UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

EXPERIMENTS ON ELECTROMAGNETIC LEAKAGE FROM LAPTOP COMPUTERS

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

MASTER OF SCIENCE

By

LESYA BOROWSKA
Norman, Oklahoma
2017

EXPERIMENTS ON ELECTROMAGNETIC LEAKAGE FROM LAPTOP COMPUTERS

A THESIS APPROVED FOR THE
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

BY

Dr. Ronald Barnes, Chair

Dr. Joseph Havlicek

Dr. Robert Palmer

Dr. Guifu Zhang

Dr. Dusan Zrnic

Dedication

Thus far the Lord has helped me.

I dedicate this thesis to my parents whose unconditional, sacrificial love made me who I am today and helps me during all my life.

Acknowledgements

I would like to thank my committee, colleagues, and friends for their constant help and support in everything I needed during my work on this thesis.

Table of Contents

Acknowledgements **iv**

List of Figures **viii**

Abstract **xi**

1 INTRODUCTION **1**

2 THEORY **7**

2.1 Cache Hit/Miss Definition 7

2.2 Cache Hit/Miss Program 9

3 EXPERIMENTAL EQUIPMENT AND ITS ELECTROMAGNETIC CHARACTERISTICS **12**

3.1 Spectrum Analyzer 12

3.1.1 Spectrum Analyzer and Laptop with Software for the Spectrum Analyzer in the Far-Field Chamber 12

3.1.2 Shielded Spectrum Analyzer and Laptop with Software for the Spectrum Analyzer in the Far-Field Chamber 18

3.1.3 Spectrum Analyzer and an Unplugged-from-Power-Cord Laptop with Software for the Spectrum Analyzer in the Far-Field Chamber 18

3.2 Spectrum Analyzer and Tracking Generator 20

3.2.1 Tracking Generator's Frequency 60 kHz 21

3.2.2 Tracking Generator's Frequency 120 kHz 23

3.2.2.1 Center Frequency 150 kHz 23

3.2.2.2 Center Frequency 180 kHz 25

3.3 Antennas' Description and Measurement Challenges 26

4 CACHE HIT/MISS SIGNALS RADIATED FROM A LAPTOP COMPUTER 29

4.1 Experiment Setup 29

4.1.1 Spectrum Analyzer and Laptop with Software for the Spectrum Analyzer in a Room 30

4.1.2 Spectrum Analyzer, Laptop with Software for the Spectrum Analyzer, and Laptop for Running Cache Hit/Miss Program 32

4.2 Cache Hit/Miss Program's EM Radiation 33

4.2.1 Center Frequency 200 kHz 35

4.2.1.1 Program's Frequency 175 kHz 35

4.2.1.2 Program's Frequency 180 kHz 36

4.2.1.3 Program's Frequency 185 kHz 37

4.2.2 Center Frequency 700 kHz 38

4.2.2.1 The Testing Laptop Idle 38

4.2.2.2 Program's Frequency 650 kHz 39

4.2.3 Center Frequency 1.705 MHz 40

4.2.3.1 Program's Frequency 1.65 MHz 40

4.2.4 Origin of the EM Leakage 40

5 CONCLUSIONS **43**

Bibliography **45**

List of Figures

1.1 An overview of the thread points of electromagnetic attacks. Image obtained from `http://www.rand.org/pubs/reports/R609-1/index2.html` 4

2.1 The organization of a computer, showing the processor, caches, and memory. 8

2.2 Timing of the program. 9

2.3 The A/B alternation pseudo-code. Image obtained from (Callan et al., 2014) 10

3.1 Block diagram for the measurement with the SA and a Laptop only 13

3.2 A 100-point normalized flat top window in time and frequency domains 15

3.3 Power spectrum of the output of the SA. The data were collected under the setup shown in Figure 3.1 16

3.4 Power spectrum of the signals that were created by the setup shown in Figure 3.1 17

3.5 Power spectrum of signals from the shielded spectrum analyzer (block diagram Figure 3.1, but the SA was wrapped in a grounded aluminum foil) 19

3.6 Power spectrum of signals from the spectrum analyzer (block diagram Figure 3.1, but the laptop was disconnected from power and the power cord was out of the chamber) 20

3.7 The setup for checking calibration of the SA. 21

3.8 Power spectrum of signals that were created by setup shown in Figure 3.7. The tracking generator was generating a signal at 60 kHz 22

3.9 Software window setup for the tracking generator which generates 60-kHz signal and the SA which measures it 23

3.10 Power spectrum of signals that were created by setup shown in Figure 3.7. The tracking generator was generating a signal at 120 kHz. 24

3.11 Software window setup for the tracking generator which generates 120-kHz signal and the SA which measures it 25

3.12 Software window setup for the tracking generator that generates 120-kHz signal and the SA which measures it, but the center frequency set at 180 kHz 26

3.13 Power spectrum of signals created by setup shown in Figure 3.7. The tracking generator was generating a signal at 120 kHz, but the center frequency was at 180 kHz 27

3.14 The Aaronia Near Field Probes. Image obtained from http://www.aaronia.com/products/antennas/RF-Field-Probes-PBS1/ 28

4.1 The setup for cache hit/miss measurements relative to the testing laptop 30

4.2 Power spectrum of signals created by setup shown in Figure 4.3. The center frequency was at 200 kHz 31

4.3 The setup for measurements when laptop from Figure 4.1 was taken out of the room 32

4.4 The setup for measurements when laptop from Figure 4.1 was idle 33

4.5 Power spectrum of signals when the testing laptop was idle. The center frequency was at 200 kHz 34

4.6 Power spectrum of signals when testing laptop was running LDL1/LDL2 instructions at frequency of 175 kHz and performing the cache hit/miss. The center frequency was at 200 kHz 35

4.7 Power spectrum of signals when testing laptop was running LDL1/LDL2 instructions at frequency of 180 kHz and performing the cache hit/miss. The center frequency was at 200 kHz 36

4.8 Power spectrum of signals when testing laptop was running LDL1/LDL2 instructions at frequency of 185 kHz and performing the cache hit/miss. The center frequency was at 200 kHz 37

4.9 Power spectrum of signals when testing laptop was idle. The center frequency was at 700 kHz 38

4.10 Power spectrum of signals when testing laptop was running LDL1/LDL2 instructions at frequency of 650 kHz and performing the cache hit/miss. The center frequency was at 700 kHz 39

4.11 Power spectrum of signals when testing laptop was running LDL1/LDL2 instructions at frequency of 1.65 MHz and performing the cache hit/miss. The center frequency was at 1.7 MHz 41

4.12 Internal hardware of the testing laptop 42

Abstract

The possibility of an electromagnetic (EM) side channel attack on computers has been known since 1967. Each executed instruction/event from running a program on a computer/laptop causes an EM signal at particular frequency. Based on this signal, theoretically, it can be established what is happening on the computer/laptop. In practice, no one has used EM leakage to decode instructions in detail or extract full information from memories if computers work internally without exchanging information with the outside world, e.g., through the Internet, etc. The main focus of this research is determination of the EM leakage from a modern laptop. Three main experimental components that help to detect the leakage are addressed: a spectrum analyzer (SA), a tracking generator, and "victim" laptop (the one which leakage is measured). All of the research on the EM side channel attack used EM far-field probes. EM near-field probes have been applied to this EM leakage for the first time. Studying the characteristics of the leakage spectra from a laptop could lead to new protection techniques and improvements for laptop-safe instruction executions. EM data were collected in varying frequency bands, environment conditions, and running programs. A cache hit/miss program was chosen for testing the possibility of the EM leakage because of the highest radiation level compared with other instructions. The program was written in such a way that allows to specify and change the program's frequency. This frequency was successfully detected in this study.

Chapter 1

INTRODUCTION

Computers have undergone continuous evolution for seven decades. Over time, serious concerns about protection of information from inadvertent leakage have increased. These concerns are among the most important because everything is computerized in the modern world: governments, military and security organizations, airports, national laboratories, education and medical organizations, etc.

There are numerous ways to steal computerized information. Some of them are shared processor hardware channel attack, system software layer attack, and side channel attack.

The example of the shared-processor hardware-channel attack is given in Chen and Venkataramani (2014). The authors show that a Trojan horse, a type of malware often disguised as legitimate software, modulates the timing event on shared processor hardware. This modulation gives needed information to a spy process. There is no direct communication between the Trojan and the Spy. Therefore, it is difficult to detect these channel attacks. The article proposes to check unusual events in real time.

The system software layer attack is based on incorporating vulnerabilities in guest operating systems (OSs) used to support virtualization (Evtyushkin et al., 2014). In 2013, the Linux kernel alone had 189 new vulnerabilities[1]. One of the ways to protect users from this attack is to apply an isolated execution (Iso-X) which offers flexible allocation of physical memory for security-critical code (Evtyushkin et al., 2014).

