LOCALIZATION OF ELECTROMAGNETIC SOURCES IN COMPLEX PROCESSORS

A Thesis
Presented to
The Academic Faculty

by

Eric Pollmann

In Partial Fulfillment
of the Requirements for the Degree
Electrical Engineering in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
May 2017

LOCALIZATION OF ELECTROMAGNETIC SOURCES IN COMPLEX PROCESSORS

Approved by:

Dr. Alenka Zajić, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Gregory Durgin
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: December 15, 2016

ACKNOWLEDGEMENTS

I would like to thank Dr. Alenka Zajić for starting me on this project, and guiding me through the research process. I could not have imagined a better research advisor, and it has been a rewarding three years. I also owe great thanks to Dr. Rob Callan who provided insightful conversations, and was always available for consultation when I was stuck on part of my project. This thesis would not have been possible without their help. I would also like to thank my friends for making life enjoyable. Finally, I would like to thank my parents for being very supportive during the writing of this thesis, and also my younger sister for asking all the tough questions.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page

SUMMARY

Recent advances in computer hardware security research have shown that electronic devices are vulnerable to electromagnetic (EM) side-channel leakage. An attacker can steal sensitive information from an electronic device that is not connected to the network just by measuring the electromagnetic emanations produced by the device. The feasibility of a successful EM side-channel attack has grown significantly in recent years with the reduction in cost of electronic test equipment and the proliferation of electronic devices. Smartcards, cellphones, and laptops can be susceptible to side-channel attacks, and with the trend towards internet-of-things (IoT) and millions of connected devices, the side-channel will become of increasing security importance. While most of the current literature in electromagnetic side-channels focuses on demonstrating novel attack methods on various devices, relatively little research focuses on characterizing the EM emanations. Research presented in this thesis aims to develop a metric to measure the side-channel energy per instruction available to an attacker. The importance of this is to understand the effect of instruction level events (i.e. ADD, LOAD, NOP) on the electromagnetic emanations from a cellphone. Understanding the correlation between the instruction run and the corresponding electromagnetic footprint can help to understand which operations cause the greatest amount of electromagnetic leakage as well as provide a basis of measurement. In addition, a method of localization is proposed to identify the source of the EM emanations. A magnetic dipole equivalent source model is proposed and measurement results are compared with simulation results of the model. These results aim to provide a deeper insight into the nature of electromagnetic side-channels as well as provide hardware and software designers with the information needed to combat unnecessary EM emanations.

CHAPTER 1

INTRODUCTION

Introduction to Side-Channels

A side-channel is a type of an attack that exploits the information obtained purely from hardware leakages during normal operation of an electronic device. This does not require access to the device through a network connection, and as a result, side-channels are often able to by-pass normal network security measures. The susceptibility devices to side-channel leakage has been known about for many years, but the feasibility of a successful attack has grown greatly in recent years with the reduction in cost of electronic test equipment and the proliferation of electronic devices. Smartcards, cellphones, and laptops can be susceptible to side-channel attacks, and with the trend towards internet-of-things (IoT) and millions of connected devices, the side-channel will become of increasing security importance.

Types of side-channel attacks include but are not limited to power analysis, timing analysis, and electromagnetic emanations analysis. Power analysis focuses on the total power consumption of a hardware device. A theoretical attack would have an attacker place a power (current) meter at the power supply of a device, i.e. at the power cord for a laptop, and then monitor the power usage with an oscilloscope. Timing analysis focuses on the computational time it takes a processor to perform certain tasks. This is mainly exploited during a cryptographic encryption in which queries are sent to the computer to retrieve the cryptographic key by measuring the time it takes for the computer to perform the encryption and respond. Electromagnetic side-channel attacks exploit the electromagnetic radiation produced by an electronic device. As opposed to timing and power, electromagnetic emanations can be received and measured at a distance away from the source, making it ideal for eavesdropping.

Covert-Channel Attack

In contrast to side-channels, which are used to eavesdrop on a computing device, covert-channels are used to send secret information. An electromagnetic covert-channel is particularly intrusive attack because it is very difficult to detect a malicious code that is inserted into the device under attack and leaks sensitive information through an EM side-channel. For example, an attacker contributes to an open-source code and inserts the malicious code intended to leak sensitive user information. The malicious code passes the audit, because it does not access any network or hardware peripherals that are uncommon for such a device. Once the code gets distributed to targeted cellphones, the attacker can then monitor the channel and demodulate the encoded signal while the user under attack has no knowledge of such a signal being leaked.

Detecting and Measuring Side-Channel Signals

The side-channel electromagnetic energy radiated by an electronic device is very difficult to measure. The energy spread out in frequency content, making it indistinguishable from environmental EM noise. A methodology can be used to measure side-channel energy that exploits repetition in code (for- and while-loops), in which operations exciting the same circuitry for extended amounts of time will produce a strong electromagnetic signal at the frequency of operation (duration of the code loop). This methodology is explained in greater detail later, and will provide a metric by which the energy per instruction (ESE) can be measured.

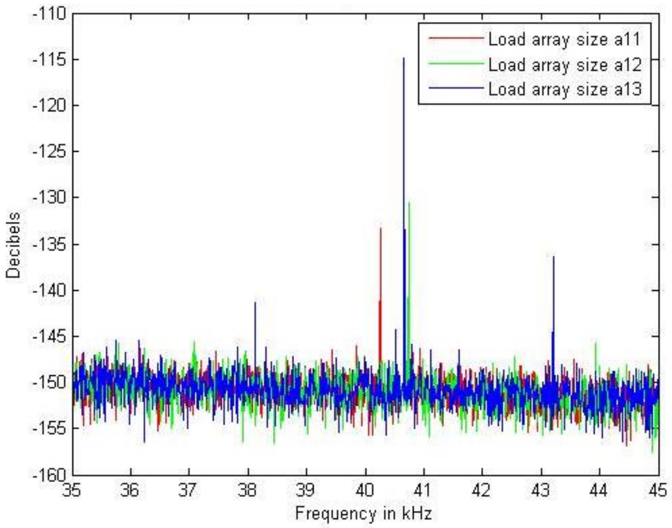


Figure 1. A spectrum of ESE generated using “covert-channel” approach proposed in [10,11].

During normal operation of the phone, there is no signal at this frequency; however, the attacker forces signal at this frequency to leak sensitive information. It is only covert because the existence of the communication channel is unbeknownst to the victim. The victim can view the frequency spectrum of his or her phone, but will not be able to easily tell if the phone is under a covert channel attack. A broadband scan of the frequency content being emitted during operation of the phone from a few kilohertz to a few gigahertz shows many frequency peaks; however, it is difficult to know which is leaking sensitive information, if any. The channel is visible to anyone that is “snooping” and knows where to look.

Overview

The findings in this research aim to develop an understanding of the physical causes of side-channel leakage and to demonstrate the viability of such an attack. First, a methodology for measuring the electromagnetic side channel energy available to an attacker for instruction level events is proposed. The importance of this is to understand the effect of instruction level events (i.e. ADD, LOAD, NOP) on the electromagnetic emanations from a cellphone. Understanding the correlation between the instruction run and the corresponding electromagnetic footprint can help to understand which operations cause the greatest amount of electromagnetic leakage as well as provide a basis of measurement. Then, a methodology for approximating an equivalent magnetic dipole source for electromagnetic side-channel signals is proposed and tested. This is important to understand the equivalent path a strong, emanating signal takes when it gets processed. This path depends on a significant number of factors, but general conclusions can be made about the nature of these signals. Finally, a review of the results and a summary of electromagnetic side-channels aims to provide a deeper insight into the fundamental causes of the EM leakages.

