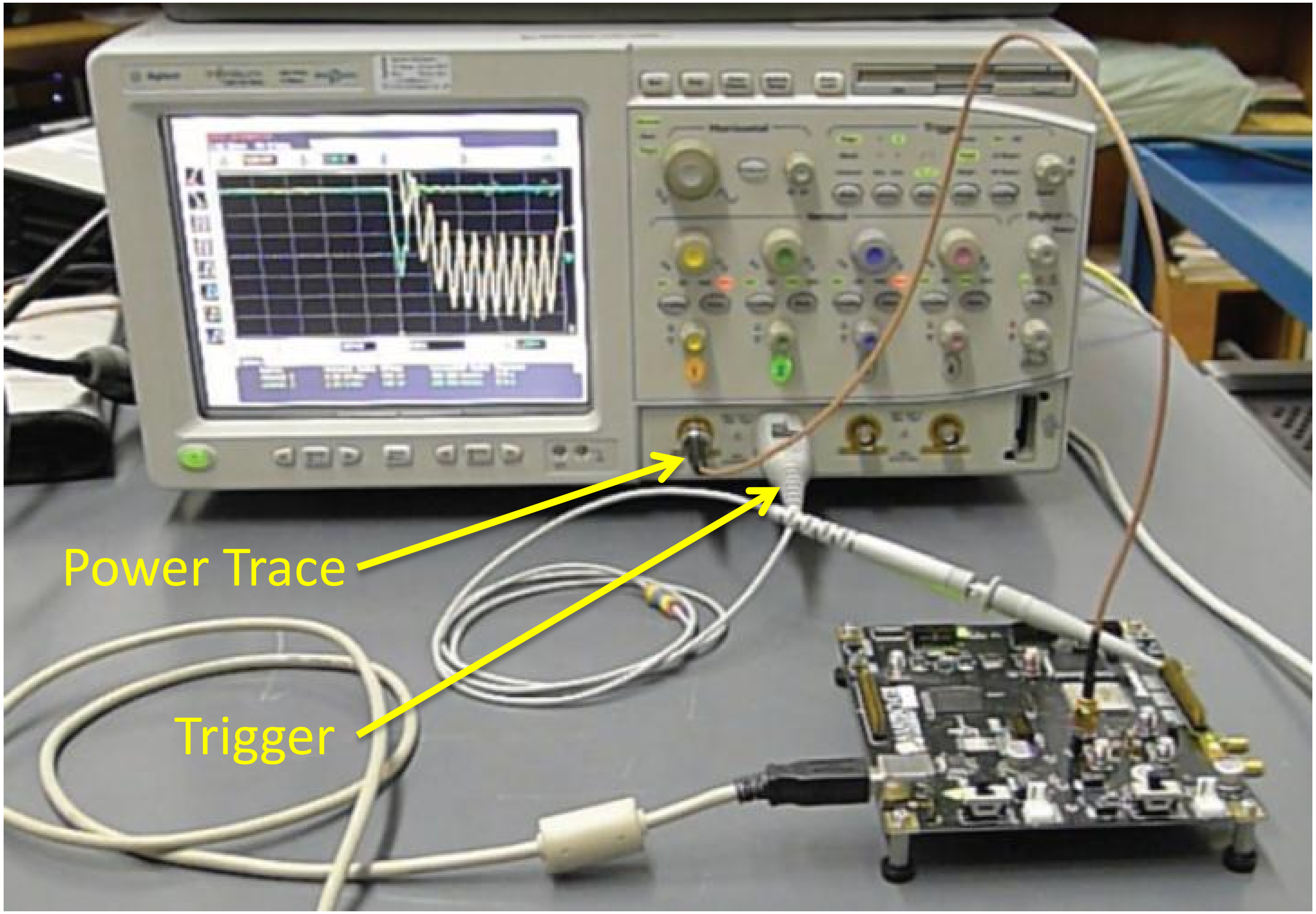
	1	2	3	4	5	6	7	8	9	
1	2B 0.8340	7E 0.9229	15 0.8400	16 0.7789	28 0.8727	AE 0.7656	D2 0.7816	A6 0.8123	AB 0.8247	F7 0.
2	A0 0.4477	39 0.5195	AE 0.4423	25 0.4397	3A 0.4638	72 0.4636	3C 0.4483	C1 0.4887	FD 0.5283	A 0.
3	6E 0.4362	2A 0.4567	03 0.4261	5C 0.4308	35 0.4488	44 0.4370	73 0.4445	C0 0.4753	E2 0.4742	C 0.
4	51 0.4326	7F 0.4512	05 0.4234	EE 0.4227	5E 0.4433	3A 0.4365	11 0.4401	ED 0.4663	B6 0.4730	67 0.
5	FE 0.4281	80 0.4200	1E 0.4212	A3 0.4116	D8 0.4375	16 0.4303	D7 0.4372	2D 0.4509	AA 0.4373	E1 0.
6	20 0.4180	33 0.4182	71 0.4124	23 0.4116	E3 0.4358	EE 0.4263	0B 0.4180	1D 0.4392	99 0.4307	D 0.
7	2A 0.4170	E1 0.4155	4F 0.4117	28 0.4113	DB 0.4129	C2 0.4116	FF 0.4093	79 0.4370	79 0.4243	F4 0.
8	9E 0.4054	0A 0.4143	C8 0.4099	0D 0.4094	92 0.4119	A8 0.4055	C3 0.4056	9F 0.4262	7F 0.4231	F5 0.
9	C8 0.4030	69 0.4099	01 0.4011	9F 0.4063	9C 0.4102	4E 0.4018	92 0.4050	04 0.4255	24 0.4221	0F 0.
10	4A 0.4023	63 0.4090	66 0.3963	FE 0.3981	C7 0.4038	F6 0.4009	B1 0.4033	70 0.4174	64 0.4163	FD 0.
11	D8 0.4020	4B 0.4029	5D 0.3959	0C 0.3976	5B 0.4038	0E 0.3987	06 0.3989	FB 0.4124	D7 0.4077	49 0.
12	5E 0.4013	AD 0.4019	9C 0.3954	F6 0.3971	73 0.4001	1F 0.3971	27 0.3980	33 0.4058	43 0.4047	F3 0.
13	FC 0.3992	ED 0.4018	BC 0.3934	0F 0.3960	09 0.3988	86 0.3967	41 0.3975	F1 0.4049	0F 0.4028	F6 0.

B=2

Analysis Byte 2

Waveform Acquisition & Low-Cost Alternatives

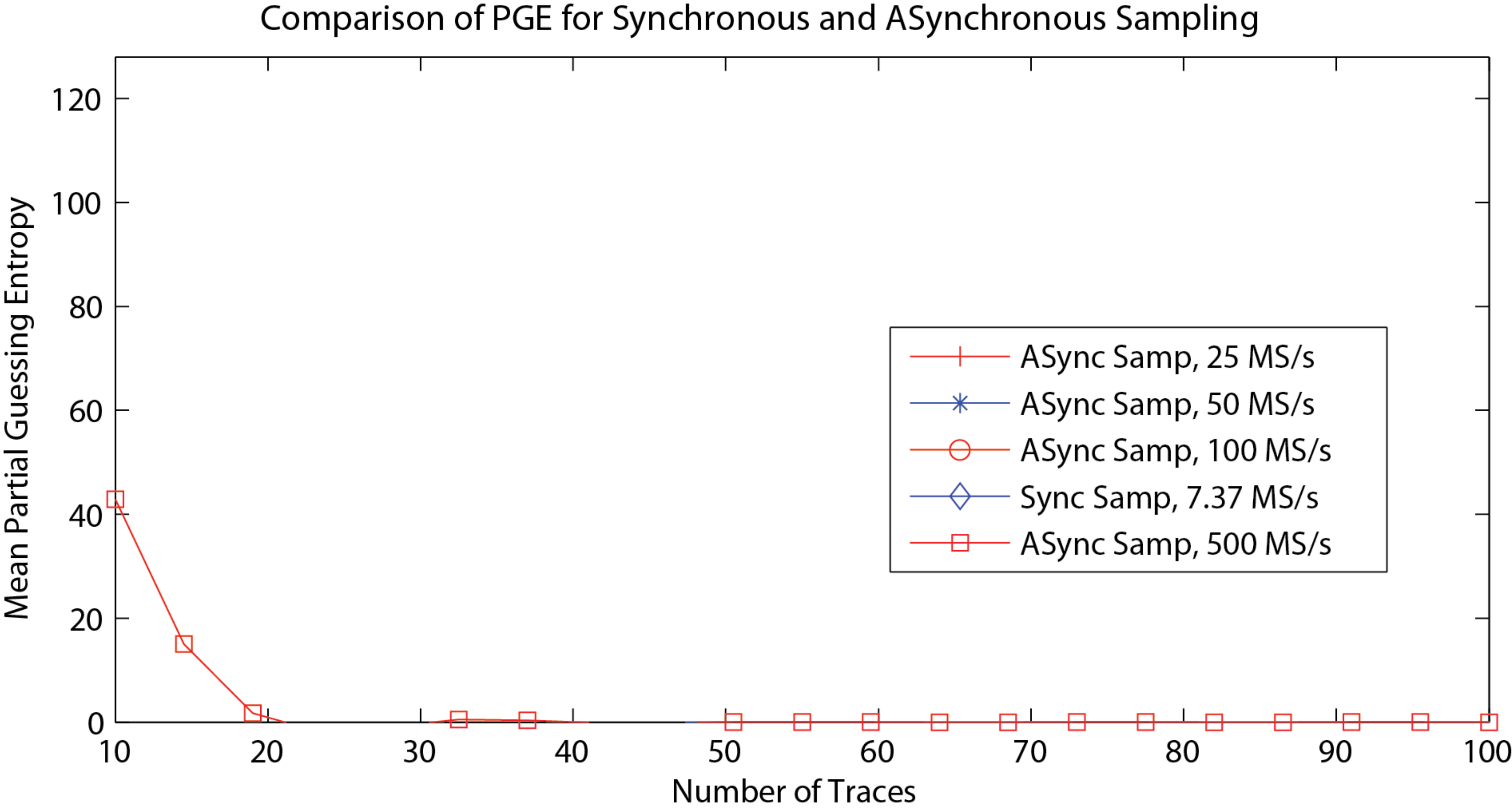
What's a 'Normal' Setup look like?



Is this Really Typical?

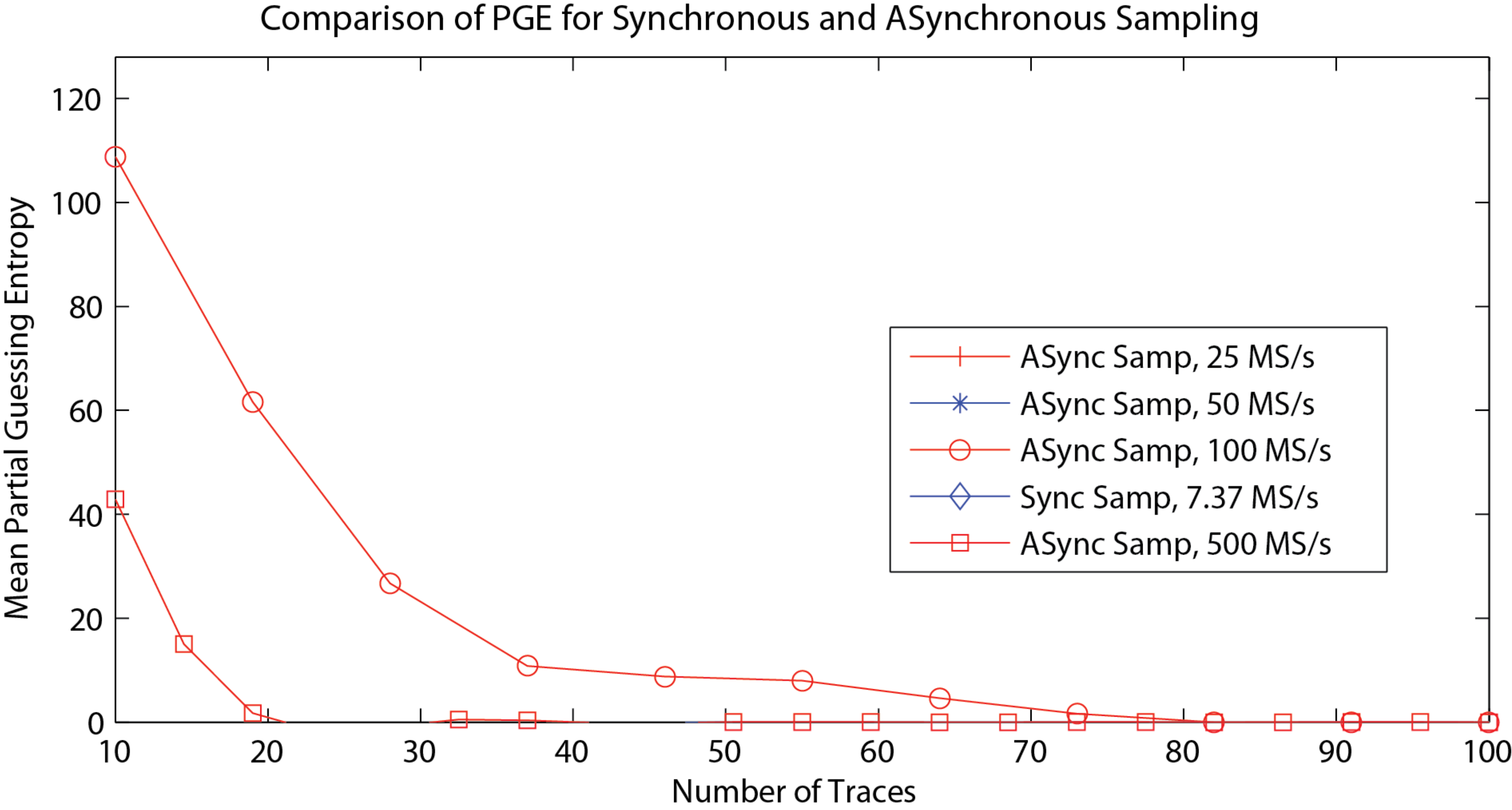
Author	Work	Year	Scope	Cost (Used, 2013)
Dario Carluccio	Electromagnetic Side Channel Analysis Embedded Crypto Devices	2005	Infiniium 5432D MSO	$8000
Youssef Souissi et al.	Embedded systems security: An evaluation methodology against Side Channel Attacks	2011	Infiniium 54855	$20 000
Dakshi Agrawal et 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

Does Sample Rate Matter?



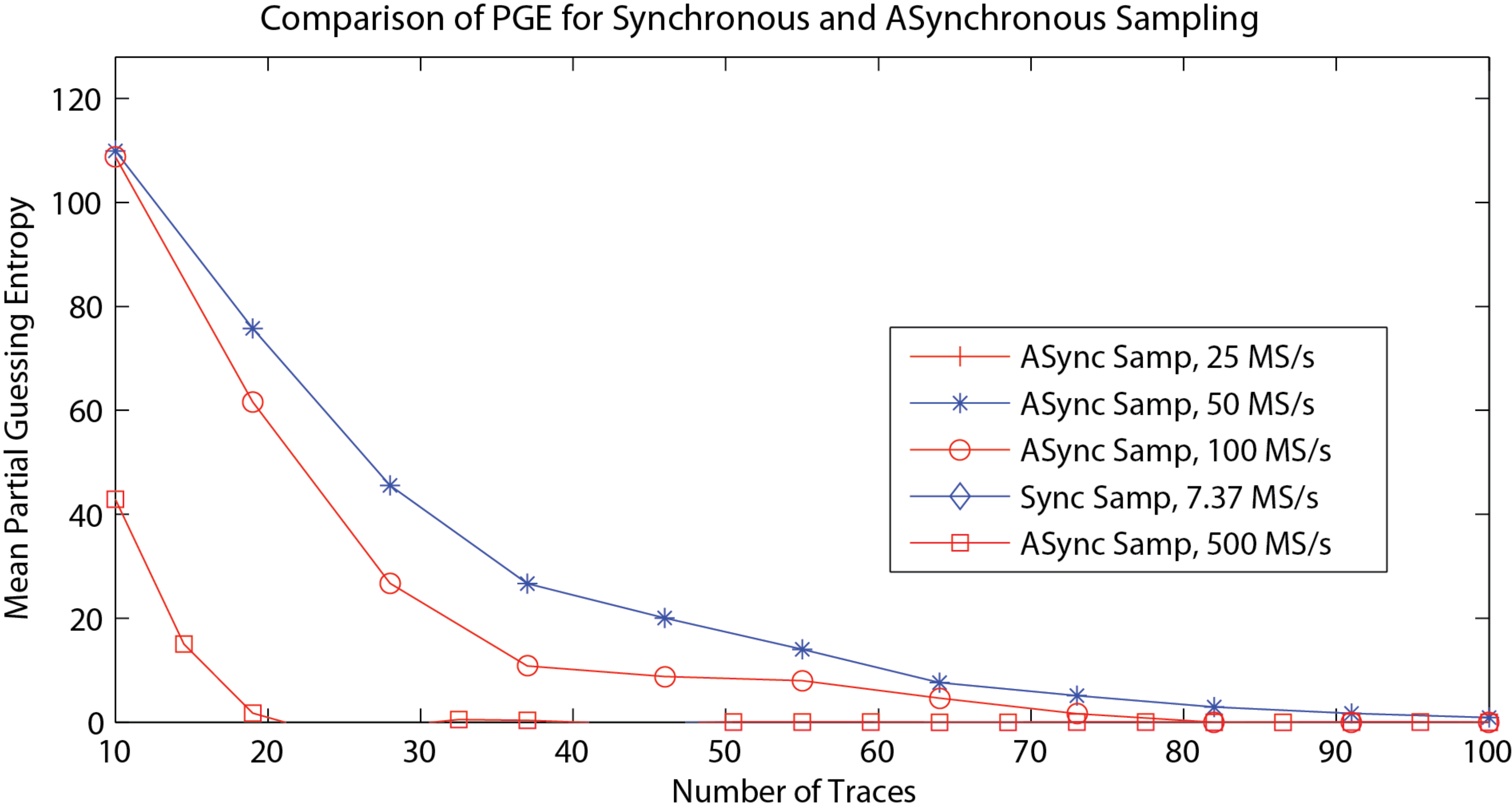
Colin O'Flynn

Does Sample Rate Matter?

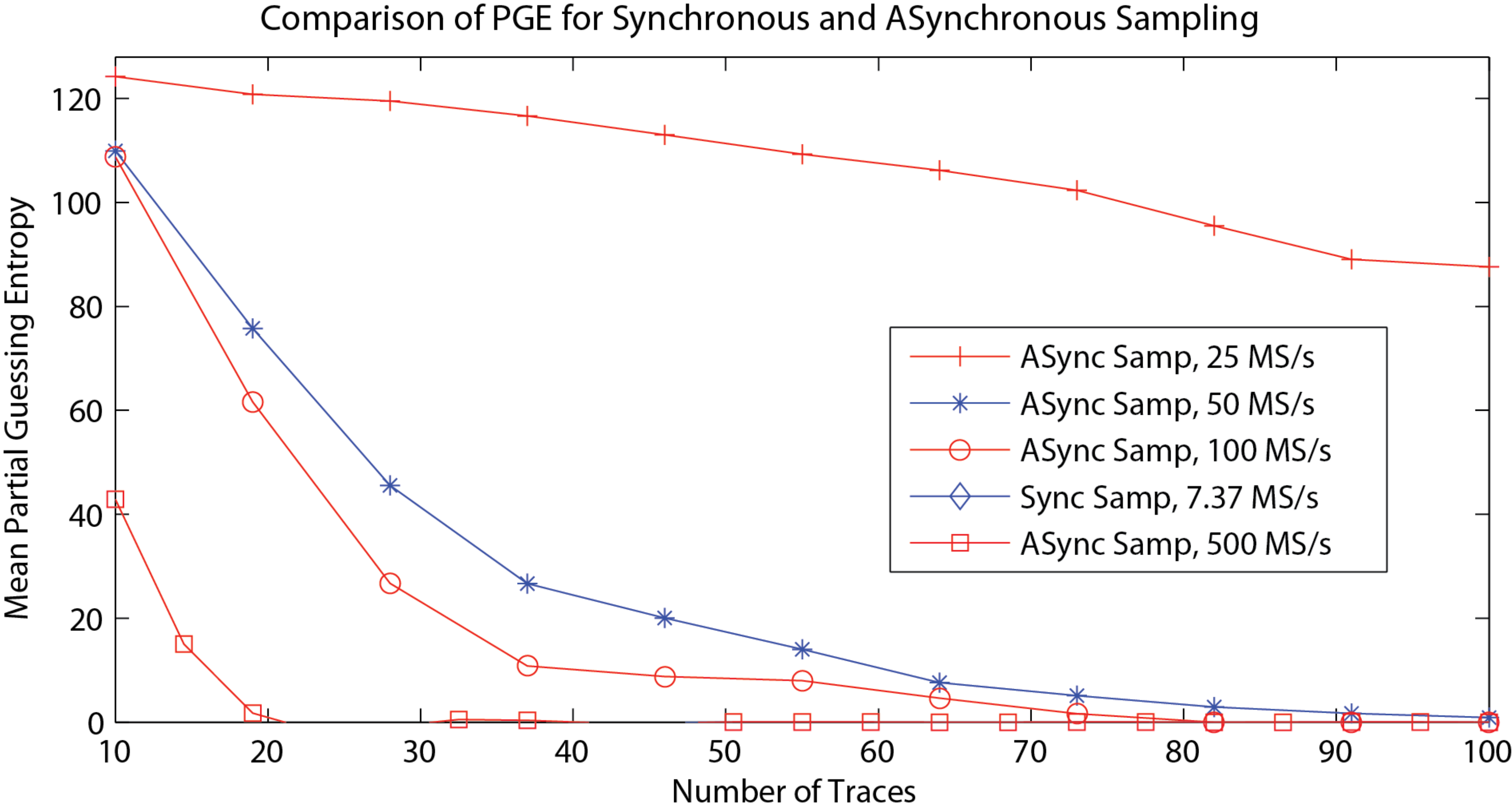


COLIN O'FLYNN

Does Sample Rate Matter?

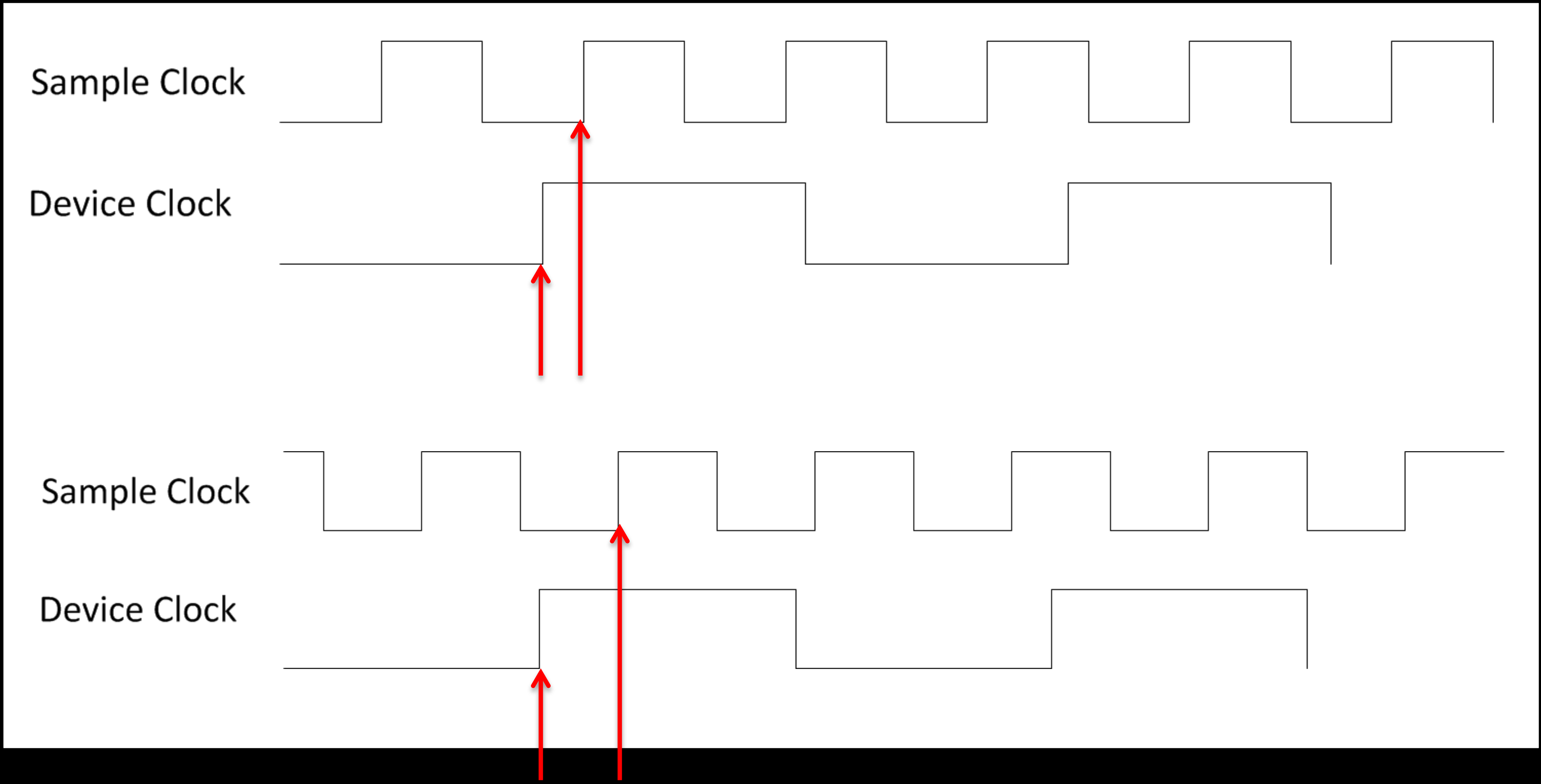


Does Sample Rate Matter?



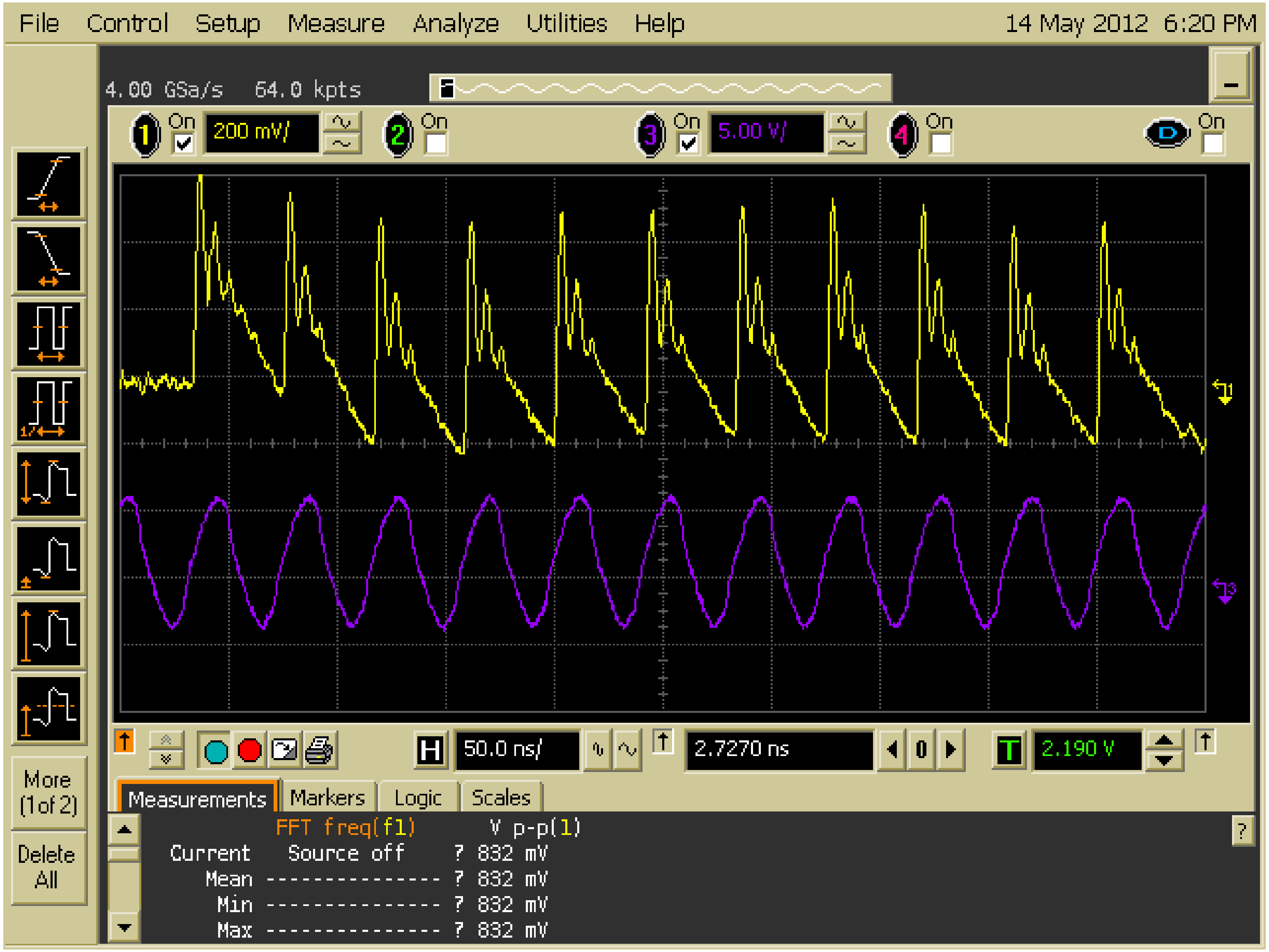
Colin O'Flynn

Explaining Trigger 'Jitter'



COLIN O'FLYNN

Can We Do Better?

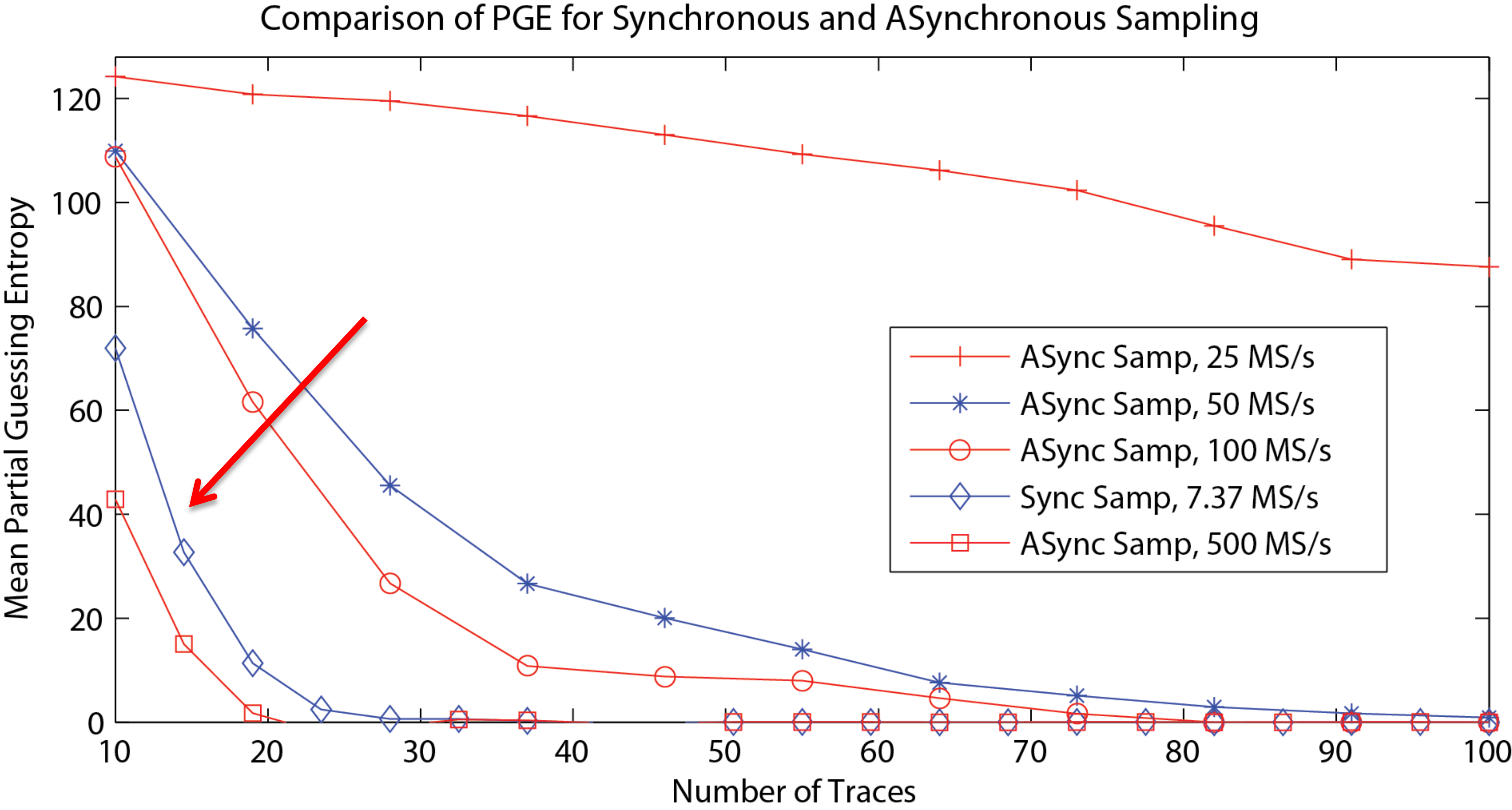


```
              FFT freq(f1)       V p-p(1)
  Current   Source off      ? 832 mV
     Mean --------------- ? 832 mV
      Min --------------- ? 832 mV
      Max --------------- ? 832 mV
```

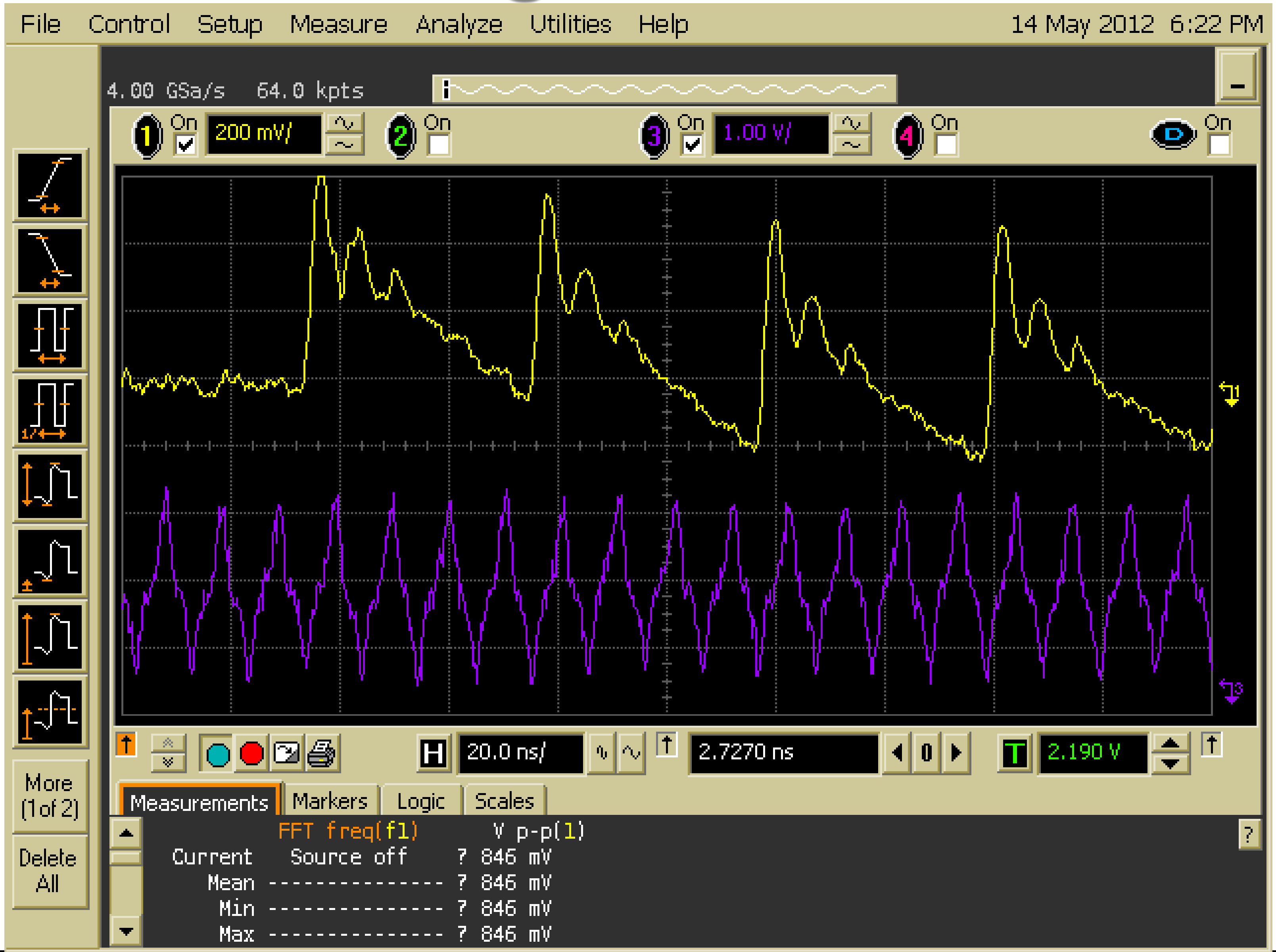
Power

Clock

Does Sample Rate Matter?