The most dangerous class of attacks is side channel attack. This type of attacks does not physically connect to the computers while observing sound, EM, etc. emanation that leak to the environment. Some side channel attacks including timing attacks (Kocher, 1996; Coppens et al., 2009), power attacks (Kocher et al., 1999; Bayrak et al., 2011), differential fault attacks (Biham and Shamir, 1997; Giraud, 2004), cache-based attacks (Tsunoo et al., 2002; Bangerter et al., 2011), and branch prediction attacks (Aciiçmez et al., 2007) use malicious procedures which can affect the system or attach to the target system equipment, and, therefore, are not as difficult to detect and prevent. However, the side channel attacks related to the emanating electromagnetic and/or sound waves from working computers are difficult to detect. This is because such illuminations could in principle be measured far away from computers without incorporations into computers' software or hardware and/or buses. Therefore, a theft of information cannot be easily detected. Acoustic attacks track the system computational sound to get sensitive information. Electrical components inside the voltage regulator on the mother board of a computer create an acoustic sound (Genkin et al., 2017). The voltage regulator consists of a few capacitors and a coil. When a computer operates, these components make noise. This sound can be detected. Different CPU (central processing unit) operations give different frequency noise. For example, in one system studied, a multiplication instruction gives about 282-kHz frequency sound, while a floating point multiplication

[1] `http://cvedetails.com`

instruction gives about 287-kHz frequency sound (Genkin et al., 2017). Electromagnetic attacks are based on measurements and analysis of electromagnetic radiation (van Eck, 1985; Highland, 1986; Gandolfi et al., 2001; Agrawal et al., 2002; Sekiguchi and Seto, 2013; Callan et al., 2014; Zajić and Prvulovic, 2014). The first report about these attacks was presented at the Spring Joint Computer Conference of 1967 by Willis H. Ware[2]. In his report, he wrote: "It is also possible to monitor the electromagnetic emanations that are radiated by the high-speed electronic circuits that characterize so much of the equipment used in computational systems. Energy given off in this form can be remotely recorded without having to gain physical access to the system or to any of its components or communication lines. The possibility of successful exploitation of this technique must always be considered." Ware classified computer network vulnerabilities as radiation from a processor, switching equipment, and output devices (printers and terminals), as well as radiation along the communication lines (Figure 1.1).

In 1985, van Eck confirmed the possibility of eavesdropping on video display units with a normal TV receiver (van Eck, 1985). In 1999, Durak detected electromagnetic leakage from a desktop's memory system at about two-meter distance[3]. In 2014, Zajić and Prvulovic showed the electromagnetic leakage from modern laptops and desktops (Zajić and Prvulovic, 2014). According to them, the EM information leakage can be detected at distances from tens of centimeters to several meters regardless of obstacles like cubicle, structural walls, metal shielding, etc. In their experiment, two types of activity were repeatedly running with period T/2 each on a computer. The frequency of these combined activities, 1/T, was observed with a radio receiver, Tecsun PL-660. Unfortunately, there is no evidence in the literature that anyone has deciphered the leakage. It

[2] http://www.rand.org/pubs/reports/R609-1/index2.html

[3] http://cryptome.org/tempest-cpu.htm

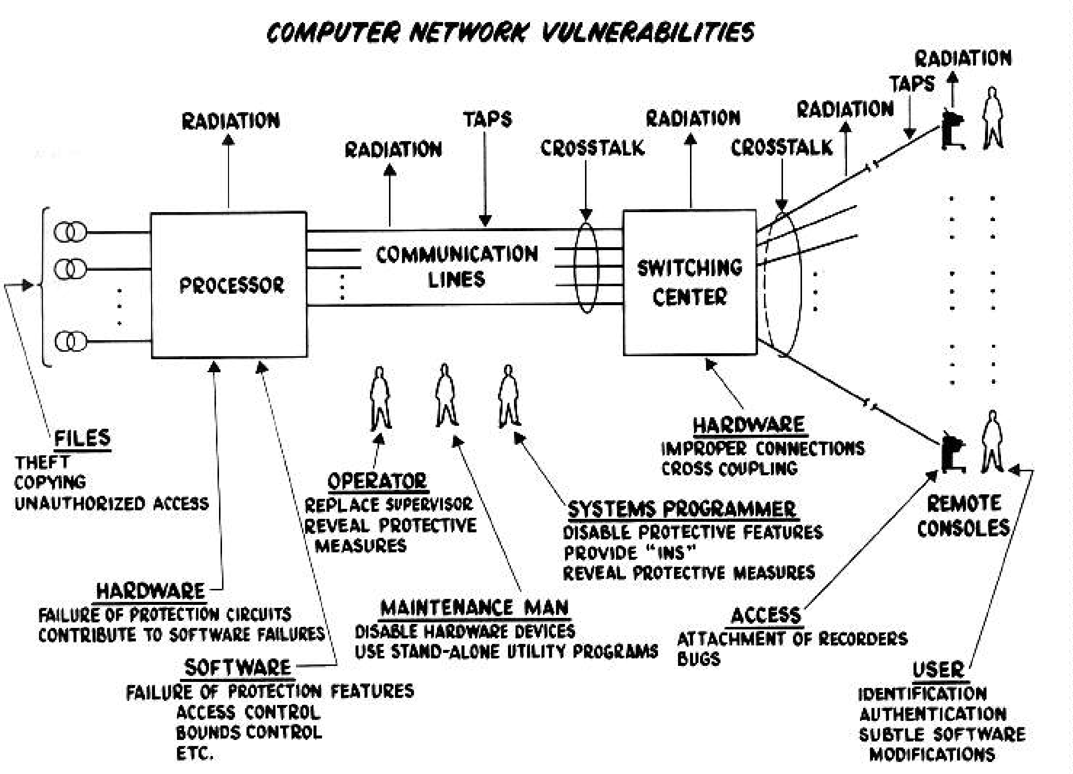


Figure 1.1: An overview of the thread points of electromagnetic attacks. Image obtained from `http://www.rand.org/pubs/reports/R609-1/index2.html`.

is one thing is to detect the radiation but it is much harder to decode it. This would require some synchronization with the leaking signal and recognition of the sequence of symbols etc.

Initial investigations for this thesis work began with measuring EM radiation from running a Raspberry Pi B+ V1.2. This unit has a single-core 700-MHz processor with 512 MB of memory. The processor executes 8 instructions simultaneously pipelined fashion. Therefore, counting cycles per instruction doesn't really give a picture of what actually happens. The main reason for choosing a Raspberry Pi was its relatively low frequency processor. It was believed that it would be easier to capture this EM leakage. Unfortunately, instructions like double precision division, multiplication, addition, etc. did not give visible-above-the-noise signals. L1 cache and L2 cache instructions (see Section 2.1 for cache definition) cause powerful enough EM leakage, but this leakage was in the frequency range out (too low) of what could be measured with the available instruments. In higher frequency processors, cache instructions would cause EM leakage at higher frequency. Therefore, I chose a modern laptop with a higher frequency processor. This gave an opportunity to examine EM signal emanations from L1 cache and L2 cache accesses.

In this thesis, results of recent papers (Zajić and Prvulovic, 2014; Callan et al., 2014) were confirmed, for the first time, on a laptop with an Intel i7-6700HQ processor (see Section 4.1 for more details) using only a simple near field antenna connected to a USB-SA124A Spectrum Analyzer. The theory behind the measurements is presented in Chapter 2. Chapter 3 describes the equipment needed for detecting the signal from a laptop's running program. Measurements performed with this equipment for understanding its behavior are explained. Chapter 4 presents a way to eavesdrop the EM signals created by a program running on a "victim" laptop and illustrates the measured results. Conclusions are presented in Chapter 5.

Chapter 2

THEORY

To demonstrate the detection of EM radiation from the laptop's processor, a program which can give a strong and distinguished EM signals is needed. Based on experimental results for an EM side channel measurement in Callan et al. (2014), a processor leaks the strongest and most distinguished signal when there is repetitive sequence of on-chip instructions and off-chip memory accesses. This means that instructions which are related to a cache hit/miss are the best candidates for this research.

2.1 Cache Hit/Miss Definition

The two main components of a computer are memory and processor. Data flow pass to the processor from memory. The memory is not typically on the same chip as the processor. Therefore, memory latency is relatively high (about 10 nsec). In reality, this can be up to 100s of processor cycles. Because of the high latency, smaller memory storages, typically, level 1 ($\sim$4-cycle latency) and level 2 ($\sim$12-cycle latency) are implemented on the same silicon die as processor cores (Figure 2.1). Cache is a small memory that contains the subset of the content of the main memory. If the data that are requested are not there, it is a cache miss. Otherwise, it is a cache hit.

