# A Case Study of Side-Channel Analysis using Decoupling Capacitor Power Measurement with the OpenADC

Colin O'Flynn and Zhizhang Chen

Dalhousie University, Halifax, Canada
{coflynn, z.chen}@dal.ca

**Abstract.** When capturing power measurements for processing with side-channel analysis, there are many options with regards to both how the measurement is taken, and also how that measurement is digitized. This work concentrates on a new technique which measures the current through a decoupling capacitor, with a probe that can easily be built in any electronics lab. In addition an open-source digitizer board is presented, which is specifically designed to measure the signals required for side-channel analysis. The techniques presented in this work facilitate sharing of repeatable measurement techniques: the measurement environment presented can easily be duplicated at a very low cost.

**Keywords:** side-channel analysis, decoupling, acquisition, case study

## 1 Introduction

Using the power consumption of a device as a 'side channel' to derive secrets held inside the device was first presented in 1998[1]. The initial two attacks, called Differential Power Analysis (DPA) and Simple Power Analysis (SPA) have since been augmented by even more powerful attacks such as template attacks[2] or Correlation Power Analysis (CPA)[3]. This work does not concentrate on the attacks; instead, this work focuses on how the power consumption of a device under attack is measured. First, an overview of current technologies used in the capture of power traces will be presented. From this we can define the requirements for a capture system, before moving onto an implementation of a capture system meeting these requirements. In addition to a low-cost capture system, a simplified probe type is proposed, which has the advantage of being easily reproducible by other researchers. Finally a comparison of the proposed capture architecture and probe will be compared to commercially available solutions, as typically used in recent literature.

## 2 Review of Capture Techniques

### 2.1 Probe Type

There are two general classes of probes used for measuring power consumption: a resistive shunt as used in the original work [1], or an electromagnetic (EM)

probe[4]. EM probes have been shown to result in more successful attacks[5], with the advantage that EM probes do not require any modification to the device under attack, and can even be performed at a moderate range[6].

Many types of EM probes have been used in published work, including commercially manufactured probes. Comparison of different probe constructions is found in [7, 8]. Smaller probes can be scanned over the chip surface to pick out specific features, such as bus/data lines.

### 2.2 Acquisition

The required acquisition characteristics depend on both the target under attack, and the type of attack being carried out. Considerations with regards to the target under attack include the clock frequency, whether the cryptographic algorithm is in hardware (HW) or software (SW), technology used for the chip, and whether or not countermeasures have been implemented. Typically the capture oscilloscope achieves around 1 GS/s, as shown in Table 1.

**Table 1.** A few examples of capture rates in recently published papers. Sample rates only appear if the tested attack was successful at that sample rate.

| Reference | Sample Rate(s) - MS/s | Target Type |
|---|---|---|
| [9] | 5000 | HW - 24 MHz |
| [7] | 500, 2000 | HW |
| [10] | 200 | SW |
| [8] | 125, 250, 500 | SW - 24 MHz |
| [11] | 500, 1000 | HW |

## 3 Ideal Acquisition System - Requirements

### 3.1 External Clock Inputs

Commercial oscilloscopes typically provide their own sampling clock which is not synchronized to the device clock. In many devices, however, the device clock is readily available either as a digital signal or by adding a buffer circuit to the crystal oscillator. The sample clock can be derived from the device clock to measure a consistent point; for example it can be used to measure the power consumption on the clock edge. A comparison of measurements taken with an unsynchronized and synchronized sample clock is shown in Fig. 1. In section 6 it will be demonstrated that this synchronized sample clock significantly relaxes the requirement of using a high sample rate for certain attacks.

Note that sample clock synchronization is different from the trigger input that all oscilloscopes provide. With a real-time oscilloscope, the internal sample clock of the oscilloscope will be running at all times, and the sample occurs at the

next clock edge after the trigger. Thus even though the oscilloscope is triggered at a repeatable time, there will be some random jitter between when the first sample occurs relative to this trigger for unsynchronized (free-running) sample clocks[12]. Some oscilloscopes do provide a synchronous sampling ability, such as the CleverScope with the 'external sampler clock input', or the PicoScope 6000 series.

