Analysis of a Cross-Platform DES Power Signature

CSE 8393 – Project Report

Adam Critchley

Southern Methodist University
CSE 8393: Power Analysis Attacks
acritchley@lyle.smu.edu

***Abstract* — *The pursuit of a power analysis vulnerability in crypto-systems is appealing because a compromised system yields insight into past, present, and future ciphers. However, compromising such a system requires a large amount of power traces with varying inputs to determine the vulnerability. Such a limitation dictates that the attacker has direct access to the device and prior knowledge to the interface and internal crypto-algorithm. This paper will analyze Data Encryption Standard (DES) power traces from an Altera and Xilinx Field-Programmable Gate Array (FPGA) in an effort to determine a universal signature that will identify the DES algorithm from FPGA power traces and assist in compromising the device under attack.*

Keywords—fpga;power analysis;crypto;des;spa;dpa

I. Introduction

The goal of this research is to derive a standard DES power signature for FPGAs. The signature will be derived from two implementations of Data Encryption Standard each targeting a different FPGA. The first implementation of DES targets the Altera Stratix with the Agilent oscilloscope traces collected for use in a Differential Power Analysis (DPA) contest. The second implementation of DES targets the Xilinx Spartan 3 with traces collected using a Mini-DSO oscilloscope for the sole purpose of this project. The purpose of collecting traces from two different FPGA platforms will be to identify similarities in power traces from the DES implementation. Identifying the crypto algorithm from the power trace of the Device Under Attack would benefit analysis of future power traces from which the algorithm was unknown. Knowing the algorithm would assist in making assumptions concerning the operations performed, processing duration, and size of transistor network as well as understanding of the expected inputs and outputs when stimulating the Device Under Attack without documentation.

II. DES

The Data Encryption Standard is a 16 round 64 bit key (effectively 56 bit key) Feistel Cipher based crypto-algorithm. The DES algorithm uses a symmetric key for decryption and encryption. Thus, discovering the key from either the decryption or encryption operation allows for use in the complementary operation. The standard DES algorithm is documented with NIST 46-3[4] and this research assumes the implementations conform to the standard. Otherwise, implementing and verifying the NIST suggested conformance tests would exceed the time allotted to finish research.

A. Altera Implementation

The Altera DES implementation power traces were collected for a DPA competition (http://www.dpacontest.org/home/index.html) held during the international Cryptographic Hardware and Embedded Systems (http://www.chesworkshop.org/) conference. These traces are meant to symbolize an ideal situation with a commercial grade oscilloscope and an expert capturing the traces. Thus, these traces will be the control of the experiment in which the Xilinx DES implementation will be compared against.

B. Xilinx Implementation

The Xilinx DES implementation power traces will be collected as part of the exercises for the project. The DES implementation is a variation of the core found on OpenCores.com (http://opencores.com/project,des) optimized for a smaller bounded I/O pin configuration which will fit on the Xilinx evaluation board. The modified DES will reside on a Xilinx Spartan 3 XC3S200-FT256AF evaluation board (http://www.digilentinc.com/Products/Detail.cfm?Prod=S3BOARD) and the traces will be collected using a voltage probe connected to the Mini-DSO DS203 (http://minidso.com/bbs/index.php). The DES algorithm will be synthesized to the Spartan 3 and stimulated with input internal to the FPGA.

III. Research Activities

The project will involve comparing the traces to identify similarities or predictable differences. Potential issues will be the clock frequency difference between the traces. The Altera's frequency is not known while the Xilinx can be set to any frequency. A small amount of feature matching may be necessary to help transform between the two power traces in order to identify similarities. Also, care must be taken to not set the Xilinx's frequency too fast such that aliasing is introduced into the power traces. After the similarities have been identified they can be used to create a generic power trace for a standard DES algorithm which can be used to identify DES from traces of unknown algorithms. And with a generic power trace defined we can quantitatively determine the quality of future DES traces.