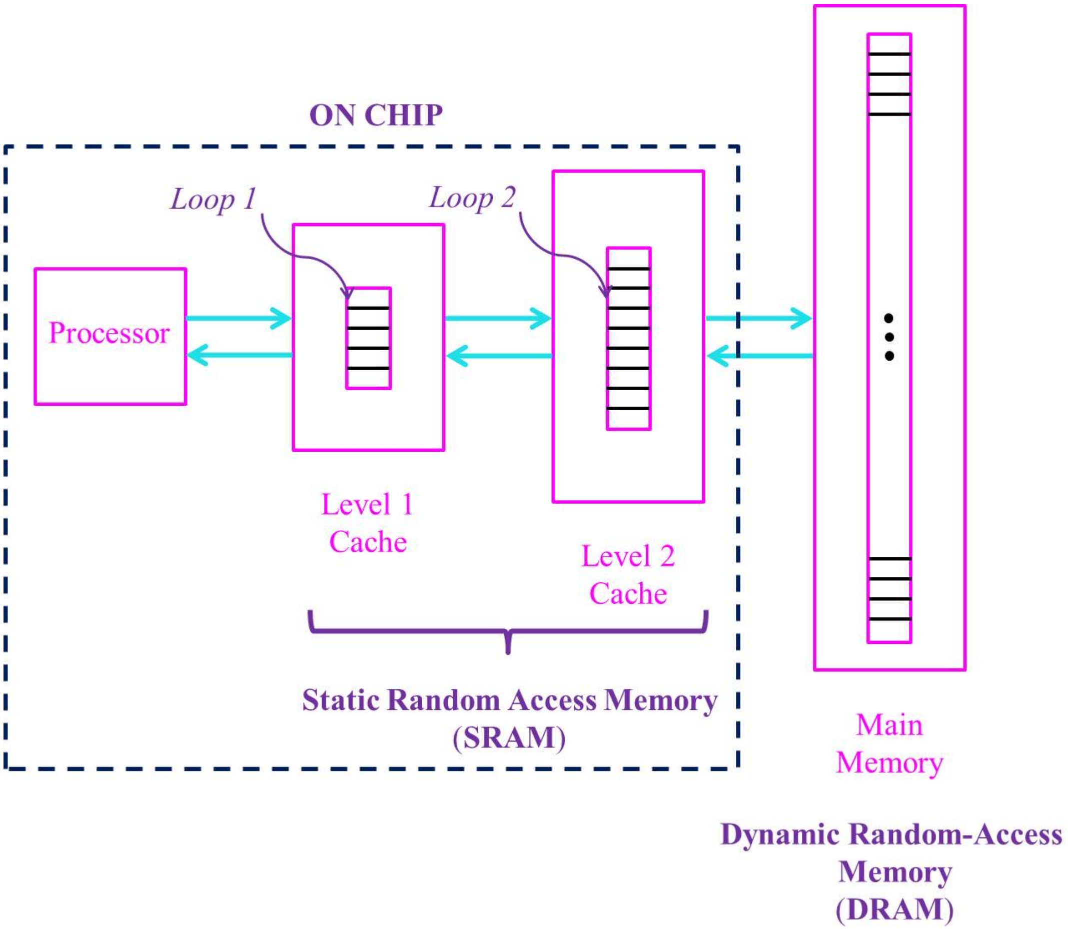

ON CHIP
Loop 1
Loop 2
Processor
Level 1 Cache
Level 2 Cache
Static Random Access Memory (SRAM)
Main Memory
Dynamic Random-Access Memory (DRAM)

Figure 2.1: The organization of a computer, showing the processor, caches, and memory.

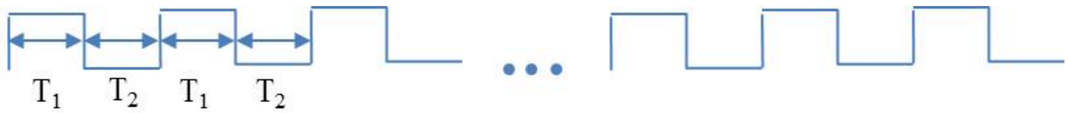


Figure 2.2: Timing of the program.

2.2 Cache Hit/Miss Program

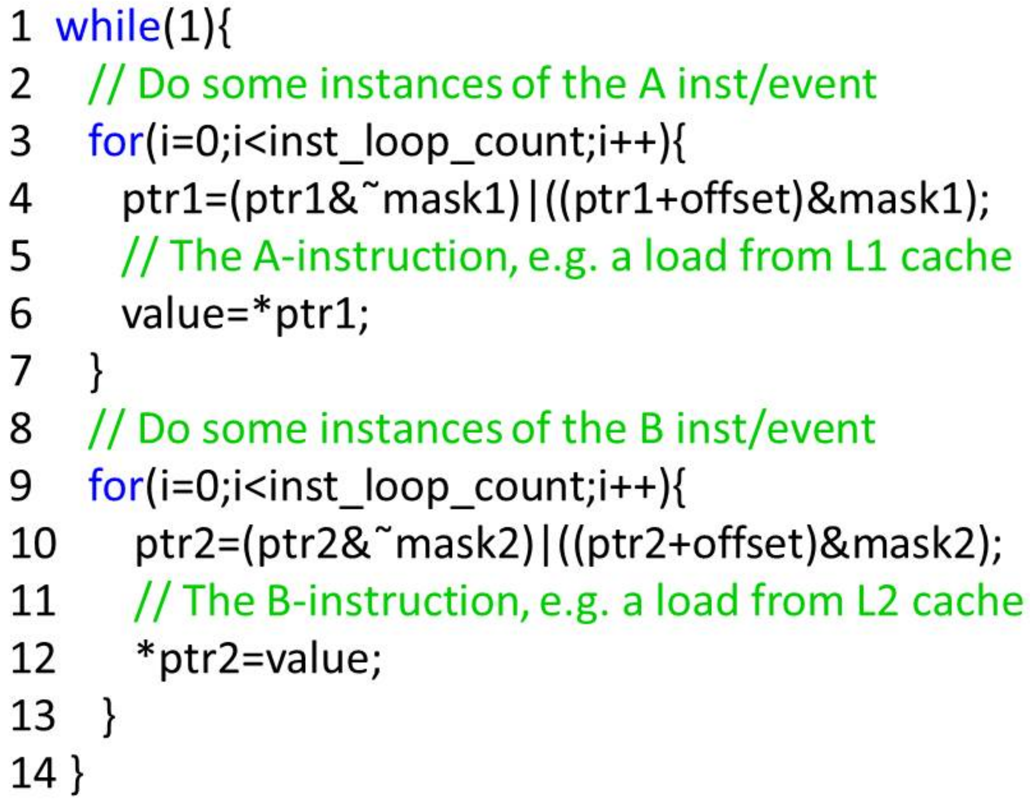
A program which creates cache hit/miss was given by Dr. Callan (personal communication with R. Callan, 2016). It is the same program used in his and his colleagues' articles (Callan et al., 2014; Zajić and Prvulovic, 2014). According to Zajić and Prvulovic (2014), differences in code execution create electromagnetic signals which can be measured with simple tools. The program has two loops. The loops have equal periods

$$T_1 = T_2 = T/2, \tag{2.1}$$

where $T = T_1 + T_2$. The first loop runs for T_1 seconds then the second loop runs for T_2 seconds then the sequence repeats (Figure 2.2).

When the program executes, it creates signals at frequency 1/T. I will call this frequency the "program's frequency" later. The code is run as a single-threaded 32-bit user mode application under a 64-bit version of Windows 7 (Callan et al., 2014). The pseudo-code of the cache hit/miss program is shown in (Callan et al., 2014).

In this study, during period T_1, the code instructs the processor to load from L1 cache (LDL1). This is the A instruction/event (lines 2 through 7 in Figure 2.3). Then, during period T_2, the code instructs the processor to load from L2 cache (LDL2). This is the B instruction/event (lines 8 through 13 in Figure 2.3). The two executions make one A/B alternation. This alternation is repeated as long as it is needed to measure the side channel signal. Periods A and B events are controlled by the value of inst_loop_count. To create the



```
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 from L1 cache
    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 load from L2 cache
    *ptr2=value;
  }
}
```

Figure 2.3: The A/B alternation pseudo-code. Image obtained from (Callan et al., 2014)

desired cache hit/miss behavior, the address of the accessed location updates repeatedly (lines 4 and 10 in Figure 2.3). To avoid the differences in EM signals during repetitions of the experiment, all instructions outside of lines 1 through 14 (Figure 2.3) should be executed identically. Therefore, the actual code is written in x86 assembly.

Chapter 3

EXPERIMENTAL EQUIPMENT AND ITS ELECTROMAGNETIC CHARACTERISTICS

In order to detect the EM leakage from a laptop, I used a spectrum analyzer and near field EM probes (antennas). In this Section, I describe their EM characteristics.

3.1 Spectrum Analyzer

3.1.1 Spectrum Analyzer and Laptop with Software for the Spectrum Analyzer in the Far-Field Chamber

After studying the instruments, a spectrum analyzer as a digital receiver with a single side band was chosen. It has an analog to digital (A/D) converter and frequency downconverter; shifts frequency to base band by a selectable amount. The selectable amount is called the center frequency. It can optionally record time series data. This option gave the flexibility to capture and analyze the data using Fourier analysis offline.

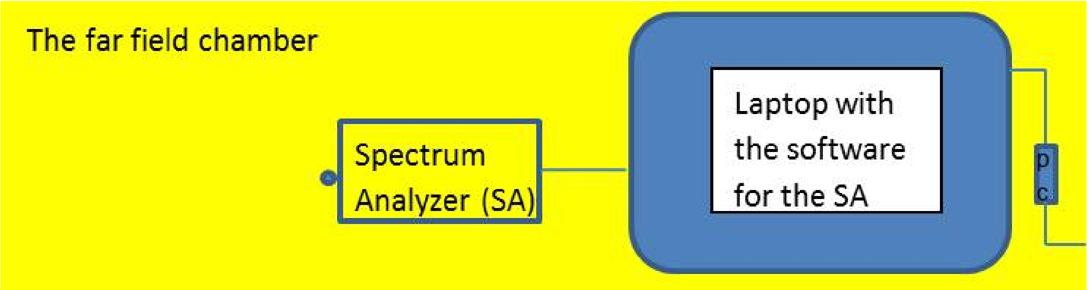


Figure 3.1: Block diagram for the measurement with the SA and a Laptop only.

For my measurements, USB-SA124A Spectrum Analyzer was chosen (Demodulator: AM-FM-SSB-CW real time; Max. Frequency: 12.4 GHz; Min. Frequency: 100 kHz; Max. Level: 10 dBm; Min. Level: -152 dBm; Min. Resolution: 1 Hz). In a far-field chamber, several measurements with this SA were done under different setups. Initially, the SA was only connected to a laptop with the software for the spectrum analyzer (Figure 3.1). This laptop was connected to a power cord (PC in Figure 3.1) which was plugged in chamber's outlet.

