My Funding Provided By:

Special Thanks:
Dr. Zhizhang Chen
Cryptography Research Inc
The Way Forward

- What is Side Channel Analysis (SCA)
- Your First Attack!
- Waveform Acquisition
- Magnetic Field Probe
- Amplifiers/Front-End Stuff
- Measuring Current in Real Devices?
- Some Loose Ends
The Side Channel
Side Channel?
Side Channel?

Power

Main Channel

Secret
Side Channel.
1. Capturing the Data
2. Modeling the Expected
3. Measure the Fit
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
Differential Power Analysis

3× Traces With Expected Transitions

3× Traces With No Expected Transitions

Major difference between two sets
# 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
Note we use a resistive divider to scale the 5V signals to 3V – the 5V signal would immediately destroy the FPGA board!
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)

Use serial port to confirm working
Step 3: Characterize

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

2.2uF Ceramic Capacitor

+680uF Electrolytic

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

Persistence Mode in Scope

Adjust gain, trigger, etc to get reliable signal

Fixed Plaintext
Step 4: Acquire

- Use AESE Explorer ‘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
Step 5: Break It

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

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

```python
```
Waveform Acquisition & Low-Cost Alternatives
What’s a ‘Normal’ Setup look like?

- Power Trace
- Trigger
## Is this Really Typical?

<table>
<thead>
<tr>
<th>Author</th>
<th>Work</th>
<th>Year</th>
<th>Scope</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dario Carluccio</td>
<td>Electromagnetic Side Channel Analysis Embedded Crypto Devices</td>
<td>2005</td>
<td>Infiniium 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>Infiniium 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>
Can We Do Better?

Power Clock
Using 4x Source Clock

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 & Zhizhen Chen
OpenADC
OpenADC

• Can use up to 105 MSPS in oscilloscope-like mode
• Supports synchronizing to sample clock of device, so can attack high-speed targets well even!
• Built-in amplifier
• Open Source design!
Magnetic Field Probes
Rohde & Schwarz 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

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

Price: $2,505

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></td>
</tr>
<tr>
<td>7405 01</td>
<td>Near Field Probe Set with Preamplifier</td>
<td>$2,395.00</td>
<td></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)
<table>
<thead>
<tr>
<th>PRICING INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instek GKT-006A EMI Probe Kit Set</td>
</tr>
<tr>
<td>7-piece near field probe set</td>
</tr>
</tbody>
</table>
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:
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.](http://www.compliance-club.com/archive/old_archive/030718.htm)

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 short-circuit 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. Any stray fields present outside the loop would be induced directly in the internal loop conductors but the outer sheath...
Elke De Mulder: Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices
Pre-Amplifier (Probe or Other)
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 showing the gain of ZFL-1000LN at different frequencies for 12V, 15V, and 16V.]
But we can get cheaper. We can make a pre-amplifier with similar characteristics for even less!

Amplifier chip costs $2! Just needs a little support circuitry.
Pre-amplifier: Making One

MiniCircuits lists full details of the required additional components

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
What was that?

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

Real Time Availability
Stock: 1 Can Ship Immediately
On Order: 0
Factory Lead-Time: 2 Weeks

Enter Quantity: Minimum: 1
Multiples: 1

Pricing (CAD)
1: $4,564.62

To add to a project, please Log In.
We don’t need 1000 MHz..
Uh what about E-Bay?
This chip is < $5 in single-unit quantities! Add a voltage supply & a few resistors/capacitors and you’ve got a pretty good probe.
Other Targets of Interest
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

• There is a good book that covers a LOT:

![Power Analysis Attacks](image)

• Read original DPA Paper by Kocher, look at CHES & COSADE Proceedings

• Hint: Local universities often have access to these, so use a computer on their network (e.g. from library)
Questions Etc.

Visit me on interweb: newae.com/blackhat

E-mail me: coflynn@newae.com

Please complete the Speaker Feedback Surveys!