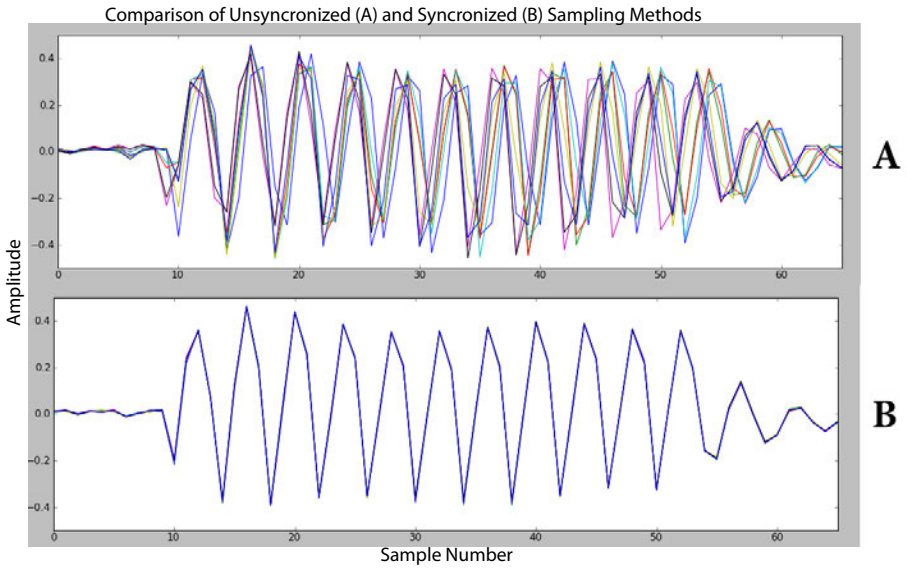


**Fig. 1.** Eight power samples with the same input are taken and overlaid to show consistency of measurements. In *A* the sample clock is 100 MHz but not synchronized to the device clock, whereas in *B* the sample clock is 96 MHz, but synchronized with the device clock.

If the clock frequency varies due to either countermeasures or a low-cost oscillator, this would not affect the acquisition quality, since samples are always based on the device clock.

### 3.2 External Clock Phase Adjust

The processing of the external clock input, the ADC, and the analog front-end will add some delay between when the rising clock occurs on the target device, and when the actual sample is recorded. In addition the point of interest for the power analysis may not lie directly on the rising edge, but sometime after this clock edge. For this reason the capture board must be able to add an adjustable delay (phase shift) between the input clock and the actual sample point.

### 3.3 Adjustable Gain

The output of a probe will vary with both the probe type and the circuit under analysis. For this reason, an adjustable gain amplifier is useful to amplify the signal up to the range of the input of the digitizer. Oscilloscopes for example provide a selectable input range - this is still insufficient for H-Field probes, which require an external Low Noise Amplifier (LNA).

## 4 Low-Cost Acquisition Architecture

The architecture of the analog front-end which is used here is shown in Fig. 2. The features previously identified as important for side-channel analysis are included: an external clock input with adjustable phase, an internal clock, adjustable gain, and a computer interface.

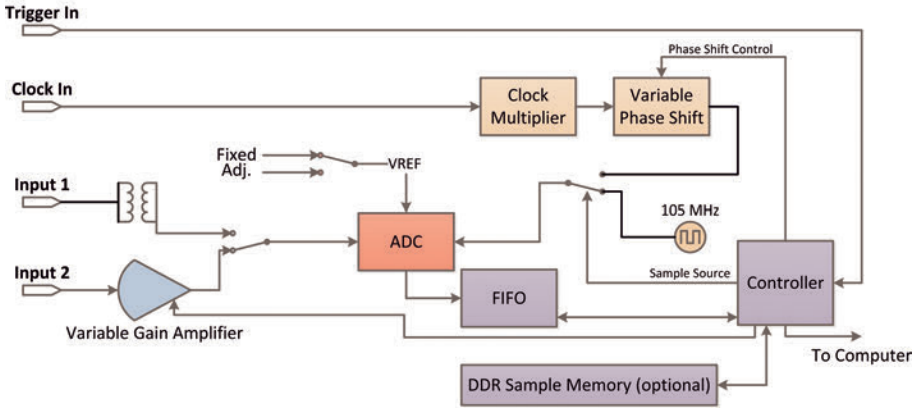


**Fig. 2.** Architecture of analog acquisition unit which is implemented in a combination open-source ADC board and COTS FPGA board.

The analog front-end and ADC board has been released in an open-source design called the OpenADC. The OpenADC hardware consists only of the low noise amplifier (LNA), ADC, input connectors, and associated support circuitry such as power supplies. This board can be connected to most FPGA development boards with sufficient IO available - it is shown mounted on a low-cost Xilinx Spartan 6 development board from Avnet in Fig. 3. The open-source solution includes not only the PCB designs, but example FPGA source code and capture applications on the PC at [13]. The total cost of this acquisition solution is $140 US.

While the sample rate is limited by the 10-bit ADC selected to 105 MS/s, the analog bandwidth is higher to maintain information on the clock edges. When the LNA input is selected the analog bandwidth is around 110 MHz, and when

the transformer-coupled input is selected the analog bandwidth is around 500 MHz. The LNA has an adjustable gain in 100 steps up to 55 dB, allowing for the direct connection of a wide range of measurement probes, including both current shunt and EM.

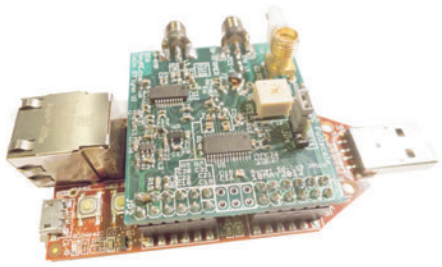

**Fig. 3.** The OpenADC mounted on a commercial FPGA development board. The FPGA board provides control, USB interface, and a 48M sample memory.

