AKA: REAL Hardware Hacking

Colin O’Flynn
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 meantime here is a simple tutorial about making a Finite Impulse Response Filter on a real ADC/DAC board.
60-Second Version

CryptoPro 9000
60-Second Version

Clock

Data[0]

Data[1]

Power
60-Second Version
• **Not** for 1337 H4X0r

• 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?

Main Channel

Secret
Side Channel?

Power

Main Channel

Secret
Power Channel.

CryptoPro 9000
Power Channel.
Data Bus Line
Data Bus Line

![Data Bus Line Diagram](image-url)
Power Channel.

Clock

Data[0]

Data[1]

Power
1. Hamming Distance

2. Hamming Weight
Side Channel.
Looking at AES-128
More Detail of AES

1-Byte of Input (Plaintext)

1-Byte of Key (Subkey)

Bitwise XOR

Substitution-Box (Lookup Table)
Simple 4-Bit Example
Simple 4-Bit Example

Plain Text → Key → Unavailable Output
## Correlation Analysis

<table>
<thead>
<tr>
<th>Input Plaintext</th>
<th>Hyp. Key</th>
<th>Hyp Result</th>
<th>Hyp HW</th>
</tr>
</thead>
<tbody>
<tr>
<td>0100 (4)</td>
<td>0010 (2)</td>
<td>0110 (6)</td>
<td>2</td>
</tr>
<tr>
<td>0111 (7)</td>
<td>0010 (2)</td>
<td>0101 (5)</td>
<td>2</td>
</tr>
<tr>
<td>0010 (2)</td>
<td>0010 (2)</td>
<td>0000 (0)</td>
<td>0</td>
</tr>
<tr>
<td>0001 (1)</td>
<td>0010 (2)</td>
<td>0011 (3)</td>
<td>2</td>
</tr>
<tr>
<td>0000 (0)</td>
<td>0010 (2)</td>
<td>0010 (2)</td>
<td>1</td>
</tr>
<tr>
<td>0110 (6)</td>
<td>0010 (2)</td>
<td>0100 (4)</td>
<td>1</td>
</tr>
<tr>
<td>0101 (5)</td>
<td>0010 (2)</td>
<td>0111 (7)</td>
<td>3</td>
</tr>
</tbody>
</table>
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:

$$z_i(T) = \int_0^T r(t) s_i(t) \, dt \quad i = 1, \ldots, M$$  \hspace{1cm} (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

Choose the $s_i(t)$ whose index corresponds to the max $z_i(T)$  \hspace{1cm} (4.16)

e.g. From “Digital Communications” by Bernard Sklar
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
• Runs on Windows/Linux/Mac
• Supports multiple different targets
• Dockable preview window (to right) shows power as measurements occurring
Waveform Acquisition & Low-Cost Alternatives
What’s a ‘Normal’ Setup look like?
## Is this Really Typical?

<table>
<thead>
<tr>
<th>Author</th>
<th>Work</th>
<th>Year</th>
<th>Scope</th>
<th>Cost (Used, 2013)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dario Carluccio</td>
<td>Electromagnetic Side Channel Analysis Embedded Crypto Devices</td>
<td>2005</td>
<td>Infinium 5432D MSO</td>
<td>$8000</td>
</tr>
<tr>
<td>Youssef Souissi et al.</td>
<td>Embedded systems security: An evaluation methodology against Side Channel Attacks</td>
<td>2011</td>
<td>Infinium 54855</td>
<td>$20 000</td>
</tr>
<tr>
<td>Dakshi Agrawal et al.</td>
<td>The EM Side–Channel(s)</td>
<td>2003</td>
<td>100 MHz, 12 bit</td>
<td>$1000</td>
</tr>
<tr>
<td>F.X. Standaert et al.</td>
<td>Using subspace-based template attacks to compare and combine power and electromagnetic information leakages</td>
<td>2008</td>
<td>1 GHz bandwidth</td>
<td>$7500</td>
</tr>
</tbody>
</table>
Does Sample Rate Matter?

Comparison of PGE for Synchronous and ASynchronous Sampling

- A Sync Samp, 25 MS/s
- A Sync Samp, 50 MS/s
- A Sync Samp, 100 MS/s
- Sync Samp, 7.37 MS/s
- A Sync Samp, 500 MS/s

Mean Partial Guessing Entropy vs. Number of Traces
Does Sample Rate Matter?

Comparison of PGE for Synchronous and ASynchronous Sampling

Mean Partial Guessing Entropy

Number of Traces

- ASync Samp, 25 MS/s
- ASync Samp, 50 MS/s
- ASync Samp, 100 MS/s
- Sync Samp, 7.37 MS/s
- ASync Samp, 500 MS/s
Does Sample Rate Matter?

Comparison of PGE for Synchronous and AASynchronous Sampling

Mean Partial Guessing Entropy vs. Number of Traces

- ASync Samp, 25 MS/s
- ASync Samp, 50 MS/s
- ASync Samp, 100 MS/s
- Sync Samp, 7.37 MS/s
- ASync Samp, 500 MS/s
Does Sample Rate Matter?