All this information is important for hardware engineers to design shielding techniques that attack the problem at its source. Hardware shielding implementations can be prioritized for particularly leaky components. Also, assembly programmers can avoid the unnecessary use of certain instruction level operations, such as memory accesses, that leak valuable information. Solutions that focus on a single implementation of a cryptographic algorithm do not provide a comprehensive understanding of the cause of EM side-channels, and general solutions require a greater understanding how they are produced.

CHAPTER 2

LITERATURE REVIEW

A side-channel is a type of attack that exploits the information obtained from hardware leakages during the physical implementation of a cryptographic algorithm. Types of side-channel attacks include power analysis, timing analysis, and electromagnetic emanations. While power and timing have been studied extensively, electromagnetic emanations provide a more powerful channel of attack. As opposed to power, electromagnetic emanations can be received and measured at a distance away from the source, making it ideal for eavesdropping. In addition, electromagnetic signals are more powerful, and different components leak different compromising information providing an attacker with multiple sources or channels to attack [1].

An electromagnetic side-channel attack is a non-intrusive attack in which the computer activity is monitored at a distance using an EM measurement setup. Smartcards and computer monitors have been shown to be susceptible to EM side-channels [2] [3]. Also, increasingly more complex processors such as field programmable gate array (FPGA) processors running AES encryption algorithms have been attacked [4]. Most recently, electromagnetic fields from laptops and desktops have been characterized, and implementations of cryptographic algorithms have been attacked [5]. However, while there has been research in methods of attacking processors via electromagnetic side-channels, there is still relatively little knowledge as to what exactly produces these side-channels or how they are produced.

Electromagnetic side-channels were first documented in the open literature as early as the 1960's. The consensus at the time was that the attacks were unreliable and could only be realized with expensive hardware. As a result, electromagnetic side-channel shielding and countermeasure techniques remained confined to defense and intelligence use and TEMPEST guidelines were put in place for military equipment to limit the potential for information leakage due to electromagnetic (EM) emanations [6]. There was little public and commercial interest until 1985, when Wim van Eck showed that an electromagnetic side-channel attack could reconstruct the information displayed on cathode ray tube (CRT) computer screens from hundreds of meters away using inexpensive hardware (< $50 worth of equipment) [3]. This was the first time commercial electronics were attacked, and there was a spike in public interest. Academic interest soon developed around providing side-channel security measures, and it led to innovative research in electromagnetic side-channel attacks and countermeasure techniques.

In particular, significant interest developed around the electromagnetic side-channels of computer processors. Computer processors execute programs and contain much of the information that is of interest to attackers. To avoid attacks, processors often run encryption algorithms to encode information. However, the implementation of these algorithms is often repetitive in nature making them susceptible to emitting electromagnetic radiation. The first work on processor side-channels focused on smartcard processors [2]. Smartcard processors have relatively few electronic connections and are simple architecturally which make them relatively susceptible to attack. For example, smartcard processors running cryptographic implementations of DES (Data Encryption Standard), COMP128, and RSA (Rivest-Shamir-Adleman) were attacked successfully and each time the complete encryption key material was obtained [7].

Research extended to more complex processors, and methods were developed for attacking cryptographic implementations in field programmable gate arrays (FPGA) and laptops. FPGA processors running an implementation of the Advanced Encryption Standard (AES) were successfully attacked using differential electromagnetic analysis [4]. More recently, laptops running RSA and El-Gamal encryption algorithms were successfully attacked through electromagnetic side-channels and the entire key was retrieved. Furthermore, the laptop attack was performed with inexpensive, low-bandwidth, low-frequency hardware and targeted the side-channels of the laptop without physical access to the device [5]. These successful attacks on complex processors demonstrate that electromagnetic side-channels are powerful enough to attack processors with multiple chips, high clock rate, and asynchronous mechanisms. Most importantly, all of this information is gathered without physical connection to the device other than the propagation of EM waves.

Once it was proven that electromagnetic side-channels provide a viable method of attack on computer processors, interest developed in designing countermeasures against such attacks. Usually, papers presenting a method of side-channel attack will also present general countermeasure methods and techniques. Countermeasures can be either hardware or software specific. Main hardware countermeasures focus on shielding techniques. Shielding is a method of enclosing particularly leaky electrical components so that the EM radiation does not propagate as far. Other techniques involve intelligent circuit design board layout to reduce electromagnetic leakage caused by processor activity. VLSI design flow can be designed to effectively shield integrated circuits from side-channel analysis by obtaining constant power dissipation of secure ICs [8]. On the software side, countermeasures mainly focus on asynchronous timing mechanisms and irregular cache accesses [9].

While there has been extensive research in electromagnetic side-channels, there is still relatively little knowledge as to what exactly produces these side-channels or how they are produced. Preliminary research showed there are effects in propagation distance depending on the activity levels and data values used in accessing memory [10]. Depending on the cache level hit or off-chip memory access, EM side-channel attacks could be performed on these systems up to several meters and through structural walls. A metric for measuring the signal available to attacker (SAVAT), was proposed to compare electromagnetic emanations of different machine level instructions. The results confirm off-chip memory accesses produce the strongest electromagnetic leakages [11].

This research proposes to extend current research in the area of EM side-channels by creating a methodology of measuring the electromagnetic side channel energy available to an attacker for instruction level events on the FPGA processor. The development of a pairwise metric for one instruction level operation versus another would allow for the characterization of electromagnetic fields produced by the processor. For example, low-level software programmers can write code that avoids the unnecessary repetition of loops and subroutines. In addition, current intensive operations such as load and store from memory could be avoided to reduce the amount of signal produced in the source code, instead of shielding or jamming strong signals after they are produced. On the other hand, repetitive operations such as "ADD/ADD" and "SUB/SUB" should not produce a measurable signal in the frequency domain.

In addition to understanding the effect of different instruction pairs, the characterization of the strength of the EM fields coming from FPGA boards would provide information about where the strongest signals on the processor are produced. The goal is to build upon current research done on laptops and desktops and localize the electromagnetic emanations coming from the FPGA board to understand which components are particularly accessible to side-channel attacks. For precise and accurate measurements, the FPGA is used for its defined layout and accessible peripherals. Characterization and localization of electromagnetic fields will advance current research in electromagnetic side-channels and greatly benefit hardware and software designers. Instead of designing hardware and software countermeasures for specific computer systems or software implementations, solutions that attack electromagnetic side-channels at the source can greatly reduce the amount of EM leakage available to attackers.

CHAPTER 3

BACKGROUND

Electromagnetic noise is any electromagnetic signal other than the desired signal that is present in a circuit. There are many causes of electromagnetic noise in electronic circuits. An engineer must take all of these in to account when testing and evaluating if a product is market ready. However, for our purpose, we can abstract all the different factors contributing to EM emission, and model the radiated emission based on top level parameters of a digital circuit. The radiation from a digital circuit can be described as either differential or common mode.

Differential-mode radiation is a result of current flowing in through the conductors in a circuit due to normal operation of the circuit. This current loop is a small loop antenna that will radiate a near-zone magnetic field.