In addition to the analog hardware and FPGA source, the PC-based capture application source is provided. This source is written entirely in Python, providing an excellent cross-platform tool which can easily be expanded. The basic library provides the hardware interface code along with the graphical display. This can be easily integrated into other applications: Fig. 4 shows two example applications that make use of this library.

## 5 Decoupling Capacitor Power Measurement

A decoupling capacitor is designed to provide a low-impedance path for high frequency current, as typically drawn at the clock edge[14]. For side-channel analysis with a resistive shunt, the decoupling capacitor significantly worsens the measured signal [15]. The higher-frequency components, which are of interest for SCA, are flowing through the decoupling capacitor and not the shunt.

Measuring the current through a decoupling capacitor for side-channel analysis was first explored in [16], which used a current transformer to measure the current flowing through individual decoupling capacitors. Current transformers use the principle of induction, which dates back to Faraday's discovery in 1831[17], to measure current flowing in a conductor without the necessity of breaking the conductor. Using induction to measure current through a decoupling capacitor in-place has also been demonstrated, but such papers employed the measurements for the design of power distribution systems, and not for side-channel analysis [18–20]. This paper builds on such previous work by looking at the performance of the inductive pickup for side-channel attacks, and the physical considerations for its use.

The method thus proposed is to wrap the target decoupling capacitor in a thin magnet wire, and connect this to the acquisition oscilloscope. Physically,

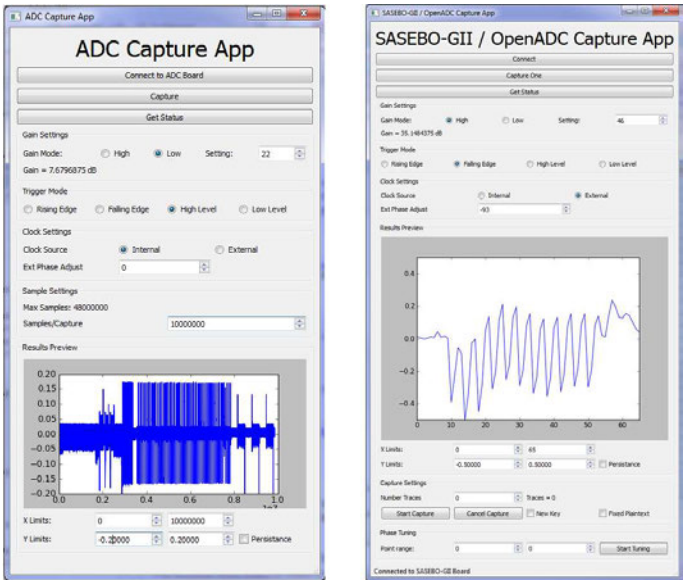


**Fig. 4.** Example capture applications provided. The *left* example controls only the OpenADC, and this example is a long (10E6 point) capture of a KeeLoq algorithm. The example on the *right* interfaces to the OpenADC and SASEBO-GII board to capture many traces with different plaintext data.

this proposed method requires no modifications to the device under test. The localized nature of the measurement provides excellent rejection of interference, and the performance when used in side-channel attacks will be demonstrated to be slightly superior to other common methods.

## 6 SASEBO-GII Correlation Power Analysis (CPA) Results

The Side-channel Attack Standard Evaluation Board (SASEBO) version GII from the National Institute of Advanced Industrial Science and Technology (AIST) in Japan provides a useful reference platform for performing side-channel analysis attacks. Characterizations are available in literature of the performance of this board under various attacks[15, 21]. The attack used here is a simple Correlation Power Attack, for which the reference code is available from AIST[22], with the cryptographic core under attack being the AES core provided for the DPA Contest Version 3[22].

The performance analysis here consists of the number of traces required for the global success rate (GSR) to stay above 80%. This performance analysis was chosen to match recent publications of a similar nature [9, 23].

### 6.1 Measurement Setup

The measurement equipment consists of an Agilent 54831B Infiniium DSO as a reference, and the OpenADC platform presented earlier as a demonstration of low-cost capture hardware. The acquisition from the Agilent 54831B is done with code from AIST[22] which has been modified to support the scope being used, with a sampling rate at 2 GS/s. This scope does not support an external clock input. Vertical voltage scale differs depending on the measurement setup being used. For the OpenADC the sampling clock (96 MHz) is 4x the AES Core Clock (24 MHz), which is derived from the actual AES Core Clock. The OpenADC capture software is written in Python and the source code is available from [13].

In all cases the internal voltage (VINT) of the FPGA is adjusted to 1.000 volts; this avoids any unintentional results occurring because the insertion of the current shunt will naturally reduce the voltage seen by the FPGA. The SASEBO-GII is equipped with a small adjustment range on the VINT voltage to null out the current shunt loss.