Comparison of PGE for Synchronous and ASynchronous Sampling

![Graph showing the comparison of PGE for synchronous and asynchronous sampling.](image)

- **ASync Samp, 25 MS/s**
- **ASync Samp, 50 MS/s**
- **ASync Samp, 100 MS/s**
- **Sync Samp, 7.37 MS/s**
- **ASync Samp, 500 MS/s**

Colin O'Flynn
Explaining Trigger ‘Jitter’

Sample Clock

Device Clock

Sample Clock

Device Clock
Can We Do Better?

Power
Clock
Does Sample Rate Matter?

Comparison of PGE for Synchronous and ASynchronous Sampling

![Graph showing the comparison of Partial Guessing Entropy (PGE) for synchronous and asynchronous sampling at different sample rates. The graph plots Mean Partial Guessing Entropy on the y-axis against the Number of Traces on the x-axis. The graph includes lines for different sample rates: 25 MS/s, 50 MS/s, 100 MS/s, 7.37 MS/s, and 500 MS/s. The graph highlights the impact of sample rate on the PGE, with asynchronous sampling generally showing lower PGE compared to synchronous sampling at the same rate.]
Using 4x Source Clock

Power Clock
Synchronization
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

![Graph showing comparison of different ADCs with varying performance metrics over the number of traces.]

- Inductive Pickup, OpenADC 96 MS/s
- H-Field Probe, OpenADC 96 MS/s
- Inductive Pickup, DSO 2 GS/s
- H-Field Probe, DSO 2 GS/s
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!

<table>
<thead>
<tr>
<th>Board Name</th>
<th>FPGA</th>
<th>FPGA Size</th>
<th>Ext Mem</th>
<th>USB Speed</th>
<th>Cost (USD)</th>
<th>Extra I/O Pins</th>
<th>Tested</th>
<th>Country</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avnet LX9 Microboard</td>
<td>Spartan 6 LX9</td>
<td>Medium</td>
<td>Yes - 64MB</td>
<td>Slow (USB-Serial only)</td>
<td>$89</td>
<td>No</td>
<td>Yes</td>
<td>USA</td>
<td>Original board used for OpenADC</td>
</tr>
<tr>
<td>Digilent Inc Nexsys 3</td>
<td>Spartan 6 LX16</td>
<td>Medium</td>
<td>Yes - 16MB</td>
<td>High Speed</td>
<td>$199 ($119 academic)</td>
<td>Yes</td>
<td>NO</td>
<td>USA</td>
<td>OpenADC fits directly in</td>
</tr>
<tr>
<td>Digilent Inc Nexsys 2</td>
<td>Small</td>
<td>High Speed</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>NO</td>
<td>USA</td>
<td>OpenADC fits directly in</td>
</tr>
<tr>
<td>SASEBO-W</td>
<td>Spartan 6 LX150</td>
<td>Huge</td>
<td>No</td>
<td>Very High Speed (FT2232H 60MB/s)</td>
<td>$1600</td>
<td>Yes</td>
<td>Yes</td>
<td>Japan</td>
<td>Includes smartcard reader, shunts, used in DPA Contest V4</td>
</tr>
<tr>
<td>DLP-HS-FPGA</td>
<td>Spartan 3S200A</td>
<td>Small</td>
<td>Yes - 32MB</td>
<td>High Speed (FT2232H, 20 MB/s)</td>
<td>$150</td>
<td>Yes (not many)</td>
<td>Yes</td>
<td>USA</td>
<td>Available from Digikey/Mouse</td>
</tr>
<tr>
<td>SIOI LX9 Board</td>
<td>Spartan 6 LX9</td>
<td>Medium</td>
<td>Yes - 32MB</td>
<td>None/Slow - Serial Only (can add external)</td>
<td>$63</td>
<td>Yes</td>
<td>NO</td>
<td>Australia</td>
<td>Currently no distributors, shipping cost high to North America. PCB edge connector required to interface</td>
</tr>
<tr>
<td>ZTEX</td>
<td>Spartan 6 LX9/LX25</td>
<td>Medium/Large</td>
<td>Yes - 64MB</td>
<td>Very High Speed (FX2)</td>
<td>$130/$200</td>
<td>Yes (enough for 3+ OpenADCs)</td>
<td>Yes</td>
<td>Germany</td>
<td>Available in LX9-LX150 versions, needs power supply board in addition to FPGA board</td>
</tr>
<tr>
<td>Papilio Butterfly One</td>
<td>XC3S200E/XC3S500E</td>
<td>Small/Medium</td>
<td>No</td>
<td>Slow (USB-Serial only)</td>
<td>$60/$30</td>
<td>Yes</td>
<td>NO</td>
<td>USA</td>
<td>?</td>
</tr>
<tr>
<td>Xess</td>
<td>Spartan 6 LX25</td>
<td>Medium</td>
<td>Yes - 32MB</td>
<td>Medium (USB Full Speed)</td>
<td>$120</td>
<td>Yes (not many)</td>
<td>NO</td>
<td>USA</td>
<td>Open source design</td>
</tr>
</tbody>
</table>
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)