Using 4x Source Clock

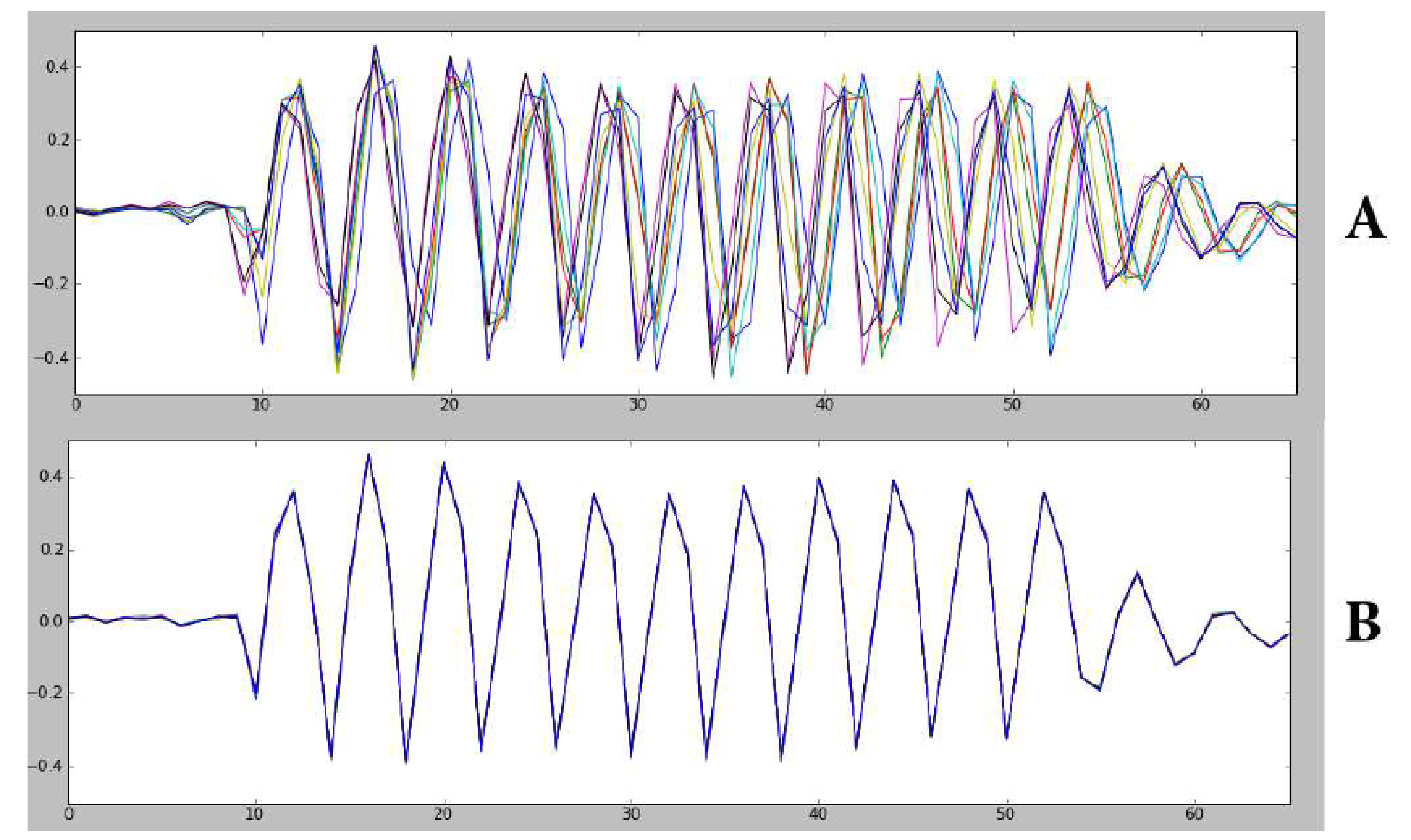


```
           FFT freq(f1)      V p-p(1)
  Current   Source off     ? 846 mV
     Mean ---------------  ? 846 mV
      Min ---------------  ? 846 mV
      Max ---------------  ? 846 mV
```

Power

Clock

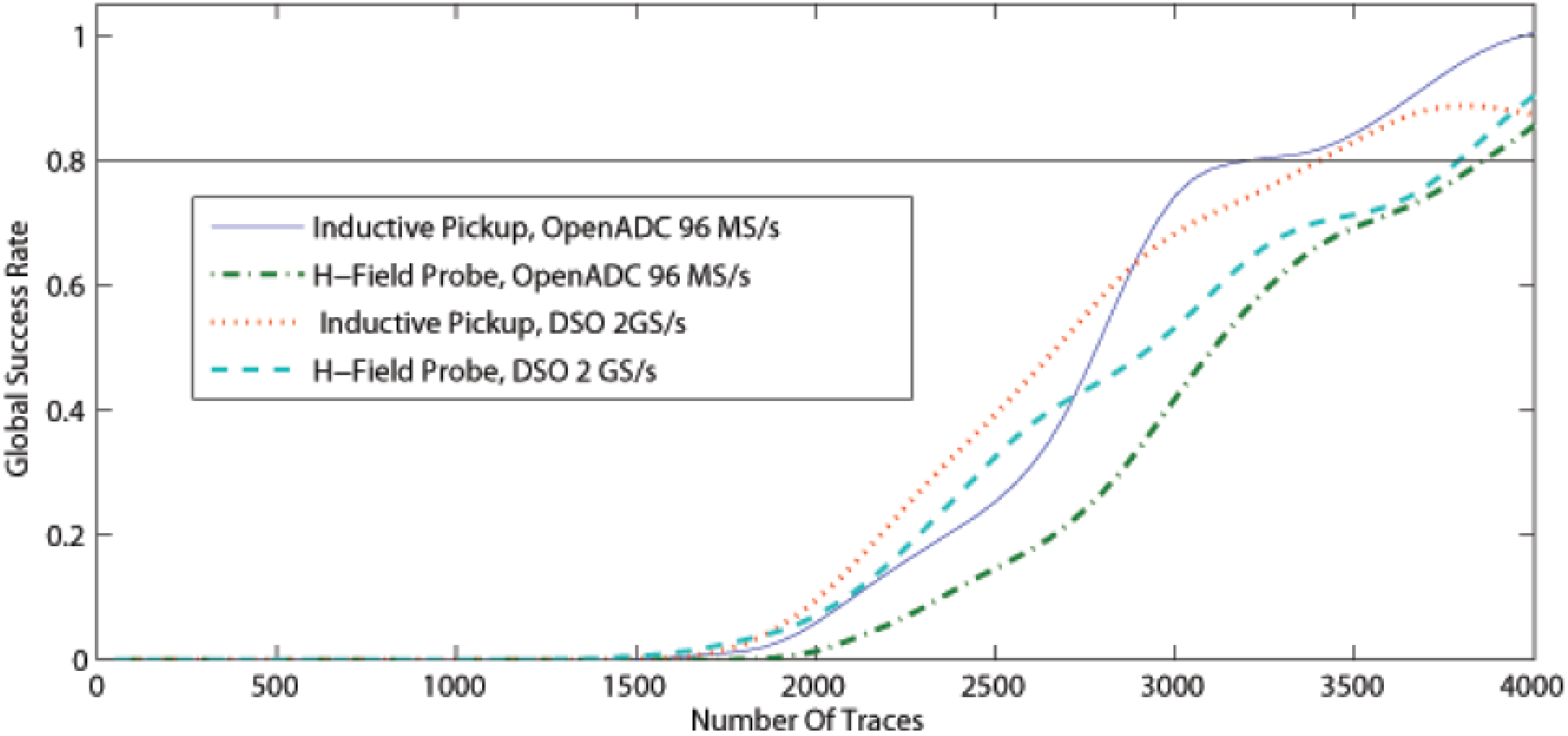
Synchronization,
Synchronization,
Synchronization



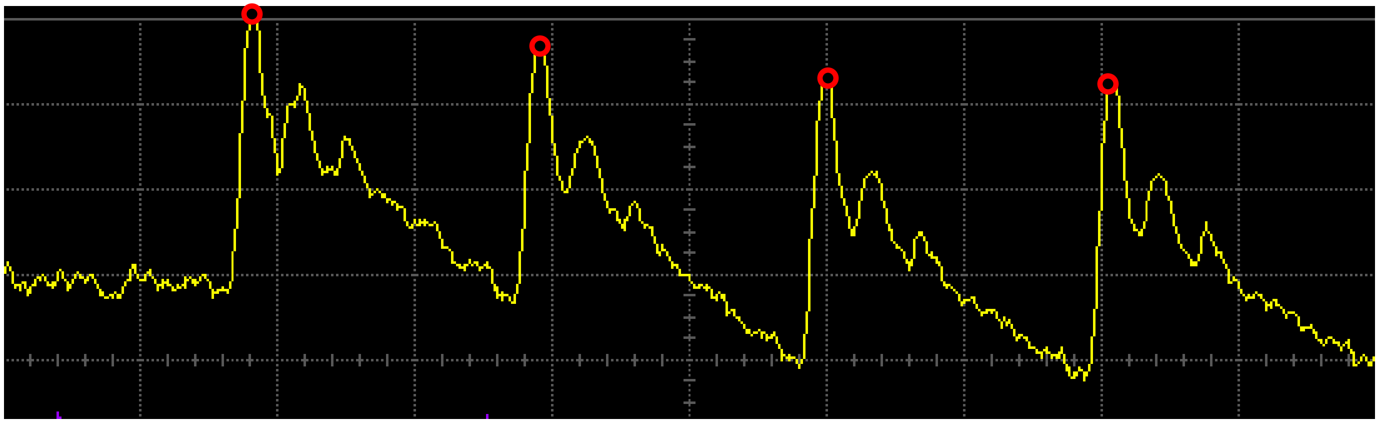
Tips for using a Normal Oscilloscope

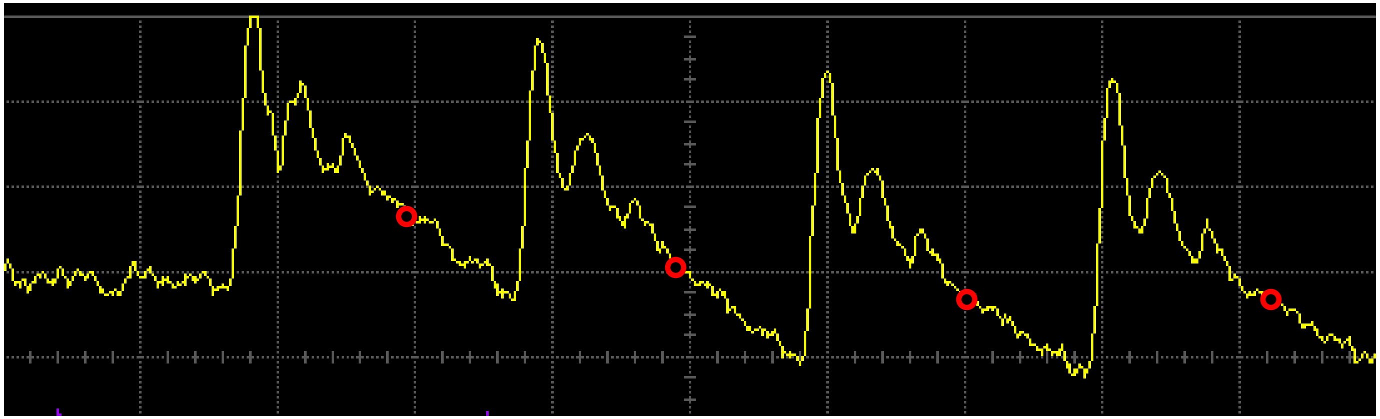
- Can hack scope to output sampling time-base, run D.U.T. from this clock or derived from this clock
- Some scopes tell you time between trigger & first sample, use this to upsample, shift offset, and downsample traces
  - Agilent calls this 'XOffset' parameter
- Sample at highest possible rate & downsample yourself

OpenADC Comparison

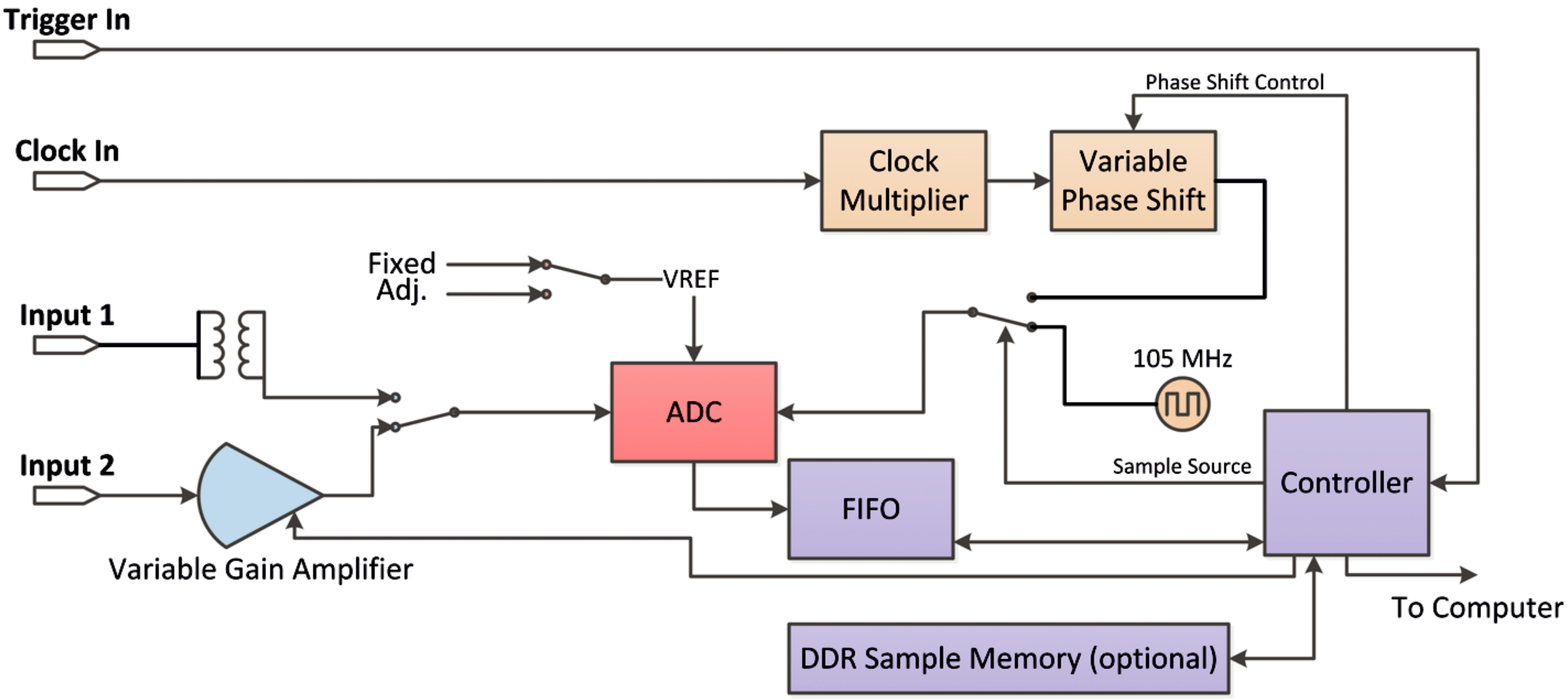


What about Phase Shift?



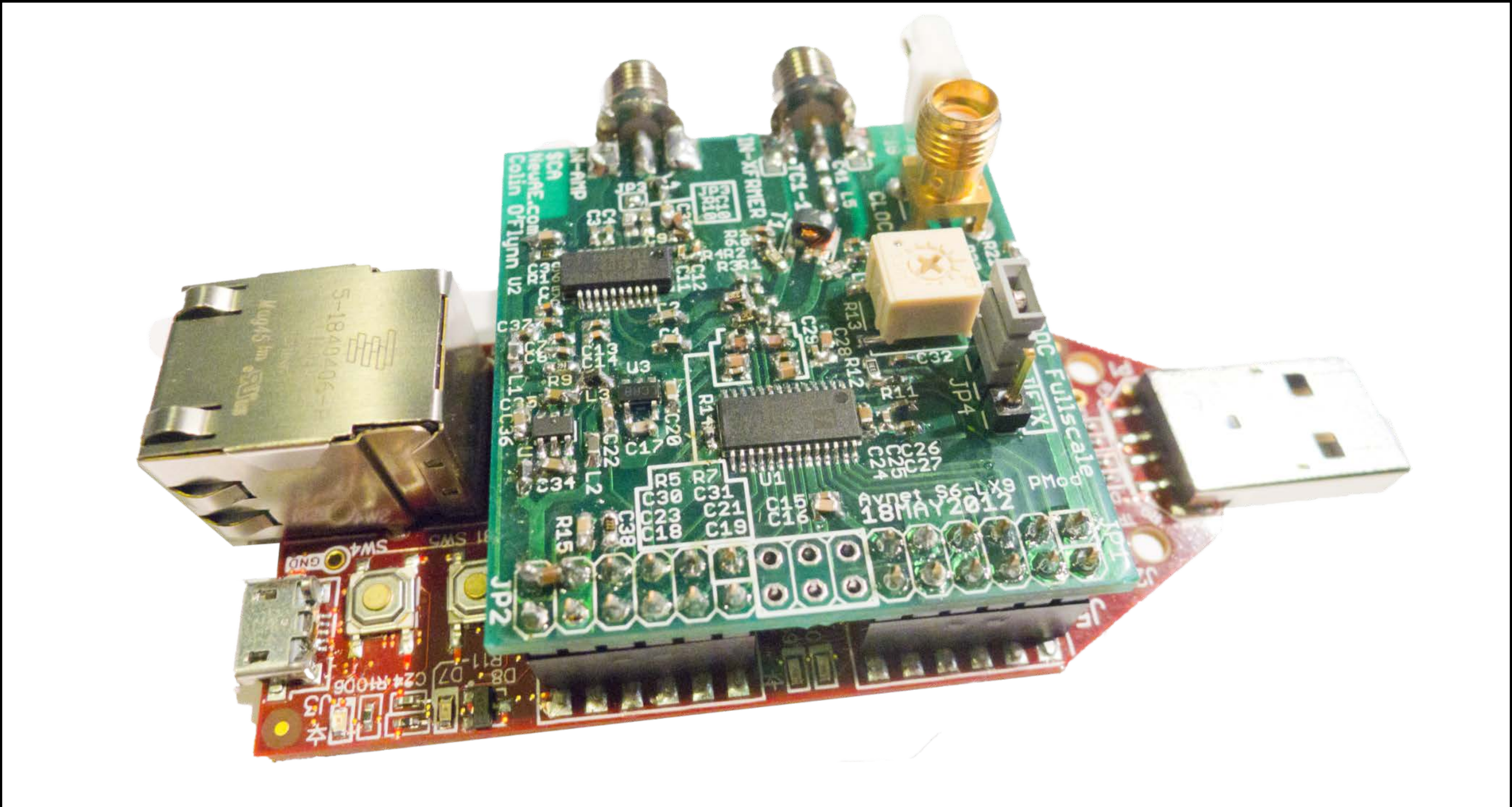


Desired Capture HW



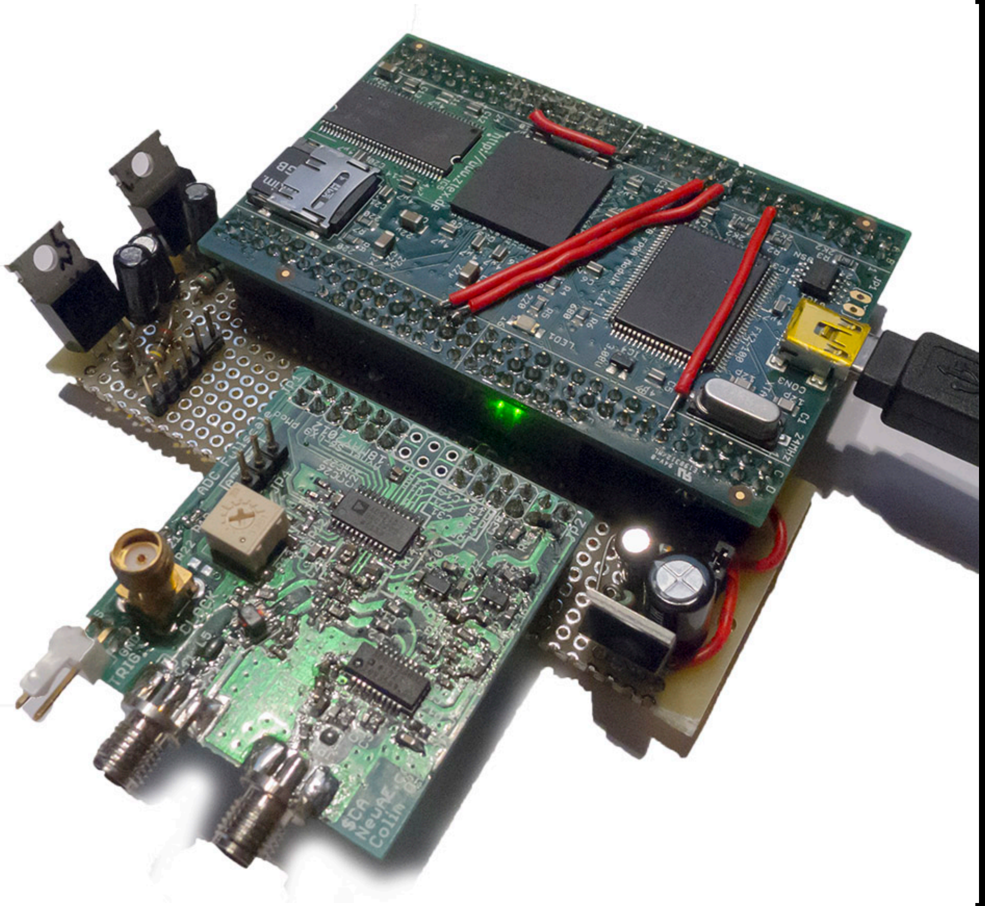
See "*A Case Study of Side-Channel Analysis using Decoupling Capacitor Power Measurement with the OpenADC*" by Colin O'Flynn & Zhizhang Chen

OpenADC + Spartan LX9 Board

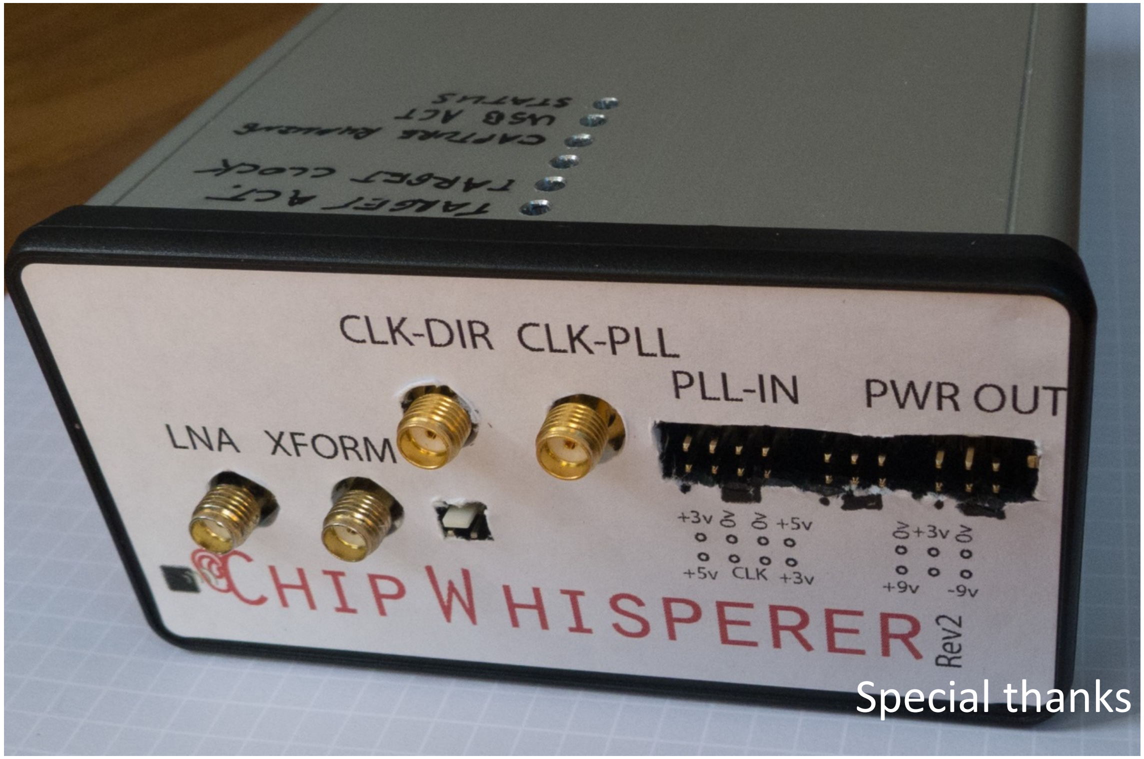


OpenADC + ZTEX Board

- ZTEX has Higher Speed USB interface
- More options on FPGA size for future development

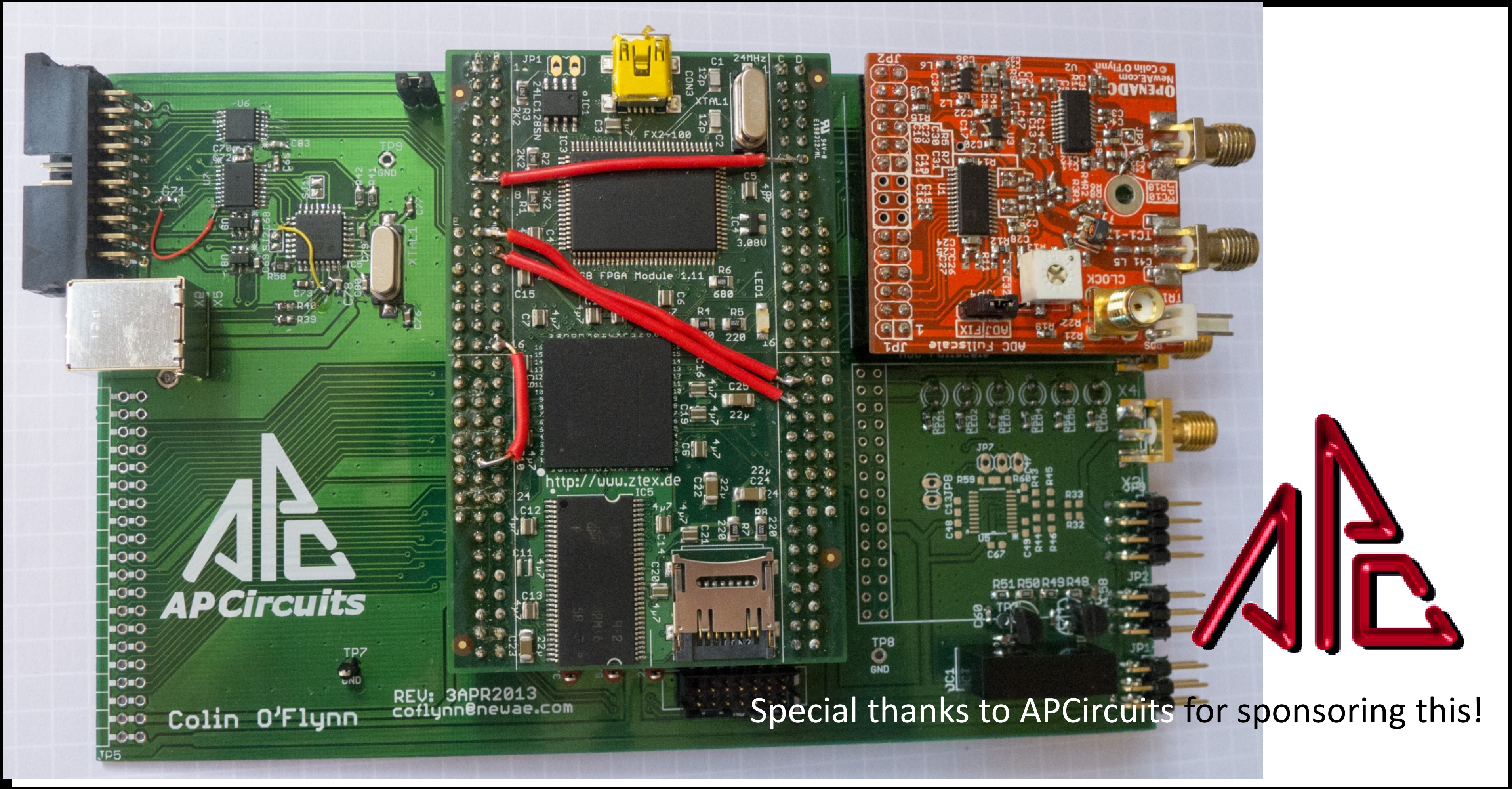


ZTEX Adapter Board



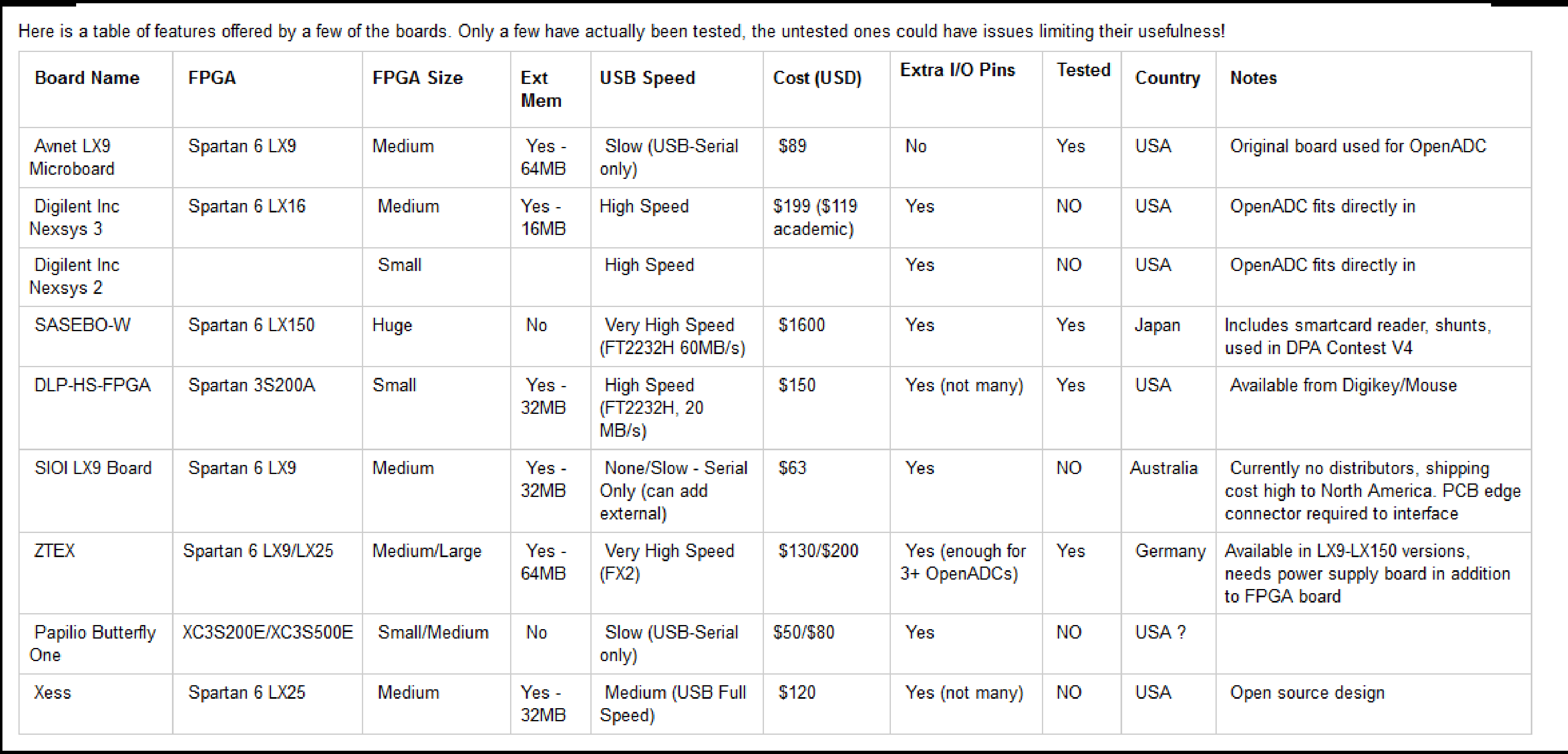
Special thanks to APCircuits for sponsoring this!