IV. MEASUREMENT SETUP

In a typical measurement setup there is a Clock Generator (CG), Device-Under-Attack (DUA), Analysis Computer (AC), Measurement Circuit/Probe, Digital Storage

Oscilloscope (DSO), and Power Supply (PS). The Xilinx evaluation board will be the DUA and comes with an integrated power supply so there is no need for an external power supply. The internal Xilinx Oscillator will be used as the CG. The Measurement Probe will be a passive voltage probe, though an EM probe would have been a better solution. And the AC will be a standard Windows laptop with the necessary Xilinx ISE to synthesize and program the Xilinx board.

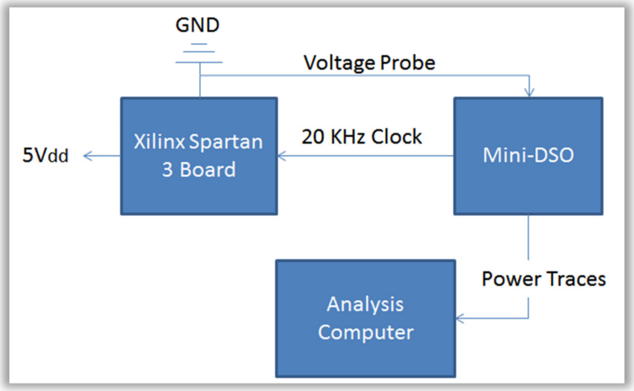


Figure 1: Measurement Setup

The initial measurement setup consisted of a Xilinx board using the integrated PS and using a clock frequency of 5 microseconds supplied from the CG. The voltage probe was connected to the PS solder terminals. Using this setup the DSO was set to sample at every 5 microseconds. After power trace capture, the traces were extracted to the AC which were analyzed using a custom application written to operate on the BUF file from the MiniDSO and the BIN file from the Agilent power traces captured for the DPA competition.

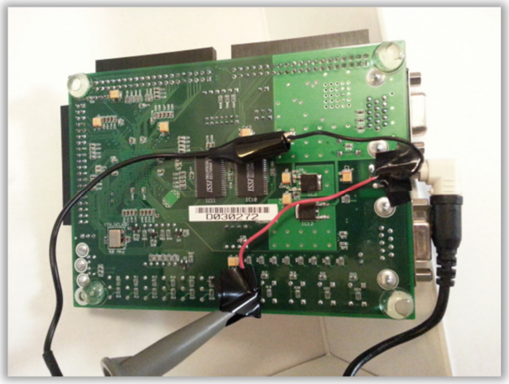


Figure 2: Spartan 3 with Voltage Probe

The Xilinx board was provided a hardcoded message and key from within the DES bitstream. The board once programmed will continuously operate on this data until the board is unplugged or re-programmed with a new message and key. The power traces were captured with a 5 microsecond sample time which is 10x faster than the 20kHz (i.e. 50 us) clock frequency.

The Trace Analysis Software was created to read Agilent trace files and MiniDSO BUF files. The Agilent trace file format was well documented and contained the voltages necessary for power analysis. However, the BUF file format was undocumented so it required reverse engineering from the OpenSource embedded software that creates the files to determine the file format. During the reverse engineering it was discovered that the measurements for the traces are contained as counts which come directly from the A/D convertor within the DSO. The measurements from the Analog Devices AD9288 require a scaling factor to convert from the native counts to voltage. The scaling factor is the A/D input 1.024 voltage over the 8-bit range which is 2.003 mV per count. After using the newly discovered conversion factor the traces resembled the voltages displayed on the DSO.

The fatal flaw of the collection process was the decoupling capacitors between the FPGA and integrated Power Supply. The capacitors ended up smoothing out the power traces essentially eliminating the features of the DES algorithm that were of interest. According to the OpenADC project [3][3], the decoupling capacitors can be circumvented by either wrapping a wire around the closest capacitor to the FPGA or using an EM Probe. (http://www.youtube.com/watch?v=_fo3Js54WfU)