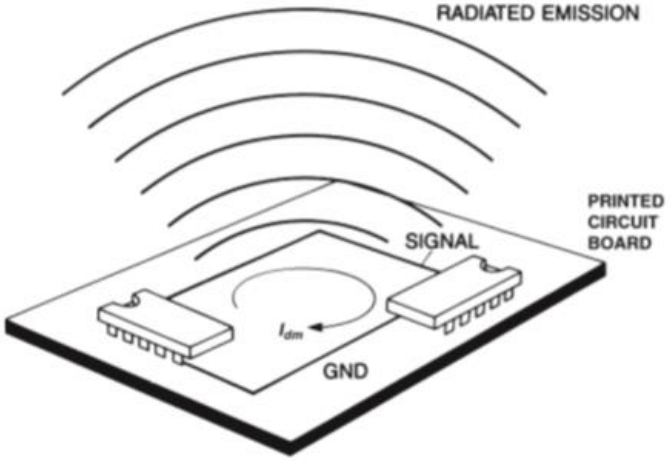


Figure 2. Differential mode radiation as illustrated in [12].

Common-mode radiation is produced when parasitics are introduced into the circuit and there is a voltage drop in the conductors in the circuit. This is usually caused when cables are connected to the circuit that have a different ground potential than that in the circuit, which creates a voltage drop, and a current that radiates a near-zone electric field.

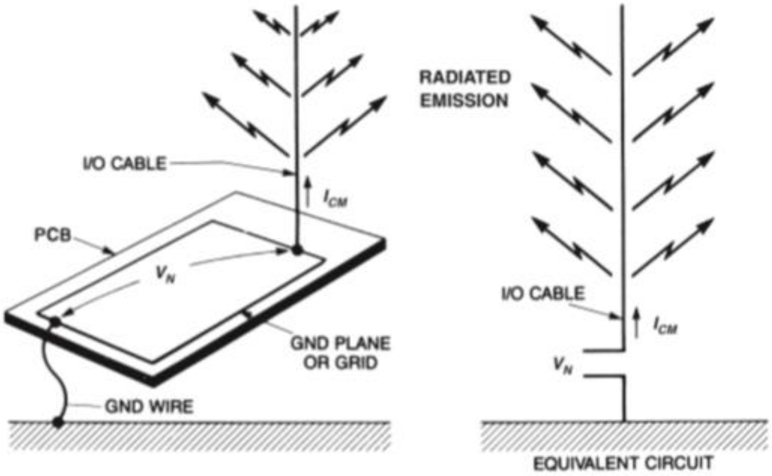


Figure 3. Common-mode radiation as illustrated in [12]

Differential-mode radiation models the radiation of a circuit during normal circuit operation, so it is of most interest to understanding EM side-channel leakage. The magnitude of the electric far-field can be approximated by the Kraus and Marhefka eqn. for a circular loop antenna over a ground plane [12].

$$E = 263 * 10^{-16}(f^2 A I_{dm})\left(\frac{1}{r}\right)\sin(\theta)$$

From the equation, it is evident that the differential-mode radiation can be suppressed by reducing the magnitude of the current, reducing the frequency of operation, or by reducing the loop area (the radiation of the small loop is dependent only on the area of the small loop and independent of the shape). A circuit board layout designer has little control over the magnitude of the current or frequency of operation of the circuit, but important consideration can be given the size of the loop. Special concern should be given to circuits in which the signal is periodic because all of the electromagnetic energy is concentrated at one frequency. For example, clock signals for the PCB operate at one frequency (usually the highest frequency on the PCB board), and so all the energy is concentrated in a few frequency bands including lower order harmonics. However, periodic signals such as the clock (CLK) signal, address latch enable (ALE), etc. and their respective EM frequency footprints are well understood, and their respective circuits are designed to minimize the amount of EM leakage each of these cause. [12]

CHAPTER 4

METHODS

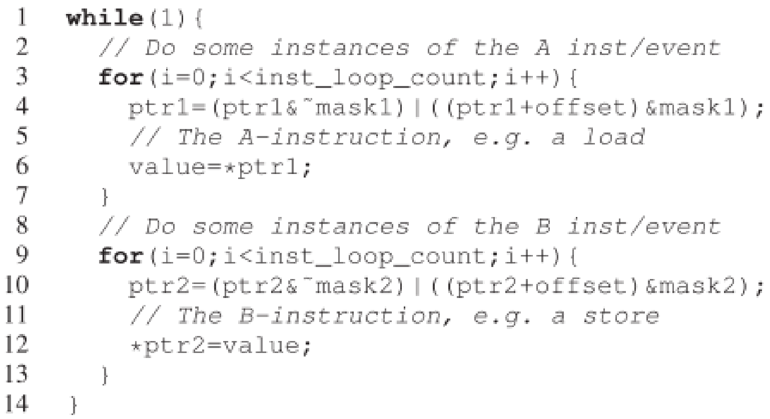
A Method for Measuring Side-Channel Energy Available to the Attacker

Measuring one instruction level event versus another is very difficult and inconsistent. The frequency domain signature of a single instruction is hardly above the noise floor or at the noise floor. A better solution for measuring the energy per instruction is to measure the signal received when running multiple instructions and divide by the number of instructions. This is done by programming the FPGA to run two loops of code, one loop for one operation and the other for another set of operations. These alternating loops of operation can be adjusted to run at some carrier frequency that is tunable by altering the number of instructions in each for loop.

Once the electromagnetic side-channel energy (ESE) is measurable, ESE values can be obtained for each instruction pair. For example, an "ADD/LDM" instruction pair can be measured and compared to an "ADD/ADD." Values can be received for nine different operations, which can be assembled into a 9x9 table for a total of 81 ESE values at a certain carrier frequency. Also, it is useful to know how the ESE values vary with frequency of operation. The side-channel energy dependence on frequency should be measured so that the electromagnetic field can be predicted at any frequency, based on a baseline frequency metric. Finally, the EM fields should be characterized by simulation and experimental measurements. EM fields can be simulated using High Frequency Structural Simulation (HFSS). The simulation results can then be compared to the measured EM field trace of the processor.

Circuit layout designers do not account for periodic circuits (loops in software) that form at runtime. It is impossible to know what signal path each circuit will take depending on what software is being run on the processor. Most of the time, the EM frequency trace caused by code at runtime is so insignificant that it does not matter how much EM leakage there is for a segment of code. For example, the electromagnetic signal produced by a single instruction pair (i.e.

"ADD/SUB") run on an FPGA processor is too small to provide conclusive measurements. However, using a different approach, the signal produced by a single instruction pair can also be calculated by running instruction A ("ADD") multiple times, running instruction B ("SUB") multiple times, and then dividing by the number of instructions. Example pseudo-code for this type of signal generation is shown in Figure 1.



```
while(1){
  // Do some instances of the A inst/event
  for(i=0;i<inst_loop_count;i++){
    ptr1=(ptr1&~mask1)|((ptr1+offset)&mask1);
    // The A-instruction, e.g. a load
    value=*ptr1;
  }
  // Do some instances of the B inst/event
  for(i=0;i<inst_loop_count;i++){
    ptr2=(ptr2&~mask2)|((ptr2+offset)&mask2);
    // The B-instruction, e.g. a store
    *ptr2=value;
  }
}
```

Figure 4. Example pseudo-code for the generation of instruction A/B alternation [11].