ZTEX Adapter Board



Special thanks to APCircuits for sponsoring this!

Other FPGA Boards (from Wiki)



Here is a table of features offered by a few of the boards. Only a few have actually been tested, the untested ones could have issues limiting their usefulness!

Board Name	FPGA	FPGA Size	Ext Mem	USB Speed	Cost (USD)	Extra I/O Pins	Tested	Country	Notes
Avnet LX9 Microboard	Spartan 6 LX9	Medium	Yes - 64MB	Slow (USB-Serial only)	$89	No	Yes	USA	Original board used for OpenADC
Digilent Inc Nexsys 3	Spartan 6 LX16	Medium	Yes - 16MB	High Speed	$199 ($119 academic)	Yes	NO	USA	OpenADC fits directly in
Digilent Inc Nexsys 2		Small		High Speed		Yes	NO	USA	OpenADC fits directly in
SASEBO-W	Spartan 6 LX150	Huge	No	Very High Speed (FT2232H 60MB/s)	$1600	Yes	Yes	Japan	Includes smartcard reader, shunts, used in DPA Contest V4
DLP-HS-FPGA	Spartan 3S200A	Small	Yes - 32MB	High Speed (FT2232H, 20 MB/s)	$150	Yes (not many)	Yes	USA	Available from Digikey/Mouse
SIOI LX9 Board	Spartan 6 LX9	Medium	Yes - 32MB	None/Slow - Serial Only (can add external)	$63	Yes	NO	Australia	Currently no distributors, shipping cost high to North America. PCB edge connector required to interface
ZTEX	Spartan 6 LX9/LX25	Medium/Large	Yes - 64MB	Very High Speed (FX2)	$130/$200	Yes (enough for 3+ OpenADCs)	Yes	Germany	Available in LX9-LX150 versions, needs power supply board in addition to FPGA board
Papilio Butterfly One	XC3S200E/XC3S500E	Small/Medium	No	Slow (USB-Serial only)	$50/$80	Yes	NO	USA ?	
Xess	Spartan 6 LX25	Medium	Yes - 32MB	Medium (USB Full Speed)	$120	Yes (not many)	NO	USA	Open source design

Synchronous Sampling Scope

e.g.:

- CleverScope with CS810 Option
- PicoScope PS6000
- Almost any high-speed analog FPGA/ADC Board

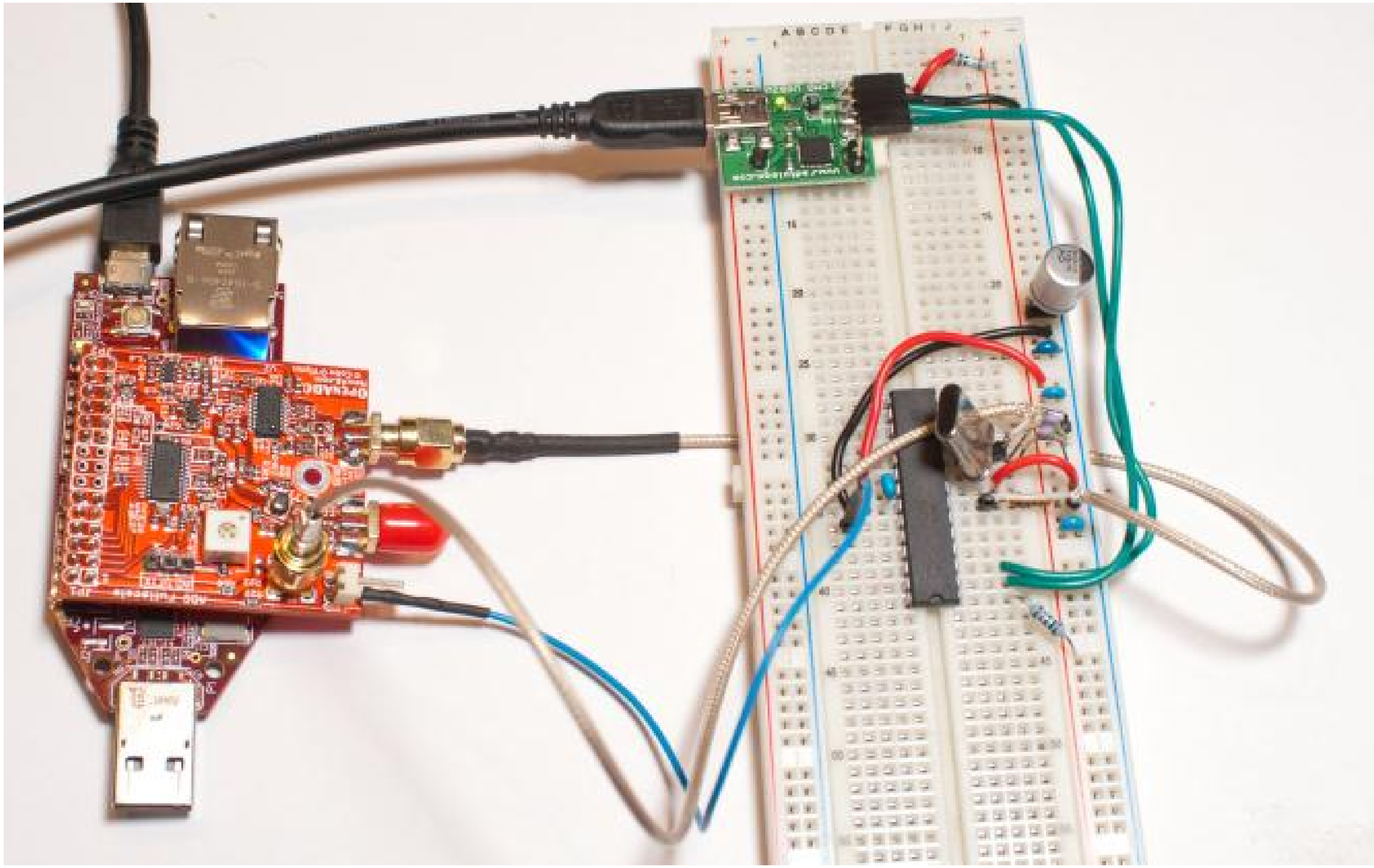
Your First Attack

Should I Attack a “Smartcard”?

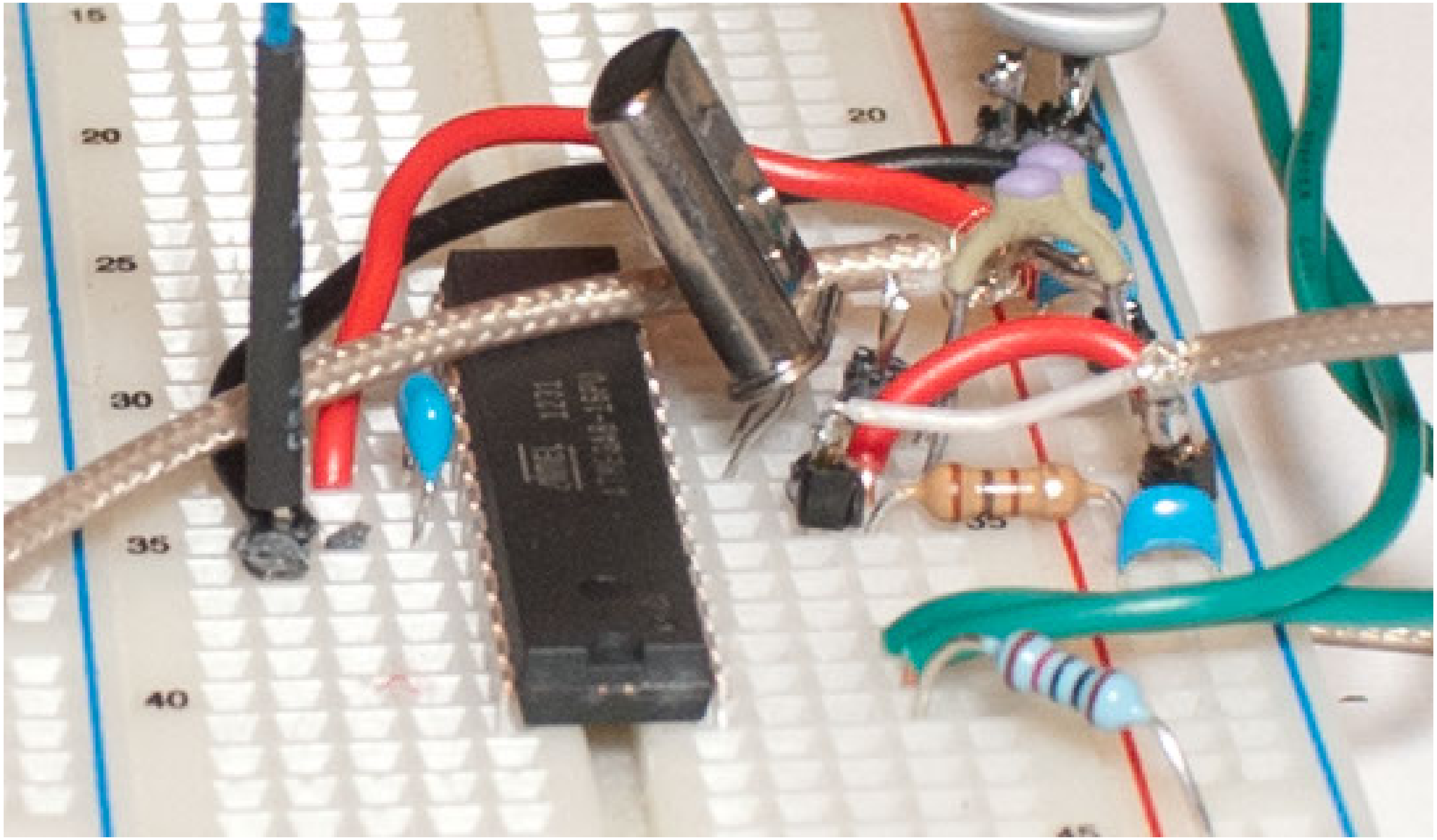
So What do you Do?

=

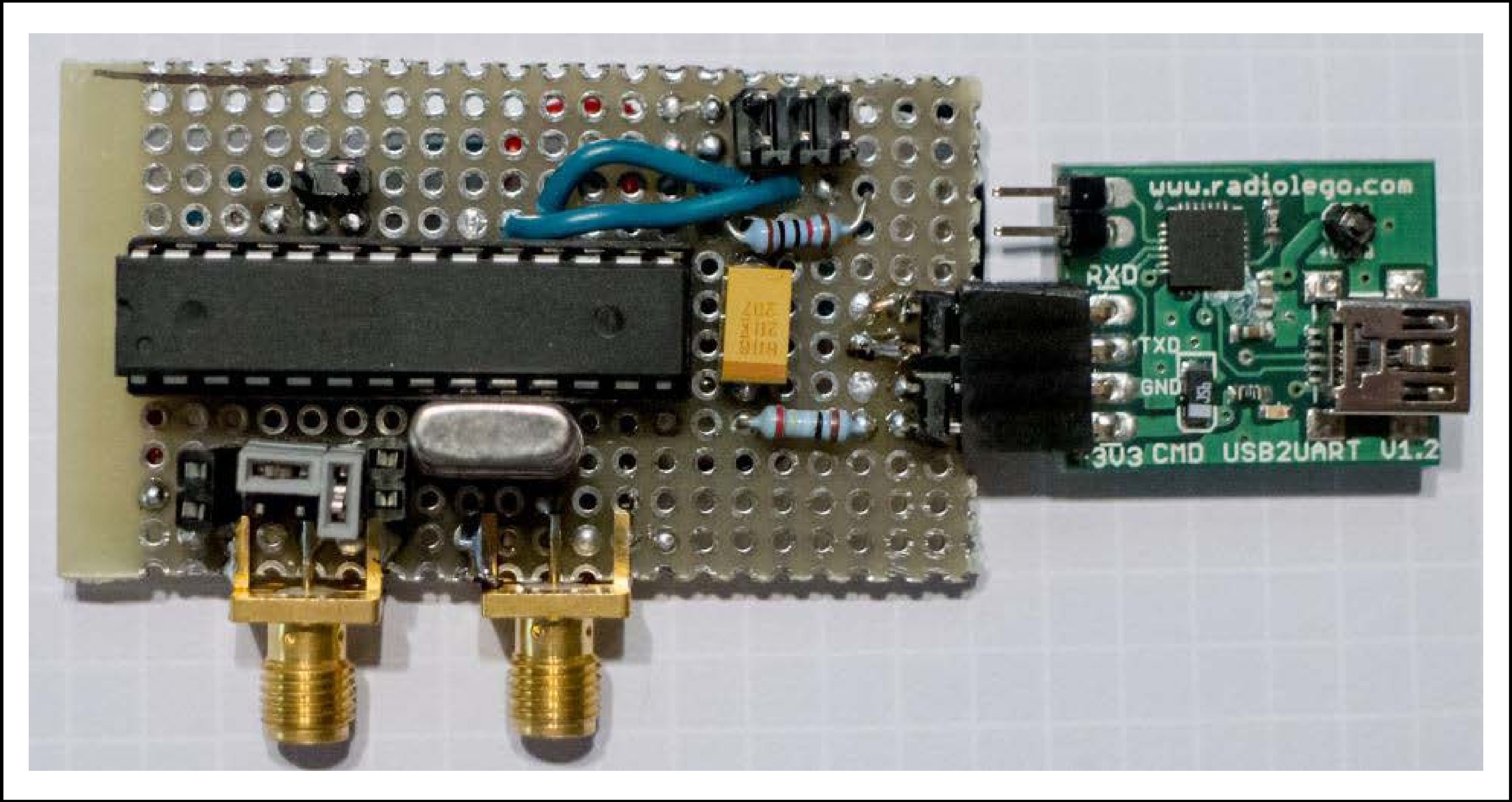
What does this Look Like?



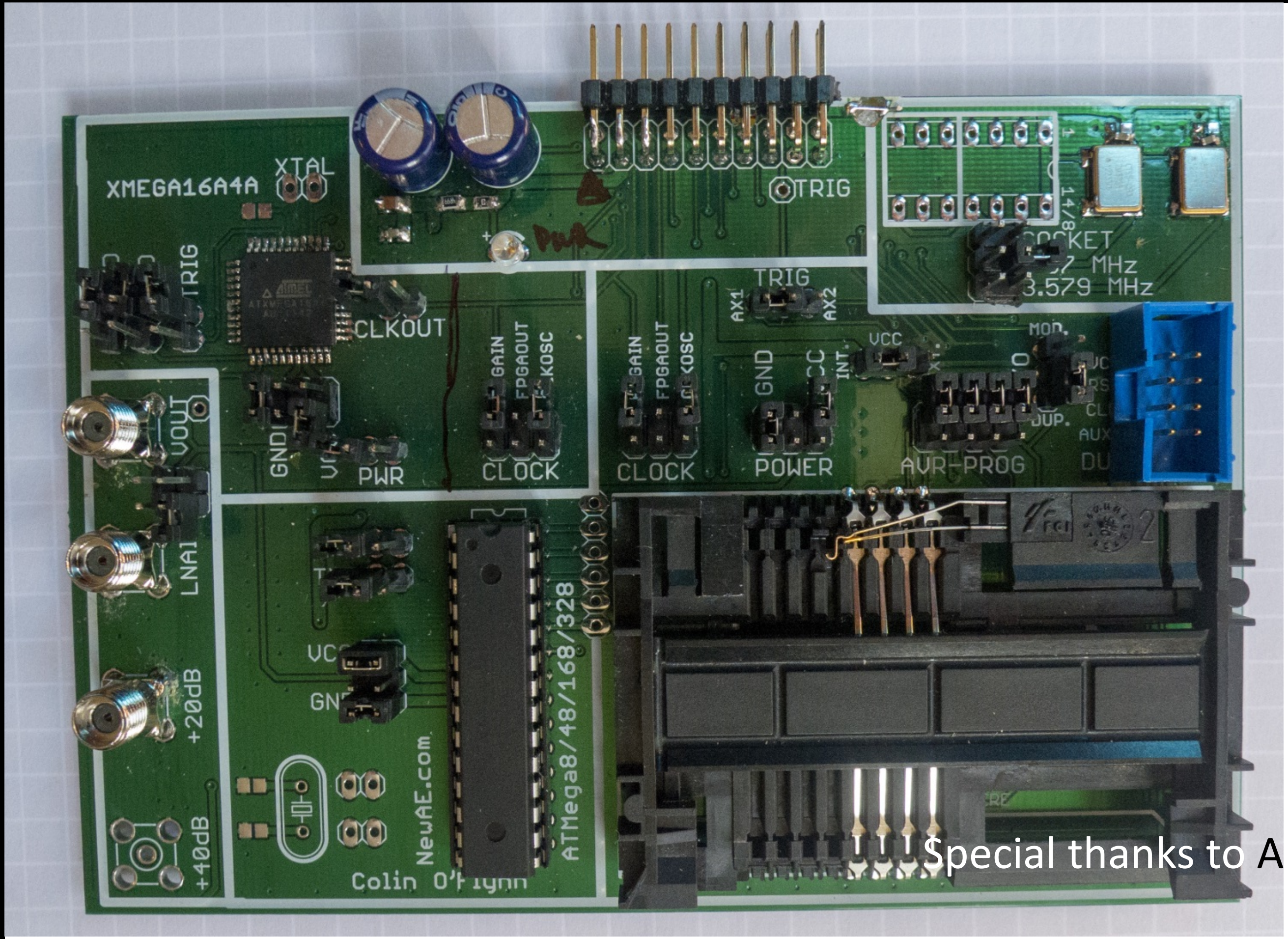
What does this Look Like?



A PCB Version



Multi-Target Victim



Special thanks to APCircuits for sponsoring this!

Let’s Do This: Shopping List

- AtMega8 / AtMega48
- 7.37 MHz Crystal
- 22pF Capacitors
- 100 ohm resistors
- 220uF (or bigger) capacitor
- 1uF Ceramic Capacitor
- 0.1uF Ceramic Capacitor
- Cables/Connectors
- Breadboard
- Capture HW
- Serial-USB Adapter
- Power?
- AVR Programmer

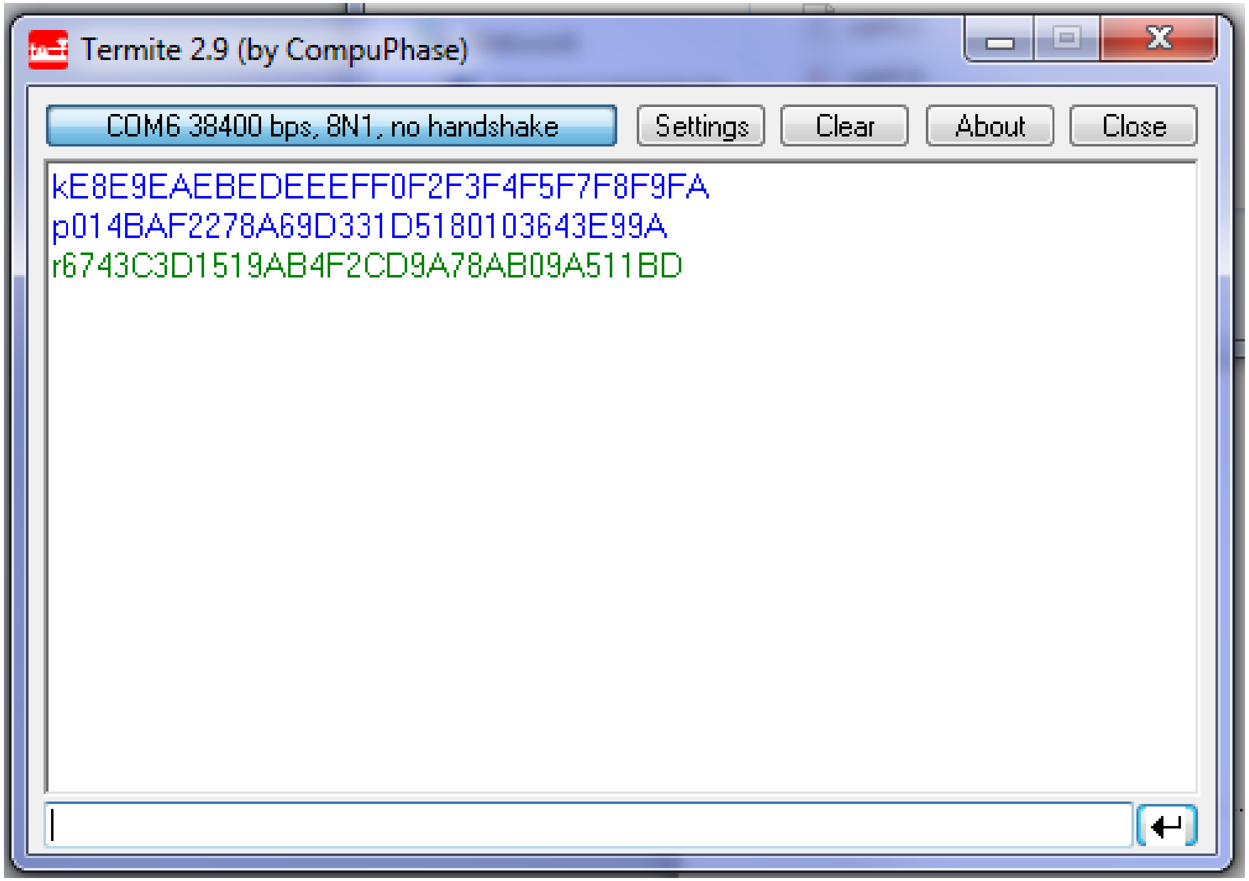
Notes on Step 1

- Ideally Get ATMega8-16PU
  - AtMega48A also works, note ‘A’ suffix means a smaller geometry used in Production = smaller power signature
- 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)

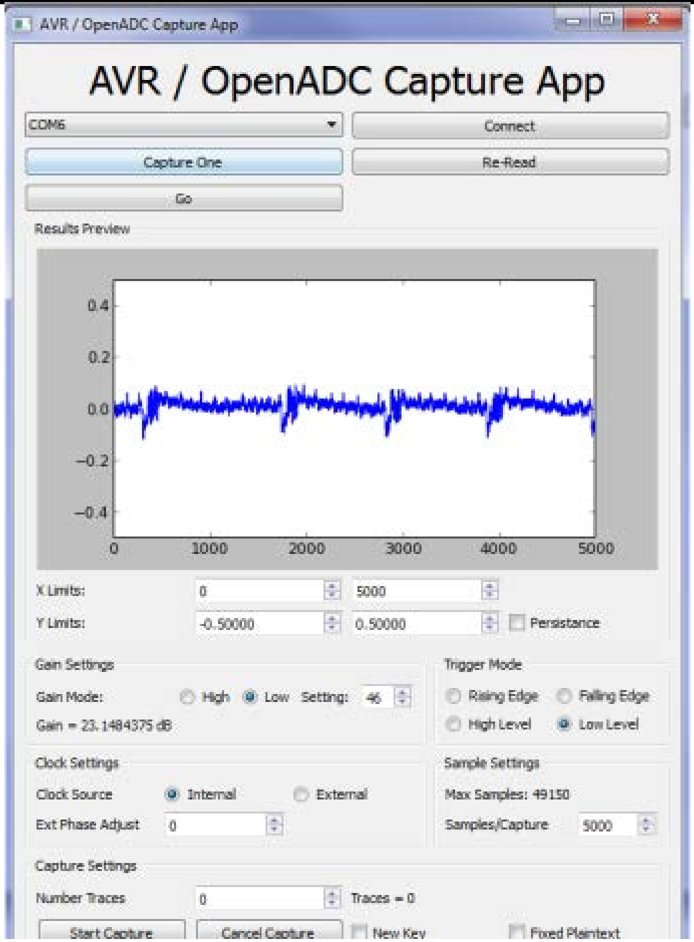
Step 2: Continued (Testing)