In a typical spectrum analyzer (including the SA that was used) there are options to set the start, stop, and center frequency. The frequency halfway between the stop and start frequencies on a spectrum analyzer display is known as the center frequency. This is the frequency that is in the middle of the display's frequency axis. Span specifies the range between the start and stop frequencies. A "Zero Span" is a span at the fix central frequency with the range equal to the bandwidth. The center frequency and span allow for adjustment of the display within the frequency range of the instrument to enhance visibility of the measured spectrum[1]. For all measurements with the SA provided in Section 3.1, the frequency is centered at 150 kHz and “Zero Span” (time series (I and Q) data can be collected only in "Zero Span" mode). The bandwidth was 250 kHz and could not be controlled. In the “Zero Span” interface, “AM Demod” was chosen. The data were recorded in comma-separated values (csv) format. The

[1] https://en.wikipedia.org/wiki/Spectrum_analyzer#Center_frequency_and_span

length of the data is 486111 elements (I and Q pairs). The time of collection was 1 sec. Therefore, the sampling frequency is

$$F_S = 486111 \text{ Hz}. \tag{3.1}$$

The I and Q values are scaled to mW via software-applied corrections. FIR filters were used to apply amplitude corrections on the data before they were saved in csv format. Correction factors are collected and stored on each unit before shipping to customers. Before applying the fast Fourier transform (FFT) to the raw I and Q data obtained, the data were multiplied by a normalized Flat Top window. Flat Top windows have very low passband ripple ($<$ 0.01 dB) and are used primarily for calibration purposes. Their bandwidth is approximately 2.5 times wider than a von Hann window (raised cosine). Flat top windows are summations of cosines. The coefficients of a flat top window are computed from the following equation[2]

$$w(n) = a_0 - a_1 \cos\left(\frac{2\pi n}{N-1}\right) + a_2 \cos\left(\frac{4\pi n}{N-1}\right) - a_3 \cos\left(\frac{6\pi n}{N-1}\right) + a_4 \cos\left(\frac{8\pi n}{N-1}\right), \tag{3.2}$$

where $0 \leq n \leq N-1$ and $w(n) = 0$ elsewhere. The window length is $L = N$ ($L =$ 486111 for this experiment). The coefficient values are $a_0 = 0.21557895, a_1 = 0.41663158, a_2 = 0.277263158, a_3 = 0.083578947,$ and $a_4 = 0.006947368$. In Figure 3.2, a 100-point normalized flat top window is shown in time and frequency domains.

The power spectrum was computed from the data collected with the SA using a 486111-point normalized flat top window in order to compare the power spectrum calculated with the software obtained power spectrum (The manufacturer uses the 486111-point normalized flat top window).

The SA provides the time series data (I and Q) are shifted to base band. The amount of shift is equal to the center frequency. Then the spectral value of the

[2] `https://www.mathworks.com/help/signal/ref/flattopwin.html`

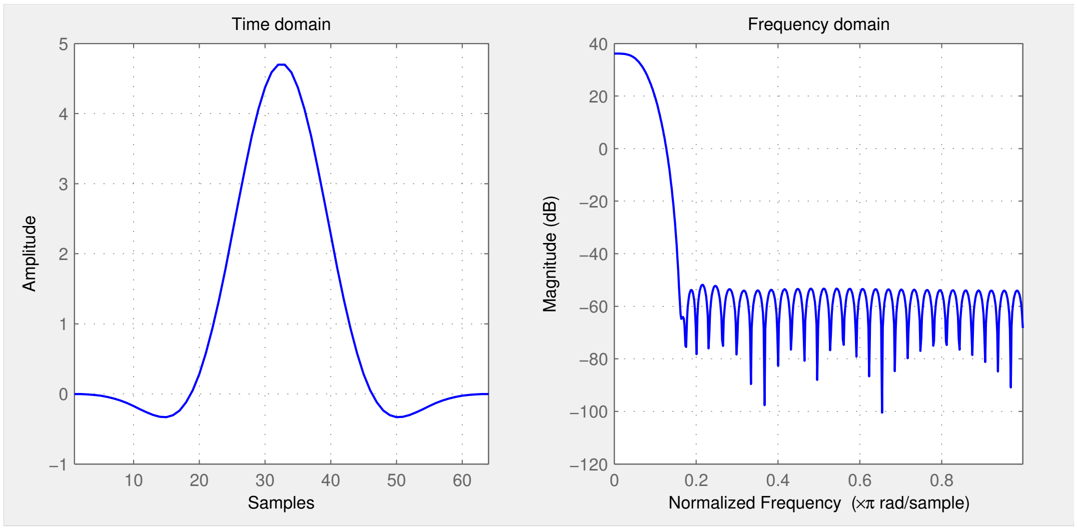


Figure 3.2: A 100-point normalized flat top window is shown in time and frequency domains.

center frequency appears as DC. The power spectrum of the shifted data collected under the setup shown in Figure 3.1 is shown in Figure 3.3. The frequencies in ranges [-243.1, -125.25] and [125.25, 243.1] correspond to the noise. These are enhanced after window application.

Because DC of the I and Q data correspond to the center frequency, I needed to add this frequency to the fast Fourier transform's (FFT) frequency in order to have the true frequencies in my plot. This addition shifts the FFT output (see Figure 3.4 and all other related Figures).

In Figure 3.4, we see the power spectrum of the signals that were created by the setup shown in Figure 3.1.

There are several peaks. The highest one is at 28.56 kHz. The peak at 145.4 kHz corresponds to the center frequency. The peak at the center frequency is due to the DC offset (the mean value of the waveform) in the SA receiver and downconverter. As we will see later, there is always a peak near the center frequency in the power spectrum. It is close, but never equal to the setup center

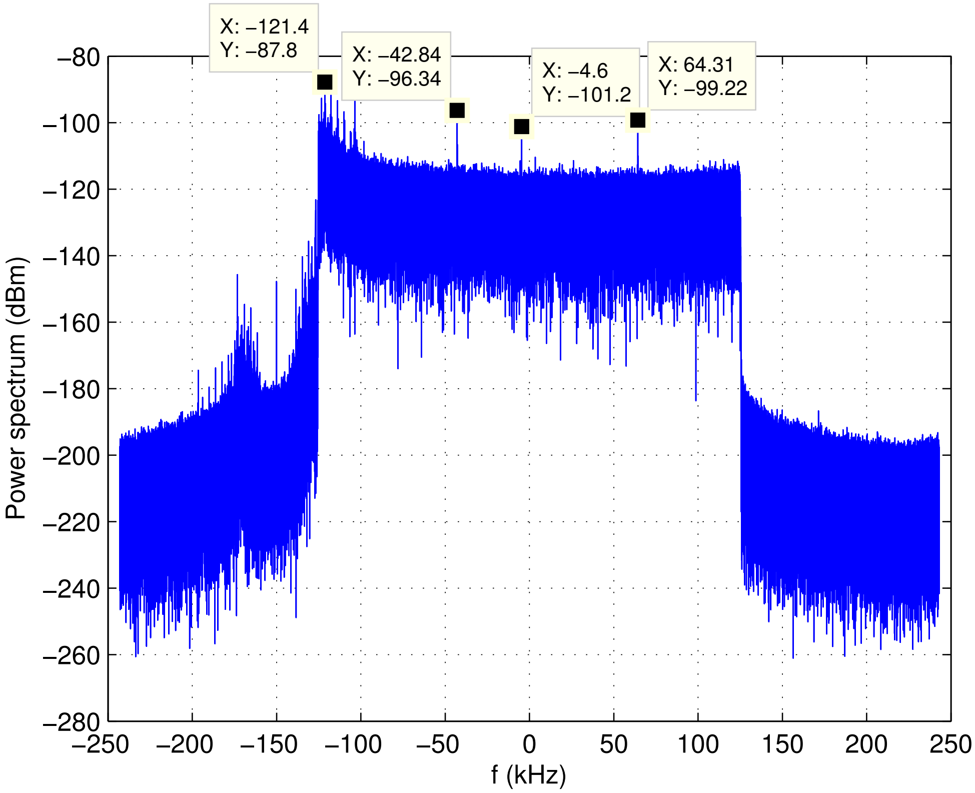


Figure 3.3: Power spectrum of the output of the SA. The data were collected under the setup shown in Figure 3.1.

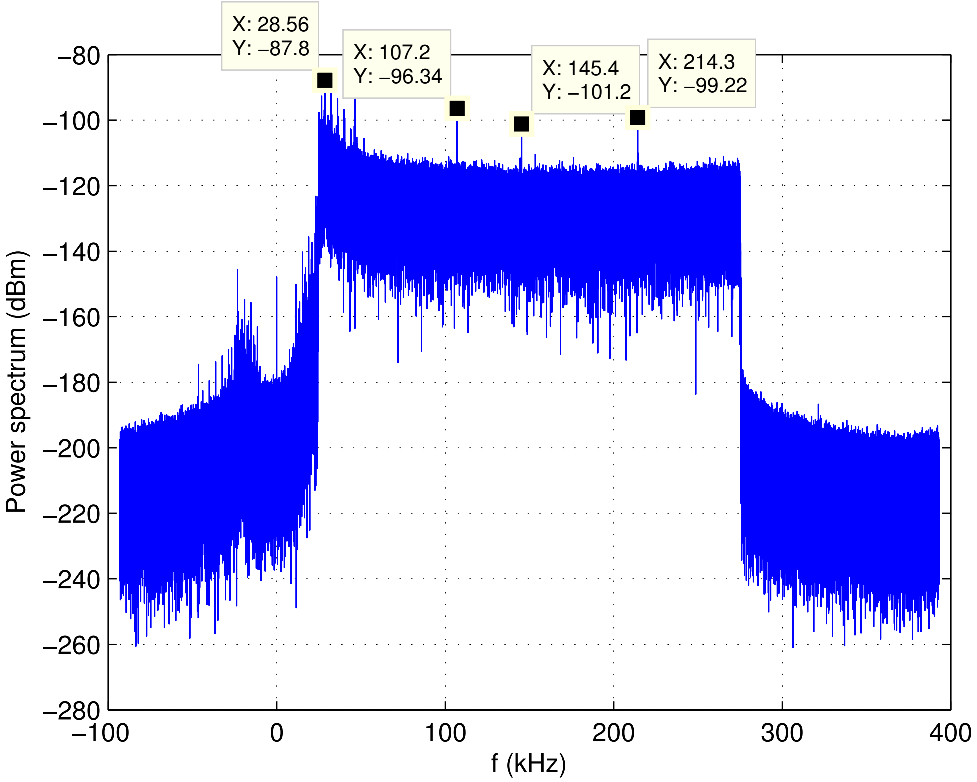


Figure 3.4: Power spectrum of the signals that were created by the setup shown in Figure 3.1.

frequency. All peaks related to center frequencies are a little bit shifted from the setup values of the center frequencies. This relates to the frequency error that exists in any spectrum analyzer. The frequency resolution is also limited by resolution bandwidth. In order to understand the nature of other peaks, the power spectrum for several other modifications (cases) of the block diagram are plotted in the subsections below.