The code requires some key parameters as inputs including: operation type, carrier frequency, and duty cycle. Operations are selected based on common assembly level instructions run by a processor. Operations used in this experiment include on-chip instructions ADD, SUB, MULT, DIV, and NOI, as well as memory accesses, LDM, STM, LDL1, and STL1, which can be either on-chip or off-chip depending on the array size accessed. The carrier frequency can be tuned by increasing or decreasing the amount of instructions run for instructions A and B. This frequency can be tuned to find less noisy parts of the spectrum, so that more accurate measurements can be obtained. Noise is created by normal operation of the processor, and there are peaks in the frequency spectrum due to other components such as voltage regulators and clock cycles. Additionally, the duty cycle can be changed by increasing or decreasing the number of times instruction A is performed relative to instruction B. The duty cycle was maintained at 50% for the measurements in this paper.

The FPGA or cellphone can be programmed to run these two loops of instructions to produce a signal with a measureable peak in the frequency domain. Each operation takes a different route through the processor exciting different wires and transistors to perform the computation. This difference in processor activity between the two instructions produces a radio frequency (RF) signal at the desired carrier frequency that can be measured on the spectrum analyzer. An example of the time-domain waveform of instruction A versus instruction B is shown in Figure 2. Intuitively, it can be expected that if instructions A and B are the same operation, then no measureable activity can be observed due to there being no difference in processor activity.

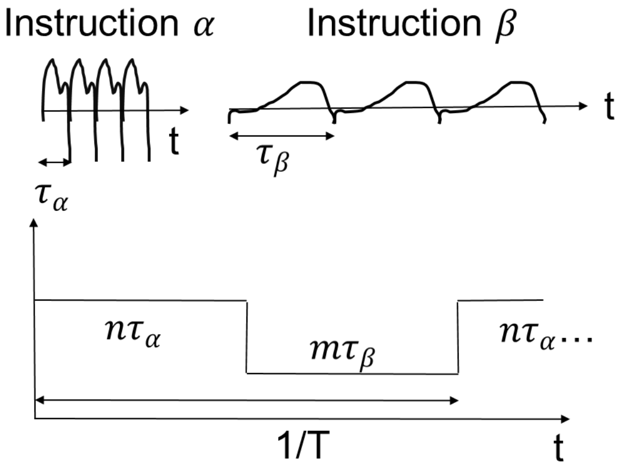


Figure 5. Time-domain waveform of instruction A versus instruction B.

A Method for Magnetic Loop Antenna Localization

Magnetic loop antennas have a size much smaller than the wavelength of the signal being transmitted or received (less than 1/10 the wavelength). If the frequency of the signal we are measuring is approximately 100 kHz, then its wavelength is well below 1/10 the wavelength of the signal. The electromagnetic fields in this experiment are measured using a magnetic induction loop probe. The probe orientations are maintained such that the x-orientation measures only the x-component of the magnetic field. Induction loop probes work according to Faraday's law of induction [13]. The electromotive force (emf), or the voltage induced in the probe is proportional to both the number of turns in the probe and the change in magnetic flux through the cross sectional area of the loop. Since the flux through the coil is non-zero along a single coordinate axis, the loop probe only measures one component of the magnetic field. The received power is measured in dBm by the spectrum analyzer and converted into Watts.

$$P = \frac{V^2}{R}$$

where P is the power received converted into Watts, R is the impedance of the spectrum analyzer (which is approximately 50Ω),

$$V = \sqrt{PR} = emf$$

$$\varepsilon mf = -N\frac{d\Phi_B}{dt} = -N\frac{dB}{dt}\pi r^2 = -\frac{NB\pi r^2}{\frac{2\pi}{f}} = -\frac{NBfr^2}{2} = \sqrt{PR}$$

N is the number of turns in the coil inductor probe, f is the frequency (which for our purpose is the alternation frequency being used in the code ~120kHz), and r is the radius of the probe.

$$B = \frac{2\sqrt{PR}}{Nfr^2} = \mu H$$

where μ is the electromagnetic permeability of the material inside the loop probe.

CHAPTER 5

EXPERIMENTAL SETUP

Electromagnetic Side Channel Energy Measurement Setup

The Altera DE1 Educational FPGA Board is programmed using Nios II 12.1 Software Build Tools for Eclipse. Measurements are taken with an orthogonal induction loop probe, shown in Figure 6.

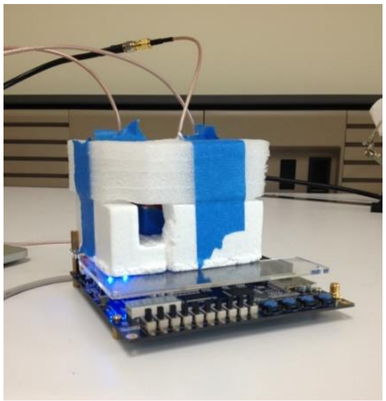


Figure 6. Picture of orthogonal loop probe taking measurements on FPGA processor.

Data is collected on the Agilent N9020A MXA Signal Analyzer, and the results are recorded on the laptop, as shown in Figure 7. Measurements are taken over multiple days and averaged to provide results that are independent of the environmental conditions of a single time and day.

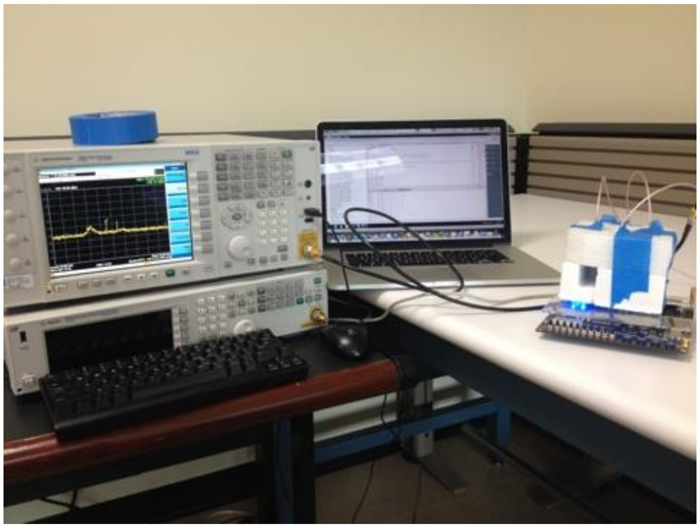


Figure 7. Picture of experimental setup.

Electromagnetic Localization Setup

Measured values of the electromagnetic field vary depending on slight changes in position or angle of the coil inductor probe measurement axis. To address this problem, the measurements were automated using Arduino controlled 2-Dimensional XY plotter with a support bracket to position the coil inductor probe anywhere within a 310x390 mm area along a z-plane above the device. The measurement setup allows for precise, high-resolution raster scans of the electromagnetic field at a constant height and angle above the target device. A picture of the measurement setup is shown in Figure 8, in which the device under test (in this case the FPGA) is alternating instruction level operations at a rate of 120kHz producing the electromagnetic side-channel signal. The XY-plotter scans an area of the device specified by the user, stopping at each position to allow the spectrum analyzer to update and record the data on the laptop.