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

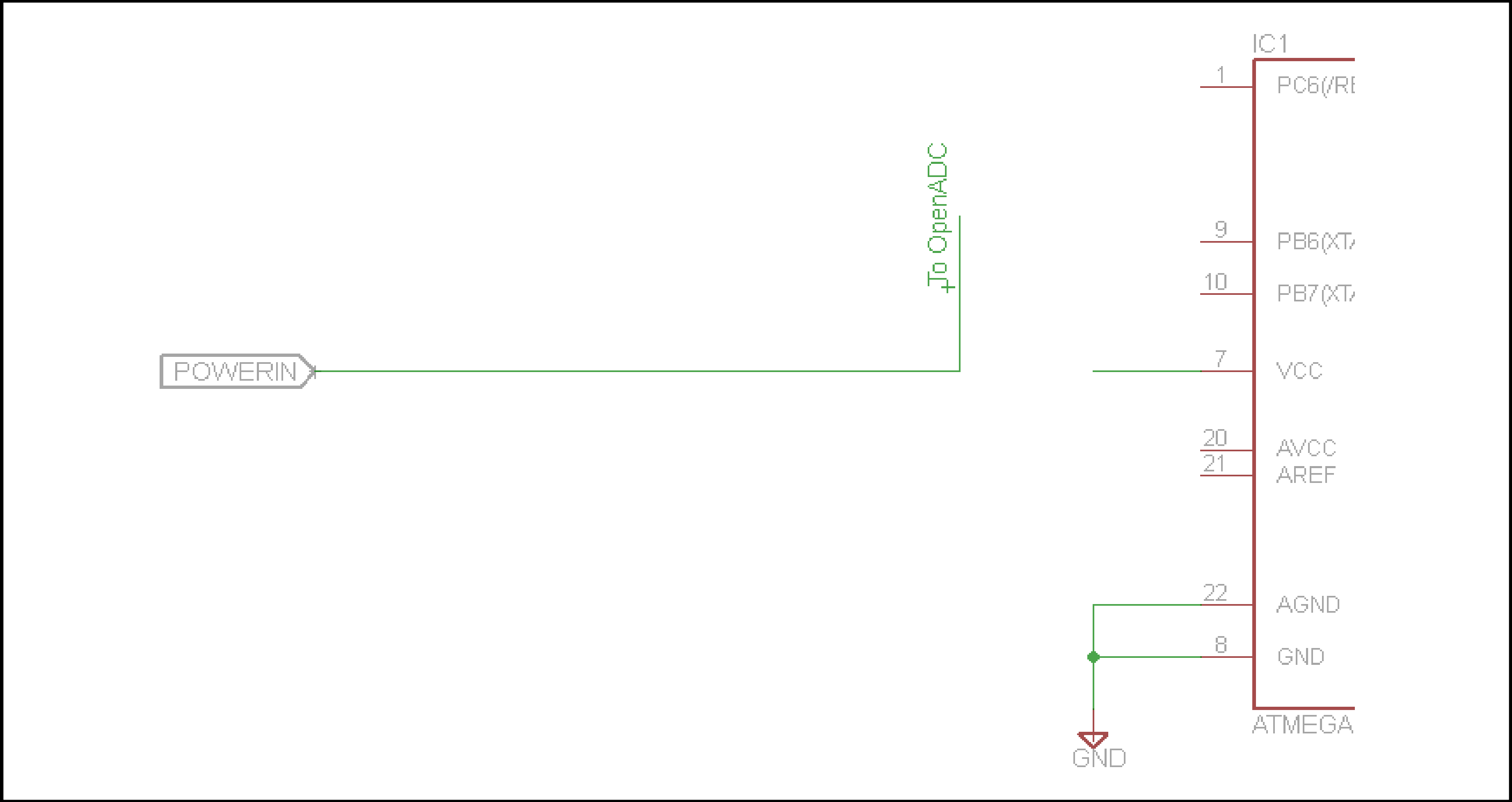
Capture Settings

Number Traces 0 Traces = 0

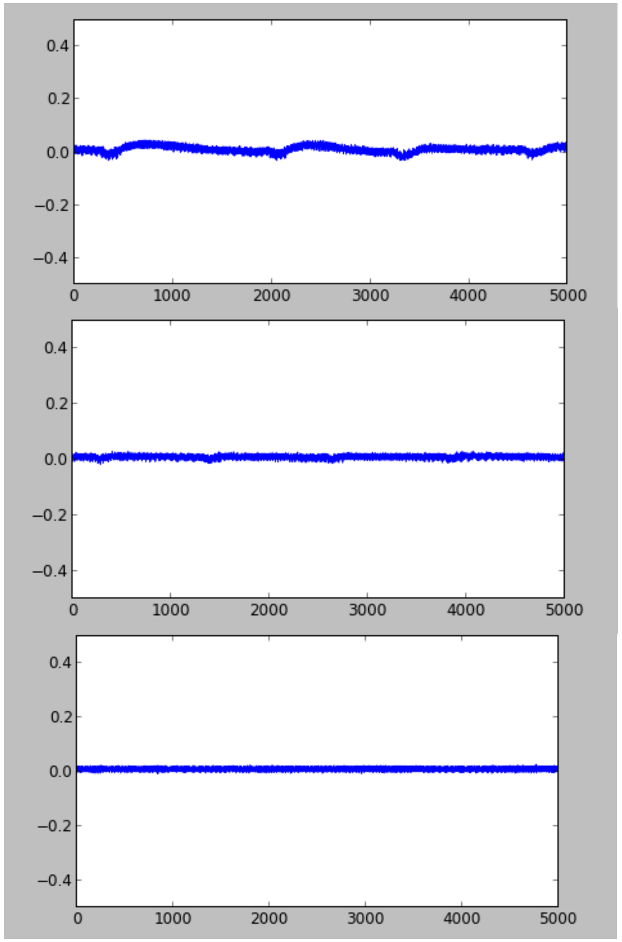
□ New Key □ Fixed Plaintext

- Probe connected to VCC rail, not across shunt

Step 3: Characterize



Step 3: Characterize

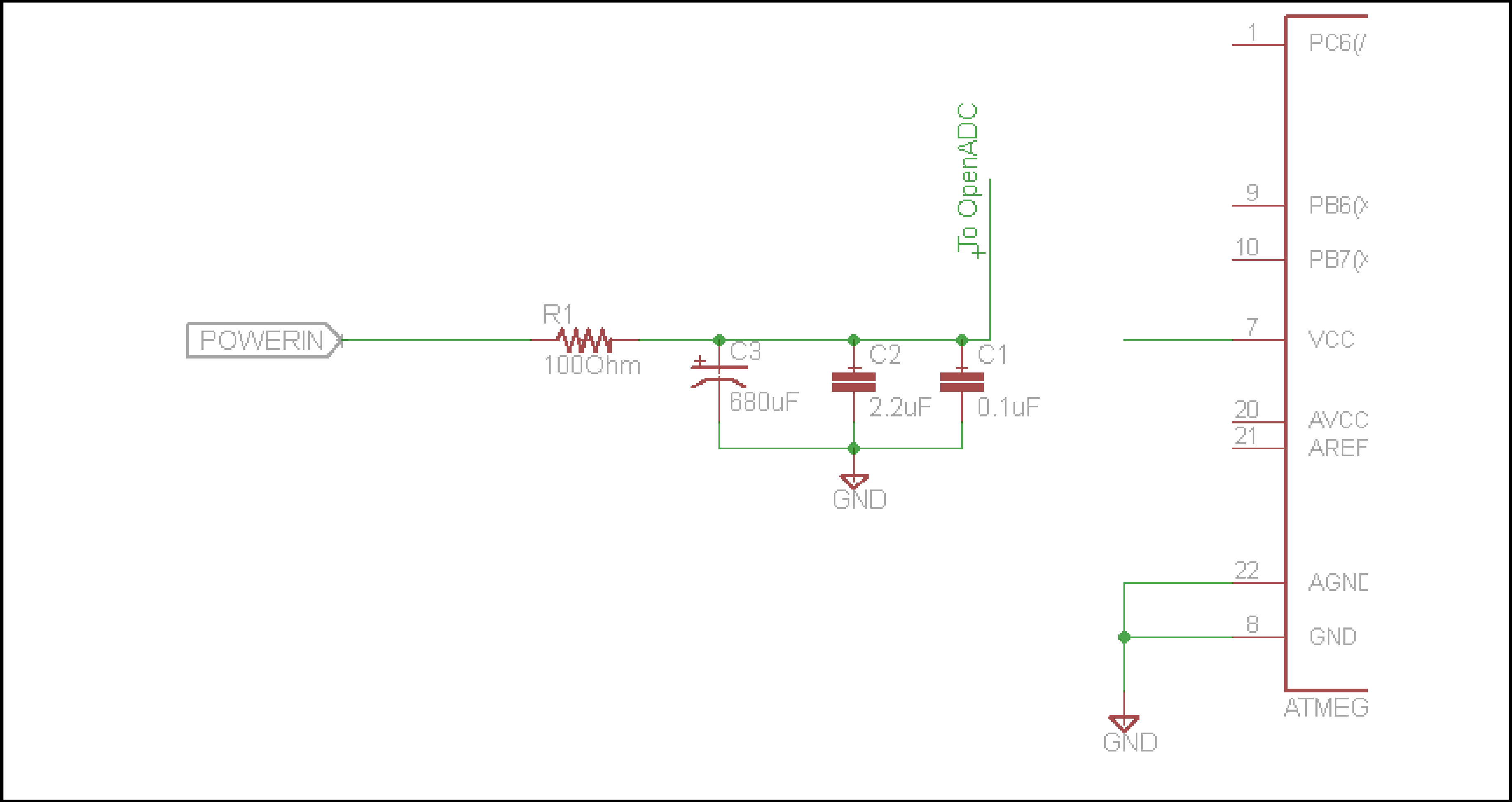


2.2uF Ceramic Capacitor

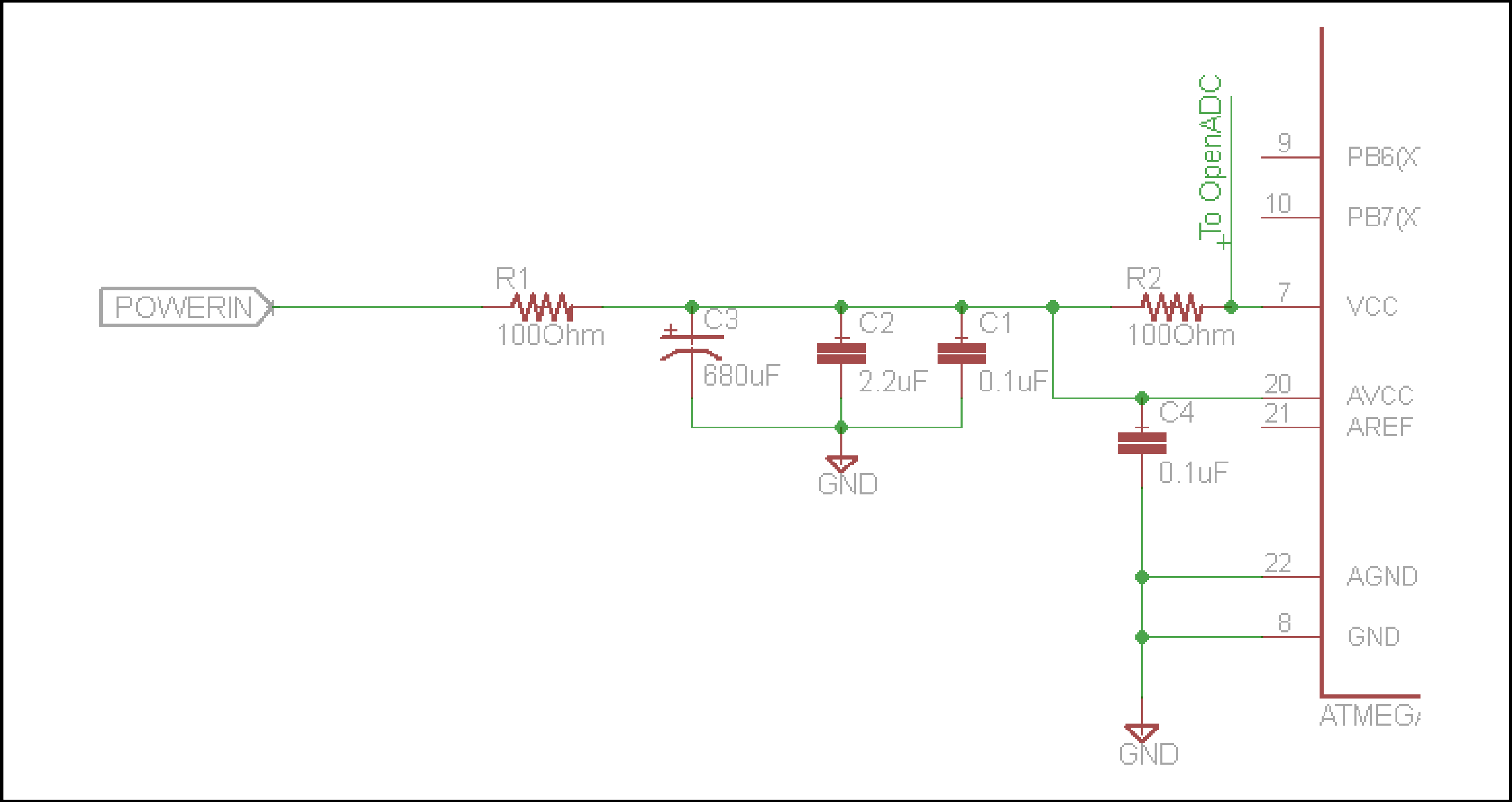
+680uF Electrolyctic

+100 ohm series resistor

Step 3: Characterize

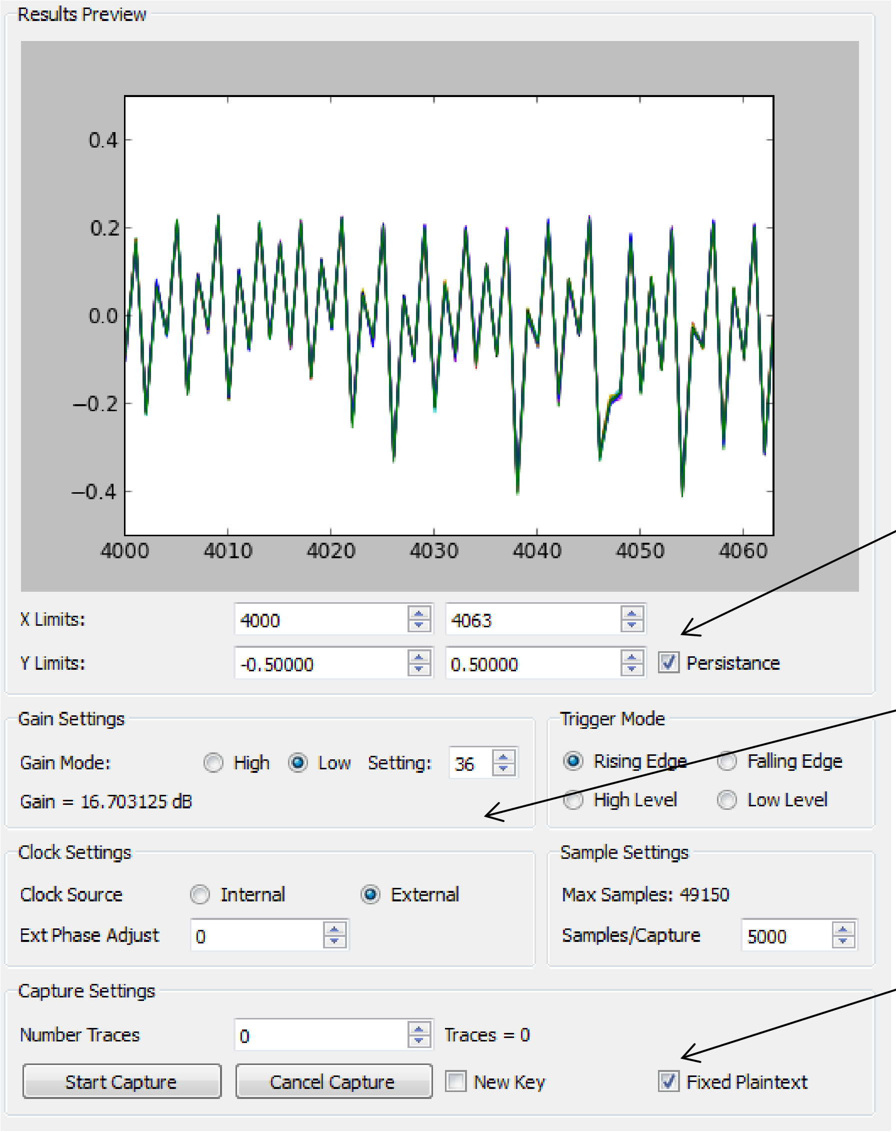


Step 3: Shunt



POWERIN
R1
100Ohm
C3
680uF
C2
2.2uF
C1
0.1uF
GND
R2
100Ohm
To OpenADC
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

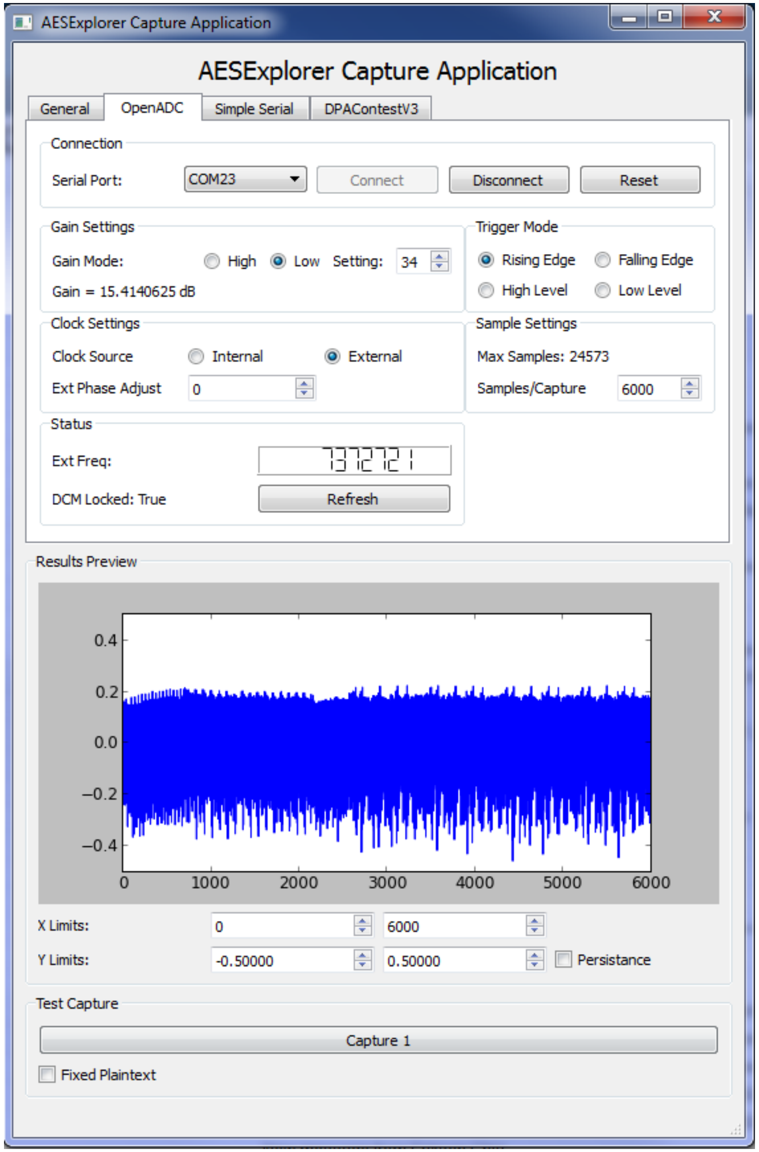
☐ New Key ☑ Fixed Plaintext

Persistence Mode in Scope

Adjust gain, trigger, etc to get reliable signal

Fixed Plaintext

Step 4: Acquire



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

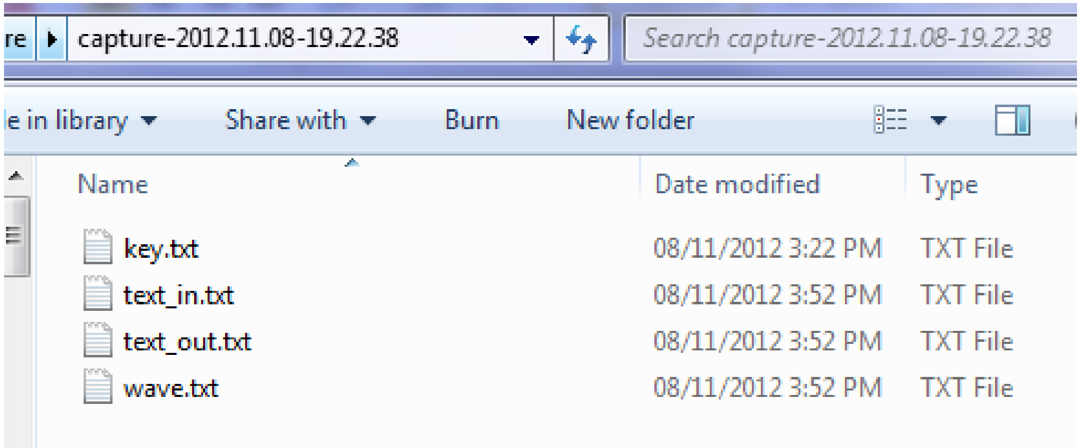
Y Limits: -0.50000 0.50000 □ Persistance

Test Capture

□ Fixed Plaintext

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

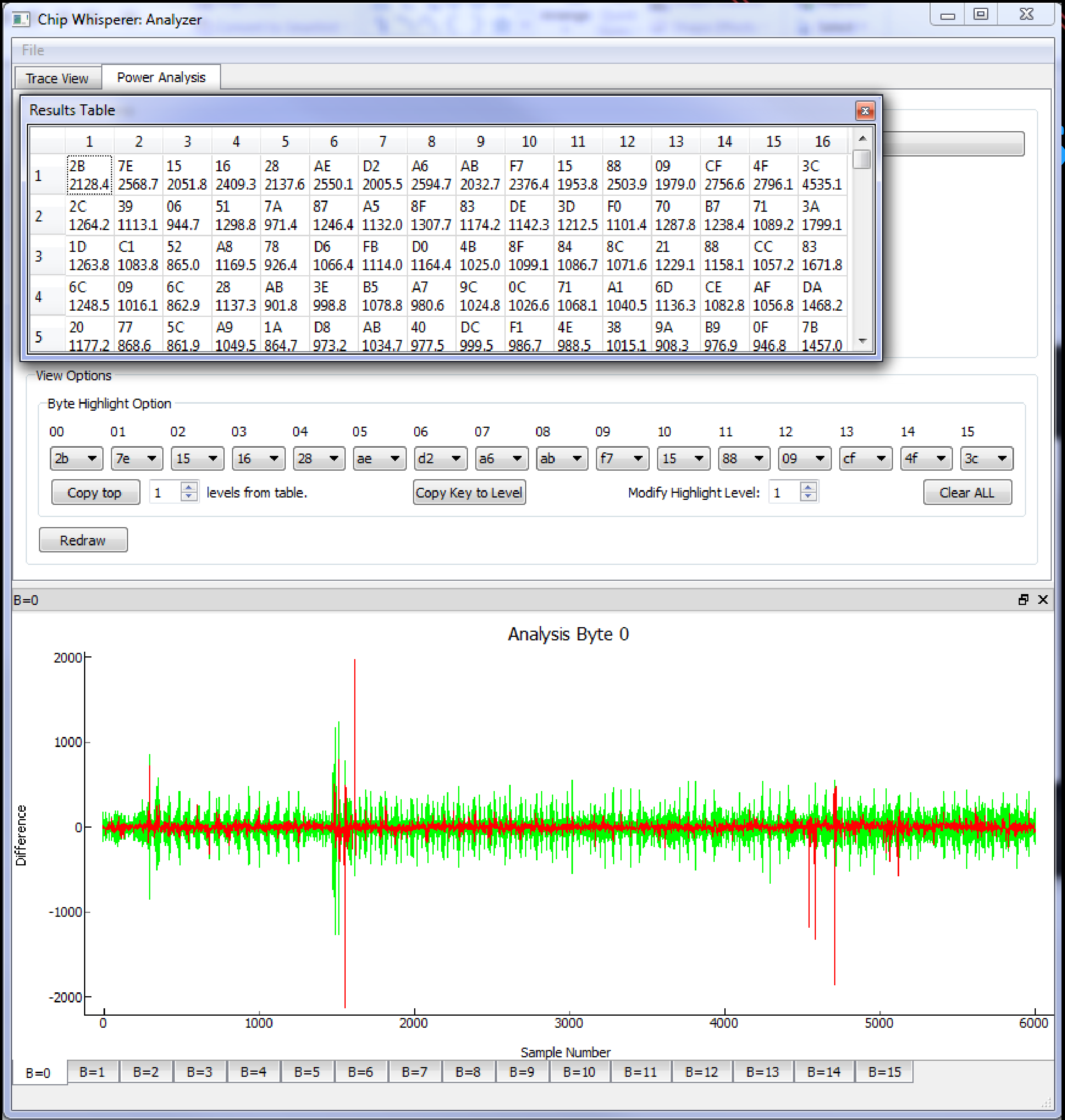
Step 4: Acquire



capture-2012.11.08-19.22.38

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



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

View Options

Byte Highlight Option

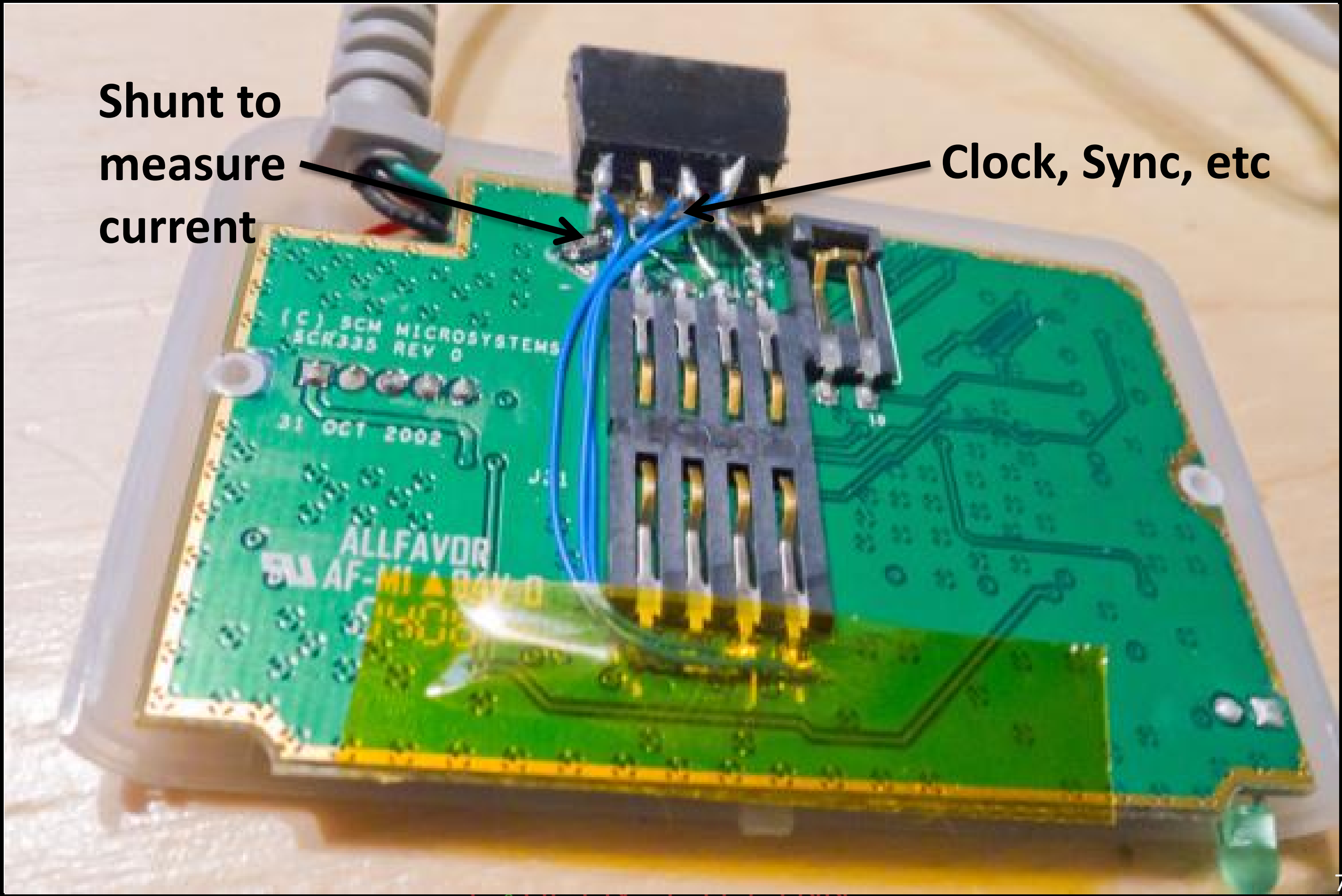
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
2b	7e	15	16	28	ae	d2	a6	ab	f7	15	88	09	cf	4f	3c

Copy top 1 levels from table.

Modify Highlight Level: 1

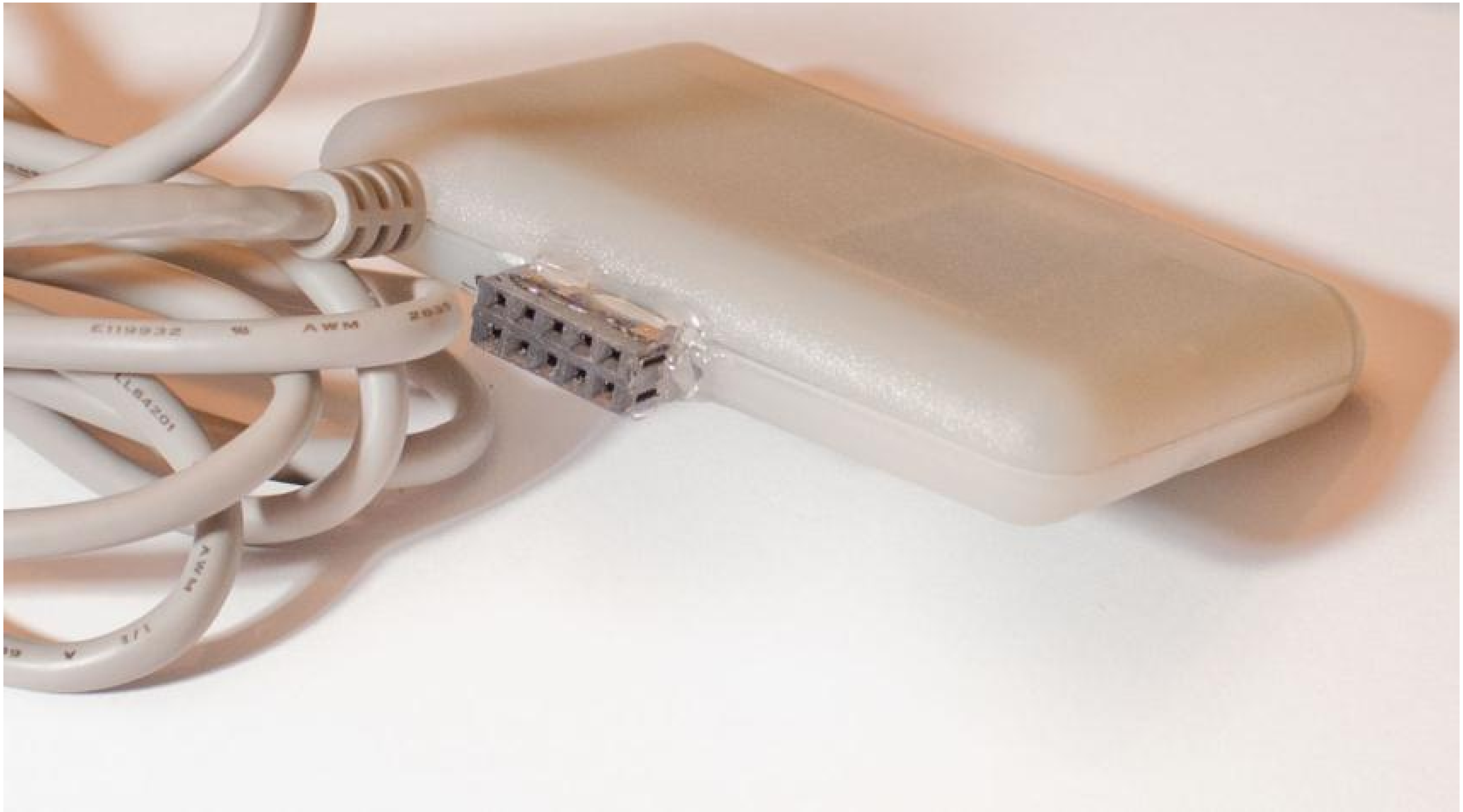
SMARTCARD STUFF

Attacks against Smart Card

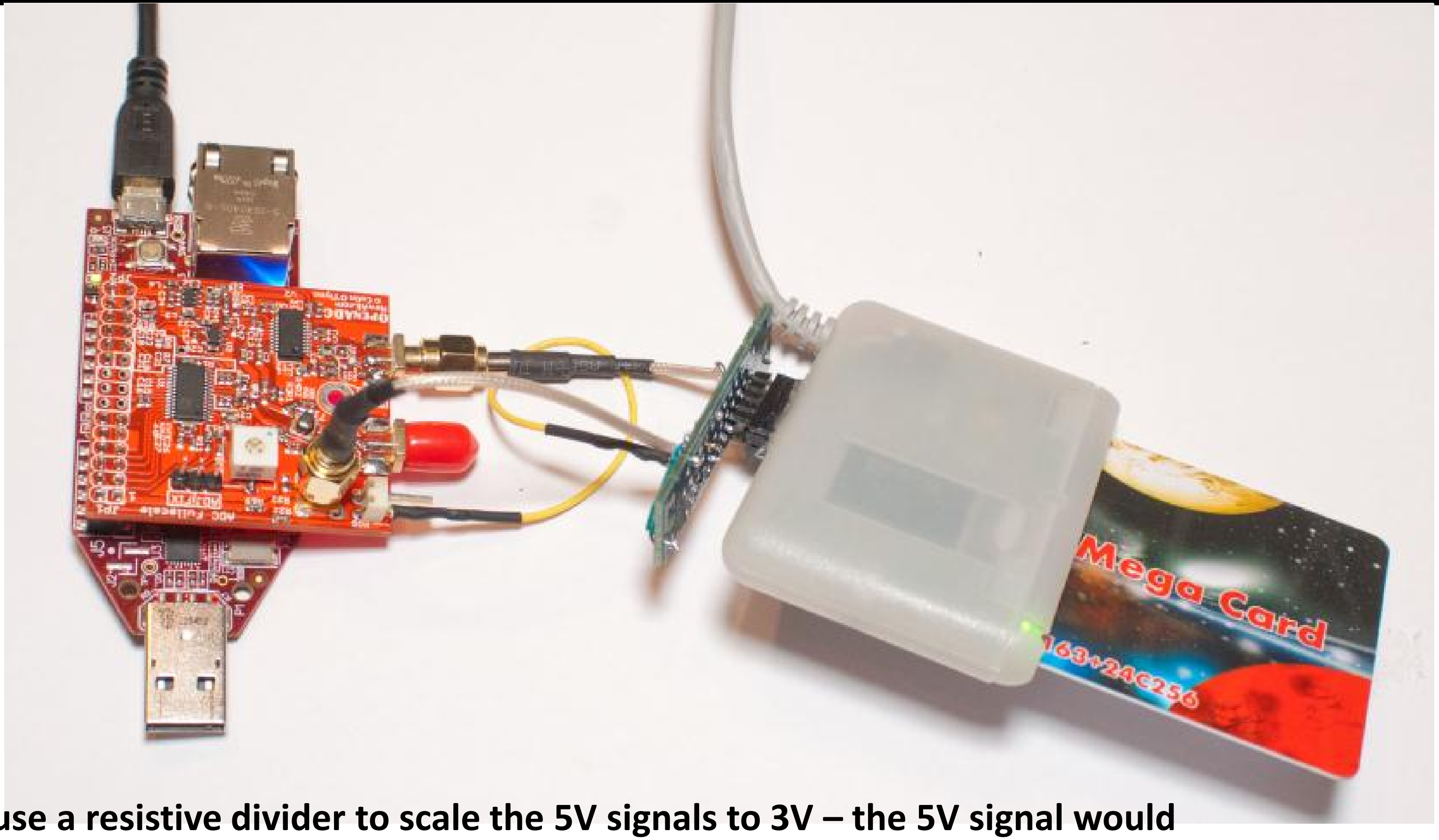


Shunt to measure current

Clock, Sync, etc

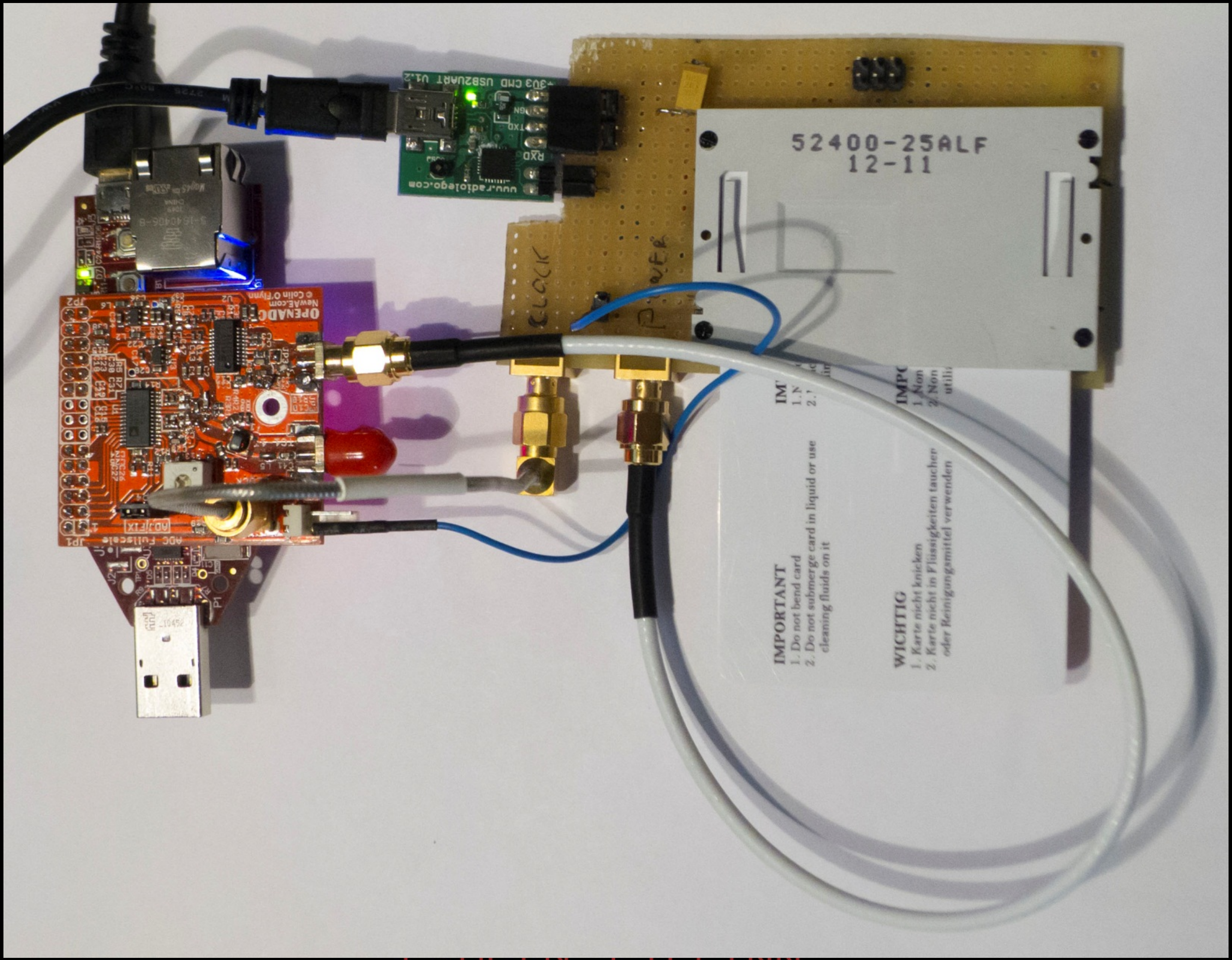

E119932
AWM
LL84201
AWM

SmartCard Capture

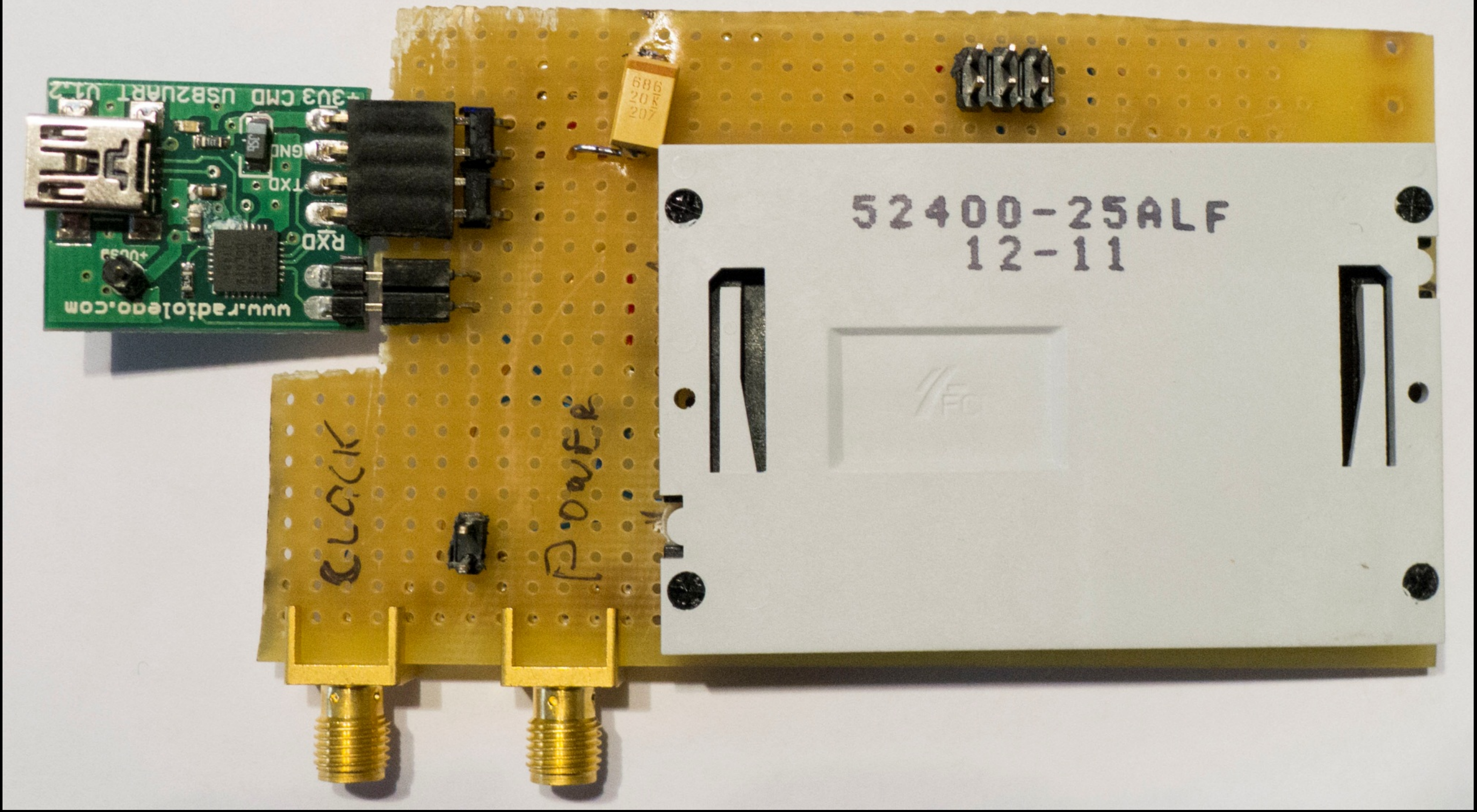


Note we use a resistive divider to scale the 5V signals to 3V – the 5V signal would immediately destroy the FPGA board!