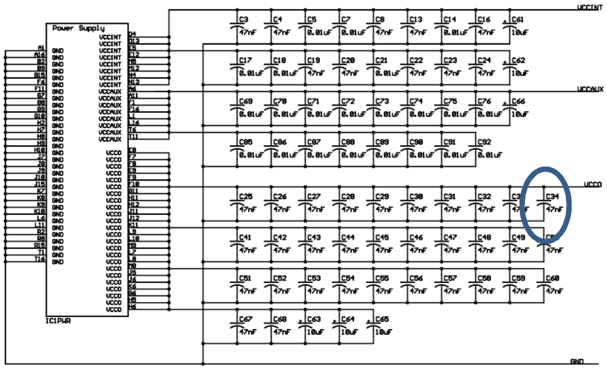


Figure 3: Power Schematic from Xilinx Evaluation Board

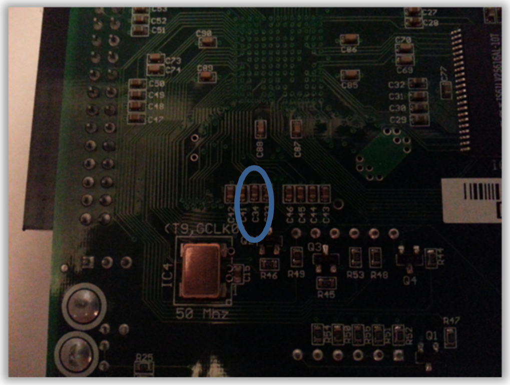


Figure 4: Decoupling Capacitor

The power trace information will still be collected and analyzed but the alternative methods were impossible due to the size of the capacitor and cost/availability of an EM Probe.

Thus, the collected power traces will be scrutinized and will not be included for the DES signature derivation.

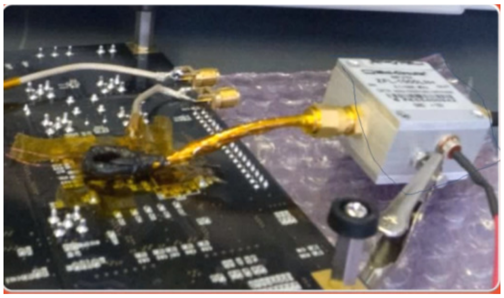


Figure 5: Example EM Probe (OpenADC)

V. POWER TRACE CAPTURE

The sampling time for the MiniDSO was set to 5 microseconds and the clock frequency set to 50 microseconds. The graph when viewed with the DSO appears to be very flat.

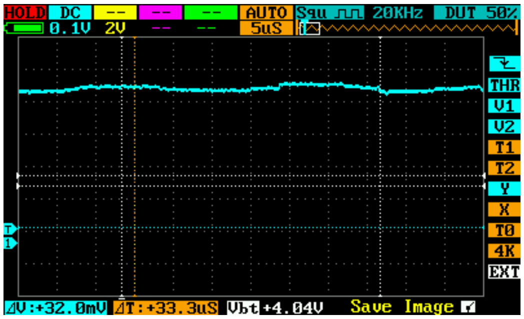
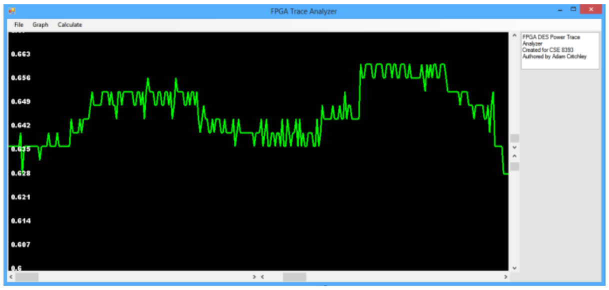


Figure 6: MiniDSO display

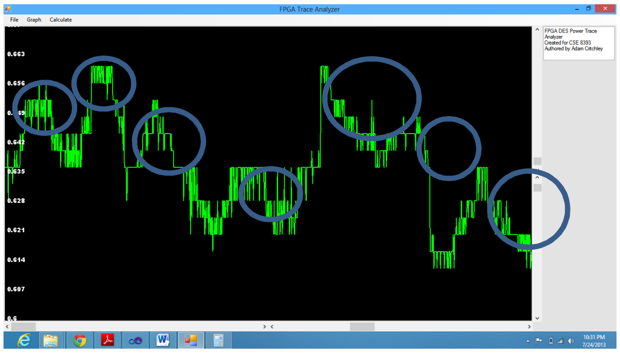
Instead of relying on the DSO to identify features of interest we'll be creating a custom application. The Power Trace Analysis Toolbox (PTAT) will be developed to assist in Simple Power Analysis (SPA) attacks. We'll be using the first revision of the PTAT to analyze our Xilinx traces from the MiniDSO. Using PTAT we can zoom into the trace which reveals faint features.