3.1.2 Shielded Spectrum Analyzer and Laptop with Software for the Spectrum Analyzer in the Far-Field Chamber

The SA was wrapped in a grounded aluminum foil. Everything else was the same as the setup in Figure 3.1. In Figure 3.5, the power spectrum of the signals from this modification is plotted. All peaks are at the same positions as they are in Figure 3.4 only slight variations in the magnitudes are present. Therefore, I conclude that the SA is very well shielded by itself and no additional aluminum shielding is needed.

3.1.3 Spectrum Analyzer and an Unplugged-from-Power-Cord Laptop with Software for the Spectrum Analyzer in the Far-Field Chamber

The setup is the same as in Figure 3.1, but the laptop was disconnected from the power and the power cord was out of the chamber. In Figure 3.6, the power spectrum of the signals from this setup is plotted. The highest peak and peak related to the center frequency are at the same positions as they are in Figure 3.4. Two other peaks, 104 and 208 kHz, are shifted left by about 3% relative

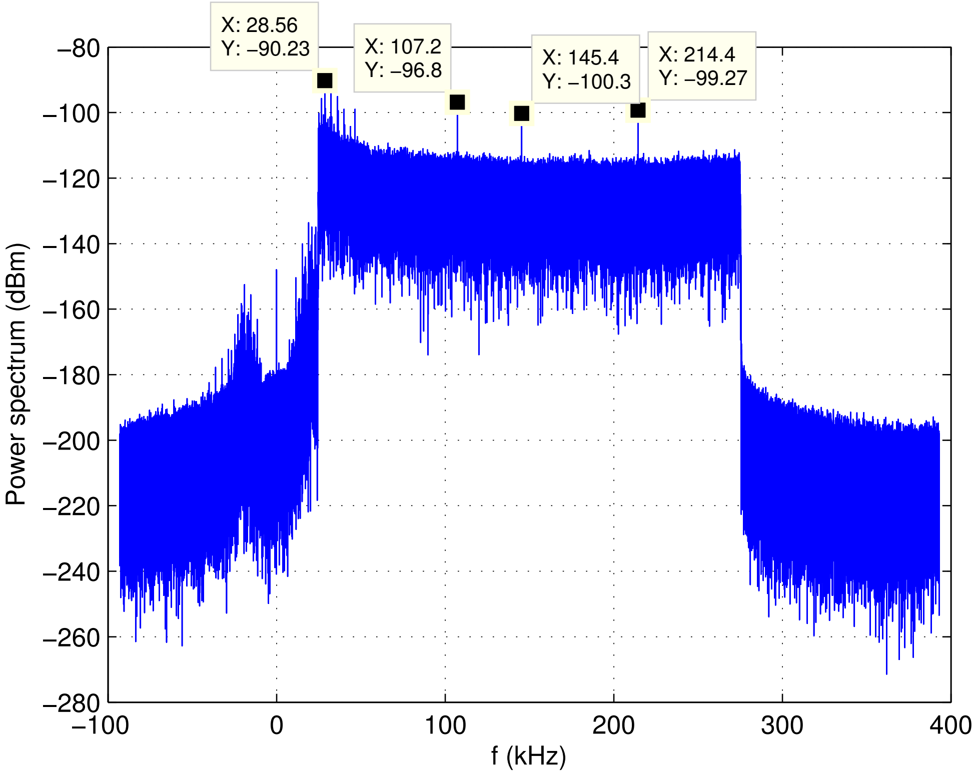


Figure 3.5: Power spectrum of signals from the shielded spectrum analyzer (block diagram Figure 3.1, but the SA was wrapped in a grounded aluminum foil).

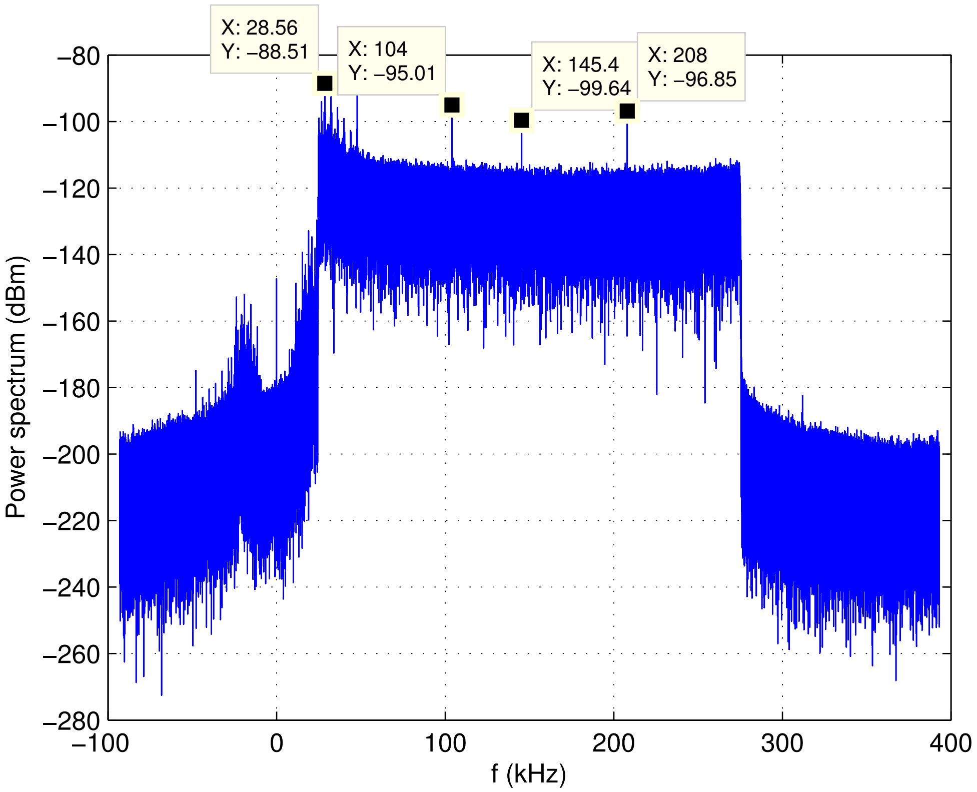


Figure 3.6: Power spectrum of signals from the spectrum analyzer (block diagram Figure 3.1, but the laptop was disconnected from power and the power cord was out of the chamber).

to their values when computer was connected to the power cord. I speculate that electromagnetic radiation that comes from the power cord affects these two frequencies.

3.2 Spectrum Analyzer and Tracking Generator

In order to check calibration of the SA, several measurements with the Signal Hound USB-TG44A tracking generator connected to the SA were made. The

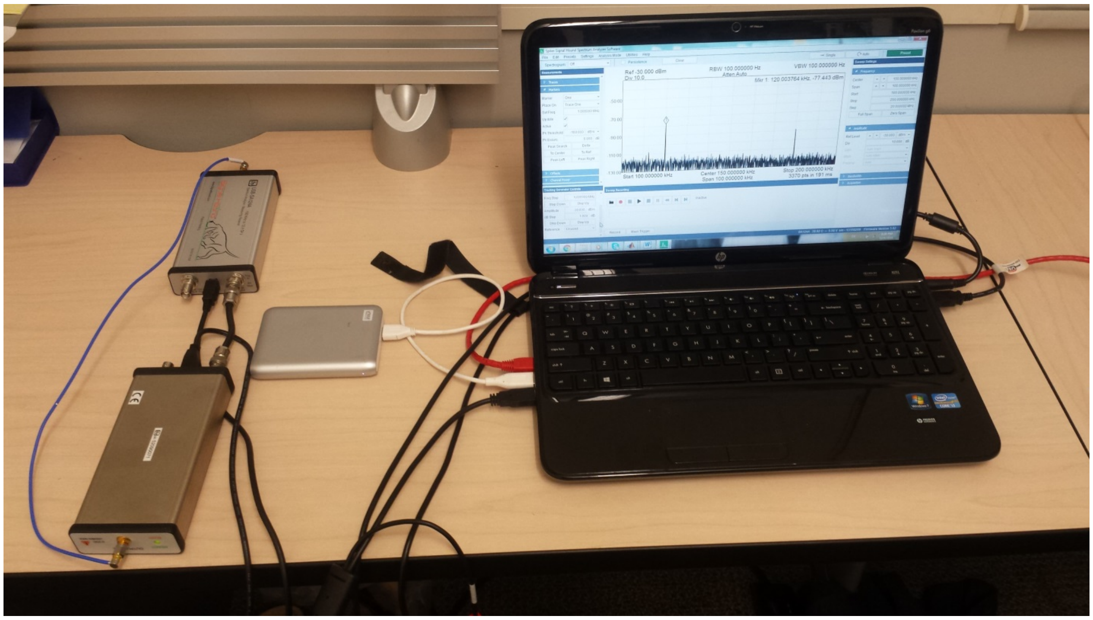


Figure 3.7: The setup for checking calibration of the SA.

tracking generator generates signals at RF range 10 Hz to 4.4 GHz with amplitude range from -30 dBm to -10 dBm. The setup of these measurements is shown in Figure 3.7. All calibration measurements were made in room 4644 located on 4th floor at the National Weather Center (NWC) in Norman, OK. No isolations from the external EM signals were made.