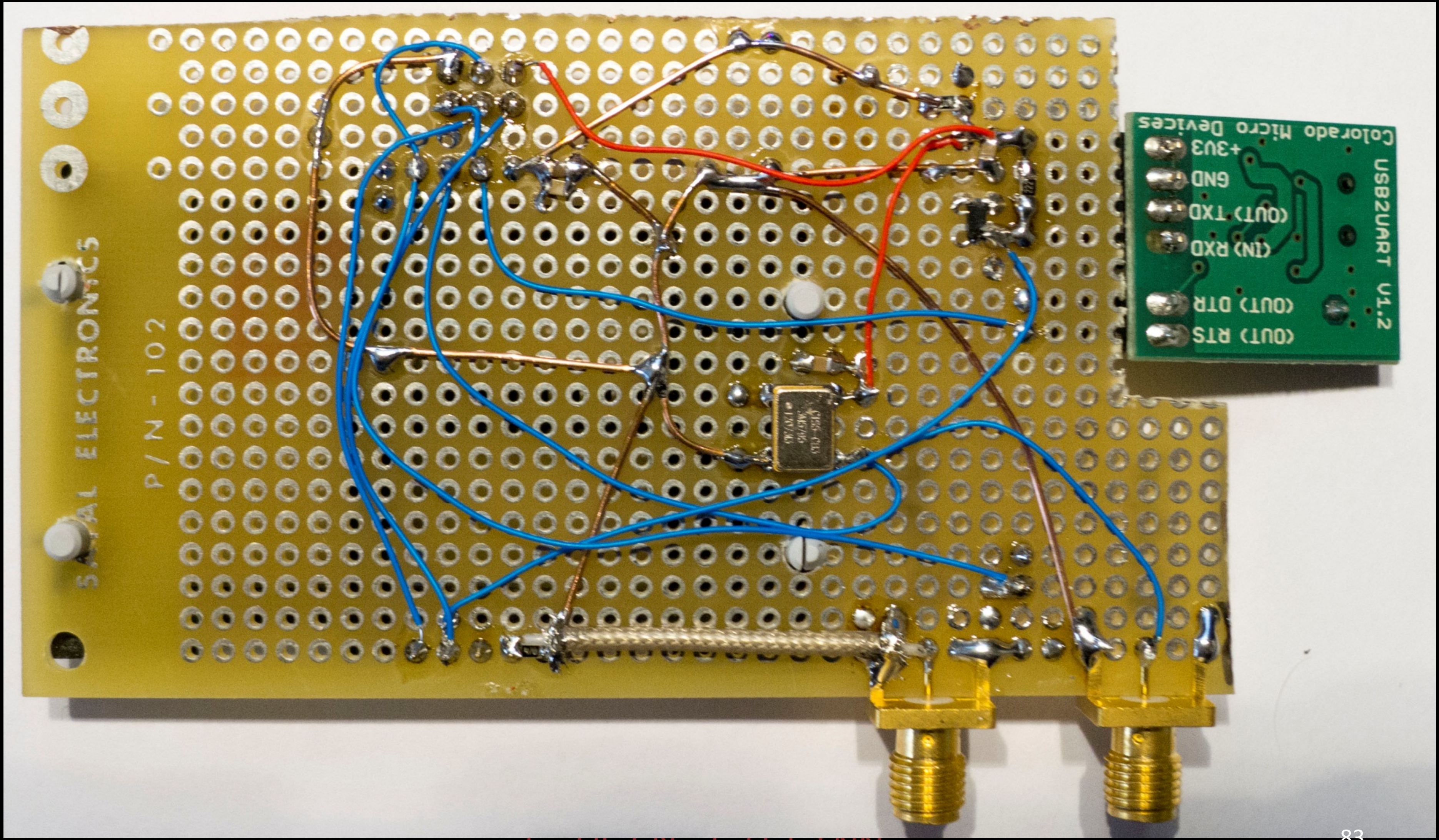
SmartCard Capture - Cheap



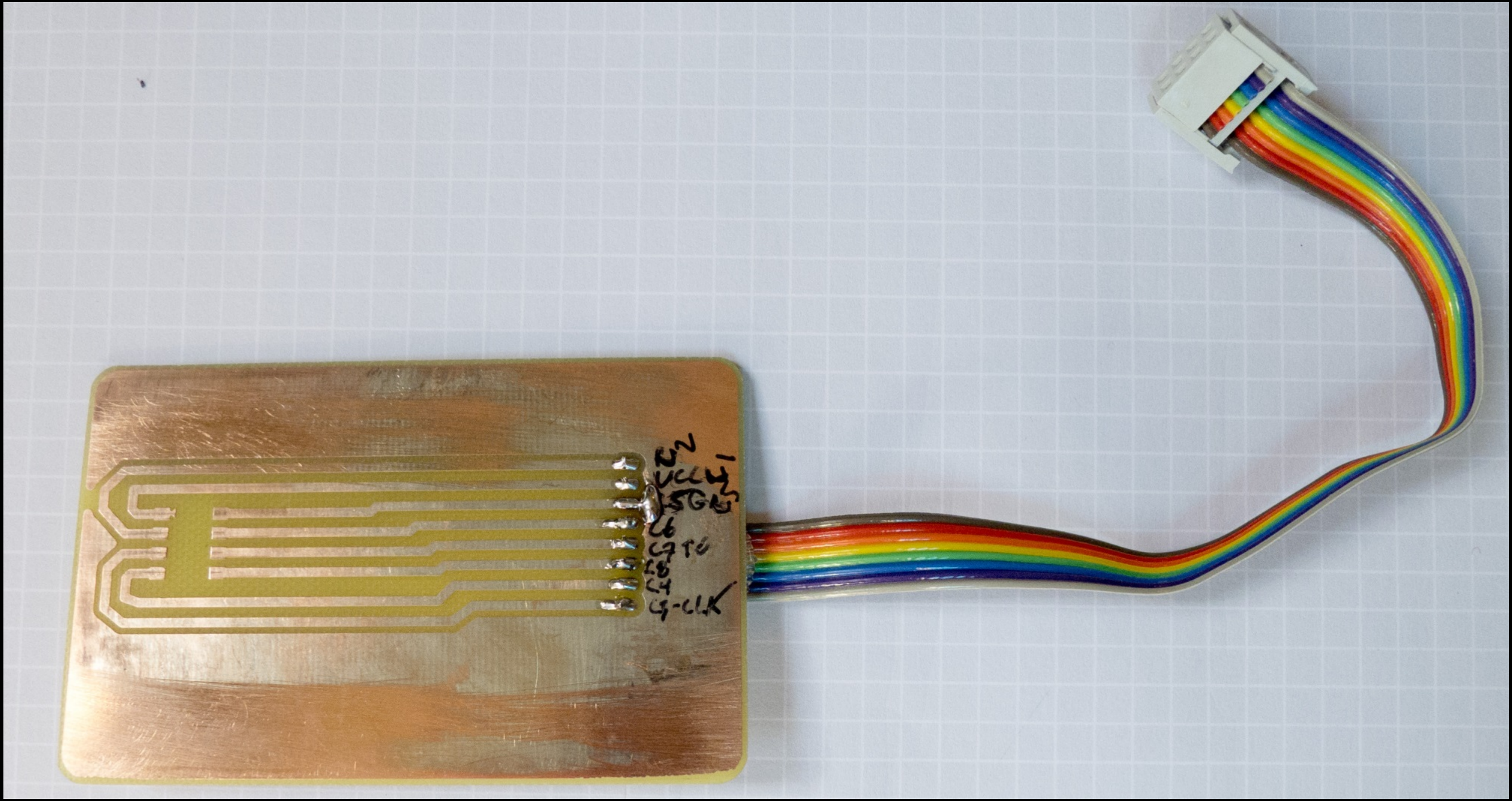
SmartCard Capture - Cheap



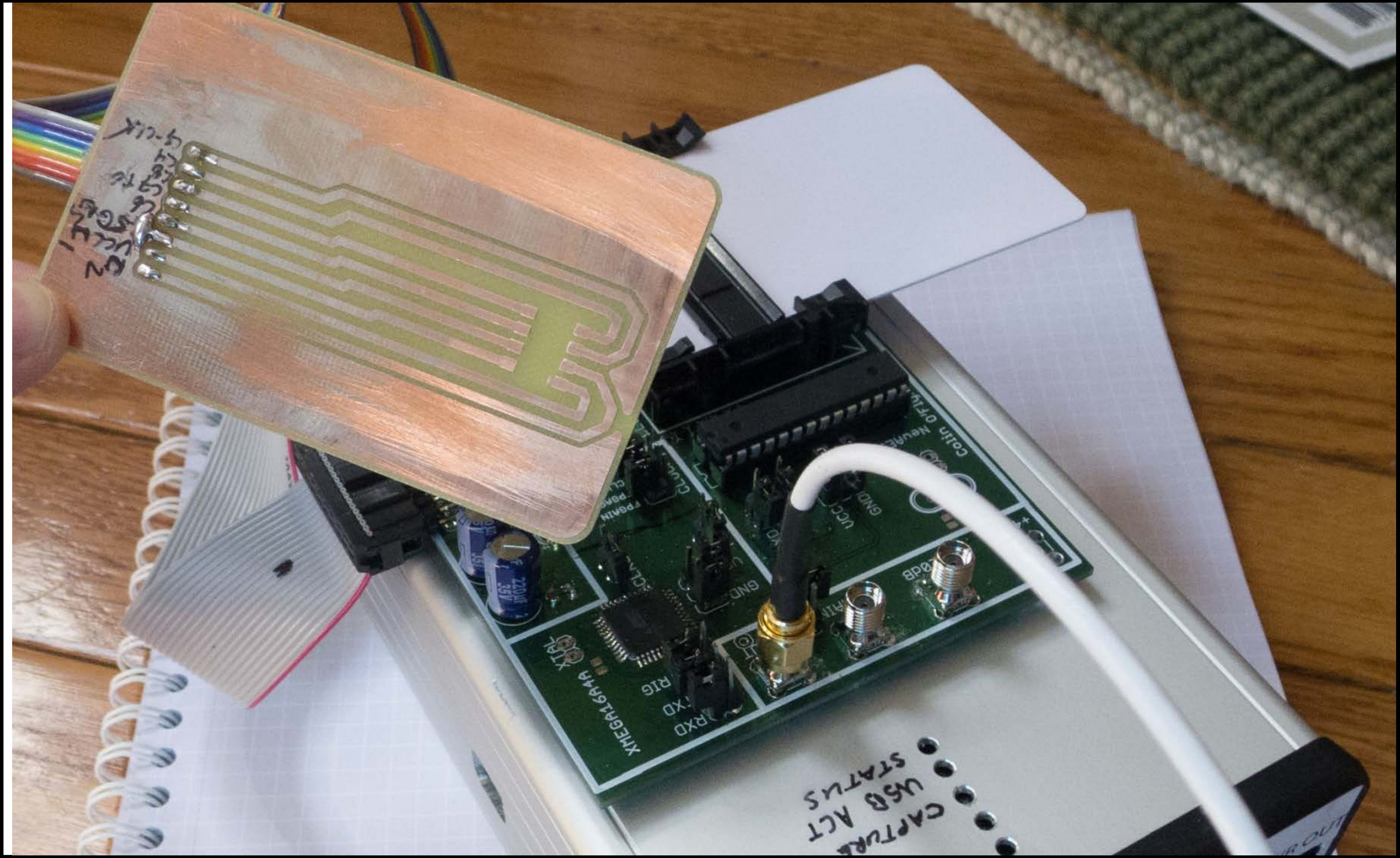
SmartCard Capture - Cheap



SmartCard Capture - Inbetween

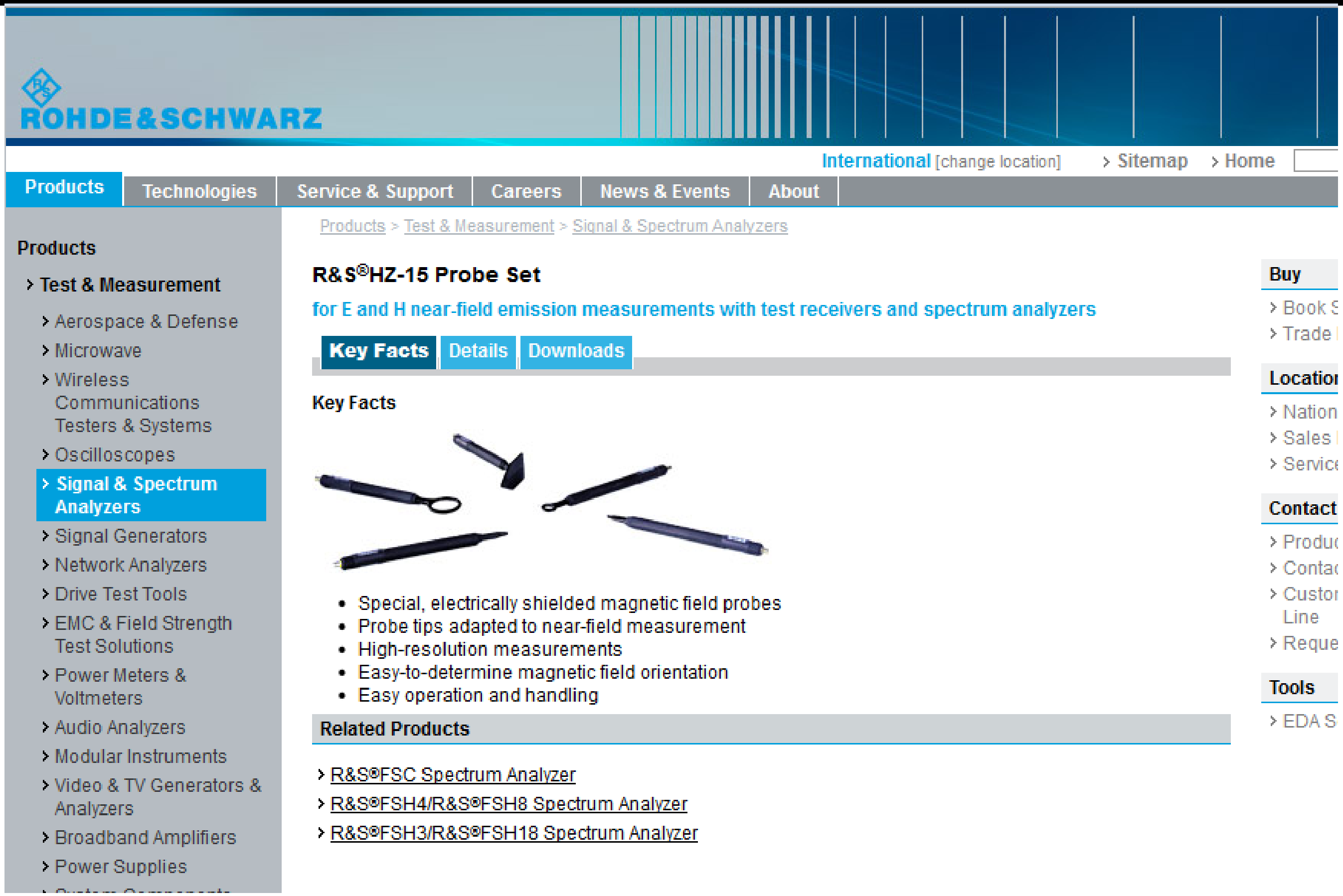


SmartCard Capture - Inbetween



MAGNETIC FIELD PROBES

Rohde & Schwarz



ROHDE&SCHWARZ

International [change location] › Sitemap › Home

Products | Technologies | Service & Support | Careers | News & Events | About

Products > Test & Measurement > Signal & Spectrum Analyzers

Products

- › Test & Measurement
  - › Aerospace & Defense
  - › Microwave
  - › Wireless Communications Testers & Systems
  - › Oscilloscopes
  - › Signal & Spectrum Analyzers
  - › Signal Generators
  - › Network Analyzers
  - › Drive Test Tools
  - › EMC & Field Strength Test Solutions
  - › Power Meters & Voltmeters
  - › Audio Analyzers
  - › Modular Instruments
  - › Video & TV Generators & Analyzers
  - › Broadband Amplifiers
  - › Power Supplies

R&S®HZ-15 Probe Set

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

Key Facts | Details | Downloads

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

Buy

- › Book S
- › Trade

Locatio

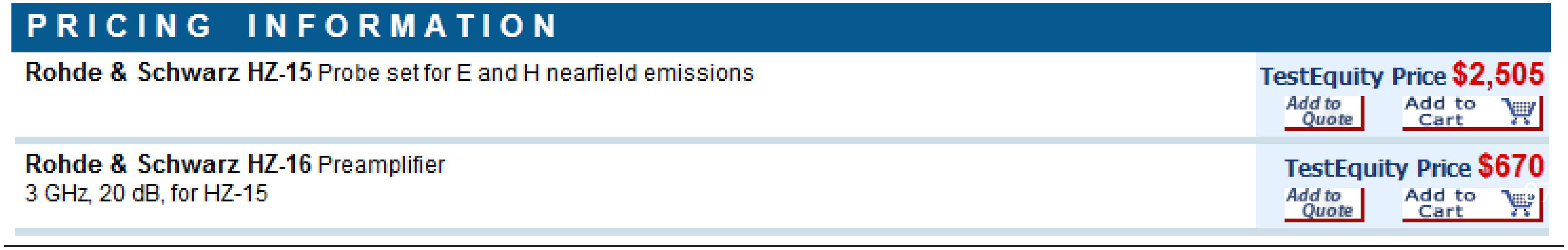
- › Nation
- › Sales
- › Servic

Contact

- › Produ
- › Conta
- › Custo Line
- › Reque

Tools

- › EDA S

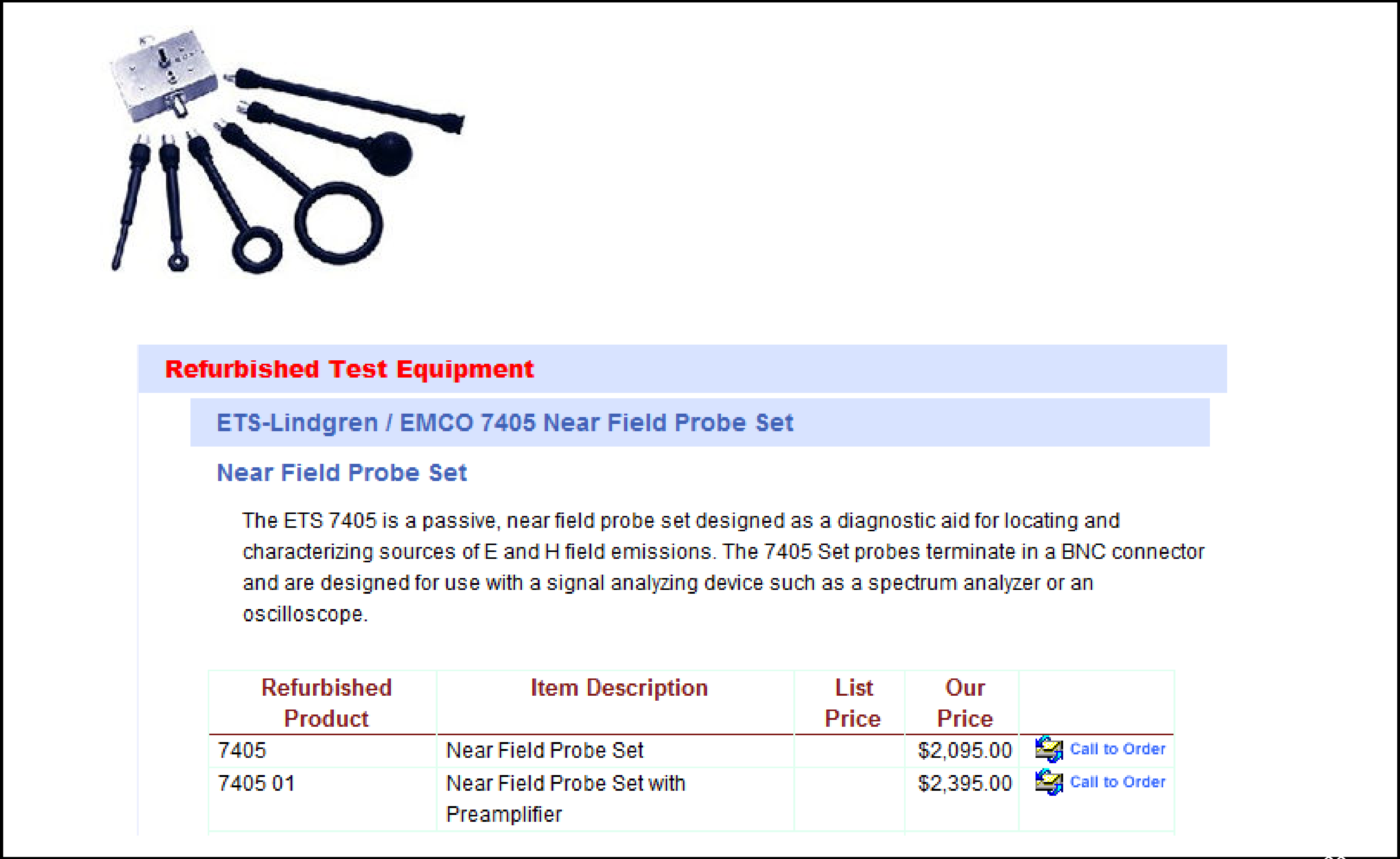


PRICING INFORMATION

Rohde & Schwarz HZ-15 Probe set for E and H nearfield emissions — TestEquity Price **$2,505**

Rohde & Schwarz HZ-16 Preamplifier
3 GHz, 20 dB, for HZ-15 — TestEquity Price **$670**

ETS-Lindgren



Refurbished Test Equipment

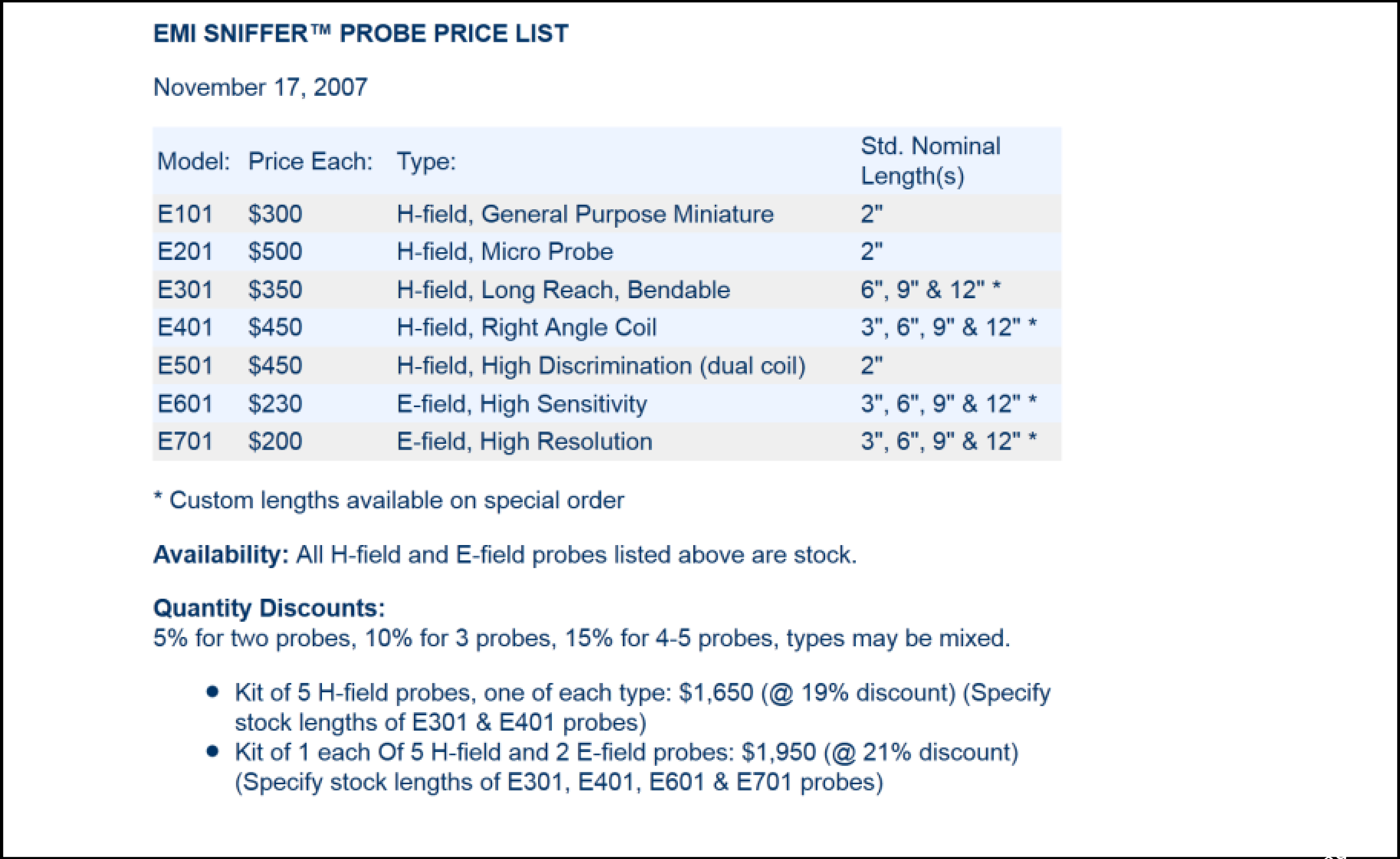
ETS-Lindgren / EMCO 7405 Near Field Probe Set

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" *

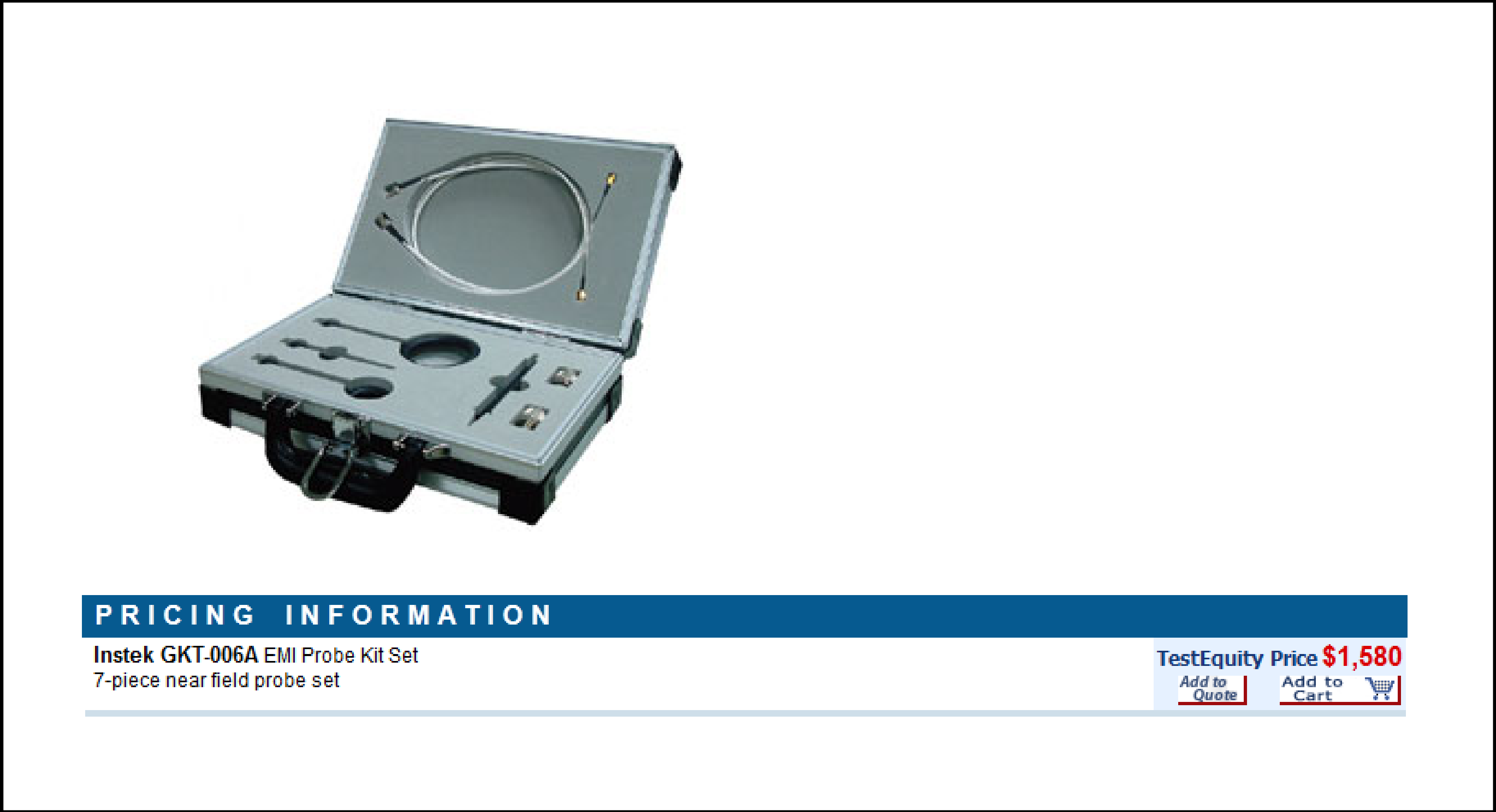
* Custom lengths available on special order