FPGA DES Power Trace Analyzer
Created for CSE 8383
Authored by Adam Critchley

Figure 7: Zoomed Xilinx Power Trace using PTAT

Zooming out to 6,135 samples reveals several peaks hidden in the suspected noise. The number of samples contains 122 clock cycles with 16 cycles necessary for a full DES encryption. There should be 7 full DES encryptions contained in the graph. And, on inspection approximately 7 collections of peaks can be seen in the graph although the waveforms are definitely malformed.



FPGA DES Power Trace Analyzer
Created for CSE 8383
Authored by Adam Critchley

Figure 8: Zoomed to 6,135 samples

Investigating further, we zoom in to 162 samples which contain the first collection of peaks. There are approximately 16 peaks present in the collection which could correspond to the 16 rounds in the DES algorithm. The biggest concern is that even though a pattern is visible the pattern may be statistically irregular which prevents us from using the DPA attack.

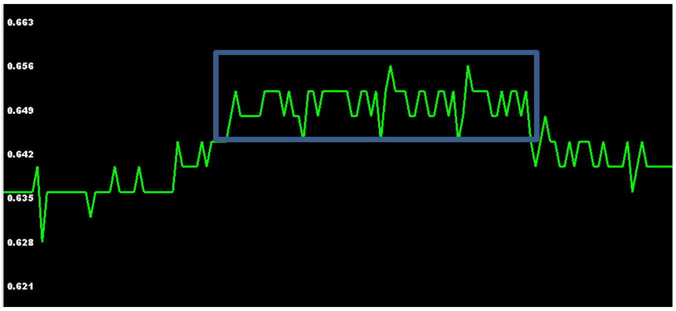


Figure 9: Zoomed to 162 samples

VI. POWER TRACE ANALYSIS

First we analyzed the data from the DPA contest. The reason for attacking the DPA contest data first is on the assumption that the data is ready to be analyzed. The data is assumed to be collected by an expert with properly calibrated devices which are capable of capturing power traces that can more easily be analyzed.

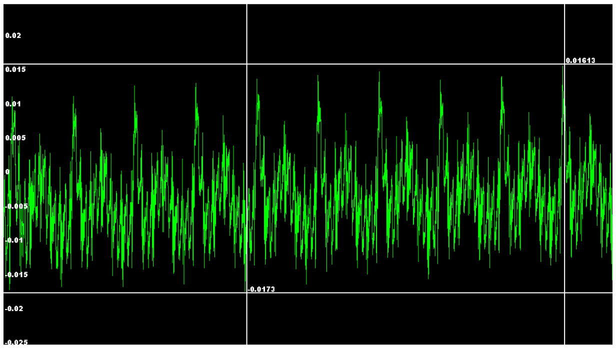


Figure 10: Agilent Power Trace viewed using PTAT

Immediately the differences between the Xilinx trace and the DPA contest trace are noticeable without performing statistical analysis. The DPA contest traces contain far more regular and well-defined features.

The traces contain 50,003 samples which is too much data to visually locate power features. That amount of data warrants a SNR of each point be calculated which will identify points of interest. Thus, using the SNR calculation will significantly reduce the amount of samples to inspect. For this reason the SNR calculation was added to the PTAT.

PTAT will be used to perform the SNR analysis on two traces. The 67,753 trace files each with the same key will be used to assist in distinguishing the signal from the noise. The first SNR analysis will be conducted on the trace with a key of 6b64796b64796b64, message of 0000000000000000, and cipher of 25526b3ee6a6fc22. This trace will be hereby referred to as Power Trace 1.