The board as shipped did not have decoupling capacitors mounted on VINT, which correspond to C46 - C52. Where a decoupling capacitor is mounted in these tests, only a single 100 nF capacitor is mounted on C46, for which a Murata GRM155R61A104KA01D size 0402 capacitor is used.

**Current Shunt** The SASEBO-GII board provides connections for measuring current used by the cryptographic FPGA via a 1-ohm current shunt. This measurement uses the 'VINT' supply for the FPGA, which is measured at J2. This measurement is performed both with C46 mounted and unmounted.

**H-Field Probe** An H-Field probe was constructed from a loop of semi-rigid coax. When using the 54831B oscilloscope, a MiniCircuits ZFL-1000LN Low Noise Amplifier (LNA) boosts the signal to achieve a better response. The OpenADC is directly connected to the H-Field probe, as the OpenADC contains an integrated LNA. A photo of the magnetic field probe is shown in Fig. 5. Detailed information about the construction process is found in [14], with some additional examples for side-channel analysis in [7].

**Fig. 5.** Shielded magnetic field probe, before wrapping in an insulator to allow safe probing of any area of the device under test.

**Shunt Measurement on Individual Capacitors** The current through an individual capacitor was measured with a 0.22 ohm current shunt placed in series with the capacitor. The voltage was read directly from the current shunt and fed into the oscilloscope.

**Power Pin Measurements** If the decoupling capacitors are not mounted, the device will naturally see drops in its voltage supply as measured at the power pin, since the power distribution system is unable to provide a low-impedance source close to the power pin. For the SASEBO-GII board, the measurement is taken on the underside of the board, on the positive pad of the decoupling capacitor specified. Each decoupling capacitor pad aligns directly with the power pin of the cryptographic FPGA, see Fig. 6

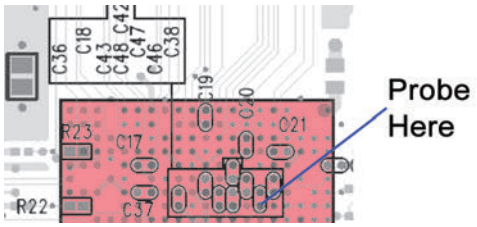


**Fig. 6.** The decoupling capacitors line up directly with the power pins; if the capacitors are not mounted this provides a good source to measure the ripple on the voltage rail due to high-frequency power demands. The pink square is the location of the chip under attack on the top side of the board.

**Inductive Wrapping** The proposed inductive wrap method uses 7 wraps of AWG34 magnet wire around the decoupling capacitor C46. One end of the magnet wire is soldered to the negative pad of the capacitor. The other side of the wire connects through a low-noise amplifier (ZFL-1000LN) for the DSO, or directly to the OpenADC. Fig. 7 shows a detailed photo of this setup.

### 6.2 Measurement Results

Results for the Global Success Rate (GSR) of the CPA attack are shown in Fig. 8; Table 2 provides the number of traces require for the GSR to exceed 0.8. All of these measurements are taken with the Agilent DSO, a comparison between the DSO and OpenADC platform is given in Fig. 10.

**Current Shunt, H-Field Probe** In order to confirm the test setup, several of the results duplicated work done elsewhere. For example, the shunt measurement on the entire VCC-INT power system was expected to perform poorly when the

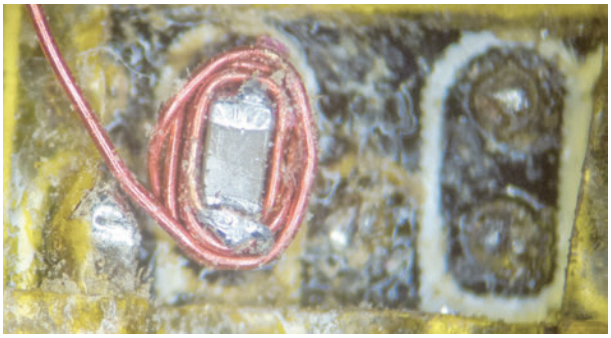

**Fig. 7.** 7 wraps of AWG34 magnet wire around a 0402 capacitor. The yellow visible around the capacitor is Kapton tape used to isolate the rest of the PCB.

**Table 2.** Traces required to achieve 1st order Global Success Rate (GSR) higher than 80% with a Correlation Power Analaysis (CPA) attack for several measurement techniques.

| Measurement Method | Traces for GSR $>$ 0.8 |
|---|---|
| VCC-INT Shunt Measurement | 4800 |
| VCC-INT Shunt Measurement w/ decoupling | $>$5000 |
| Inductive Pickup w/ decoupling w/ amplifier | 3450 |
| H-Field Probe w/ decoupling w/ amplifier | 3850 |
| Decoupling capacitor shunt w/ decoupling | 4350 |
| Voltage Probe | 4550 |

single decoupling capacitor was mounted. This can be seen by comparing Fig. 2-A to Fig. 2-B. In addition, the H-Field probe should provide better results than the shunt measurement in order to agree with [5]. This is confirmed by looking at Fig. 2-D.