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



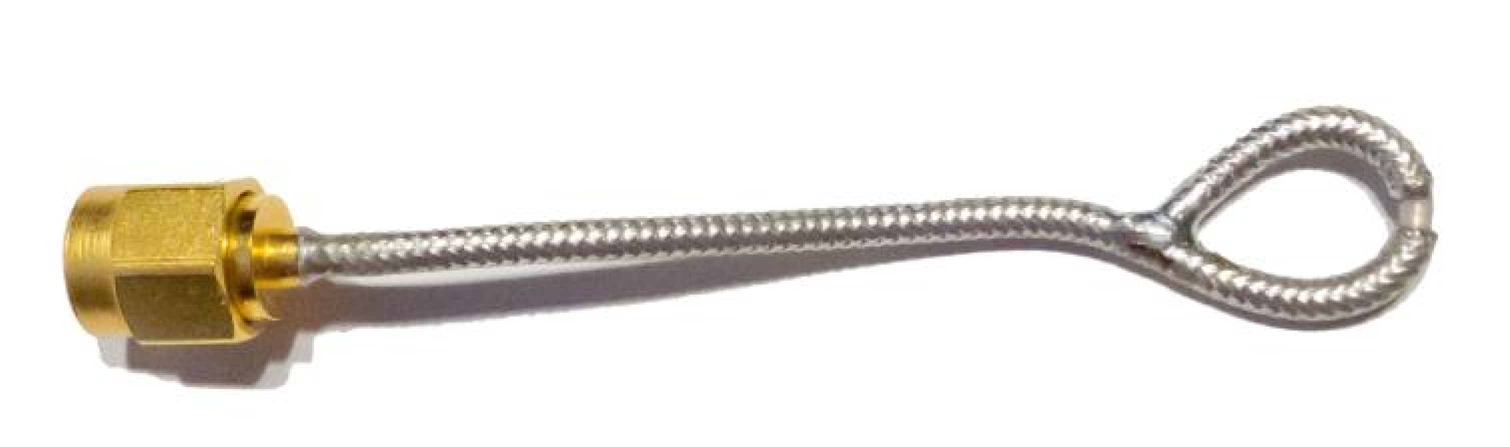
PRICING INFORMATION

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

TestEquity Price $1,580

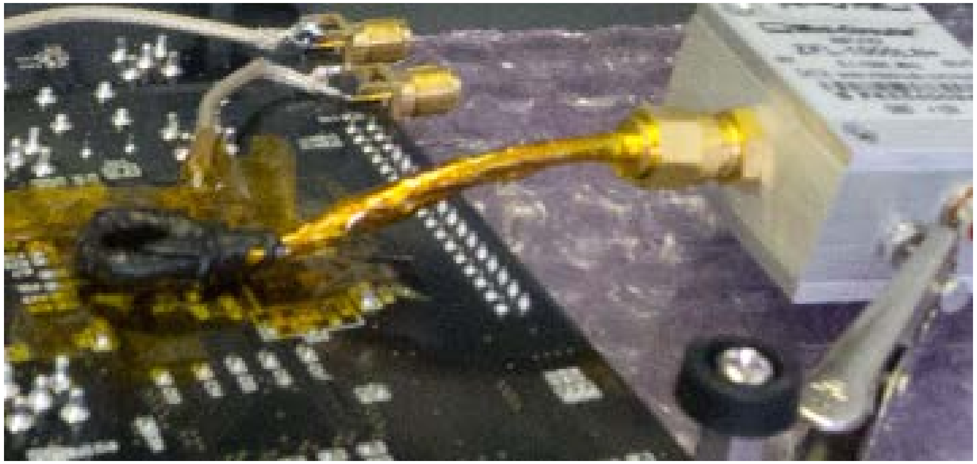
DIY: Example

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

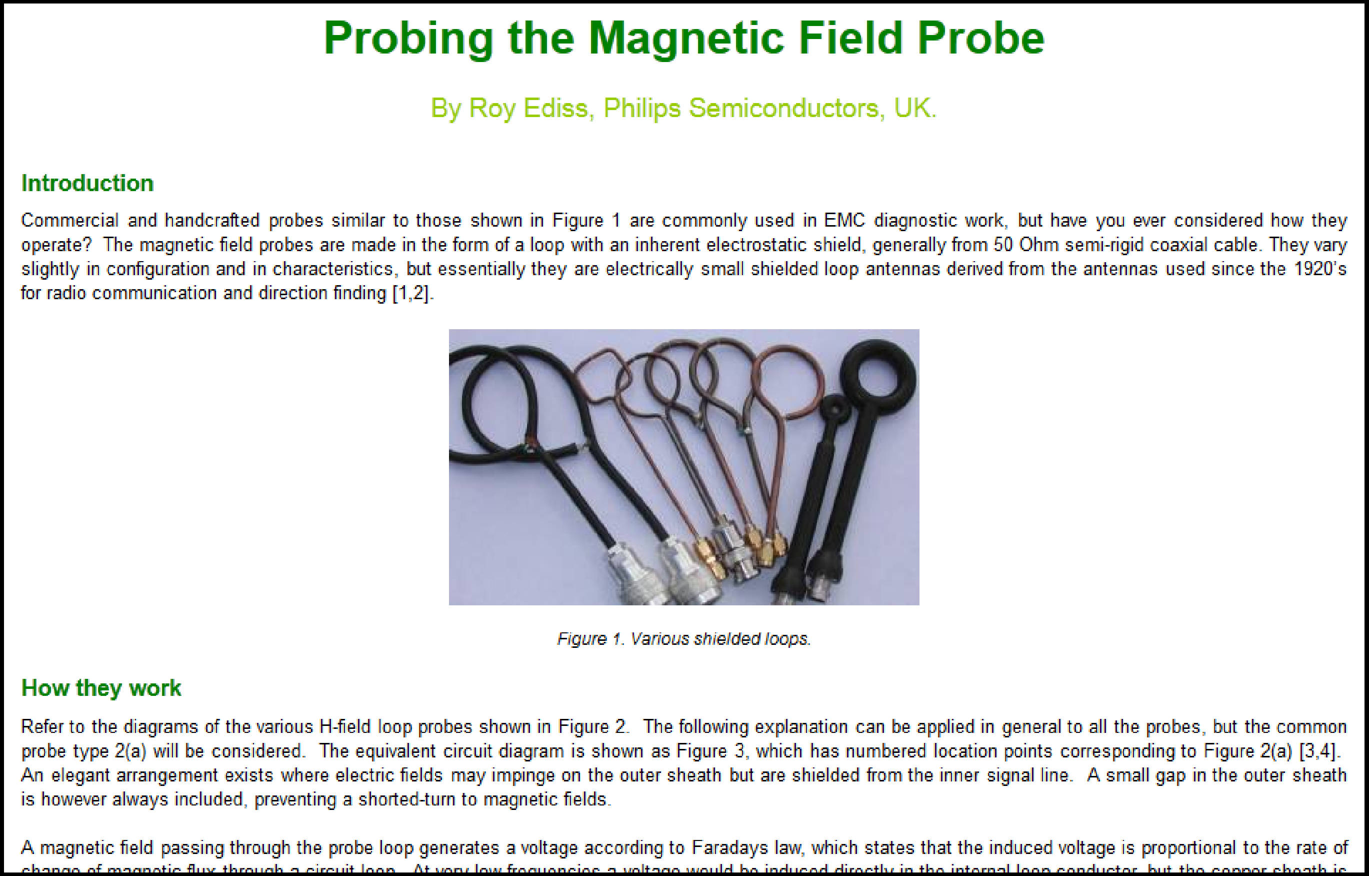


DIY: Example

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.

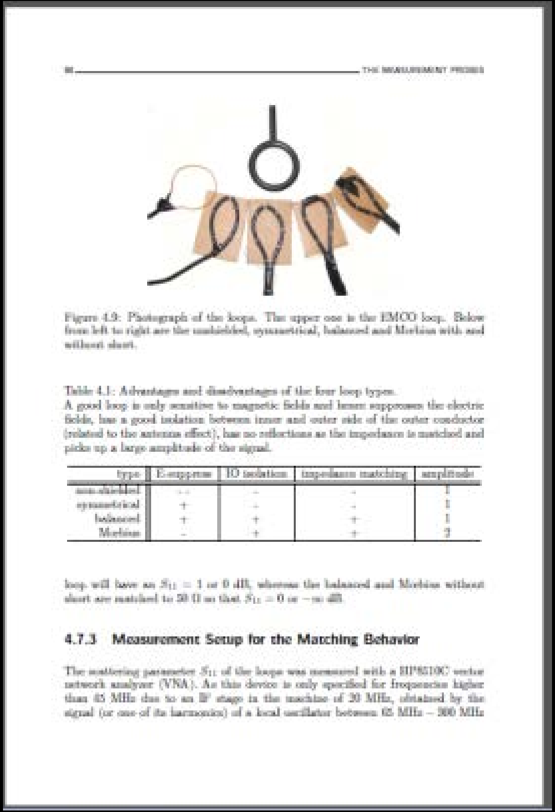
How they work

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.

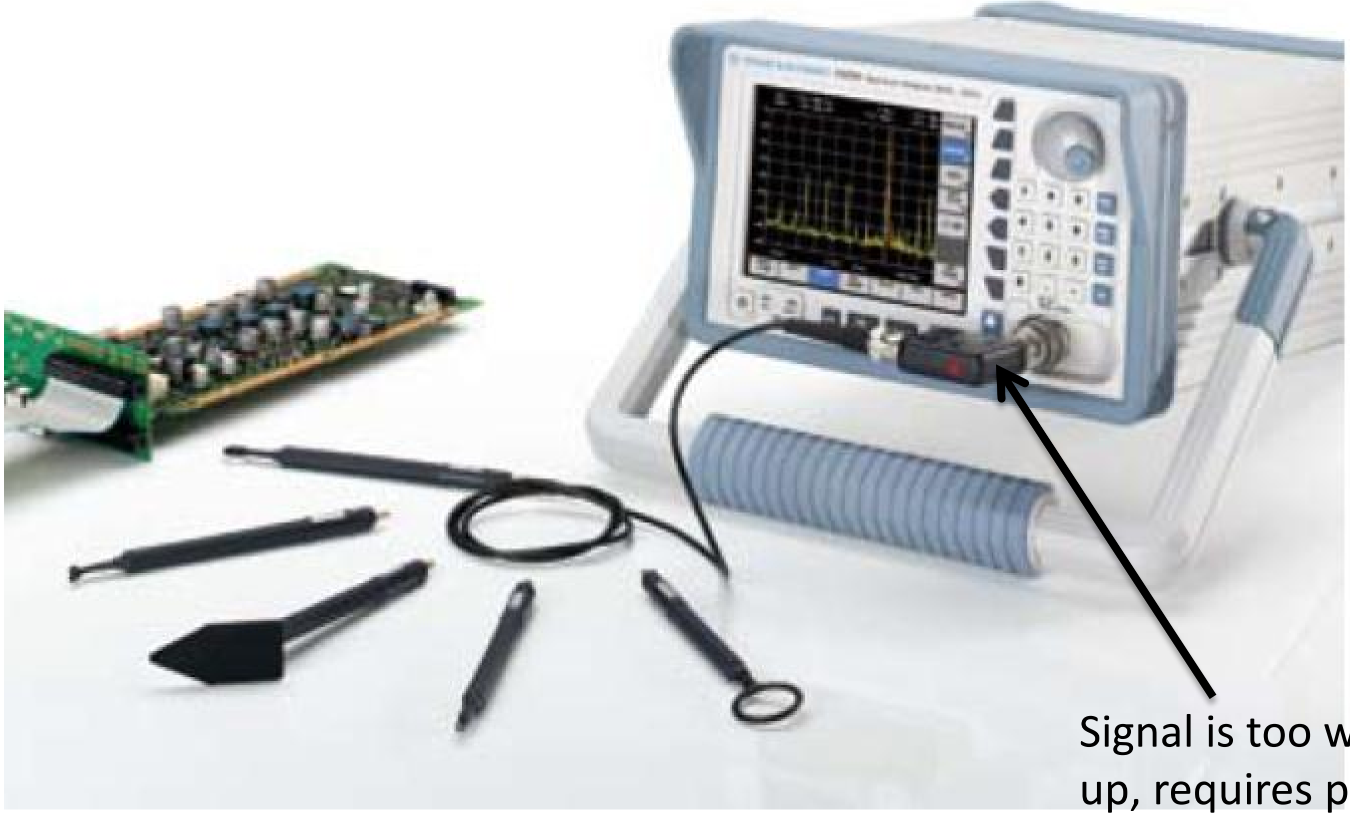
4.7.3 Measurement Setup for the Matching Behavior

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

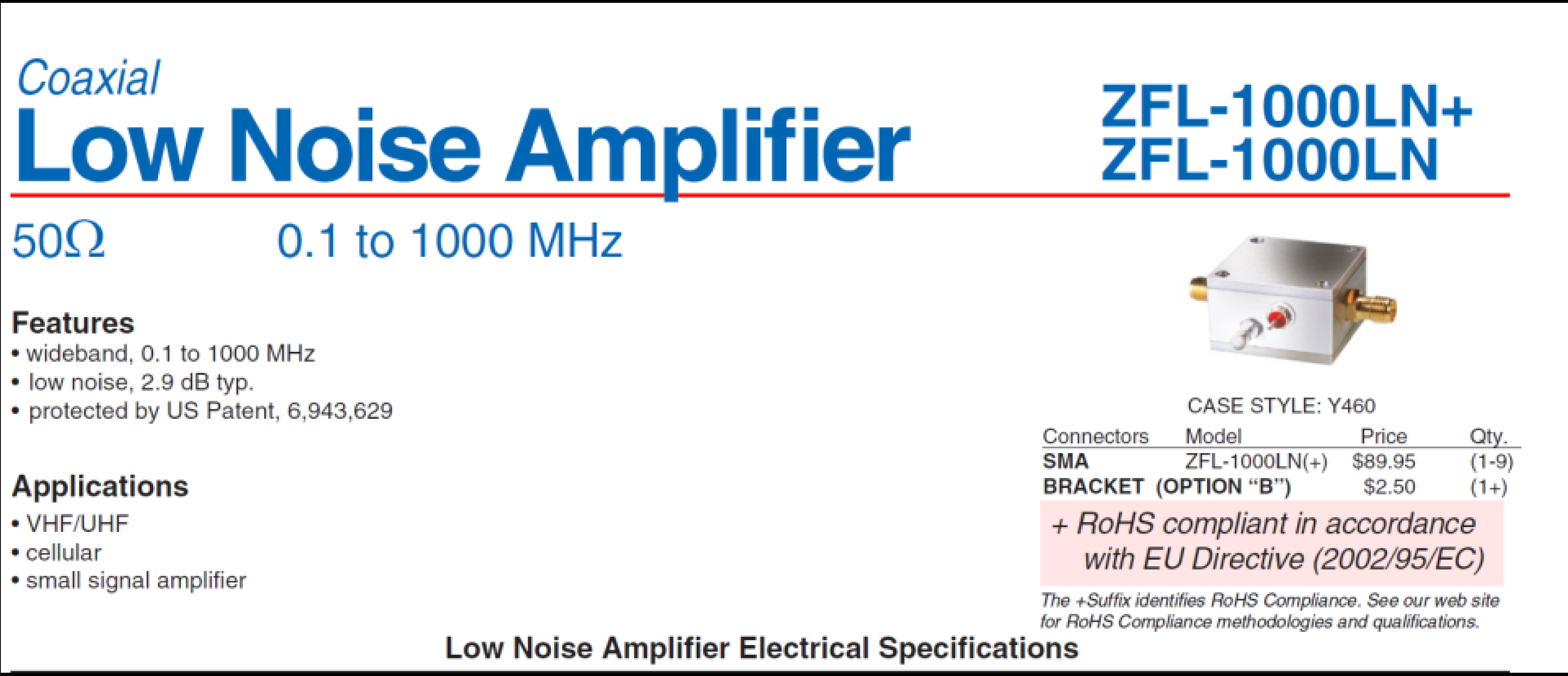
PRE-AMPLIFIER

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+)

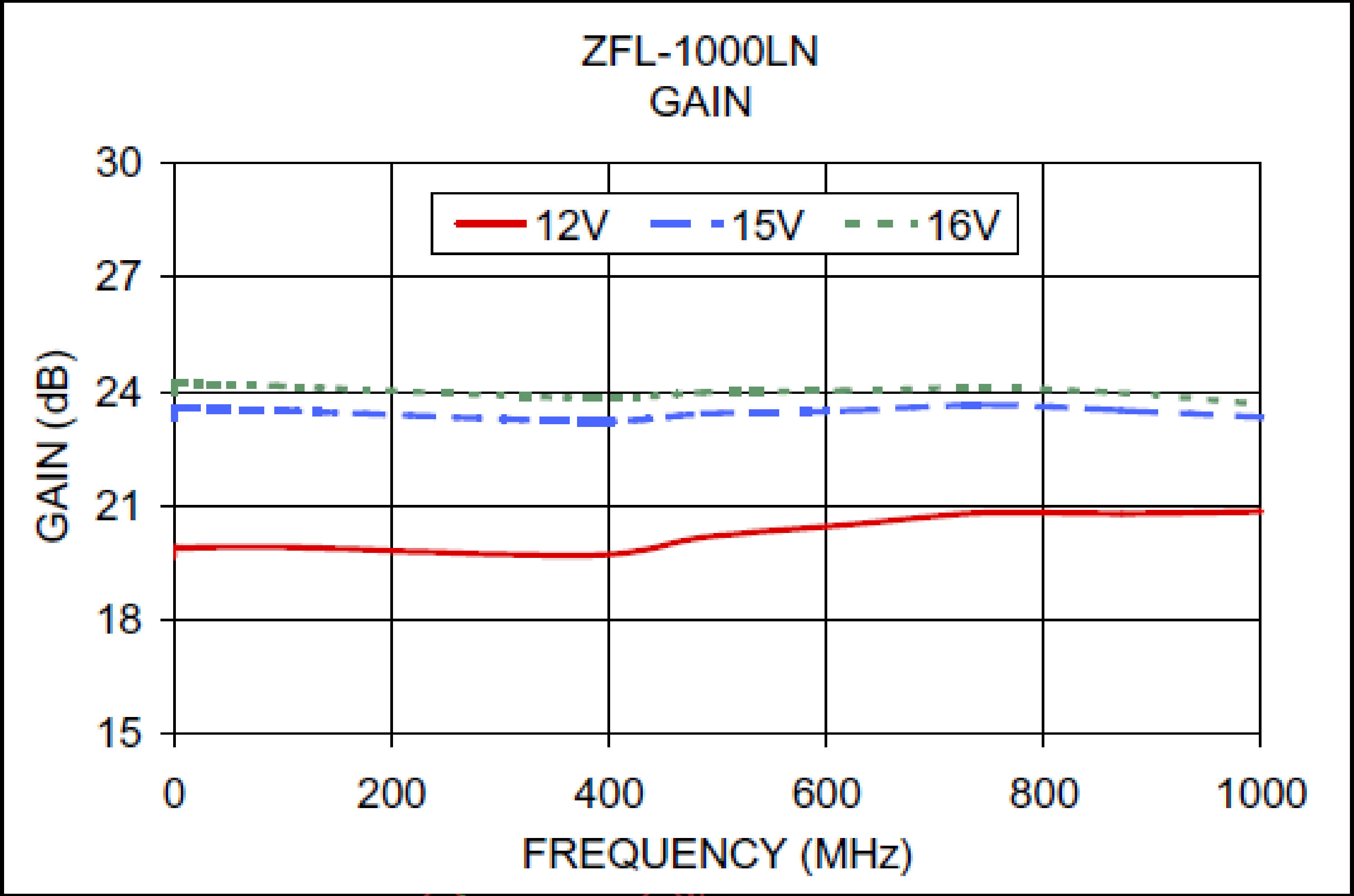
+ RoHS compliant in accordance with EU Directive (2002/95/EC)

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

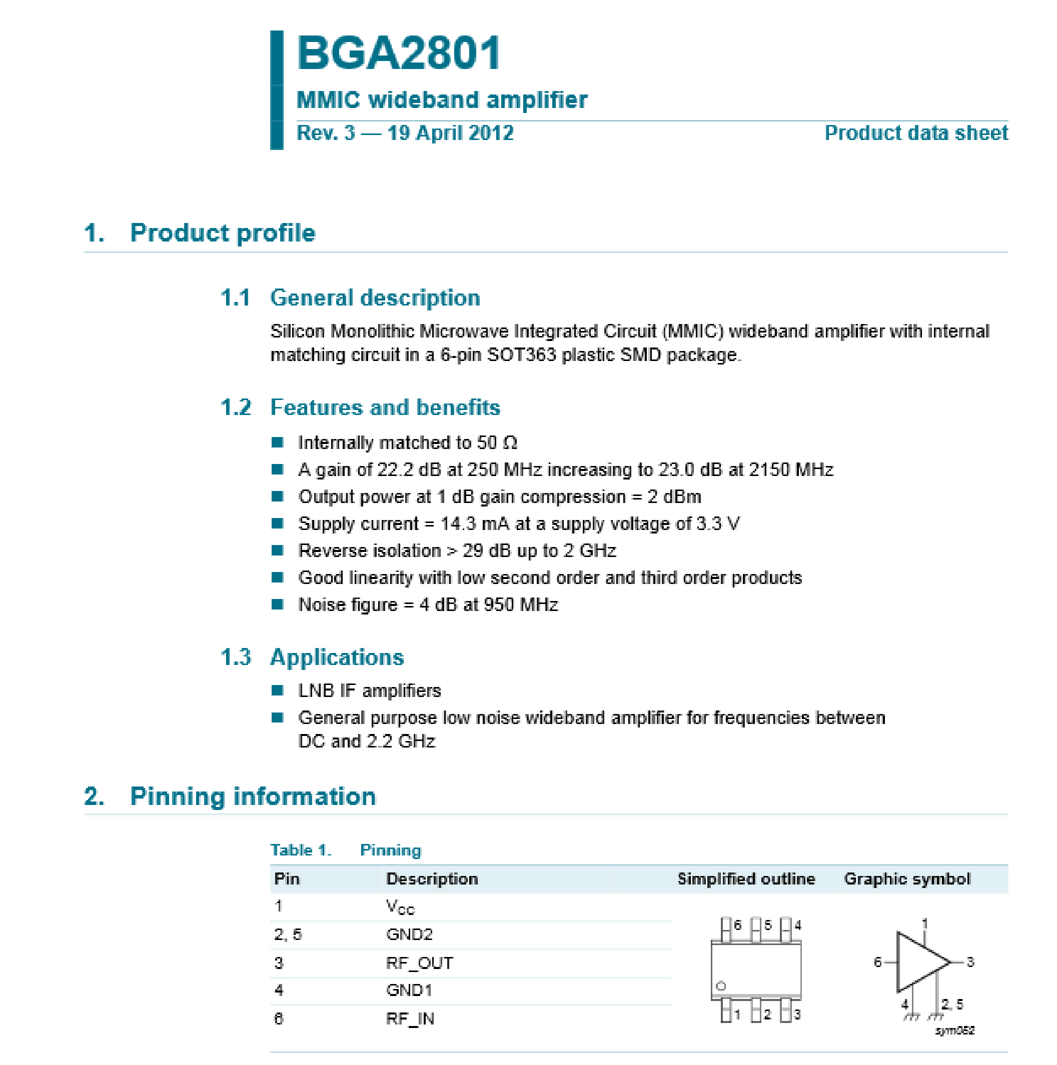
Low Noise Amplifier Electrical Specifications

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



BGA2801

MMIC wideband amplifier

Rev. 3 — 19 April 2012 Product data sheet

1. Product profile

1.1 General description

Silicon Monolithic Microwave Integrated Circuit (MMIC) wideband amplifier with internal matching circuit in a 6-pin SOT363 plastic SMD package.

1.2 Features and benefits

- Internally matched to 50 Ω
- A gain of 22.2 dB at 250 MHz increasing to 23.0 dB at 2150 MHz
- Output power at 1 dB gain compression = 2 dBm
- Supply current = 14.3 mA at a supply voltage of 3.3 V
- Reverse isolation > 29 dB up to 2 GHz
- Good linearity with low second order and third order products
- Noise figure = 4 dB at 950 MHz

1.3 Applications

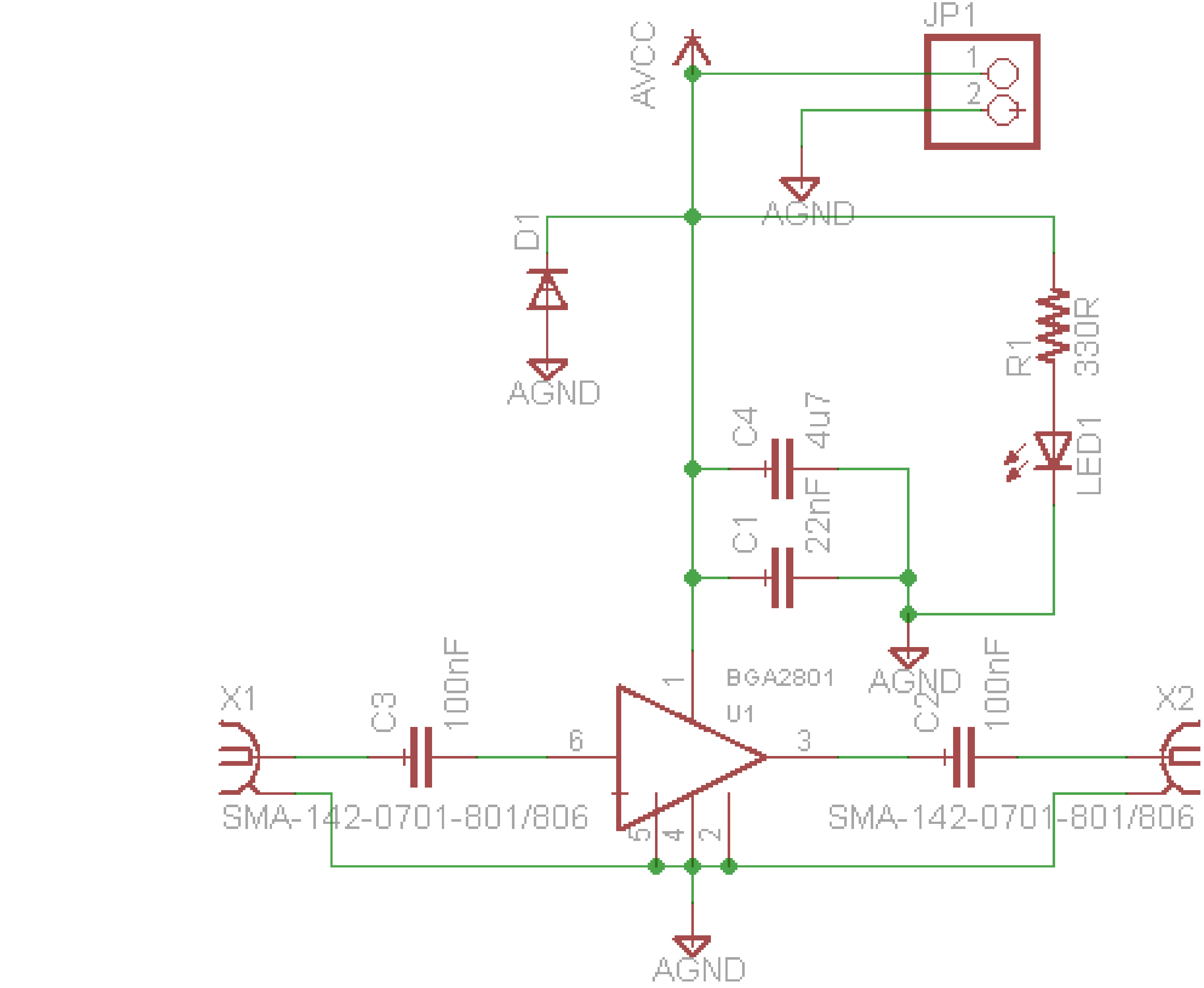
- LNB IF amplifiers
- General purpose low noise wideband amplifier for frequencies between DC and 2.2 GHz

2. Pinning information

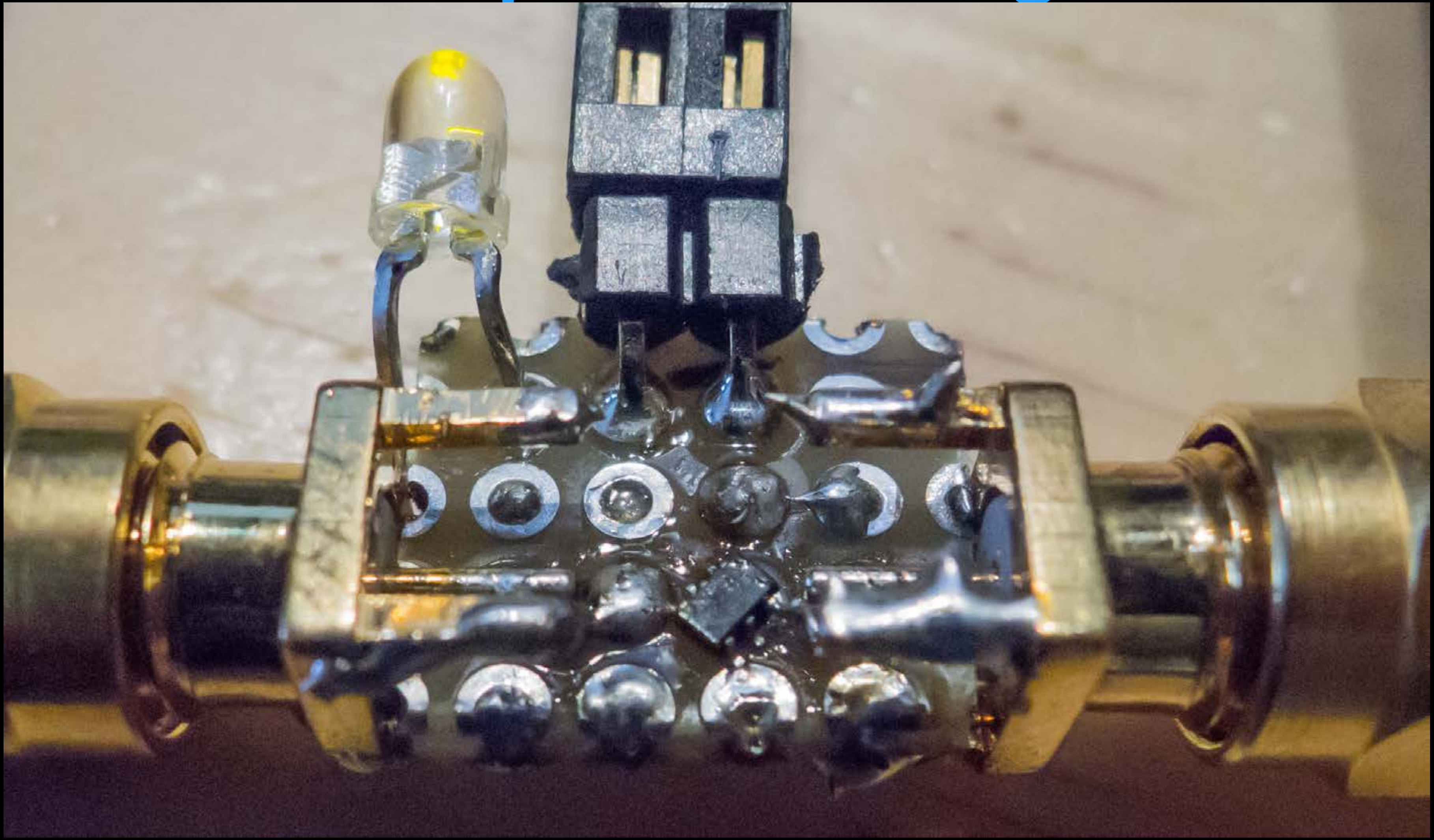
Table 1. Pinning

Pin	Description	Simplified outline	Graphic symbol
1	V_{CC}		
2, 5	GND2		
3	RF_OUT		
4	GND1		
6	RF_IN		