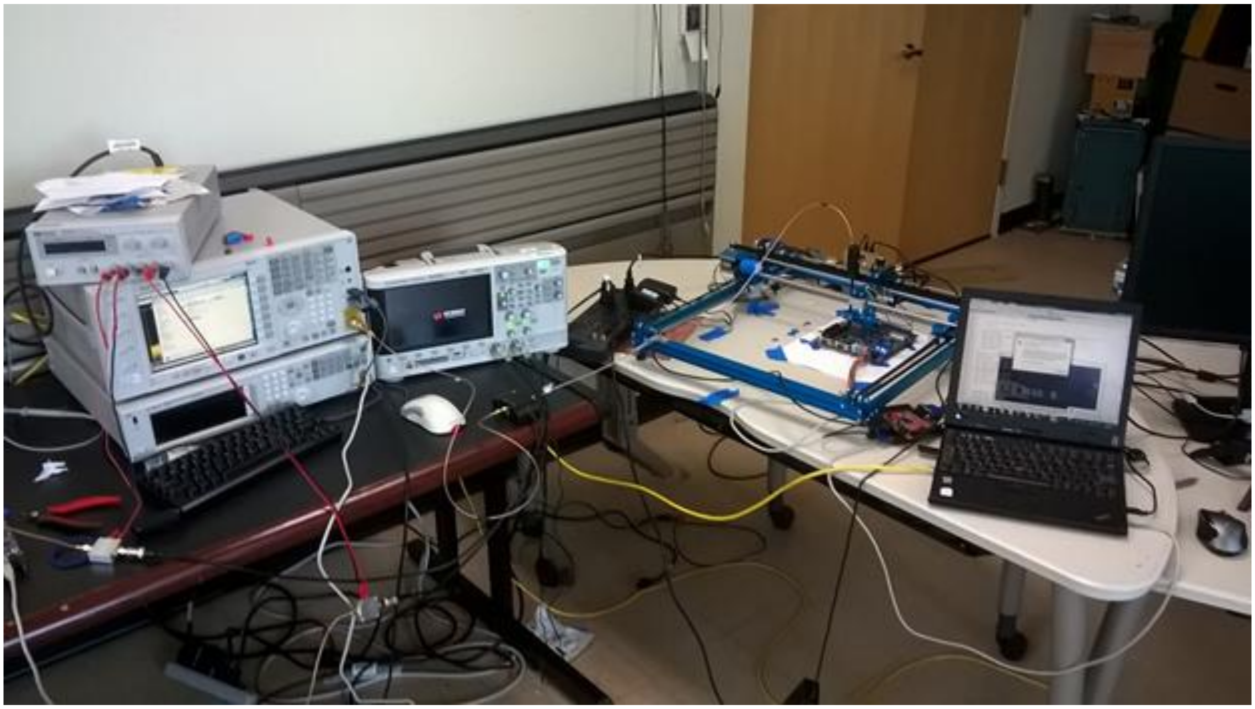


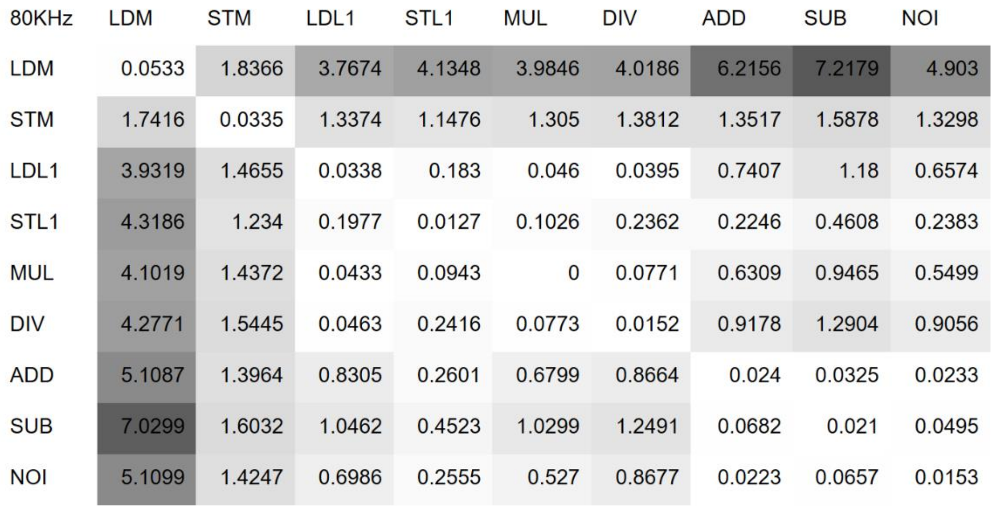
Figure 8. Photo of localization measurement setup.

CHAPTER 6

RESULTS

Measurement of ESE values from FPGA

Some preliminary results show noticeable trends in the ESE values for different instruction pairs. Table 1 shows the ESE values measured from the FPGA processor at an alternation frequency of 80 kHz. It is worth noting that the values in Table 1 are on the order of zepto-joules or 10-21 Joules. Without the methodology described in the methods section above, these ESE values are not discernable from the noise floor and are very difficult to measure.



80KHz	LDM	STM	LDL1	STL1	MUL	DIV	ADD	SUB	NOI
LDM	0.0533	1.8366	3.7674	4.1348	3.9846	4.0186	6.2156	7.2179	4.903
STM	1.7416	0.0335	1.3374	1.1476	1.305	1.3812	1.3517	1.5878	1.3298
LDL1	3.9319	1.4655	0.0338	0.183	0.046	0.0395	0.7407	1.18	0.6574
STL1	4.3186	1.234	0.1977	0.0127	0.1026	0.2362	0.2246	0.4608	0.2383
MUL	4.1019	1.4372	0.0433	0.0943	0	0.0771	0.6309	0.9465	0.5499
DIV	4.2771	1.5445	0.0463	0.2416	0.0773	0.0152	0.9178	1.2904	0.9056
ADD	5.1087	1.3964	0.8305	0.2601	0.6799	0.8664	0.024	0.0325	0.0233
SUB	7.0299	1.6032	1.0462	0.4523	1.0299	1.2491	0.0682	0.021	0.0495
NOI	5.1099	1.4247	0.6986	0.2555	0.527	0.8677	0.0223	0.0657	0.0153

Table 1. ESE values on FPGA processor at 80 kHz carrier frequency.

In addition, the frequency dependence of the ESE values of each of the operations was measured and plotted in Figure 9. The ESE values at 50, 60, 70, and 80 kHz are measured and normalized to the ESE values at 40 kHz, and trends can be determined by calculating the slope of line of best fit for each of the other alternation frequencies.

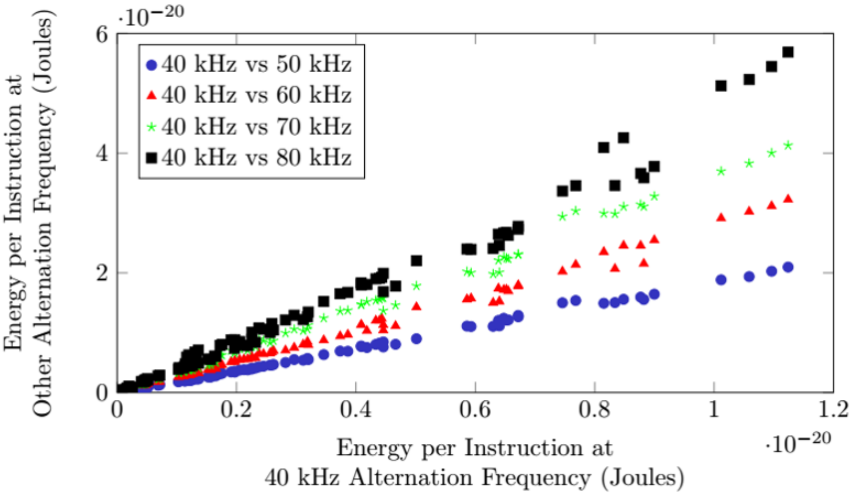


Figure 9. ESE at various alternation frequencies vs. 40 kHz alternation frequency.