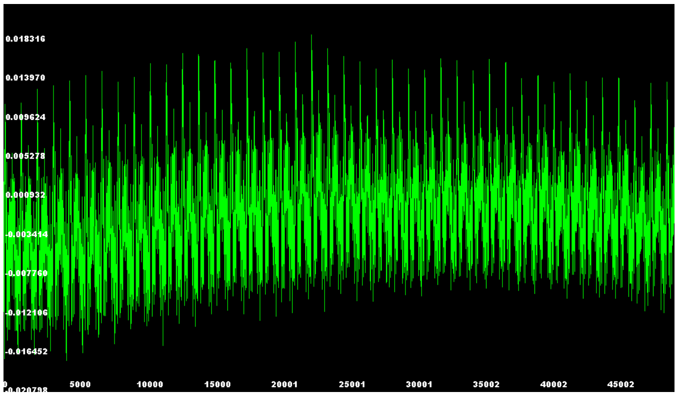


Figure 11: Power Trace 1

The first trace reveals several points with large SNR. The ranges of the SNR calculation are from -22 dB to 56 dB. And a visual inspection confirms that the majority of the features in the original trace data correspond to points with a large amount of SNR.

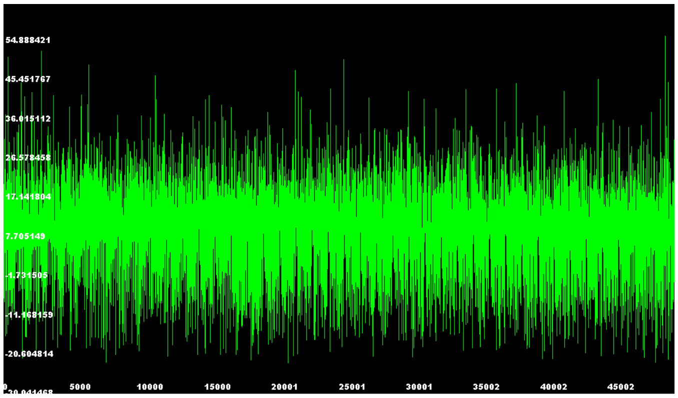


Figure 12: SNR (dB) of Power Trace 1

The decision on which threshold to use is made primarily on how much that threshold reduces our data. For our example, a threshold of 30 dB will be used to reduce our sample size to 205 samples of interest.

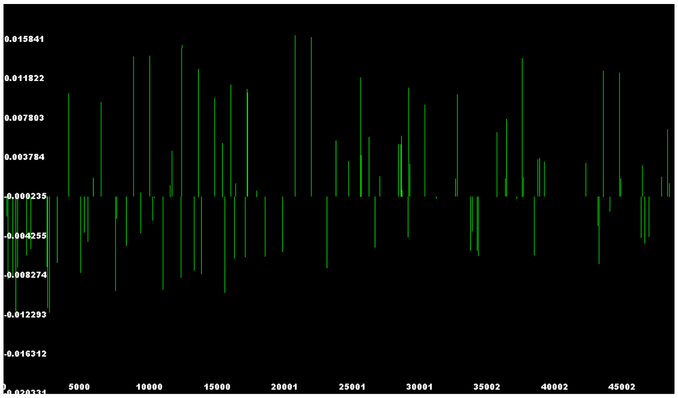


Figure 13: 205 samples of interest from Power Trace 1

The second trace has a key of 6b64796b64796b64 (same key as Power Trace 1), message of d768f6404e0129a7, and cipher of e37843ccfa2e6d78. This trace will be hereby referred to as Power Trace 2.

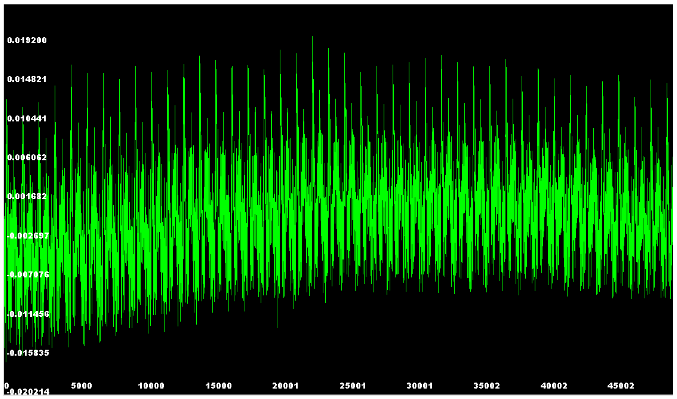


Figure 14: Power Trace 2

The SNR calculation for Power Trace 2 reveals ranges from -26 dB to 73 dB.