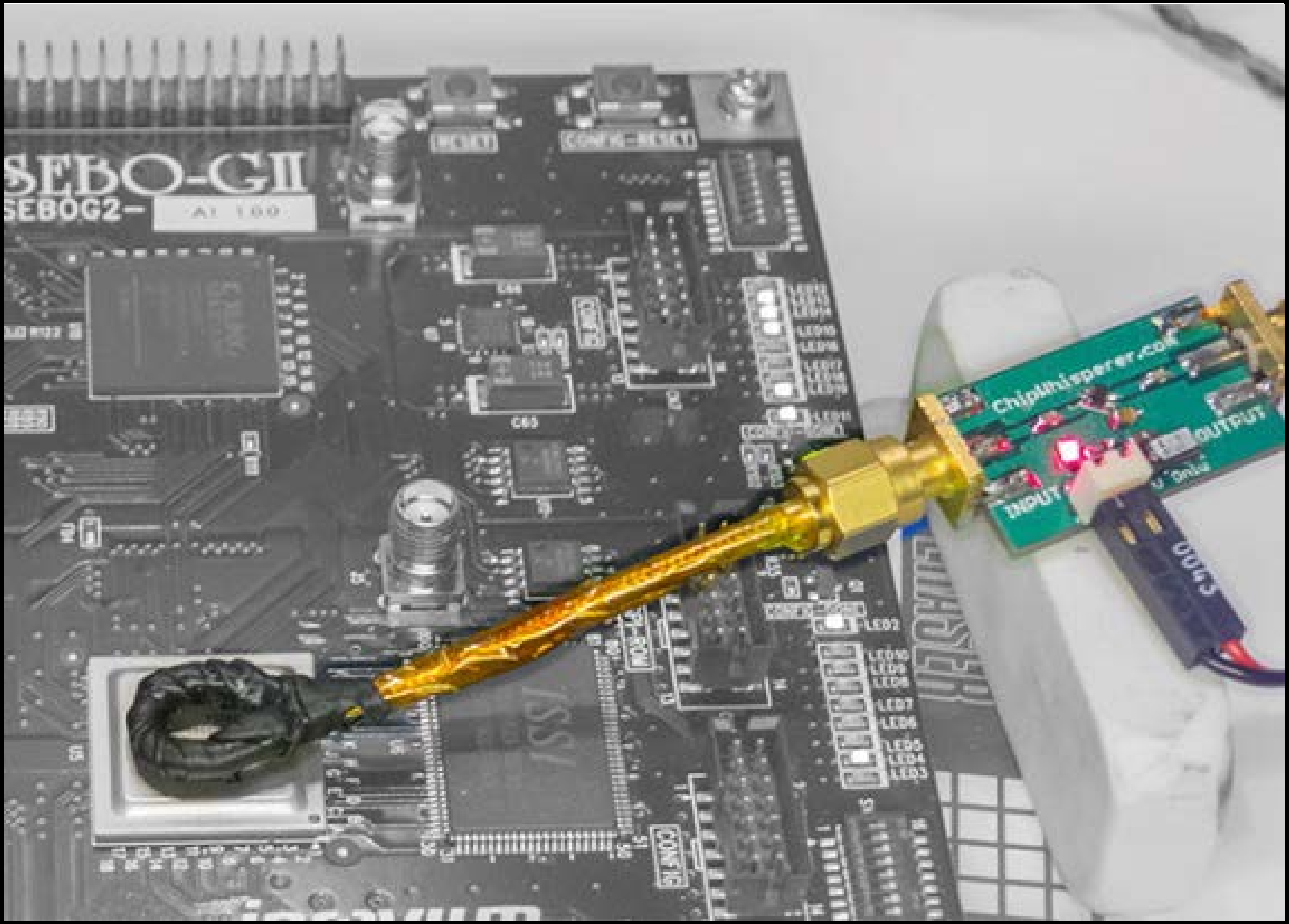
~ $0.60

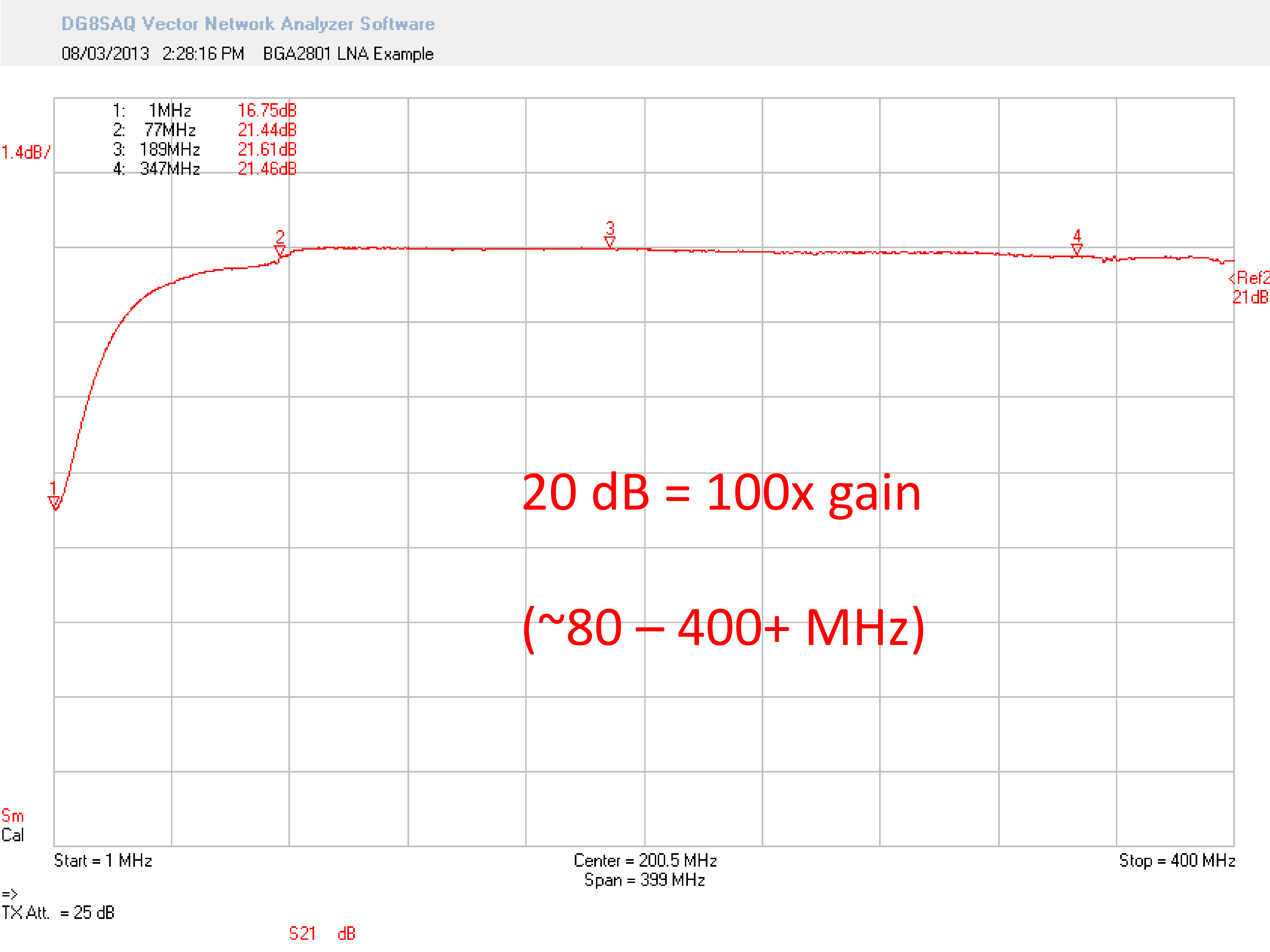

JP1
1
2
AVCC
AGND
D1
AGND
R1
330R
C4
4u7
C1
22nF
LED1
AGND
BGA2801
U1
1
6
3
5
4
2
X1
C3
100nF
SMA-142-0701-801/806
C2
100nF
X2
SMA-142-0701-801/806
AGND

Pre-Amplifier: Making One



Pre-Amplifier: Making One





DG8SAQ Vector Network Analyzer Software

08/03/2013 2:28:16 PM BGA2801 LNA Example

1:	1MHz	16.75dB
2:	77MHz	21.44dB
3:	189MHz	21.61dB
4:	347MHz	21.46dB

Start = 1 MHz

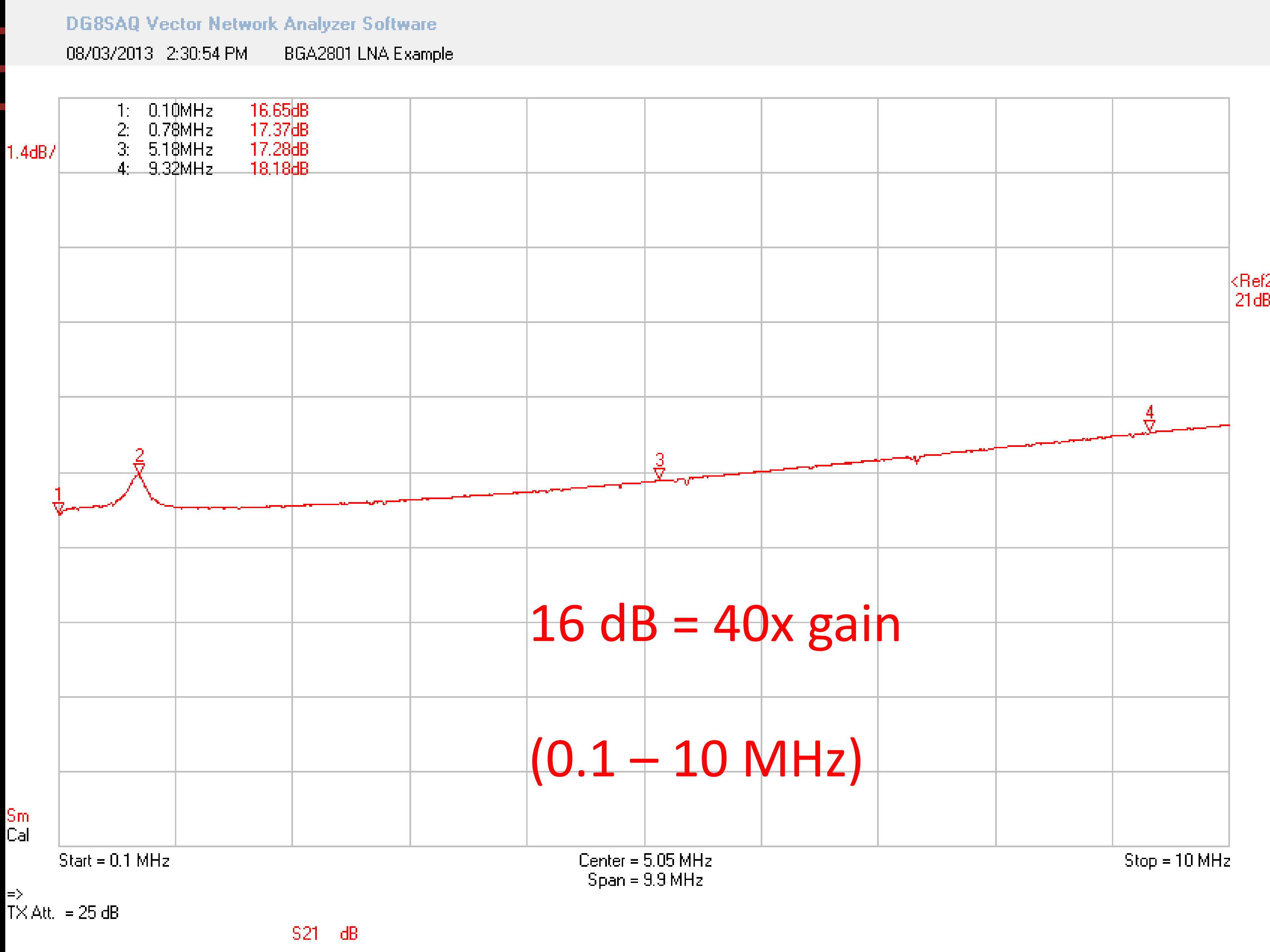
Center = 200.5 MHz
Span = 399 MHz

Stop = 400 MHz

TX Att. = 25 dB

20 dB = 100x gain

(~80 – 400+ MHz)



DG8SAQ Vector Network Analyzer Software

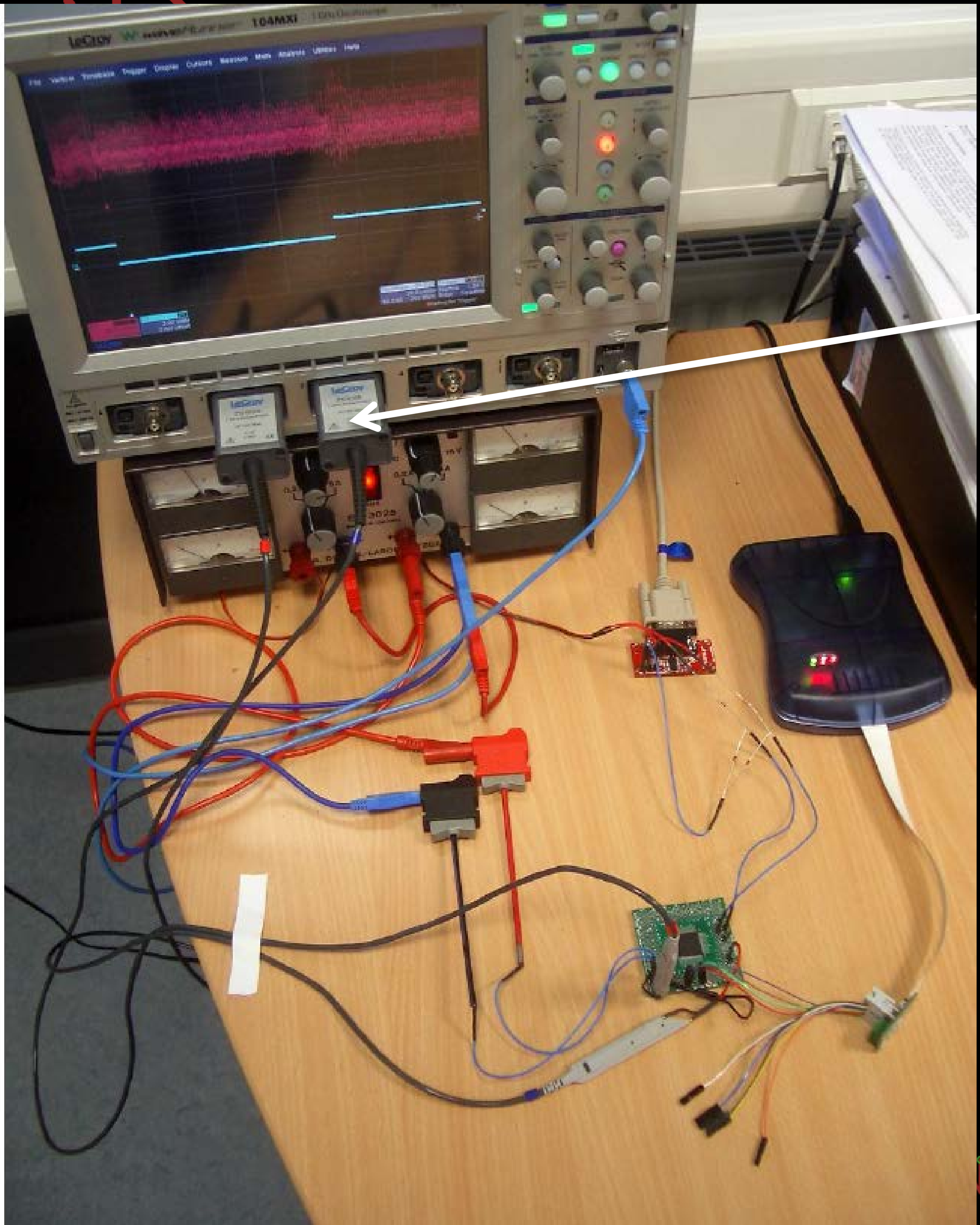
08/03/2013 2:30:54 PM BGA2801 LNA Example

```
1:   0.10MHz   16.65dB
2:   0.78MHz   17.37dB
3:   5.18MHz   17.28dB
4:   9.32MHz   18.18dB
```

16 dB = 40x gain

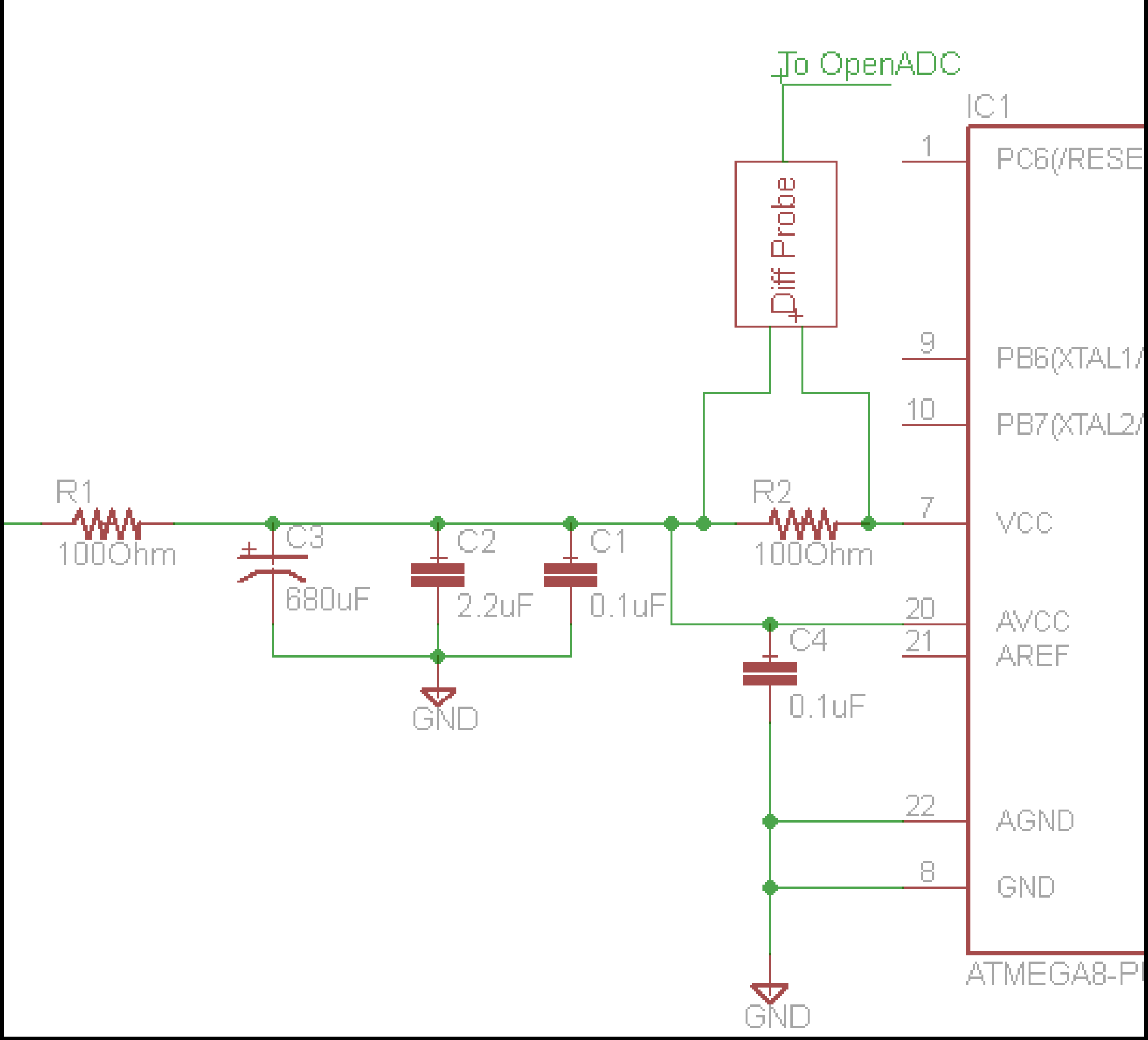
(0.1 – 10 MHz)

DIFFERENTIAL PROBE



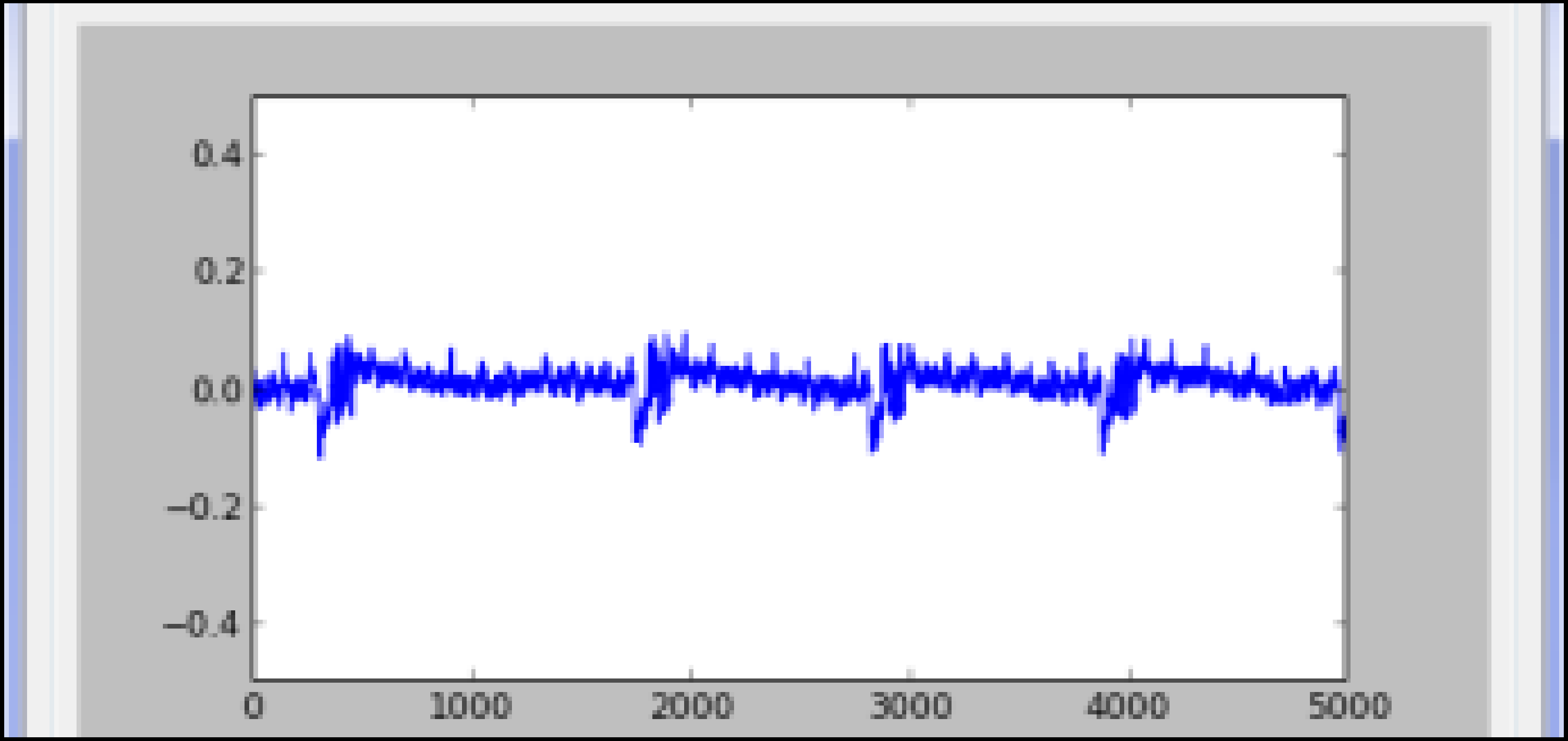
Differential Probe

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



Colin O'Flynn

Common-Mode Noise

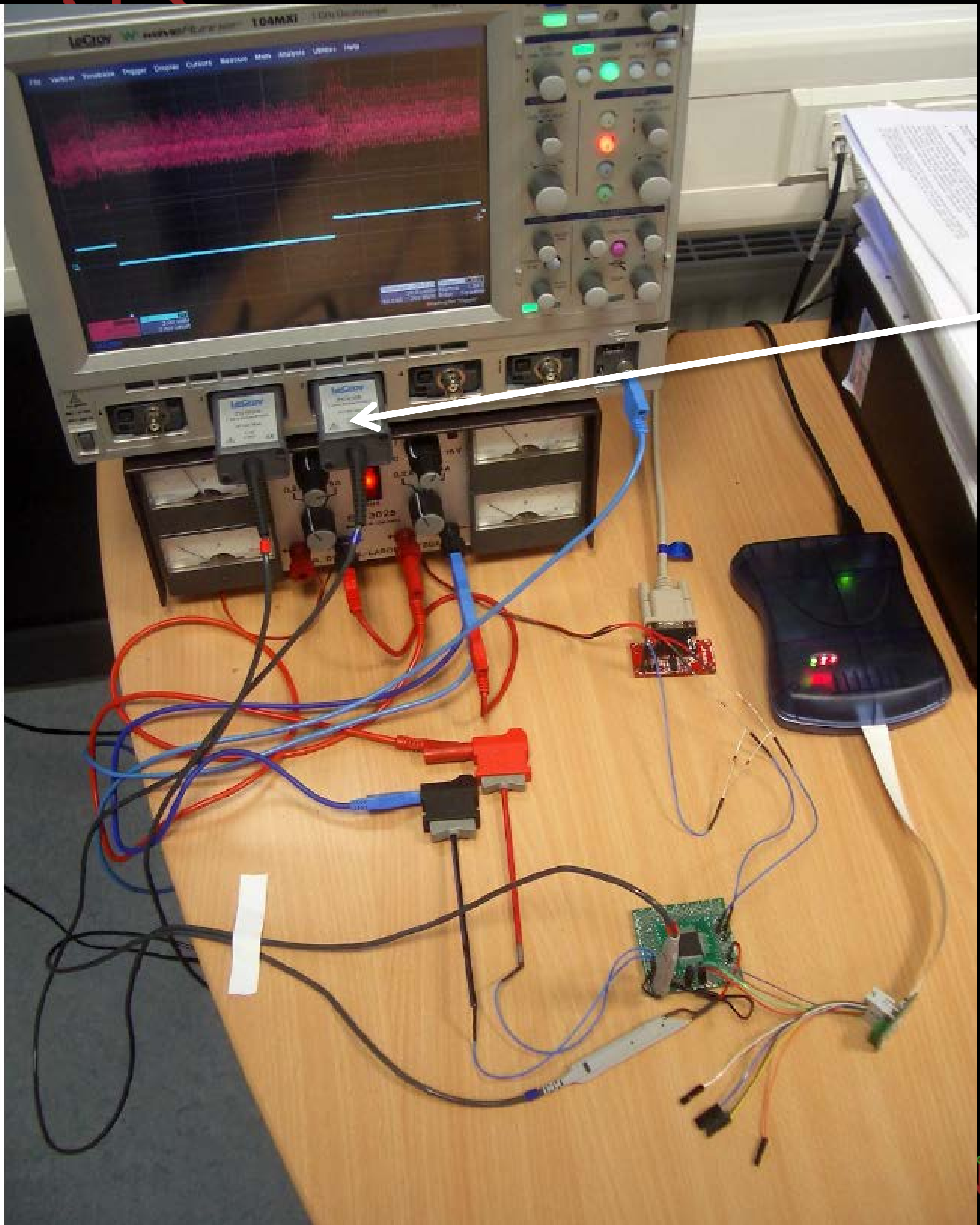


Background

$$V = I R$$

i.e. say signature was 0.2 mA, shunt was 75 ohms

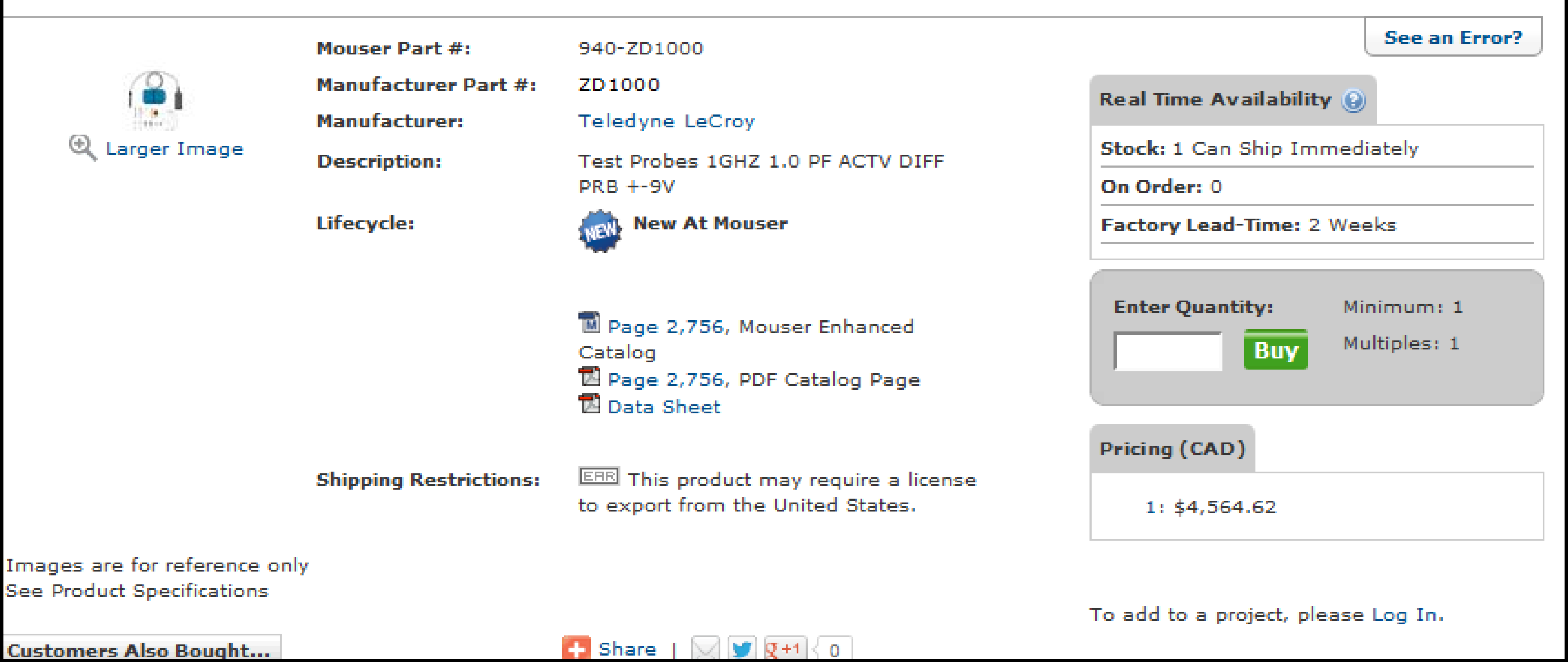
$$0.0002 \times 75 = 0.015 = 15 \text{ mV}$$



Differential Probe

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

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**

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.

Larger Image

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: Minimum: 1

Multiples: 1

Buy

Pricing (CAD)

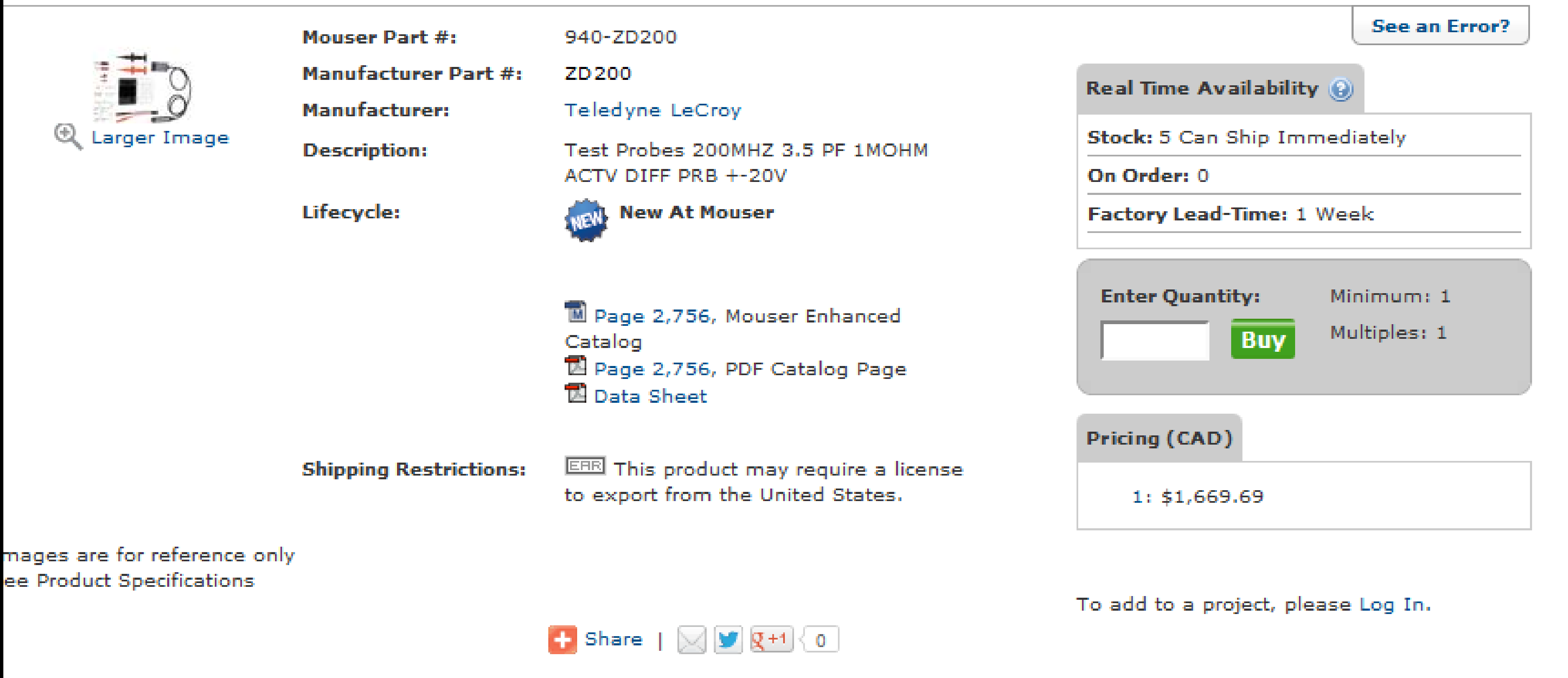
1: $4,564.62

To add to a project, please Log In.

Customers Also Bought...

Share | 0

We don’t need 1000 MHz..