Finally, the distance dependence of ESE values is determined by measuring the LOAD/ADD received power (in dBm) starting at 20 cm from the FPGA, and moving away from the FPGA in 5 cm increments and recording the results. The results in Figure 10 show the difference in the theoretical prediction of the distance decay to the actual measurement for 2 ESE values: LOAD/ADD and ADD/DIV. The theoretical model is represented by the equation: $P_r = P'_t * \left(\left(\frac{a}{r^2}\right)^2 + \left(\frac{b}{r^3}\right)^2\right)$, where a and b are scale constants that depend on a variety of factors and have units $[m^2]$ and$[m^3]$.

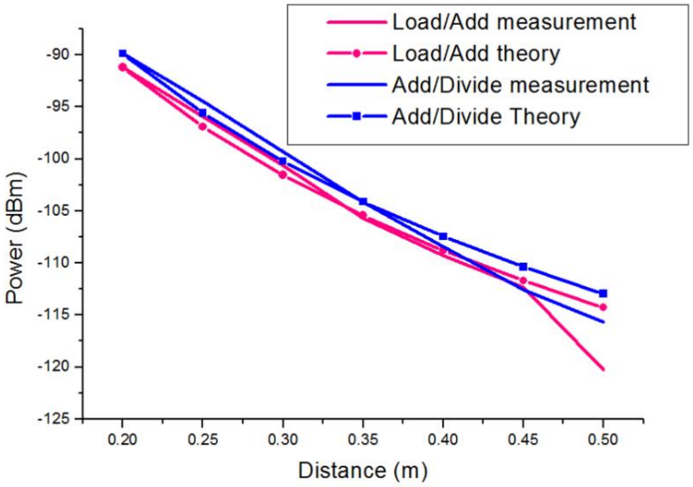


Figure 10. Experimental decay rate follows the theoretical prediction of Hertzian dipole and magnetic monopole.

Electromagnetic source localization

Some observations recorded when taking measurements of ESE values on the FPGA showed that the ESE values vary significantly based on placement and orientation making it difficult to obtain repeatable results. Therefore, some error can be reduced through automation of the measurement process. Instead of taking measurements manually, the probe can mechanically be placed in 3-D plotter and controlled to perform traces of the FPGA board. For this project, the XY plotter from Makeblock was chosen due to cost, accuracy, and Arduino controlled stepper motors.

The magnetic field at a z-plane above the loop antenna was measured experimentally and simulated in HFSS. A simple loop antenna above a ground plane was excited with 10 dBm and the field was measured at a height z=15mm above the ground plane. A simulation was done in HFSS using the same port excitation and measurement plane and the results are summarized below. Figure 11 shows the loop antenna used in this experiment. The plotter performs an automated raster scan over the ground plane at a distance of z=30mm.

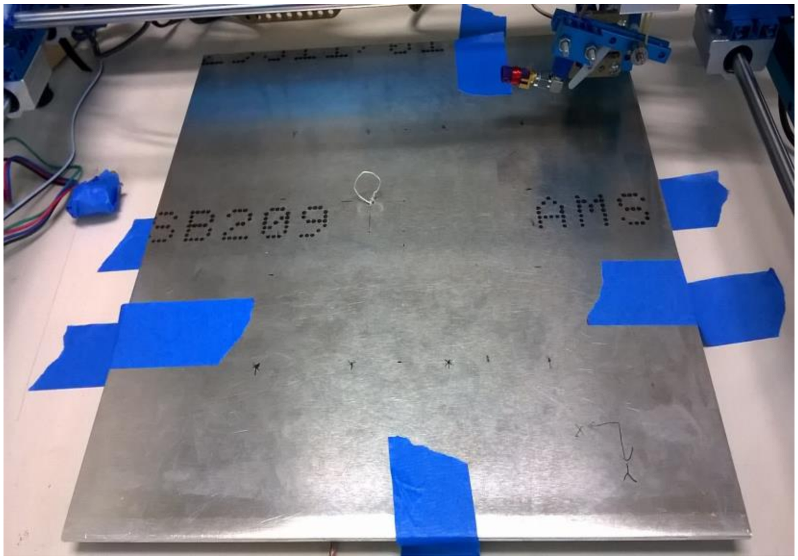


Figure 11. Loop antenna above ground plane with Makeblock XY plotter for automated measurements.

A visual representation of x, y, and z probe orientations is provided in Table 2. It shows the orientation of the coil if the observer is looking down upon the measurement setup.

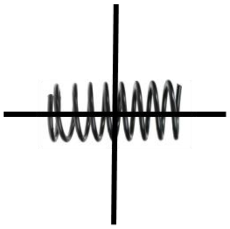
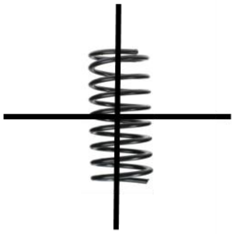
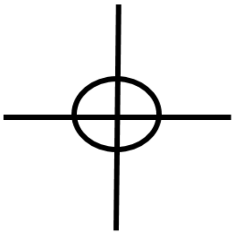
Magnetic Field	Hx	Hy	Hz
Probe Orientation			

Table 2. Model of probe orientations as seen from above.

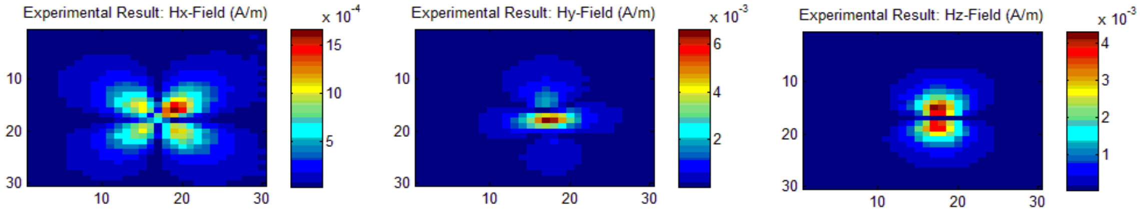


Figure 12. Experimental measurements for Hx, Hy, and Hz.

Loop Antenna Simulation Results

A picture of the HFSS model setup is shown in Figure 13. The excitation for the simulation is a current source where the current is solved for by converting 15 dBm into Watts and then solving for current using R=50Ω. The results are plotted in Figure 14.

$$P = I^2R = 15dBm$$

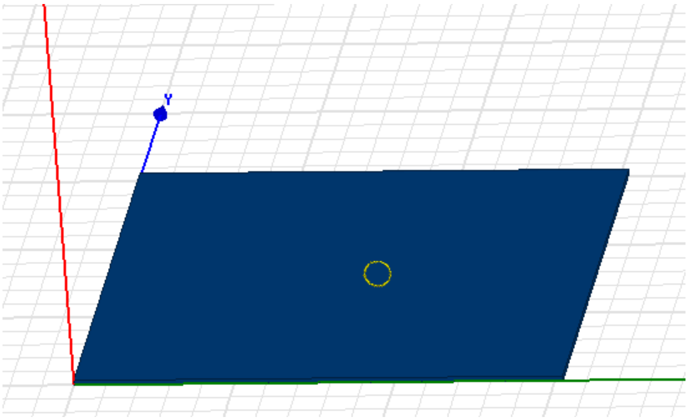


Figure 13. HFSS loop antenna model as seen from above.