**Inductive Wrapping** It can be seen that the proposed measurement technique requires the smallest number of traces to achieve a GSR higher than 80% ($>$0.8). The signal from this technique is considerably stronger than with the H-field probe. The measured signal from the inductive wrap technique is about 10x larger in amplitude (Vp-p) than that from the H-field probe.

The stronger signal slightly relaxes the requirements of the amplifier, and means that the resulting SNR will be better compared to the H-field probe. The results here show slightly better performance for the inductive wrapping technique compared to the H-Field probe due to this improved SNR. The number of wraps used does appear to impact the GSR, as shown in Fig. 9. Here 7 wraps results in a better GSR than 2 wraps - the 7 wraps again resulted in a stronger signal, reducing noise in the measurement front-end.

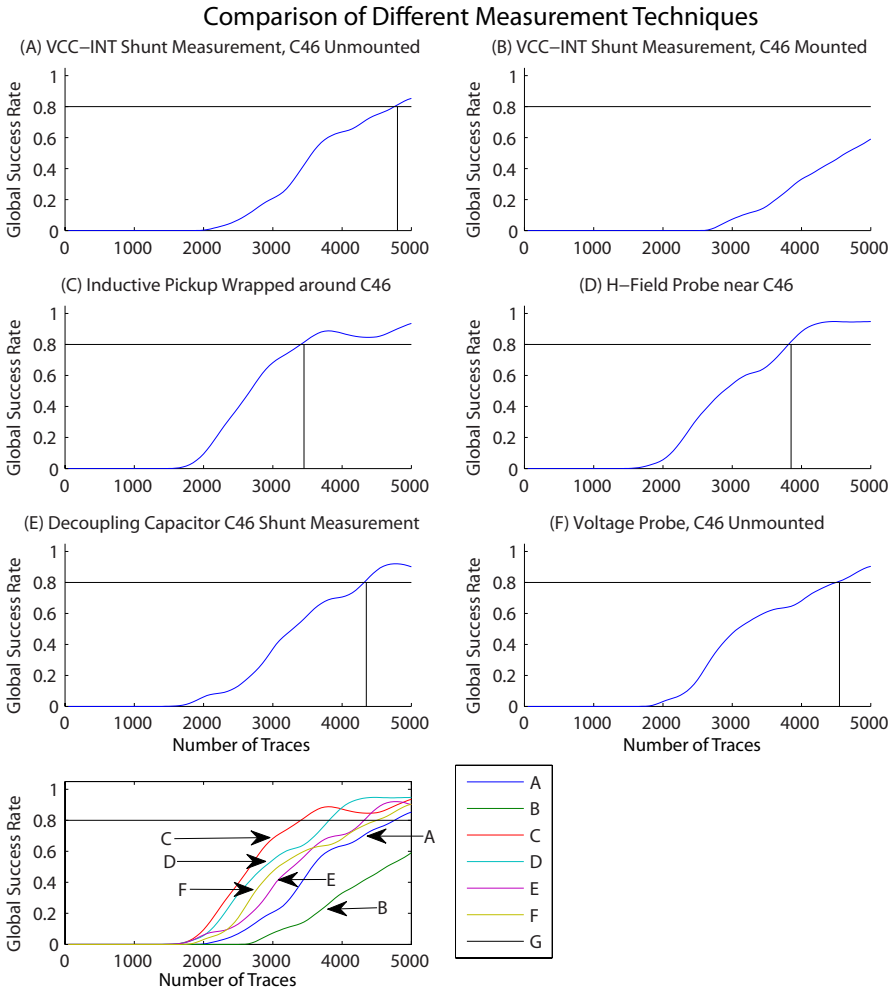


**Fig. 8.** The first order global success rate (GSR) vs. the number of traces processed for a simple CPA attack. *A* through *F* show different measurement techniques; the final figure shows a comparison of the first-order GSR for each of the measurement techniques. The vertical lines show the intercept of the 1st order GSR exceeding 0.8, where the numeric value of these intercepts is given in Table 2.

**Shunt on Decoupling Capacitor** The results here confirm the decoupling capacitor measurement does provide a significant improvement over attempting to measure the current drawn through the entire system. The performance is still lower than electromagnetic techniques; it is assumed that adding the shunt reduces the impedance of the capacitor, thus reducing the current which flows through it. In [16] a Current Transformer (CT) is used instead of a resistive

shunt. Inserting the CT would also slightly increase the impedance, since the CT must be clamped around a wire in series with the decoupling capacitor.

**Voltage Probe** The voltage probe is an extremely simple method of measuring local variations in the current demand. It does require the decoupling capacitor to be removed: for the best signal it would likely demand all nearby capacitors to be removed, as the nearby capacitors provide some additional decoupling that dampens the signal. For devices under attack which require the decoupling capacitors to run, this method may not be possible.