3.2.1 Tracking Generator's Frequency 60 kHz

In Figure 3.8, we see power spectrum of the signals that were created by the setup shown in Figure 3.7. The tracking generator was generating the -30-dBm signal at 60 kHz (see software window setup in Figure 3.9). In spite of the statement that the minimum detected frequency is 100 kHz for the USB-SA124A spectrum analyzer, the highest peak with power equal to -32.14 dBm which the SA detected is at 60 kHz in Figure 3.8. There are also three of its harmonics: 120 kHz (-76.49-dBm peak power shown as -77.519-dBm peak power in Figure 3.9), 180 kHz (-86.44-dBm peak power shown as about -87-dBm peak power in

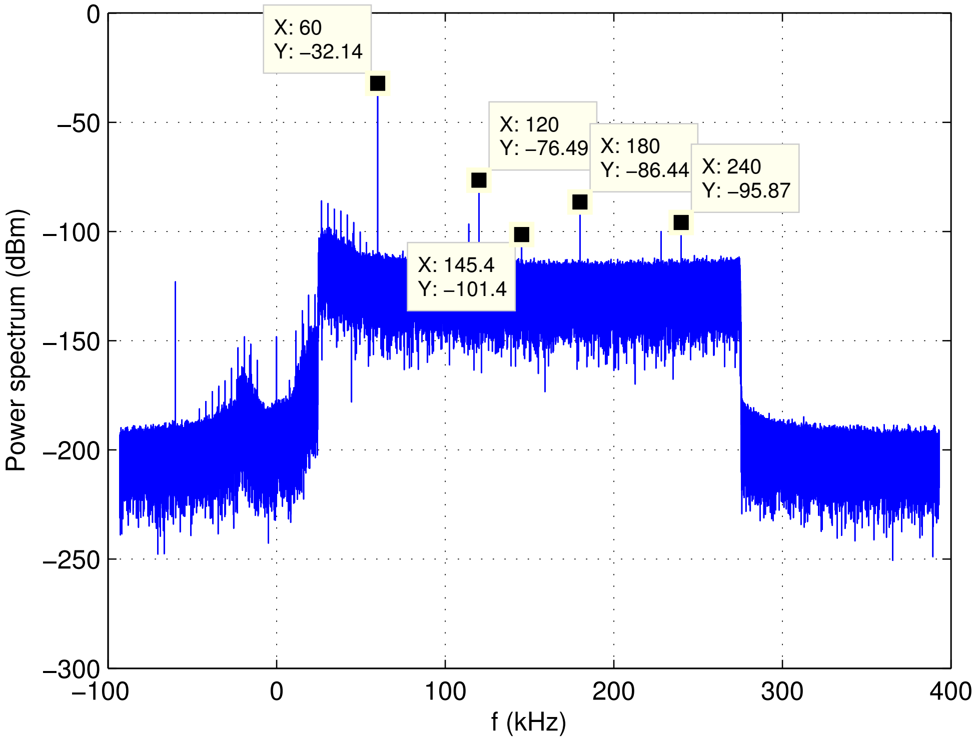
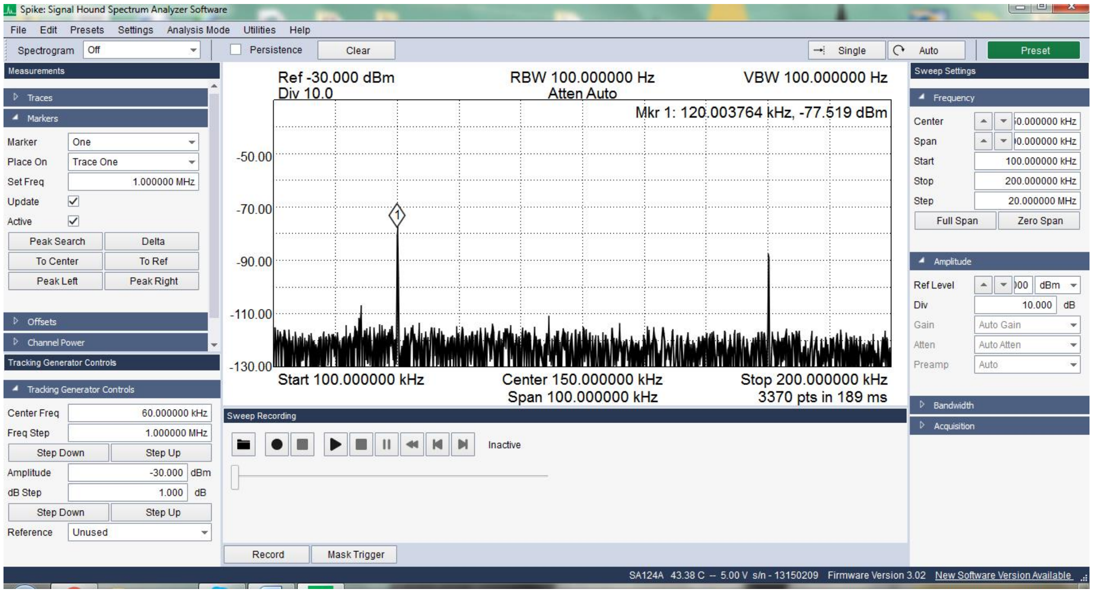


Figure 3.8: Power spectrum of signals that were created by setup shown in Figure 3.7. The tracking generator was generating a signal at 60 kHz.

Figure 3.9), and 240 kHz (-95.87-dBm peak power) in Figure 3.8. The power spectrum's values are decreasing with increasing the harmonic's number which was expected. The differences in the power spectrum's values from Figure 3.8 and the power values from Figure 3.9 are caused by the differences in processing between the output of the standard sweep mode and I and Q data. The center frequency was 150 kHz. Therefore, there is a peak with power -101.4 dBm at 145.4 kHz in Figure 3.8. This peak has power close to the peak power in Figure 3.4.



Spectrogram: Off

Marker: One
Place On: Trace One
Set Freq: 1.000000 MHz
Update: ☑
Active: ☑

Tracking Generator Controls
Center Freq: 60.000000 kHz
Freq Step: 1.000000 MHz
Amplitude: -30.000 dBm
dB Step: 1.000 dB
Reference: Unused

Ref -30.000 dBm
Div 10.0
RBW 100.000000 Hz
Atten Auto
VBW 100.000000 Hz
Mkr 1: 120.003764 kHz, -77.519 dBm
Start 100.000000 kHz
Center 150.000000 kHz
Span 100.000000 kHz
Stop 200.000000 kHz
3370 pts in 189 ms

Center: ;0.000000 kHz
Span:)0.000000 kHz
Start: 100.000000 kHz
Stop: 200.000000 kHz
Step: 20.000000 MHz

Ref Level:)00 dBm
Div: 10.000 dB
Gain: Auto Gain
Atten: Auto Atten
Preamp: Auto

SA124A 43.38 C -- 5.00 V s/n - 13150209 Firmware Version 3.02 New Software Version Available

Figure 3.9: Software window setup for the tracking generator which generates 60-kHz signal and the SA which measures it.

3.2.2 Tracking Generator's Frequency 120 kHz

3.2.2.1 Center Frequency 150 kHz

Figure 3.10 shows the power spectrum when the tracking generator was generating the -30-dBm signal at 120 kHz (see Software window setup in Figure 3.11). The result is similar to the case when the tracking generator was creating the signal at 60 kHz. The highest peak with power -30.19 dBm which the SA detected is at 120 kHz in Figure 3.10. There is also one of its harmonics: 240 kHz (-75.9-dBm peak power) in Figure 3.10. The center frequency was again 150 kHz. Therefore, there is a peak with power -106 dBm at 145.4 kHz in Figure 3.10. This peak power is close to the peak power in Figure 3.4.