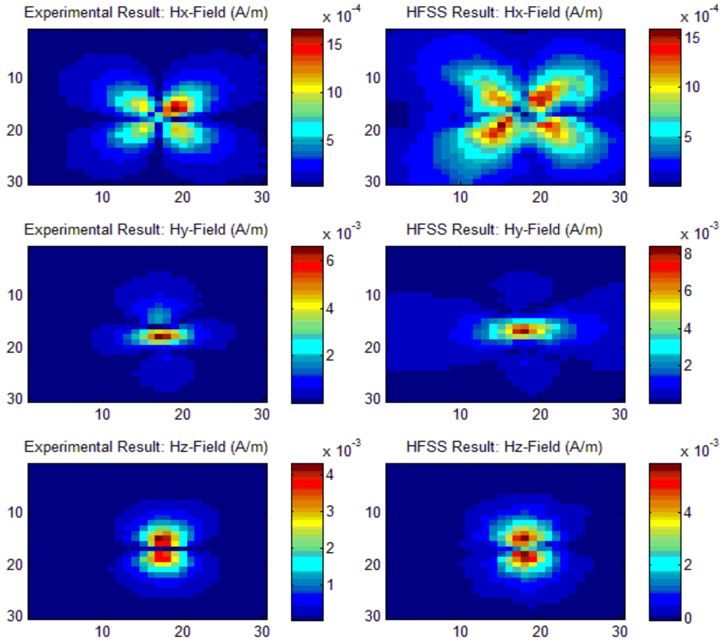


Figure 14. Experiment vs Simulation results for x, y, and z-orientations.

Cellphone Measurement Results

The Samsung Galaxy S5 was used for the localization of fields from a smartphone. The code run on the phone is the same as the code run on the FPGA and explained in the background section of the paper. The transitions in the spectral power content of the signal are shown in Table 3.

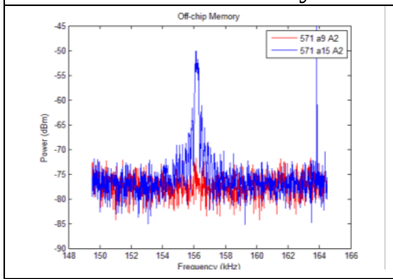
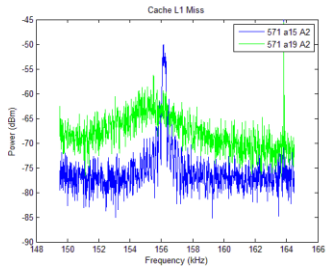
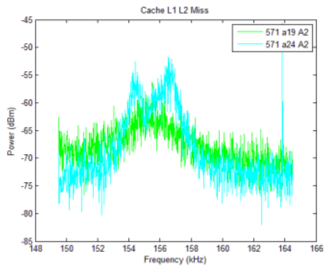
Cache L1 = 2^{15} Bytes	Cache L2 Little = 2^{19} Bytes	Cache L2 Big =2^{24} Bytes
		

Table 3. Change in spectral power of the signal due to increasing store array size.

After choosing a store array size so that there is a Cache L1 miss, but Cache L2 hit, a raster scan of the cellphone while transmitting was done in the same manner as the loop antenna in the previous section. Results of the raster field scan for the Samsung S5 cellphone are plotted in Figure 15. The left plot is the raster scan data of the cellphone while the right plot shows the contour map.

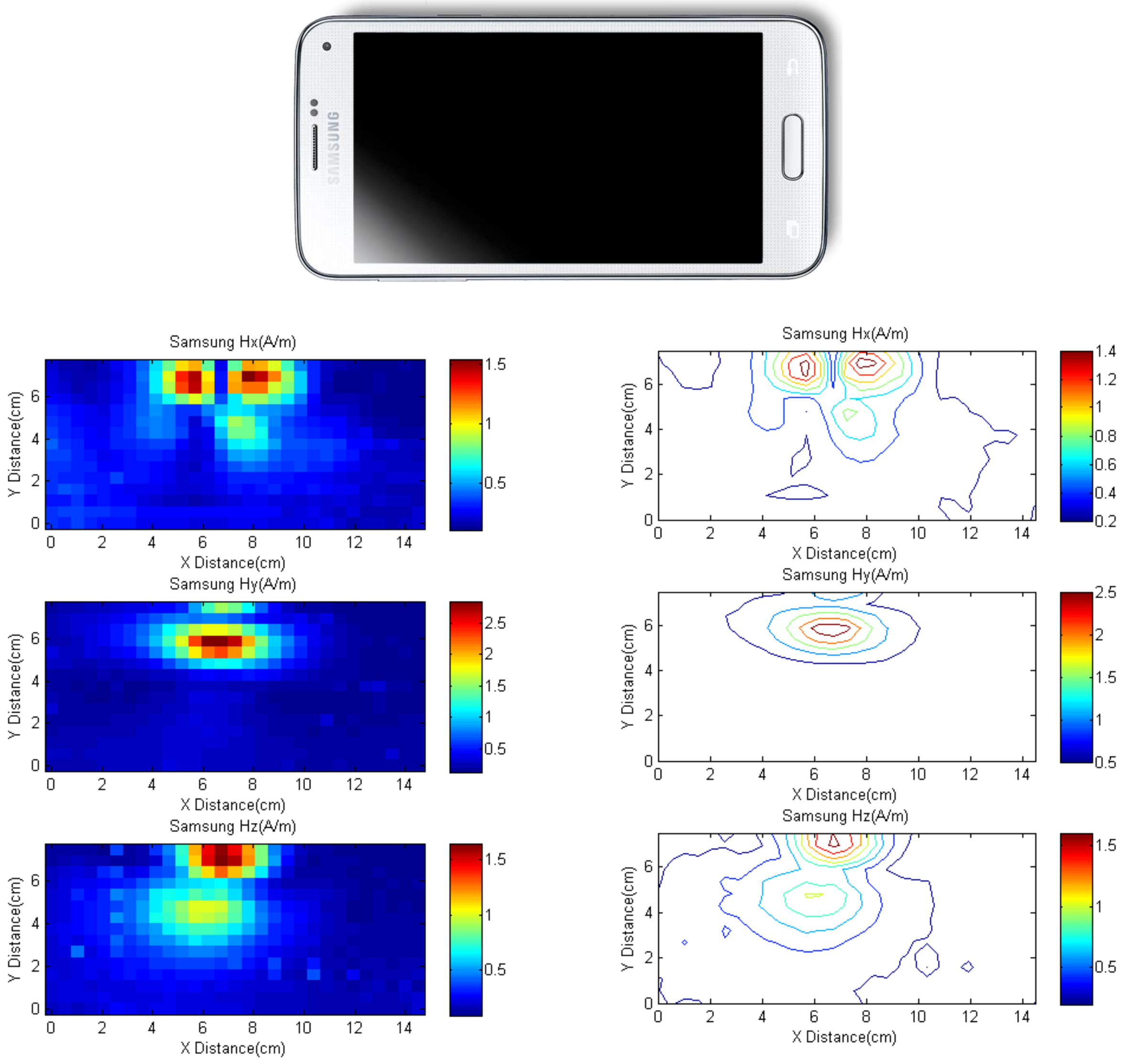


Figure 15. Plot of Samsung S5 magnetic field components shown with raster plot and contour map.