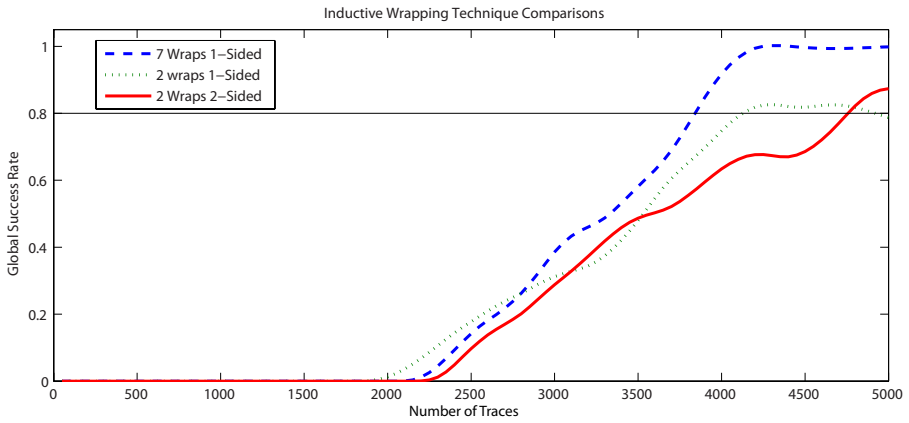


**Fig. 9.** Comparison of different variations of the inductive wrapping technique. The maximum number of wraps was set based on the physical ability to keep the wraps around the decoupling capacitor. An '1-sided' wrap has one end soldered to the ground pad of the capacitor as in Fig. 7, where a '2-sided' wrap has both ends of the wrapping wire connected to the oscilloscope as in Fig. 13. Appendix B provides some information about the '1-sided'/'2-sided' wrapping.

### 6.3 OpenADC Measurement Results

The results in Fig. 10 show that the OpenADC performs well using the inductive wrapping technique. The OpenADC is only sampling at 96 MSPS - but the sampling clock is synchronized to the device clock. When the sampling clock is not synchronized, it fails to recover the encryption key (GSR = 0). This agrees with previously published results on a similar board, which showed a failure of the attack at 100 MS/s [11]. The reference measurement at 2 GS/s is using the oscilloscope's internal timebase; that is to say a timebase that is unsynchronized to the device clock.

The OpenADC has fine granularity on the gain of the input signal, along with the full-scale reference voltage for the ADC. The DSO by comparison does

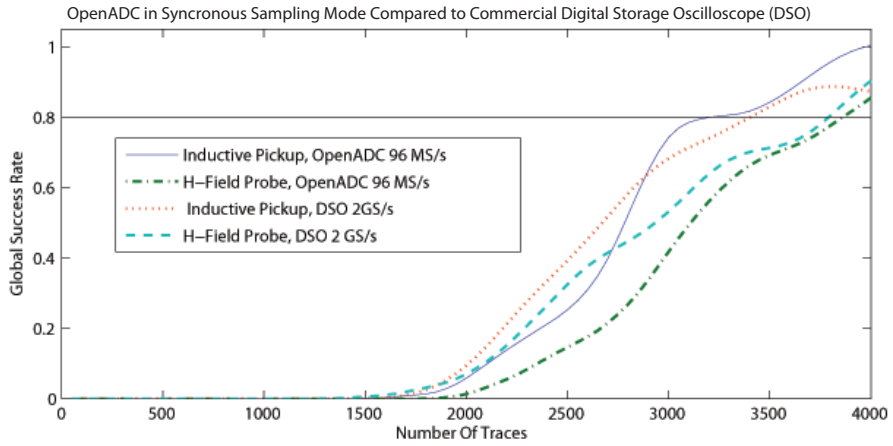


**Fig. 10.** Comparison of GSR for traces gathered with the OpenADC and a normal Digital Storage Oscilloscope (DSO), for both H-Field probe and inductive wrapping.

not provide such fine granularity on the input scaling. For the inductive wrap technique it is expected that this partially contributes to the slightly better performance of the OpenADC: the number of bits used to represent the full-scale signal is higher with the OpenADC compared to the DSO, since the OpenADC allows adjustment of the signal to reach closer to the full-scale range of the ADC input.

## 7 Conclusions

Previous work in side-channel analysis has shown that the electromagnetic (EM) field provides better results than a current shunt. The EM probe, however, suffers from being more complex to use: it requires careful positioning if repeatable experiments are necessary, requires a Low Noise Amplifier, and often requires an expensive high-speed oscilloscope.

This work has shown a low-cost alternative that solves both problems: rather than using a probe which must be positioned, the probe is built around the decoupling capacitors, which will naturally have most of the high-frequency (e.g.: clock edge) currents flowing through them. It is also trivial to report the measurement setup in a repeatable manner, requiring the following three characteristics: the part number of the decoupling capacitor, type of wire used, and number of wraps around the capacitor.