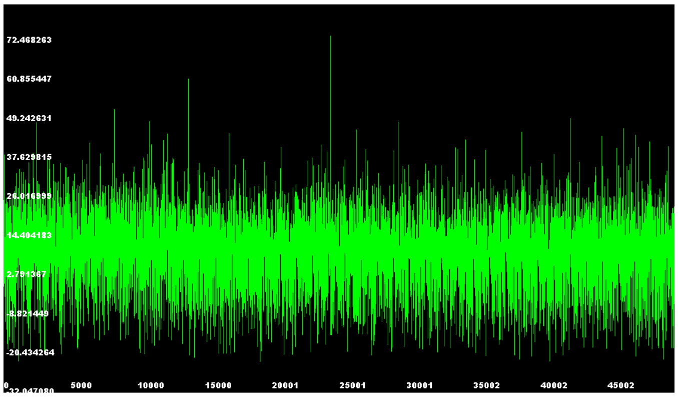


Figure 15: SNR (dB) of Power Trace 2

Again, we will use a threshold of 30 dB to determine which samples are of interest.

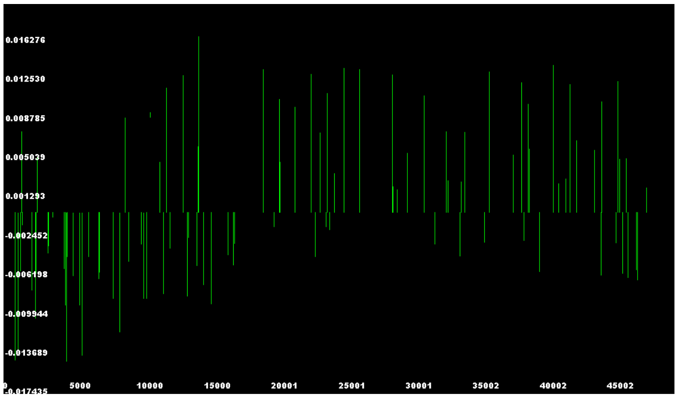


Figure 16: 233 samples of Power Trace 2

Now that we have the highest signal samples for both Power Trace 1 and 2 the similarities can be observed. Out of our two traces one sample had a commonly high SNR. The lack of more samples with commonly high SNR might suggest that the SNR threshold used was too aggressive for the number of compared traces. More traces would increase the occurrence of high SNR samples even with an aggressive SNR threshold. The goal of this exercise is to find the samples that contribute similarly to the common key of the traces. With enough samples a distribution can be created which can be used to determine the keys of unknown traces within a certain probability. With the addition of one more trace, in order to add more SNR samples of interest, we can create what our high SNR distribution looks like so far with three traces.

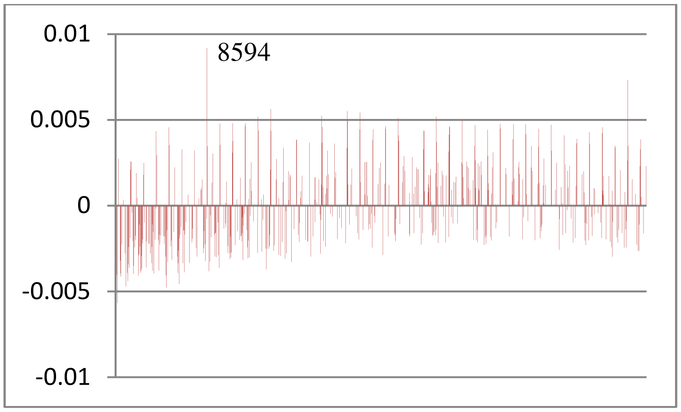


Figure 17: High SNR distribution

This distribution helps us to predict that a high SNR in sample 8594 hints that our key might be 6b64796b64796b64. Ideally, one of these distributions must be created for every key from a large amount of traces from that key. However, before we start comparing distributions we need to create a cumulative form using the sum of squares.