CHAPTER 7

DISCUSSION

Measurement of ESE values

The first clearly defined trend is shown on the diagonal of Table 1, starting with "LDM/LDM" and extending to the bottom right corner of the table. When the same operation (i.e. "STL1/STL1" or "MUL/MUL") is performed in both loops, little discernable signal produced. This is expected given that the signals are produced based on differences in processor activity, and the same operation does not produce much variation in processor activity. The other trend that ESE values show are "LDM" and "STM" operations produce the largest signals. This is due to memory accesses requiring more computational power and longer electrical wires to access the device's memory storage.

Another important result is determining the relationship between the ESE values at one carrier frequency versus another. For example, if the attacker knew the ESE values at 40 kHz, values can be extrapolated at other frequencies within some frequency range given some frequency constant. The data gathered in Figure 9 suggests that the ESE values scale linearly in frequency with the slope of the line giving the linear frequency scale factor for each set of frequencies.

Theoretical predictions predicted that the electromagnetic emanations from the FPGA board are due to a combination of a Hertzian dipole and magnetic monopole source. The received power is proportional to the superposition of two sources: a Hertzian dipole and magnetic monopole with decay factors of $1/r^4$ and $1/r^6$, respectively. This is important to take into consideration when designing models for simulating the EM fields coming from a processor. Figure 10 shows the experimental measurements compared with theoretical predictions. The experimental results reaffirm theoretical predictions and follow approximately the same decay rate.

Loop Antenna Results

The radiation patterns displayed in Figure 12 make intuitive sense using a simple check. If the receiving loop is oriented to pick up the x-component of the magnetic field, then there should be no flux through the receiving loop when it is directly above the transmitting antenna or when the receiving loop is moved up and down the y-axis. Also, the fields will cancel along the x-axis above the loop, and as a result the fields are strongest along the diagonals. Similar analysis for the y- and z-components of the magnetic field verify the plots.

First observation is that the radiation pattern is the same for experimental and simulation results. The results are accurate within an order of magnitude with the HFSS simulation producing slightly stronger fields. This is most likely due to parasitics in the receiving coil, as well as resistive loss in the antenna. However, these results prove that the simulation is accurate for modelling a current loop, and that by modifying the radius and position of the loop, an equivalent current loop source can be obtained to model the measured radiated emissions.

Cellphone Results

Some important challenges presented during the localization of electromagnetic signals from cellphones include multi-core processors, multiple cache sizes, and compact and complex PCB layout. The issue of cache size can be solved by performing a memory-access instruction such as load/add or store/add and measuring the EM emanations coming from the phone while increasing the size of the array being used for the memory access. At a certain array size, there is a “cache miss” and the processor has to find larger memory storage to perform the operation, resulting in an increase in the electromagnetic signal. For the Samsung Galaxy S5, it is evident through EM probing that the size of the smallest cache memory in the phone is about 215 = 32kB. When controlled for the processor clock cycle, this is the smallest array size that causes a sizeable signal, which suggests Cache L1 memory miss. Using the same procedure, it is determined that the sizes of Cache L2 Little and Cache L2 Big are 219 = 520kB and 224 = 16MB, respectively.

Because the currents in a cellphone follow traces on the cellphone PCB and do not form a perfect loop, the radiation patterns of the cellphone will not look like the ideal loop antenna. The radiation patterns can be matched by using different loop sizes, different polar and azimuthal angles, as well as modelling metallic structures in the phone in addition to its ground plane.

CHAPTER 8

CONCLUSION AND FUTURE RESULTS

In summary, this project successfully demonstrated a methodology for accurately measuring the side-channel energy per instruction. This provides a basis for several future projects. For example, the code can be run on different processors (cellphones, laptops, FPGAs, IoT devices) to characterize the susceptibility of attack for different devices. Future projects may also consist of using the side-channel energy per instruction algorithm to modulate strong carrier signals found in processors (i.e. clock frequencies, memory frequencies, voltage regulators, etc.). When the code is run, information is modulated on each of these carriers leaking information and providing a channel of attack. In order to find the total energy available to the attacker, future research will focus on finding these carrier signals and integrating over each of the side-bands carrying modulated information.

As for the localization part of the project, the localization model has to be refined and rigorously tested against multiple processors. Initial results are promising; however, many other factors need to be taken into consideration including operation instruction (LOAD/ADD, ADD/SUB, etc.), different transmitting equivalent loop antenna sizes, and different loop orientations. Once the localization model is verified, then optimizations can be made to the measurement process. For example, a few points around the edge of the board can be used to localize the loop without having to take a raster scan of the entire board. This saves time when performing measurements, and can be used when trying to locate the max signal radiating from a processor. Side-channels are a new and developing research area and there are many problems that need to be solved. Many of the problems are interdisciplinary and require extensive knowledge in computer architecture, electromagnetic radiation and propagation, electronic test and measurements, DSP, and machine learning.

REFERENCES

[1] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side-channel(s)," in *Cryptographic Hardware and Embedded Systems - Ches 2002*. vol. 2523, B. S. Kaliski, C. K. Koc, and C. Paar, Eds., ed, 2002, pp. 29-45.

[2] T. Kasper, D. Oswald, and C. Paar, "EM side-channel attacks on commercial contactless smartcards using low-cost equipment," in *Information Security Applications*, ed: Springer, 2009, pp. 79-93.

[3] W. van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," *Computer & Security* vol. 4, pp. 269-286, 1985.

[4] V. Carlier, H. Chabanne, E. Dottax, and H. Pelletier, "Electromagnetic Side Channels of an FPGA Implementation of AES," *International Association for Cryptologic Research,* 2004.

[5] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from pcs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *Cryptographic Hardware and Embedded Systems--CHES 2015*, ed: Springer, 2015, pp. 207-228.

[6] H. J. Highland, "Electromagnetic radiation revisited," *Computers & Security*, vol. 5, pp. 85-93, 1986.

[7] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results," in *Cryptographic Hardware and Embedded Systems — CHES 2001*. vol. 2162, Ç. Koç, D. Naccache, and C. Paar, Eds., ed: Springer Berlin Heidelberg, 2001, pp. 251-261.

[8] K. Tiri and I. Verbauwhede, "A VLSI design flow for secure side-channel attack resistant ICs," in *Proceedings of the conference on Design, Automation and Test in Europe-Volume 3*, 2005, pp. 58-63.

[9] J. Fan, X. Guo, E. De Mulder, P. Schaumont, B. Preneel, and I. Verbauwhede, "State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures," in *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*, 2010, pp. 76-87.

[10] A. Zajic and M. Prvulovic, "Experimental demonstration of electromagnetic information leakage from modern processor-memory systems," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 56, pp. 885-893, 2014.

[11] R. Callan, A. Zajić, and M. Prvulovic, "A practical methodology for measuring the side-channel signal available to the attacker for instruction-level events," in *Proceedings of the 47th Annual IEEE/ACM International Symposium on Microarchitecture*, 2014, pp. 242-254.

[12] H. W. Ott, *Electromagnetic compatibility engineering*: John Wiley & Sons, 2011.

[13] F. M. Greene, "The near-zone magnetic field of a small circular-loop antenna," *J. Res. NBS*, vol. 71, pp. 319-326, 1967.