To acquire the data, it is necessary to use an ADC which is perfectly synchronized to the clock of the device under test. This relaxes the requirement of a high sample rate, allowing low-cost ADCs to be used for side-channel analysis. In addition, the complete design is released as an open-source project, making it available for use by researchers at [13].

There are several main areas of future work to which this capture board can be applied. First, the capture hardware can be extended to support more features. If the device under attack does not provide an accessible clock, a form of 'clock recovery' would be needed, where an adjustable 'local oscillator' is locked to the remote clock. This would require the addition of a Voltage Controlled Oscillator (VCO), which can be connected in a Phase Lock Loop (PLL) circuit. This would lock onto the pulses in the power traces which are occurring at the clock edge. Secondly, the OpenADC can be used as part of a hardware implementation of attacks. Attacks could be implemented on the FPGA itself: rather than sending the traces to the computer, they would simply be processed in real-time. This real-time processing would simplify attacks which require a considerable amount of traces, since there is no requirement to store them as an intermediate step. Finally, experimentation into different analog front-end processing, such as different filters, can easily be performed with the OpenADC.

**Acknowledgments** Funded in part by NSERC Canada Graduate Scholarship. Thanks to Pankaj Rohatgi of *Cryptography Research Inc.*, and Akashi Satoh of *National Institute of Advanced Industrial Science and Technology (AIST)* for donation of the SASEBO-GII used in this work.

## References

1. Kocher, P., Jaffe, J., Jun, B.: Differential Power Analysis. In: Advances in Cryptology – CRYPTO 99, Springer (1999) 388–397
2. Chari, S., Rao, J., Rohatgi, P.: Template attacks. Cryptographic Hardware and Embedded Systems – CHES 2002 (2003) 51–62
3. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. Cryptographic Hardware and Embedded Systems – CHES 2004 (2004) 135–152
4. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic analysis: Concrete results. In: Cryptographic Hardware and Embedded Systems – CHES 2001, Springer (2001) 251–261
5. Standaert, F., Archambeau, C.: Using subspace-based template attacks to compare and combine power and electromagnetic information leakages. Cryptographic Hardware and Embedded Systems – CHES 2008 (2008) 411–425
6. Jun, B., Kenworthy, G.: Is Your Mobile Device Radiating Keys? In: RSA Conference 2012. (2012)
7. De Mulder, E.: Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices. PhD thesis, KU Leuven (2010)
8. Mateos, E., Gebotys, C.: Side Channel Analysis using giant magneto-resistive (GMR) sensors. In: International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE). (2011)
9. Duc, G., Guilley, S., Sauvage, L., Flament, F., Nassar, M., Selmane, N., Danger, J.L., Graba, T., Mathieu, Y., Renaud, P.: Results of the 2009-2010 "DPA contest v2". In: International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE). (February 2011)
10. Carluccio, D.: Electromagnetic side channel analysis for embedded crypto devices. Master's thesis, Ruhr University Bochum (2005)

11. Souissi, Y., Danger, J., Guilley, S., Bhasin, S., Nassar, M.: Embedded systems security: An evaluation methodology against side channel attacks. In: Design and Architectures for Signal and Image Processing (DASIP), 2011 Conference on, IEEE (2011) 1–8
12. Agilent Technologies: Triggering Wide-Bandwidth Sampling Oscilloscopes For Accurate Displays of High-Speed Digital Communications Waveforms. (2005)
13. O'Flynn, C.: Openadc. `http://www.newae.com/openadc` (2012)
14. Smith, D.: Signal and noise measurement techniques using magnetic field probes. In: Electromagnetic Compatibility, 1999 IEEE International Symposium on. Volume 1., IEEE (1999) 559–563
15. Katashita, T., Satoh, A., Kikuchi, K., Nakagawa, H., Aoyagi, M.: Evaluation of dpa characteristics of sasebo for board level simulations. International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE) (2010) 36–39
16. Danis, A., Ors, B.: Differential power analysis attack considering decoupling capacitance effect. In: Circuit Theory and Design, 2009. ECCTD 2009. European Conference on, IEEE (2009) 359–362
17. Faraday, M.: Experimental researches in electricity. Phil. Trans. R. Soc. Lond. **122** (1832) 125–162
18. Weaver, J., Horowitz, M.: Measurement of via currents in printed circuit boards using inductive loops. In: Electrical Performance of Electronic Packaging, 2006 IEEE, IEEE (2006) 37–40
19. Weaver, J., Horowitz, M.: Measurement of supply pin current distributions in integrated circuit packages. In: Electrical Performance of Electronic Packaging, 2007 IEEE, IEEE (2007) 7–10
20. Li, L., Kim, J., Wang, H., Wu, S., Takita, Y., Takeuchi, H., Araki, K., Fan, J.: Measurement of multiple switching current components through a bulk decoupling capacitor using a lab-made low-cost current probe. In: Electromagnetic Compatibility (EMC), 2011 IEEE International Symposium on, IEEE (2011) 417–421
21. Moradi, A., Mischke, O., Eisenbarth, T.: Correlation-enhanced power analysis collision attack. Cryptographic Hardware and Embedded Systems - CHES 2010 (2011) 125–139
22. Satoh, A.: Side-channel attack standard evaluation board (sasebo) - dpa contest. `http://www.morita-tech.co.jp/SASEBO/en/index.html` (2011)
23. Standaert, F., Malkin, T., Yung, M.: A unified framework for the analysis of side-channel key recovery attacks. Advances in Cryptology-Eurocrypt 2009 (2009) 443–461
24. Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., Shalmani, M.: On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme. Advances in Cryptology-CRYPTO 2008 (2008) 203–220