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

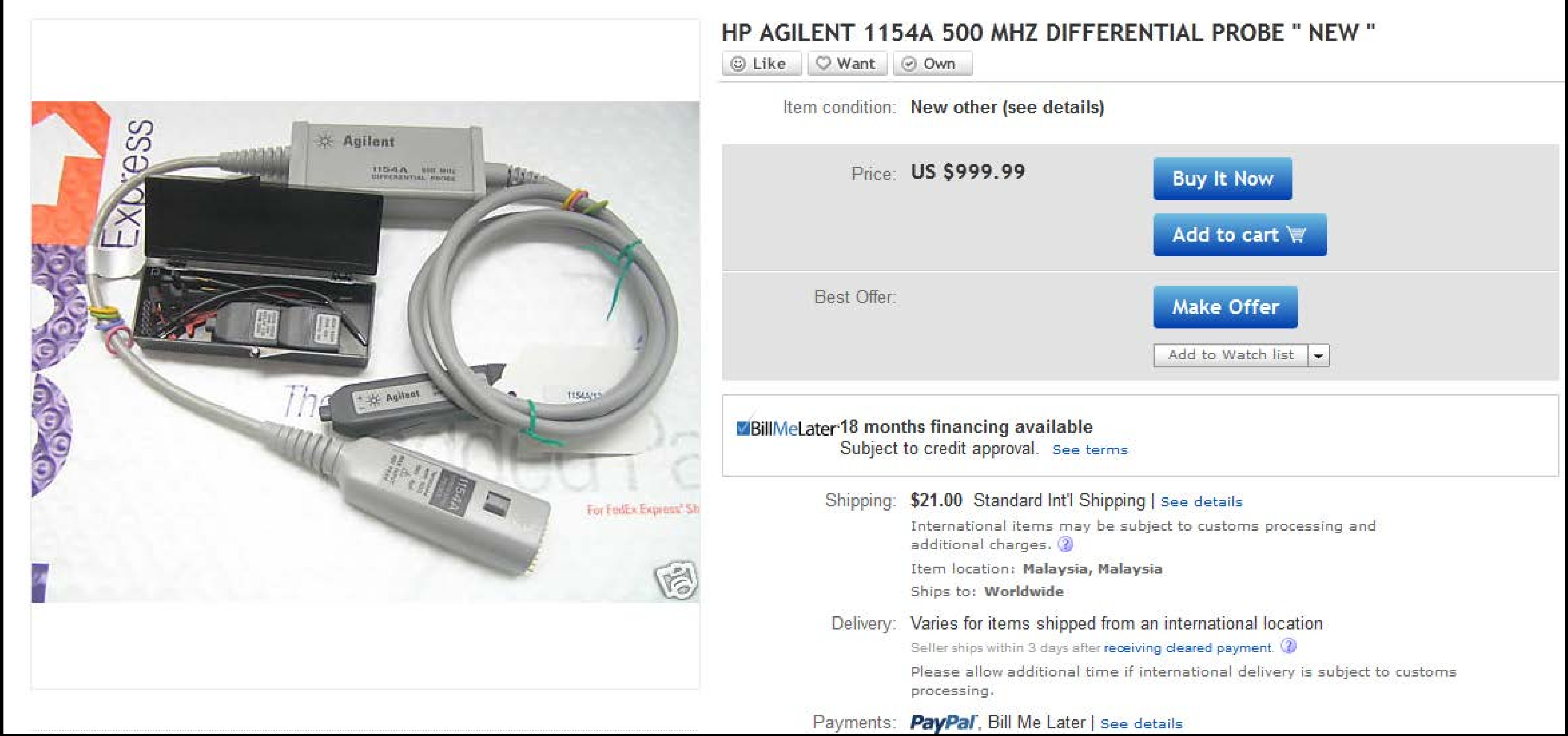
Enter Quantity: Minimum: 1 Multiples: 1

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 "

Like | Want | Own

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

Price: **US $999.99**

Buy It Now

Add to cart

Best Offer:

Make Offer

Add to Watch list

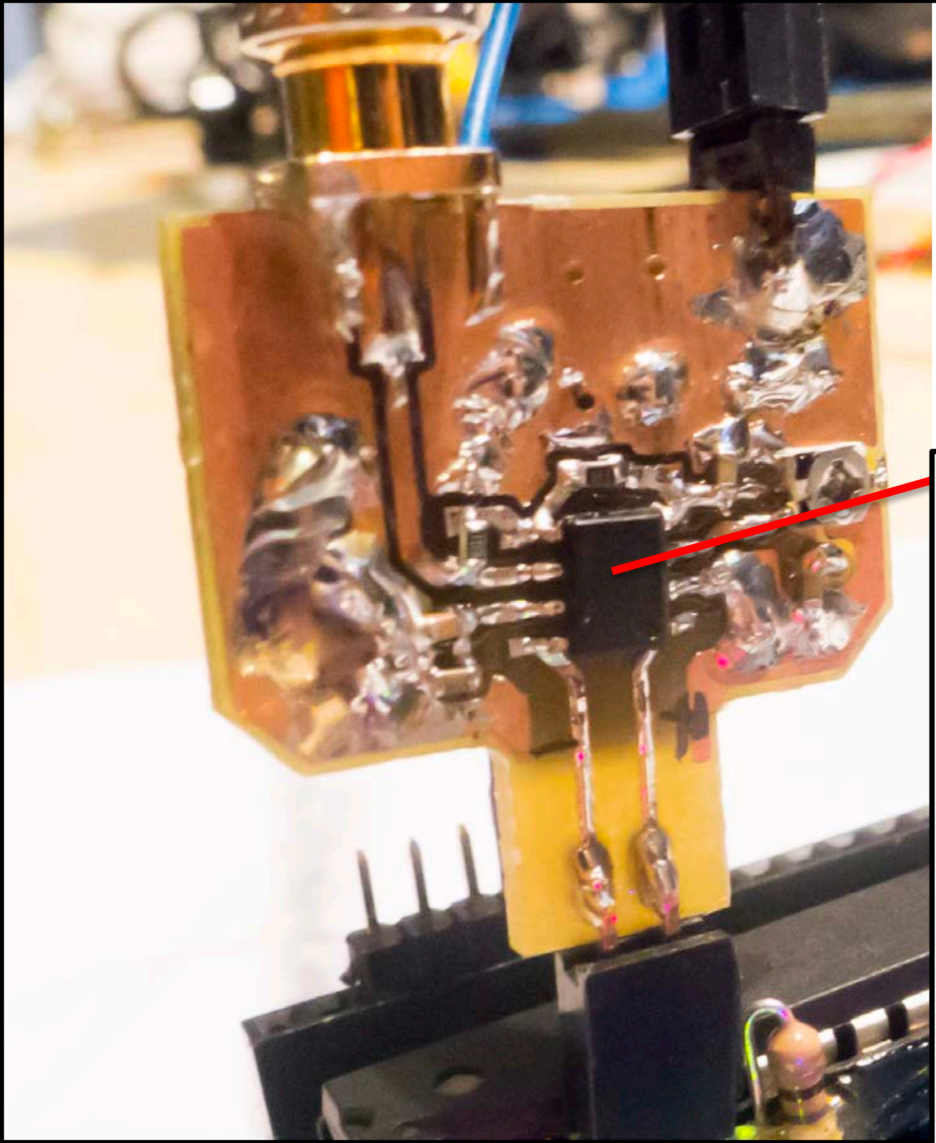
☑ BillMeLater **18 months financing available**
Subject to credit approval. See terms

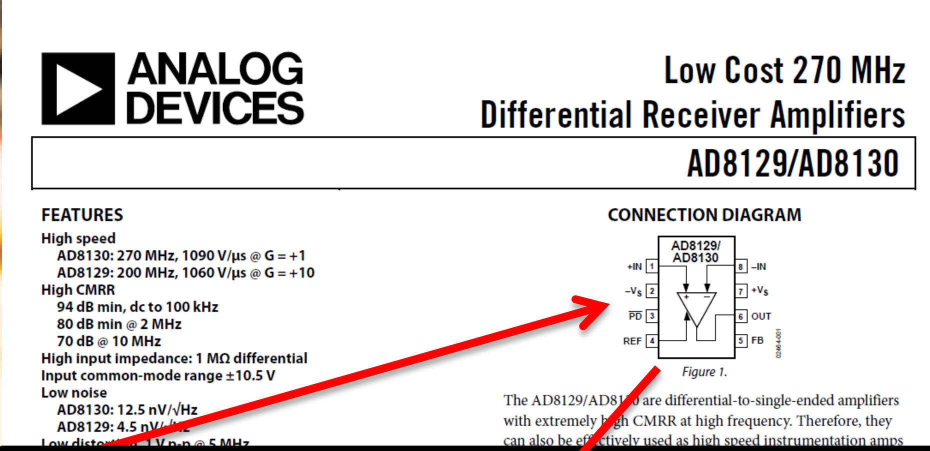
Shipping: **$21.00** Standard Int'l Shipping | See details
International items may be subject to customs processing and additional charges.
Item location: **Malaysia, Malaysia**
Ships to: **Worldwide**

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

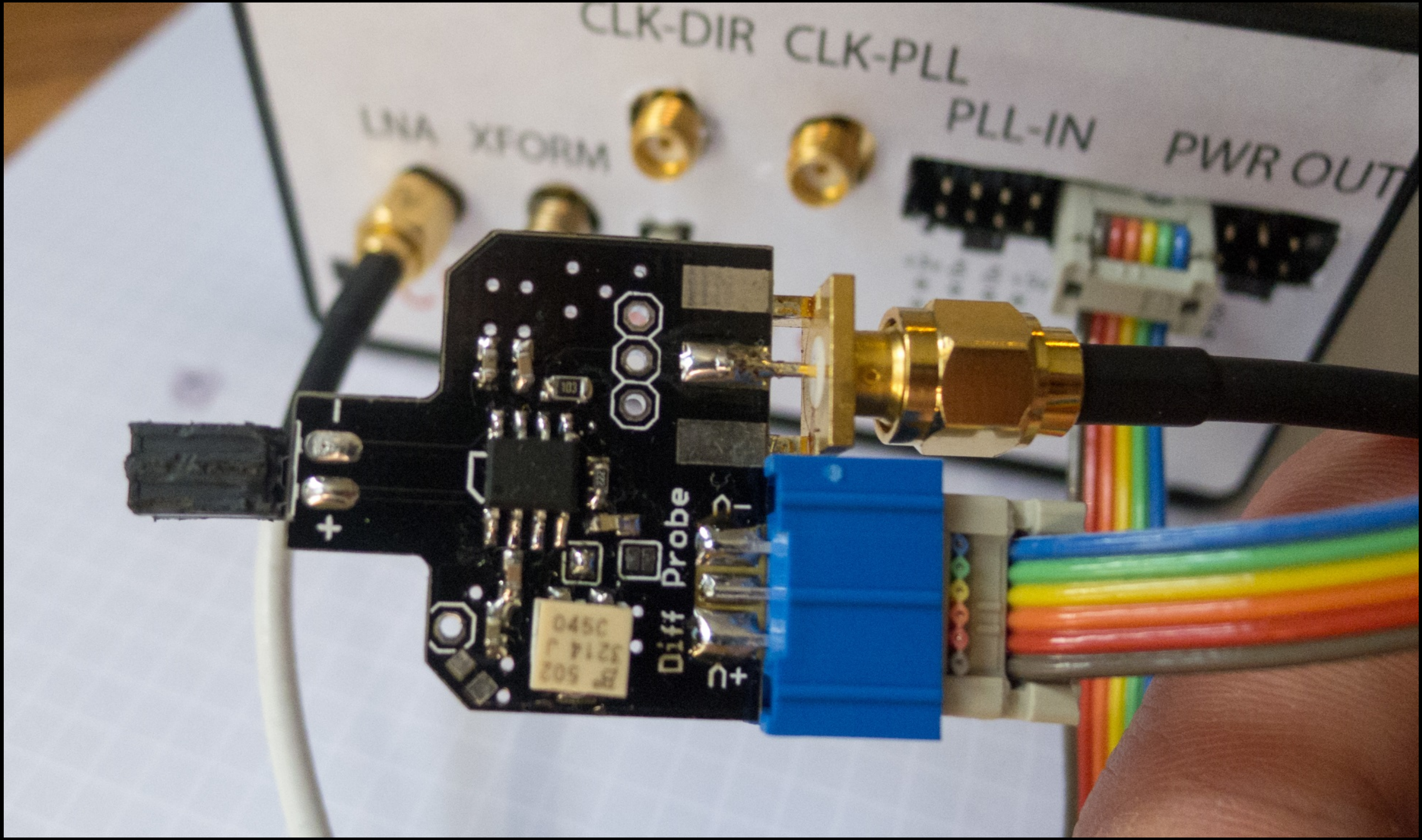
CONNECTION DIAGRAM

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

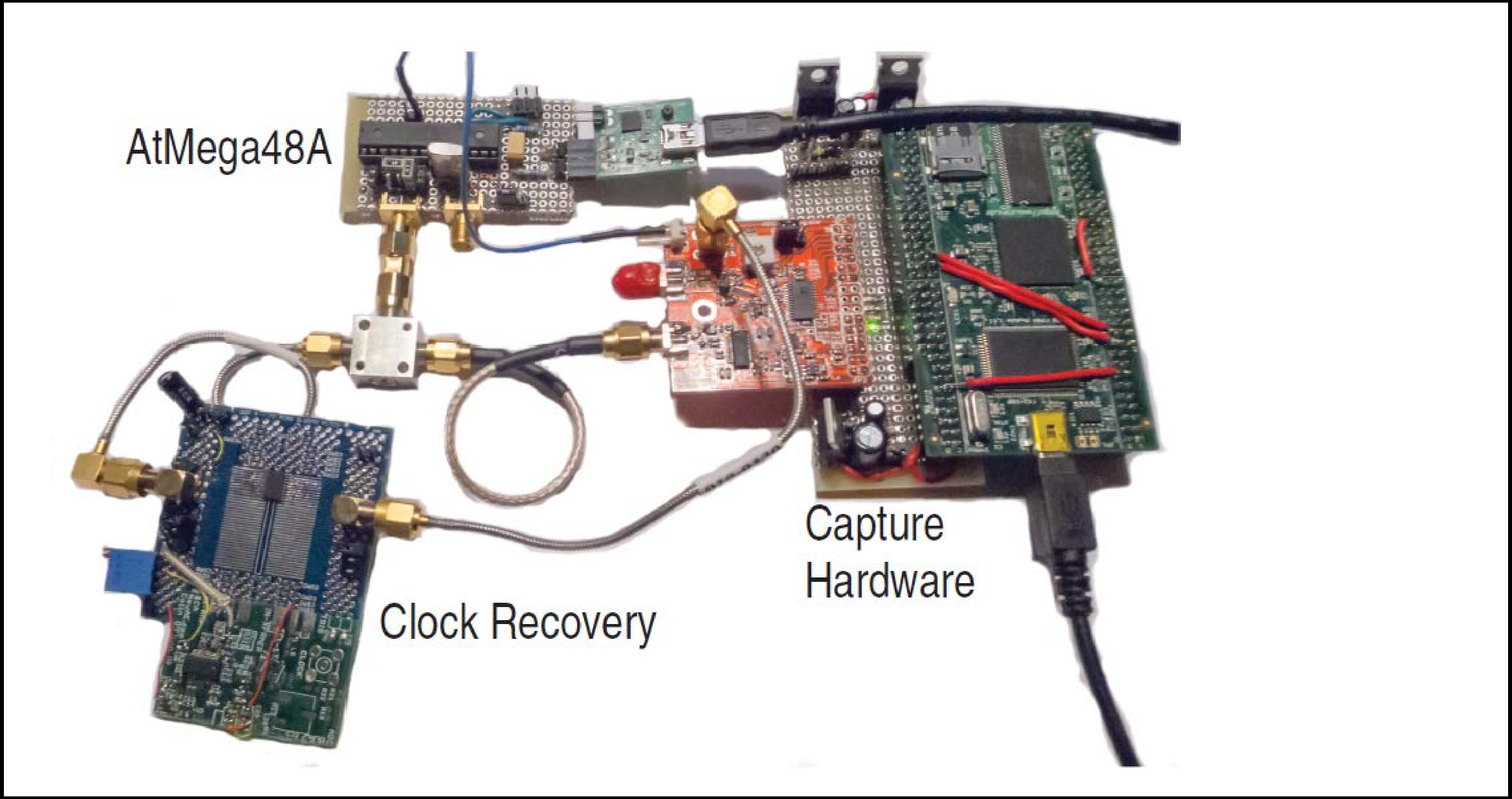
This chip is < $5 in single-unit quantities! Add a voltage supply & a few resistors/capacitors and you've got a pretty good probe.

Full Details on ChipWhisperer Wiki / Whitepaper



YOU SAID REAL SYSTEMS!

Clock Recovery



Running Encryptions

Authentication Commands:

- Commands proving a device has access to a key

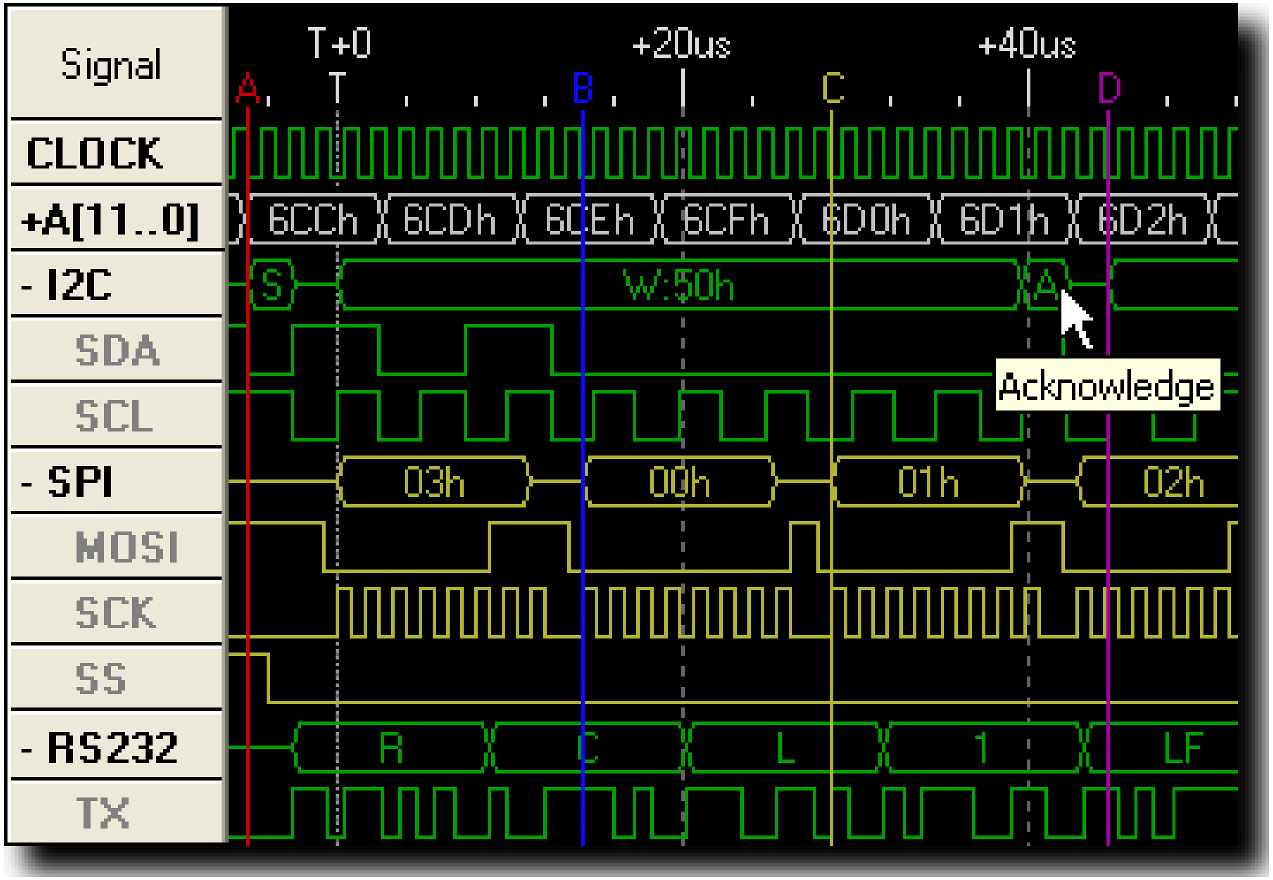
Encryption Communications:

- Send 802.15.4 device encrypted block, it will decrypt it first, and then reject it

Encrypted Bootloader:

- Send device firmware file

Synchronization



Colin O'Flynn

AND FINALLY…

What does this Mean to YOU

If you are a MANAGER:

What does this Mean to YOU

If you are an ENGINEER:

- Good standard practice helps many issues (change keys, don’t use same key everywhere, etc.)
- If someone doesn’t want to use good practice because it’s “too expensive” or “too difficult logistically”, use side-channel analysis as one example of how keys can be leaked
- Can protect against SCA but beyond this presentation

What does this Mean to YOU

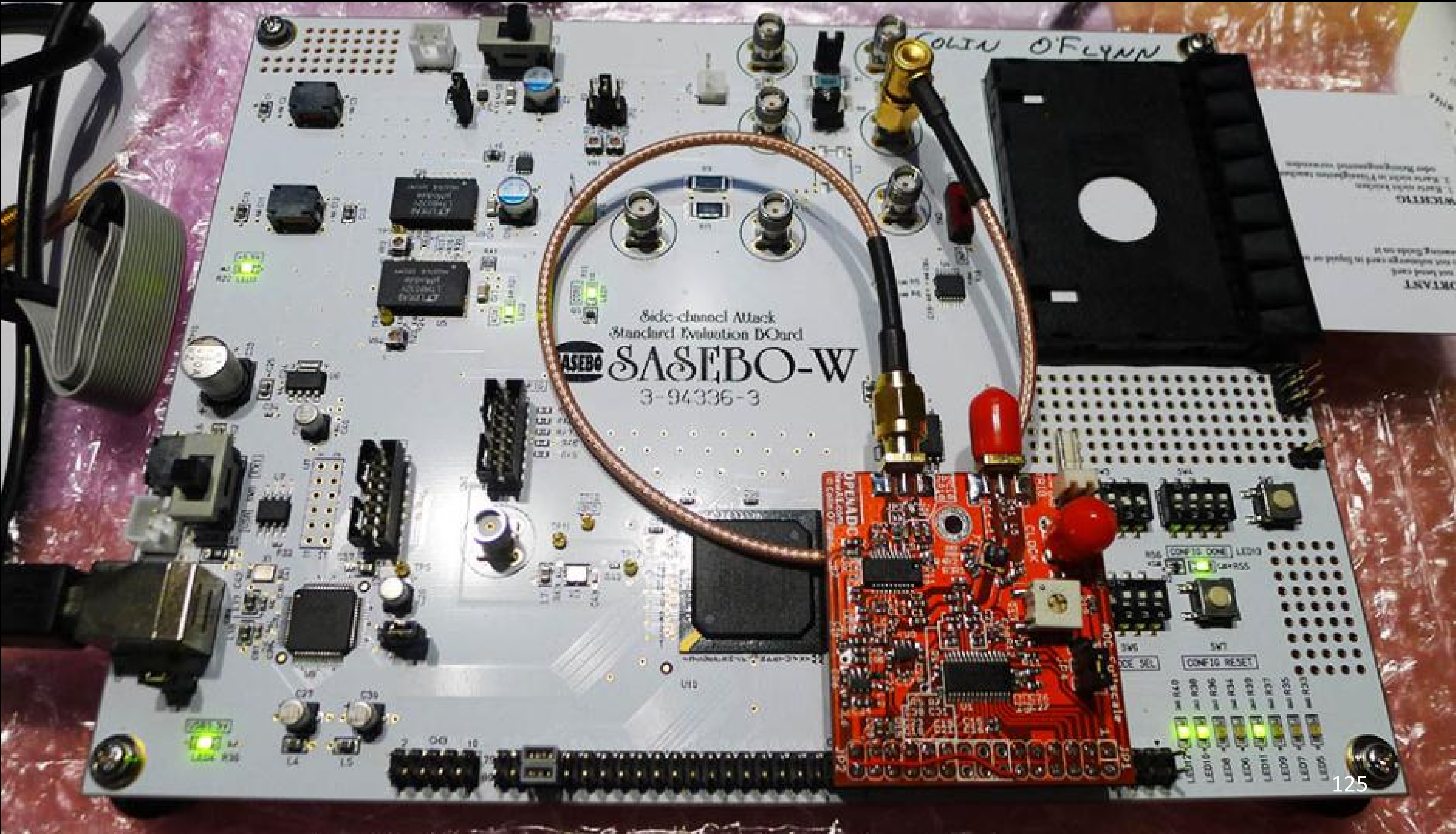
If you are an ad-hoc RESEARCHER:

- Basic principles are straight-forward
- Hardware doesn’t need to be expensive, SCA is something you can do in your spare time
- This tool/presentation is about learning, you will need to do work yourself to duplicate even basic results

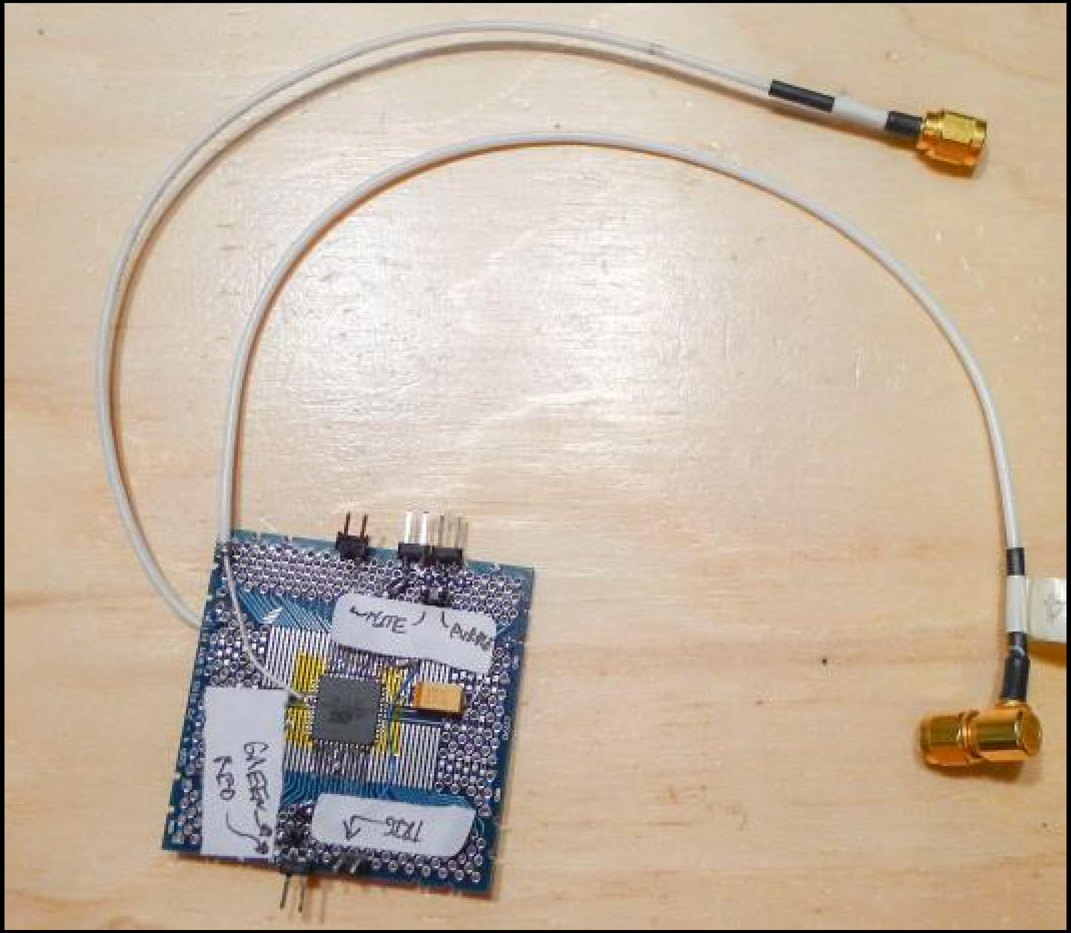
Some More Targets

SASEBO-W Board

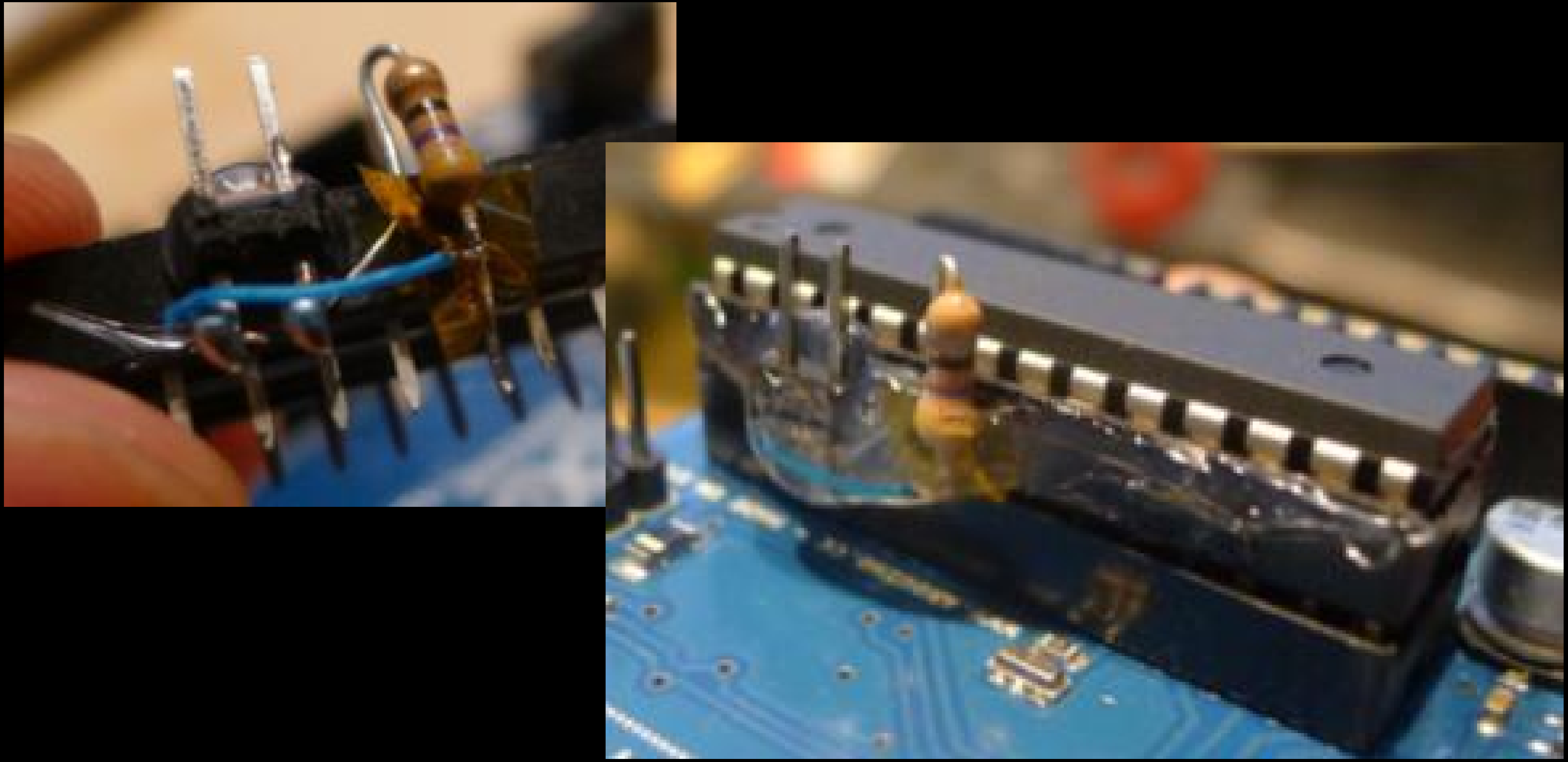
http://www.morita-tech.co.jp/SAKURA/en/hardware.html



Xmega Board

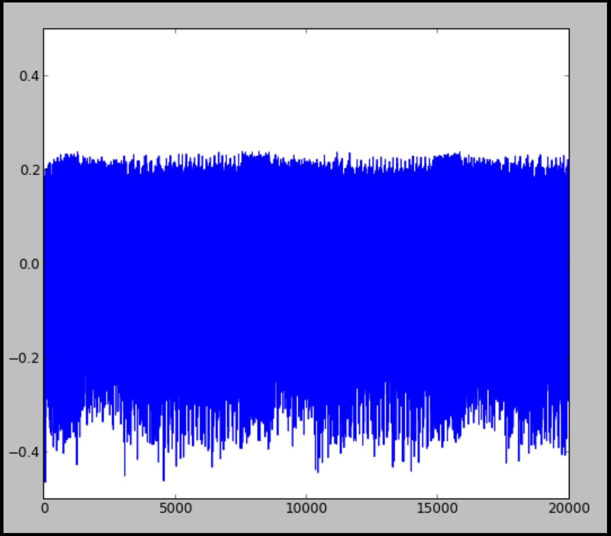


Arduino

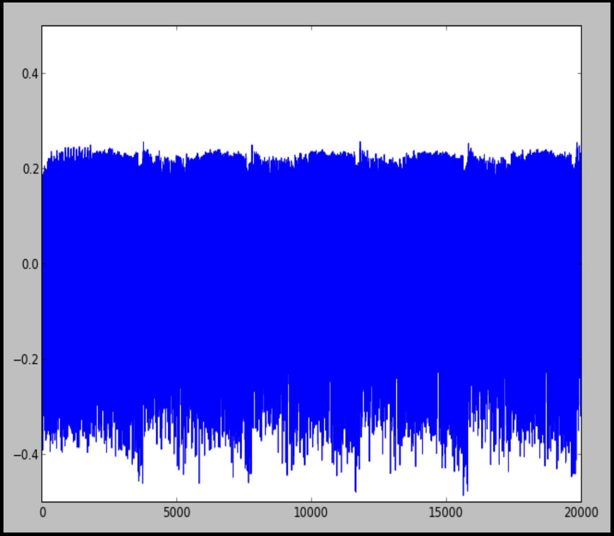


AVR: Different AES Libraries

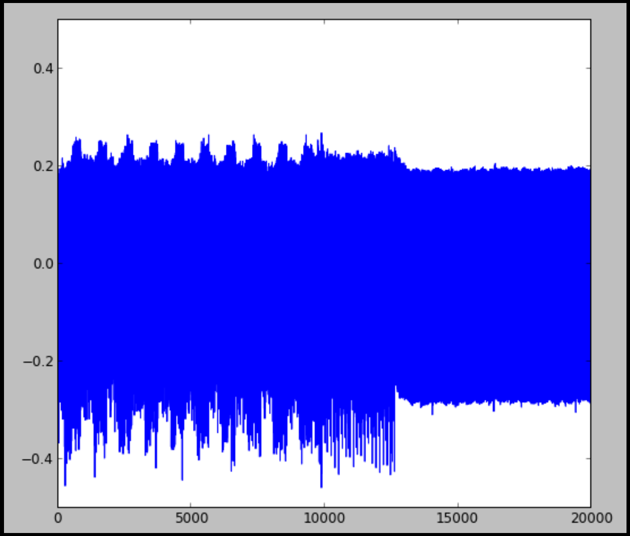
avr-crypto-lib in C



Straightforward C



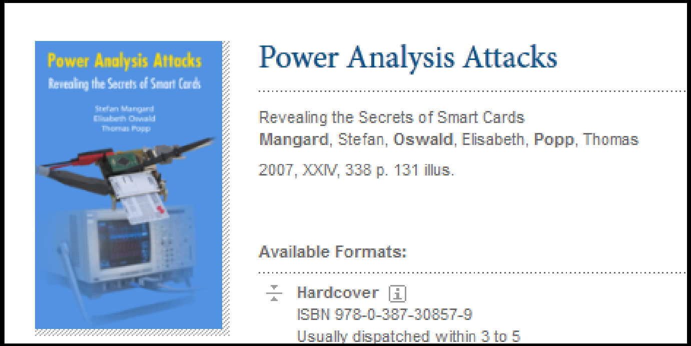
avr-crypto-lib in ASM



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
- Join ChipWhisperer Mailing List & discuss
- Two Good Books to get you Going:



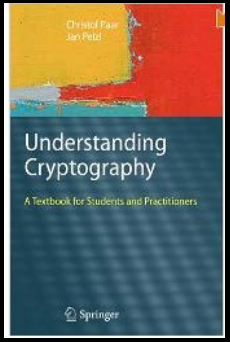
Power Analysis Attacks

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


Christof Paar
Jan Pelzl
Understanding Cryptography
A Textbook for Students and Practitioners
Springer

- 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)

Questions Etc.

Visit me on internet:	newae.com/blackhat chipwhisperer.com
E-mail me:	coflynn@newae.com
Mailing List:	chipwhisperer.com
Twitter:	colinoflynn

Please fill out Speaker Surveys!