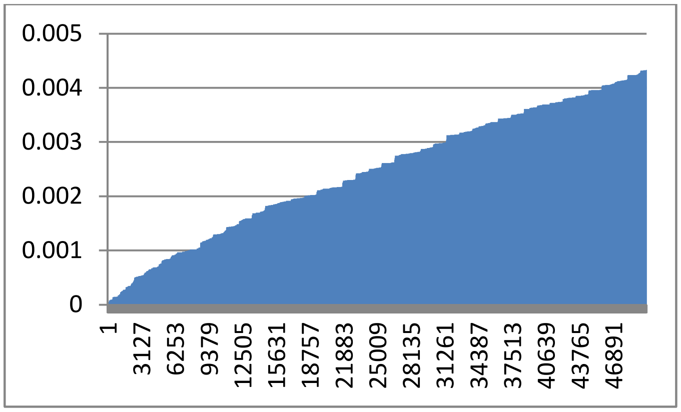


Figure 18: Sum of Squares High SNR Distribution

With a cumulative distribution we can use tests such as the Root-Sum-Squared (RSS), Lilliefors [1], or the Kolmogorov-Smirnov (K-S) which are used to quantitatively determine distribution similarities. The K-S test for the High SNR distribution against Power Trace 1 reveals that they do not match. While visually the distribution is starting to look similar to the measured power traces it is apparent through the amplitude of the high SNR distribution that many more traces are required to properly use our distribution for key prediction.

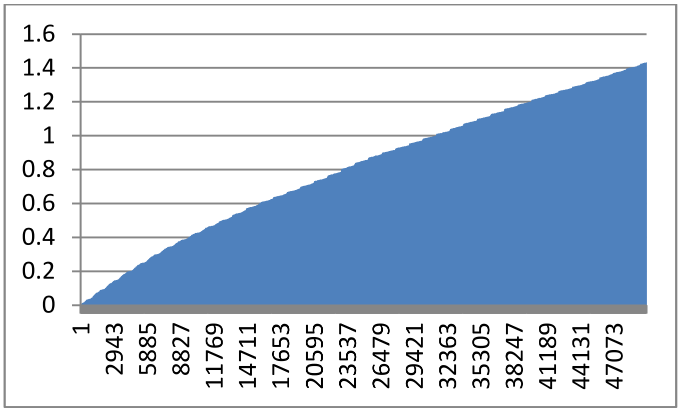
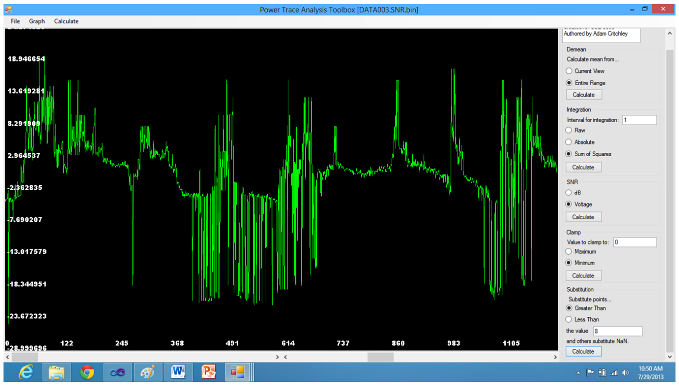


Figure 19: Sum of Squares Power Trace 1

VII. Revisiting the Xilinx Traces

Using the SNR technique we can revisit the original traces and confirm our suspicion on which parts of the trace contained the DES calculations. First we will calculate the SNR with a reference signal based off five captured traces.



Authored by Adam Critchley

Demean
Calculate mean from...
○ Current View
● Entire Range
Calculate

Integration
Interval for integration: 1
○ Raw
○ Absolute
● Sum of Squares
Calculate

SNR
○ dB
● Voltage
Calculate

Clamp
Value to clamp to: 0
○ Maximum
● Minimum
Calculate

Substitution
Substitute points...
● Greater Than
○ Less Than
the value 8
and others substitute NaN.
Calculate

Figure 20: SNR for Xilinx Trace

Next, we observe how the SNR calculations overlay onto the original trace. Ideally, in practice we would want more than five reference traces.