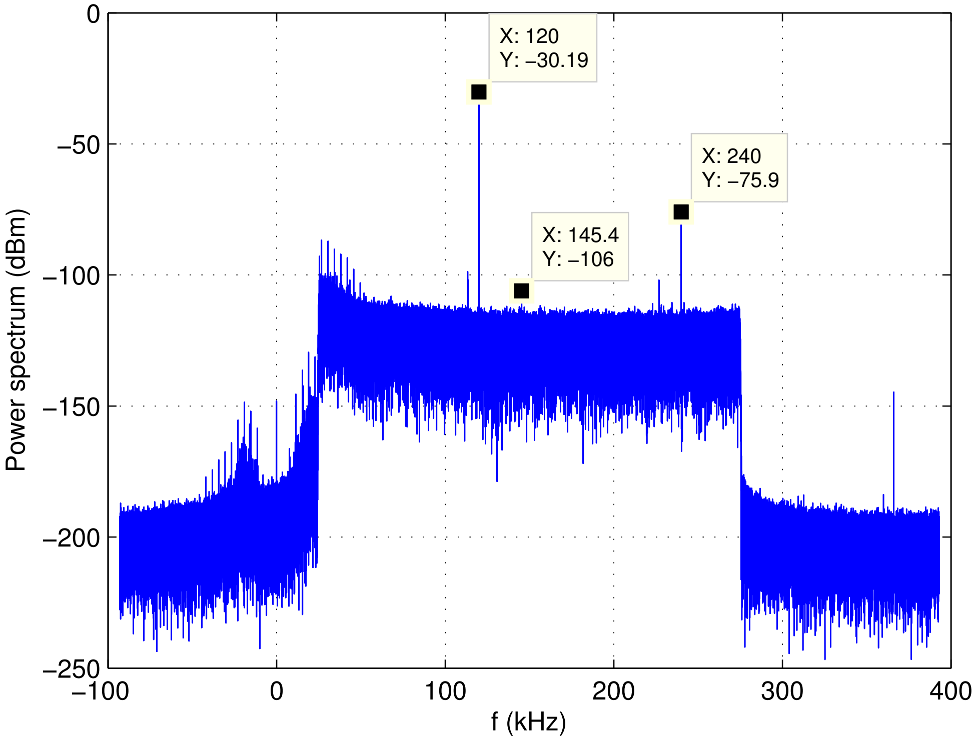
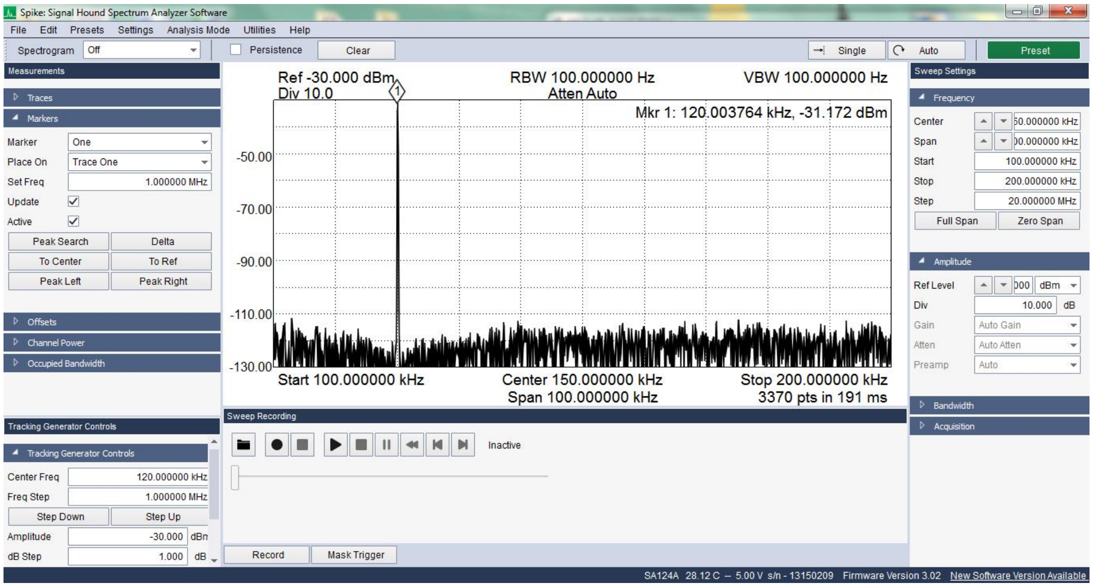


Figure 3.10: Power spectrum of the signals that were created by setup shown in Figure 3.7. The tracking generator was generating a signal at 120 kHz.



Spectrogram Off

Marker One
Place On Trace One
Set Freq 1.000000 MHz
Update ☑
Active ☑

Center Freq 120.000000 kHz
Freq Step 1.000000 MHz
Amplitude -30.000 dBm
dB Step 1.000 dB

Ref -30.000 dBm
Div 10.0
RBW 100.000000 Hz
Atten Auto
VBW 100.000000 Hz
Mkr 1: 120.003764 kHz, -31.172 dBm
Start 100.000000 kHz
Center 150.000000 kHz
Span 100.000000 kHz
Stop 200.000000 kHz
3370 pts in 191 ms

Center 50.000000 kHz
Span 00.000000 kHz
Start 100.000000 kHz
Stop 200.000000 kHz
Step 20.000000 MHz

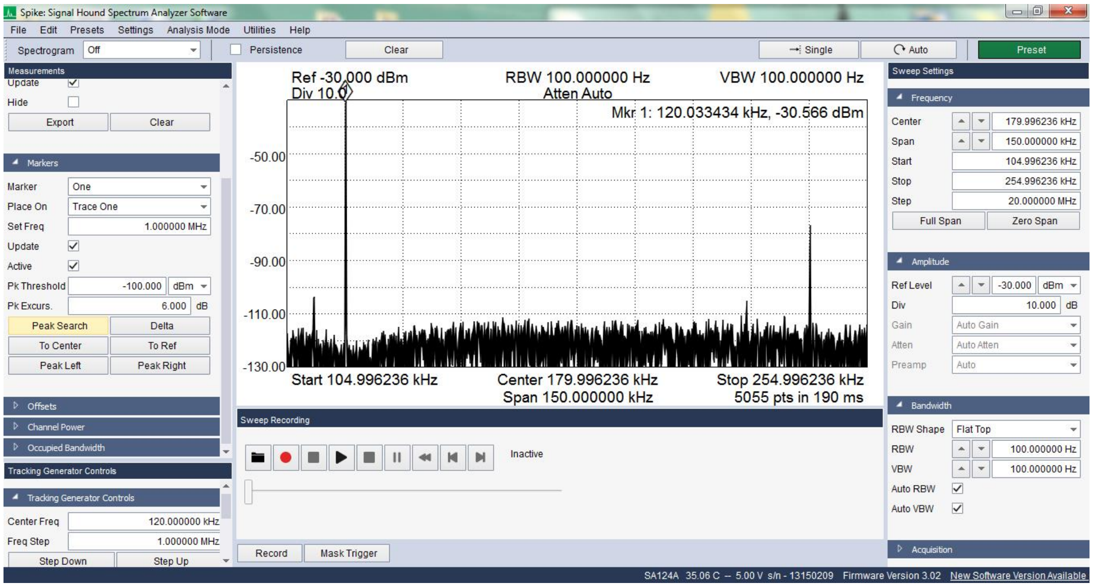
Ref Level 000 dBm
Div 10.000 dB
Gain Auto Gain
Atten Auto Atten
Preamp Auto

SA124A 28.12 C -- 5.00 V s/n - 13150209 Firmware Version 3.02 New Software Version Available

Figure 3.11: Software window setup for the tracking generator which generates 120-kHz signal and the SA which measures it.

3.2.2.2 Center Frequency 180 kHz

The last measurement with the tracking generator was when the tracking generator was generating the -30-dBm signal at 120 kHz (see Software window setup in Figure 3.12), but the center frequency was 180 kHz. Figure 3.13, shows the power spectrum for this case. Comparing Figures 3.13 and 3.10, I concluded that a new peak at 184.5 kHz which is only in Figure 3.13 corresponds to the center frequency of 180 kHz. And of course, there is no peak at 145.4 kHz in Figures 3.13. This is one more conformation that, in this SA, any center frequency produces a peak in the power spectrum.



Spike: Signal Hound Spectrum Analyzer Software

Spectrogram: Off

Measurements
Update ☑
Hide □

Markers
Marker: One
Place On: Trace One
Set Freq: 1.000000 MHz
Update ☑
Active ☑
Pk Threshold: -100.000 dBm
Pk Excurs.: 6.000 dB

Tracking Generator Controls
Center Freq: 120.000000 kHz
Freq Step: 1.000000 MHz

Ref -30.000 dBm
Div 10.0
RBW 100.000000 Hz
Atten Auto
VBW 100.000000 Hz
Mkr 1: 120.033434 kHz, -30.566 dBm
Start 104.996236 kHz
Center 179.996236 kHz
Span 150.000000 kHz
Stop 254.996236 kHz
5055 pts in 190 ms

Sweep Recording: Inactive

Sweep Settings

Frequency
Center: 179.996236 kHz
Span: 150.000000 kHz
Start: 104.996236 kHz
Stop: 254.996236 kHz
Step: 20.000000 MHz

Amplitude
Ref Level: -30.000 dBm
Div: 10.000 dB
Gain: Auto Gain
Atten: Auto Atten
Preamp: Auto

Bandwidth
RBW Shape: Flat Top
RBW: 100.000000 Hz
VBW: 100.000000 Hz
Auto RBW ☑
Auto VBW ☑

SA124A 35.06 C -- 5.00 V s/n - 13150209 Firmware Version 3.02 New Software Version Available

Figure 3.12: Software window setup for the tracking generator which generates 120-kHz signal and the SA that measures it, but the center frequency set at 180 kHz.

3.3 Antennas' Description and Measurement Challenges

To continue these investigations, antennas were needed for measuring signals from the laptop. I utilized the Aaronia Near Field Probes (see Figure 3.14) which were connected to the SA. This is a passive, high performance and accurate RF Field Probe set that allows straightforward pinpointing and measurement of interference sources from DC (1 Hz) to 9 GHz in electronic component groups as well as execution and monitoring of generic EMC measurement. The set includes a total of 5 probes: 4 probes for magnetic field measurements and one for measurements of electric fields. All probes are covered with an insulating layer, thus allowing safe measurement of oscillators or main lines. All of them