## Appendix A: Examples of Decoupling Capacitor Measurements

Where the SASEBO-GII board provides provisions for using a current shunt power measurement, commercial boards typically provide no such considerations. In addition commercial boards often contain extensive decoupling capacitors which dampen the signal measured with a current shunt. As an example the board shown in Fig. 11 has been modified to add a current shunt along with an

inductive pickup wrapped around one of the decoupling capacitors. The power trace is shown in figure Fig. 12 measured with the current shunt, and also the inductive wrapping. Note that the average of many traces shows the current shunt contains no visible signal, where the inductive wrap has picked up a very clean signal corresponding to different instructions being executed.

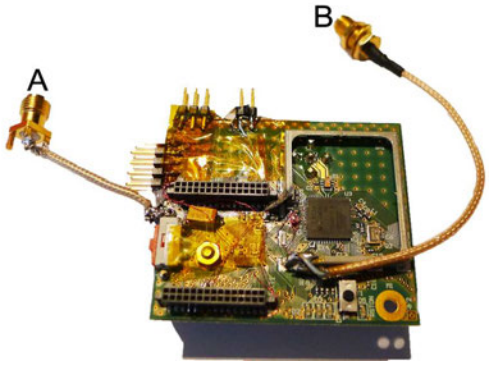


**Fig. 11.** Microcontroller board which supports a classic resistive shunt measurement at *(A)* and an EM measurement using the inductive wrap at *(B)*.

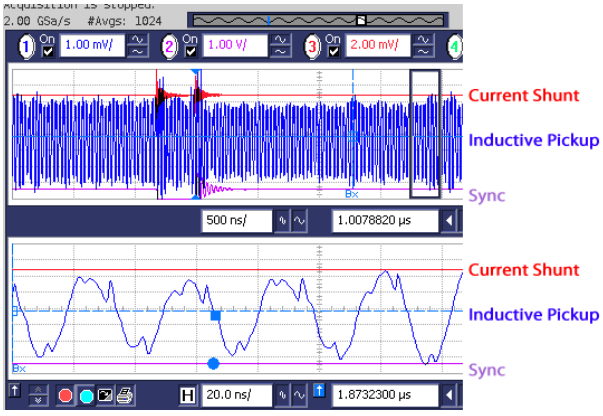


**Fig. 12.** A comparison of current shunt and inductive pickup on a commercial board with extensive and power supply decoupling. The program being executed switches from performing lower power load immediate instructions to higher power multiply instructions at time 1875 nS from the trigger. Red (top) is current shunt, blue (middle) is inductive pickup. Lower half of figure shows zoomed in area from black box in top half.

Another example of using the inductive wrapping is with small keyfob transmitters, such as those using the KeeLoq algorithm, which have been shown to be vulnerable to power analysis [24]. The decoupling capacitor is easily identified in Fig. 13, and a probe can be built around it.

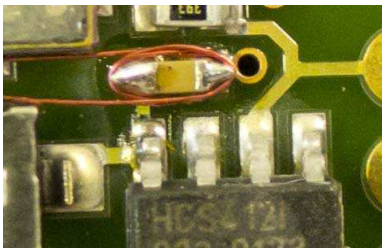

**Fig. 13.** Analyzing a small security device

## Appendix B: Physical Considerations of Wrapping

A side-view of a typical SMD solder joint is shown in Fig. 14. It should be apparent that wrapping a fine magnet wire around this will be difficult, as the shape of the fillet will naturally push the wire up and off the capacitor as it is tightened. The author used a low-temperature soldering iron to put spikes towards the top side of the SMD joint. These spikes had the effect of providing a 'core' around which to wrap the magnet wire.

This process can also be assisted by using a portable dispenser for the wire - for example the Verowire Pen. The choice to solder one end of the wire to the negative pad of the decoupling capacitor results in better mechanical stability, and simplifies connection of the coaxial cable. Extensive testing showed this resulted in a very clean signal; however all the boards tested had full ground planes. One should verify the ground connection of the capacitor will provide a clean reference path.

**Fig. 14.** Winding the pickup coil around an arbitrary decoupling capacitor is achieved by adding a form with solder. In addition the choice to connect one side of the coil to the ground of the circuit simplifies connection of the oscilloscope in some situations.