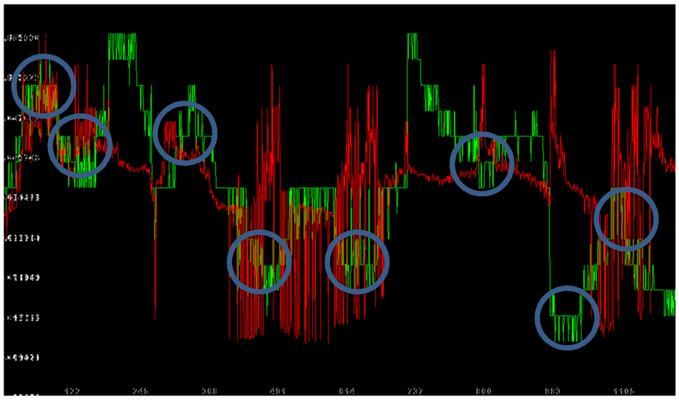


Figure 21: SNR (red) overlaid on power trace (green)

The SNR confirms that a few of our initial guesses were correct. It is promising that we are able to identify DES traces from so few reference traces and despite the decoupling capacitors [2]. Now with suspected traces we would isolate each one to create distributions based off their signals with the same technique used for the DPA contest traces.

VIII. Power Trace Analysis Tool

The Power Trace Analysis Tool (PTAP) was created specifically for this project. PTAP is a lightweight tool of only 2,405 lines of code according to the “sloccount” application. Currently supported operations are demean, clamping, substitution, SNR, and integration. The tool was not meant to be a complete solution for power trace analysis but a solution to assist with the research necessary for this project. The PTAP is uploaded to a Google project for others to use and modify without restriction (https://code.google.com/p/power-trace-analysis-toolbox/).

All charts included in this project report, with the exception of the Excel created distribution charts, were created with PTAP.

IX. Conclusion

This research attempted to create a cross-platform DES signature. To do so, the research used a technique to create a DES distribution from samples of interest based off high SNR samples from the DPA contest power traces. The Xilinx traces lacked the quality and quantity necessary to perform further analysis. The preliminary results for the DPA contest and Xilinx traces were promising given the little amount of data that was used. With more time and more traces a more thorough study of the distribution could be performed. Additionally, the PTAP could be modified to automate much of this process.

The DPA contest traces were an excellent source of data not only because of their quality but also because of their quantity. Capturing even a few traces from the Xilinx evaluation board with the MiniDSO was very laborious. Thus the process of capturing traces should be automated with a better than entry-level DSO. Though, the embedded software for MiniDSO is open source and thus could be modified to add automated trace capturing with controls through its USB port.

Future work would involve adding more functionality to PTAP such as trace alignment or SPA attacks such as the template or collision attacks. Visual analysis was already significantly helpful using the PTAP in its current state. Also, coupling automated trace captures with the MiniDSO with automated analysis using PTAP would significantly reduce the amount of work involved. Finally, the automated procedure would reduce the need for an expert to toil over capturing traces and instead allow the expert to focus on deriving analysis techniques from the captured traces that better target the DUA.

References

[1] Yongdae, Kim, Sugawara Takeshi, Homma Naofumi, Aoki Takafumi, and Satoh Akashi. "Biasing Power Traces to Improve Correlation in Power Analysis Attacks." *First International Workshop on Constructive Side-Channel Analysis and Secure Design* (2010)

[2] Sun, Song, Zijun Yan, and Joseph Zambreno. "Demonstrable differential power analysis attacks on real-world FPGA-based embedded systems." *Integrated Computer-Aided Engineering* 16.2 (2009): 119-130.

[3] Colin’O Flynn, and Zhizhang Chen, “A Case Study of Side-Channel Analysis using Decoupling Capacitor Power Measurement with the OpenADC.” YouTube.com, accessed 07/26/2013.

[4] FIPS, PUB. "46-3: Data Encryption Standard (DES)." *National Institute of Standards and Technology* 25.10 (1999).