Use serial port to confirm working
Step 3: Characterize

- Probe connected to VCC rail, not across shunt
Step 3: Characterize
Step 3: Characterize

2.2uF Ceramic Capacitor

+680uF Electrolytic

+100 ohm series resistor
Step 3: Characterize
Step 3: Shunt
Step 3: Characterization Cont’d

Persistence Mode in Scope

Adjust gain, trigger, etc to get reliable signal

Fixed Plaintext
Step 4: Acquire

- Use AESExplorer ‘Capture’ application, written in Python with PySide
  - Included on Blackhat CD
- Capture ~2500 traces, 6000 samples/capture
Step 4: Acquire

text_in.txt & wave.txt are the needed files
SMARTCARD STUFF
Attacks against Smart Card

Shunt to measure current

Clock, Sync, etc
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
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®FSH13 Spectrum Analyzer

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
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.

<table>
<thead>
<tr>
<th>Refurbished Product</th>
<th>Item Description</th>
<th>List Price</th>
<th>Our Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>7405</td>
<td>Near Field Probe Set</td>
<td>$2,095.00</td>
<td>Call to Order</td>
</tr>
<tr>
<td>7405 01</td>
<td>Near Field Probe Set with Preamplifier</td>
<td>$2,395.00</td>
<td>Call to Order</td>
</tr>
</tbody>
</table>
# EMI Sniffer™ Probe Price List

**November 17, 2007**

<table>
<thead>
<tr>
<th>Model</th>
<th>Price Each</th>
<th>Type</th>
<th>Std. Nominal Length(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>E101</td>
<td>$300</td>
<td>H-field, General Purpose Miniature</td>
<td>2&quot;</td>
</tr>
<tr>
<td>E201</td>
<td>$500</td>
<td>H-field, Micro Probe</td>
<td>2&quot;</td>
</tr>
<tr>
<td>E301</td>
<td>$350</td>
<td>H-field, Long Reach, Bendable</td>
<td>6&quot;, 9&quot; &amp; 12&quot; *</td>
</tr>
<tr>
<td>E401</td>
<td>$450</td>
<td>H-field, Right Angle Coil</td>
<td>3&quot;, 6&quot;, 9&quot; &amp; 12&quot; *</td>
</tr>
<tr>
<td>E501</td>
<td>$450</td>
<td>H-field, High Discrimination (dual coil)</td>
<td>2&quot;</td>
</tr>
<tr>
<td>E601</td>
<td>$230</td>
<td>E-field, High Sensitivity</td>
<td>3&quot;, 6&quot;, 9&quot; &amp; 12&quot; *</td>
</tr>
<tr>
<td>E701</td>
<td>$200</td>
<td>E-field, High Resolution</td>
<td>3&quot;, 6&quot;, 9&quot; &amp; 12&quot; *</td>
</tr>
</tbody>
</table>

* 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
Add to Quote Add to Cart
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短circuitting 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].

![Various shielded loops.](image)

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 Faraday’s law, which states that the induced voltage is proportional to the rate of change of magnetic flux through a circuit loop. Given low frequency, a voltage would be induced directly in the internal loop conductor, but the access sheath...
Elke De Mulder: Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices

PRE-AMPLIFIER
Pre-amplifier

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

![Graph of ZFL-1000LN Gain vs Frequency](image.png)
Pre-Amplifier: Making One

BGA2801
MMIC wideband amplifier
Rev. 3 — 10 April 2012

1. **Product profile**

1.1 **General description**
Silicon Monolithic Microwave Integrated Circuit (MMIC) wideband amplifier with internal matching circuit in a 9-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 2.15 GHz
- 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>
<thead>
<tr>
<th>Pin</th>
<th>Description</th>
<th>Simplified outline</th>
<th>Graphic symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Vcc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2, 5</td>
<td>GND2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>RF_OUT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>GND1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>RF_IN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Pre-amplifier: Making One
Pre-Amplifier: Making One
Pre-Amplifier: Making One
20 dB = 100x gain

(~80 – 400+ MHz)
16 dB = 40x gain

(0.1 – 10 MHz)
DIFFERENTIAL PROBE
From “Side Channel Analysis of AVR XMEGA Crypto Engine” by Ilya Kizhvatov
Common-Mode Noise
\[ V = I \cdot R \]

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

110
What was that?
We don’t need 1000 MHz..
Uh what about E-Bay?
How Cheap are you?

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

AtMega48A

Capture Hardware

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
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
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

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

  - 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/blackhatchipwhisperer.com

E-mail me: coflynn@newae.com
Mailing List: chipwhisperer.com
Twitter: colinoflynn

Please fill out Speaker Surveys!