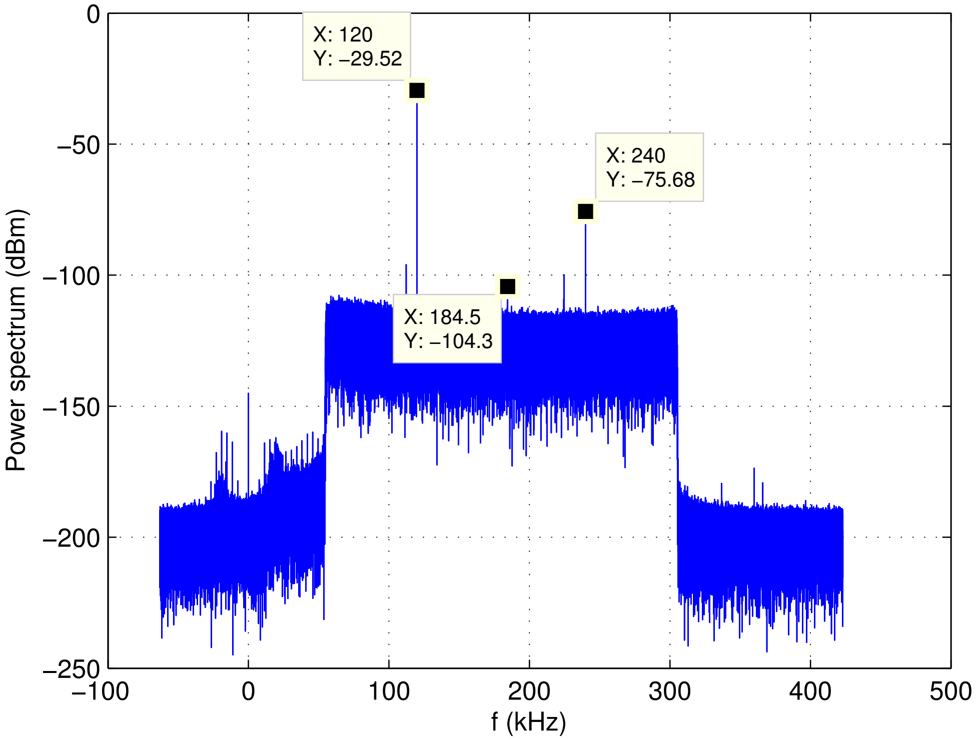


Figure 3.13: Power spectrum of signals created by setup shown in Figure 3.7. The tracking generator was generating a signal at 120 kHz, but the center frequency was at 180 kHz.

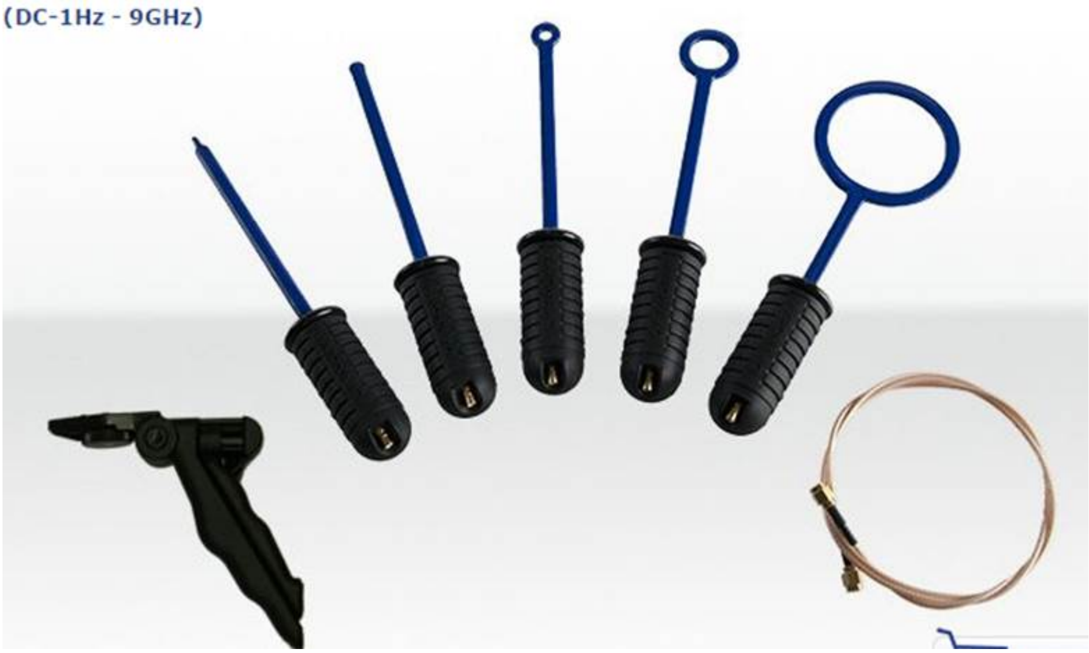


Figure 3.14: The Aaronia Near Field Probes. Image obtained from `http://www.aaronia.com/products/antennas/RF-Field-Probes-PBS1/`.

have 50-Ohm nominal impedance [3]. I measured electric field with an isotropic E-field probe. This probe has 9-GHz maximum resonance frequency. The magnetic field was measured with two probes. One probe has 6-mm sensor diameter and maximum resonance frequency of more than 6 GHz. The other probe has 50-mm sensor diameter and 700-MHz maximum resonance frequency.

Unfortunately, I was only able to see the signal of interest with the 50-mm magnetic field probe, likely because its loop has an area about 10 times large than the 6-mm sensor. One more measurement challenge was that the signal was noticed only in one specific location on the keyboard. The probes were moved at several-millimeter steps along the laptop surface until the signal of interest was found.

[3] `http://www.aaronia.com/products/antennas/RF-Field-Probes-PBS1/`

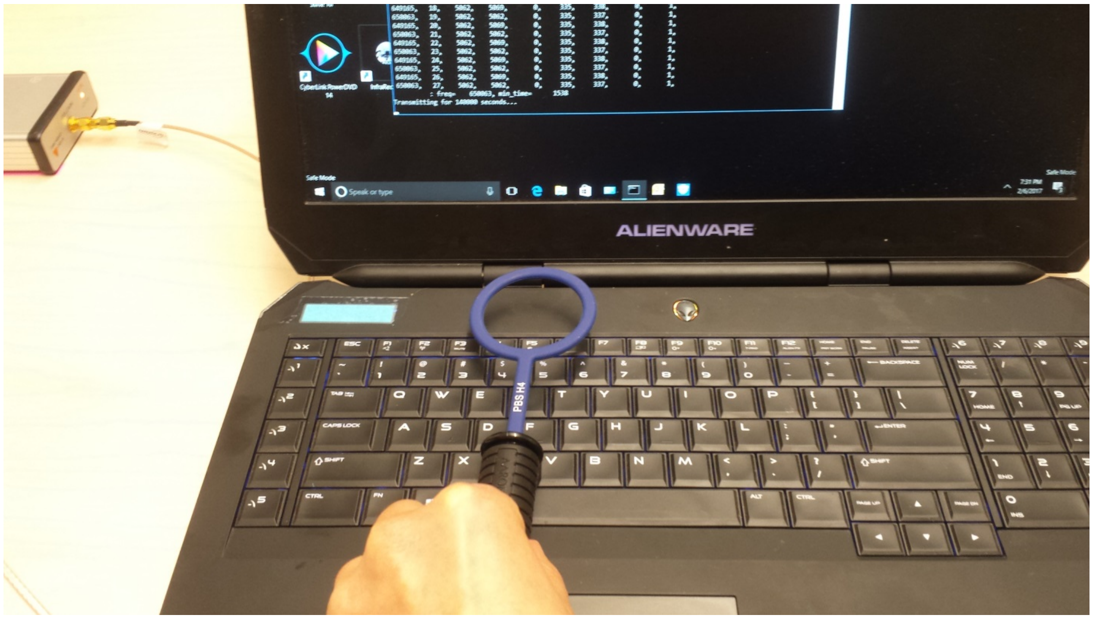
Chapter 4

CACHE HIT/MISS SIGNALS RADIATED FROM A LAPTOP COMPUTER

In this Chapter, I establish the kind of signals the cache hit/miss program causes to emanate from a laptop computer.

4.1 Experiment Setup

The SA was connected to the laptop with software for the spectrum analyzer. The laptop was connected to the power cord plugged in the room outlet (Room 4644 at the NWC). The output of the SA was connected to the 50-mm magnetic near field probe. The probe was set at 1 cm above testing laptop's keyboard (see Figure 4.1). This laptop was also connected to the power cord which was plugged in the room outlet. The testing laptop has an Intel i7-6700HQ processor. The processor runs at 2.6 GHz and has 4 cores, 2 threads per core, a 6-MB 12-way set associative L3 cache shared by all cores. Each core has a 256-kB L2 cache and a 32-kB 8-way set associative L1 data cache. A cache hit/miss program was running on the testing laptop. The description of the program is in Section 2.2. No isolations from the external EM signals were made. Before running the cache



```
649165,  18,  5062,  5069,   0,  335,  338,  0,  1,
650063,  19,  5062,  5062,   0,  335,  337,  0,  1,
649165,  20,  5062,  5069,   0,  335,  338,  0,  1,
650063,  21,  5062,  5062,   0,  335,  337,  0,  1,
649165,  22,  5062,  5069,   0,  335,  338,  0,  1,
650063,  23,  5062,  5062,   0,  335,  337,  0,  1,
649165,  24,  5062,  5069,   0,  335,  338,  0,  1,
650063,  25,  5062,  5062,   0,  335,  337,  0,  1,
649165,  26,  5062,  5069,   0,  335,  338,  0,  1,
650063,  27,  5062,  5062,   0,  335,  337,  0,  1,
          : freq=   650063, min_time=    1538
Transmitting for 140000 seconds...
```

Figure 4.1: The setup for cache hit/miss measurements relative to the testing laptop.

hit/miss program, the new setup needed to be checked for changes in the signals measured by the SA.

4.1.1 Spectrum Analyzer and Laptop with Software for the Spectrum Analyzer in a Room

In Figure 4.2, we see the power spectrum of the signals when the laptop from Figure 4.1 was taken out of room 4644 (see Figure 4.3). There are two peaks one at 118.3 and the other at 236.5 kHz in Figure 4.2 which are most likely related to the SA's internal signals. These values are shifted from the values of 107.2 and 214.3 kHz in Figure 3.4. The main reason for these shifts could be because of the connection of the SA to the magnetic near-field probe. It is also possible that the antenna was picking up some radiation from some other sources of radiation. The peak at 204 kHz corresponds to the center frequency 200 kHz.

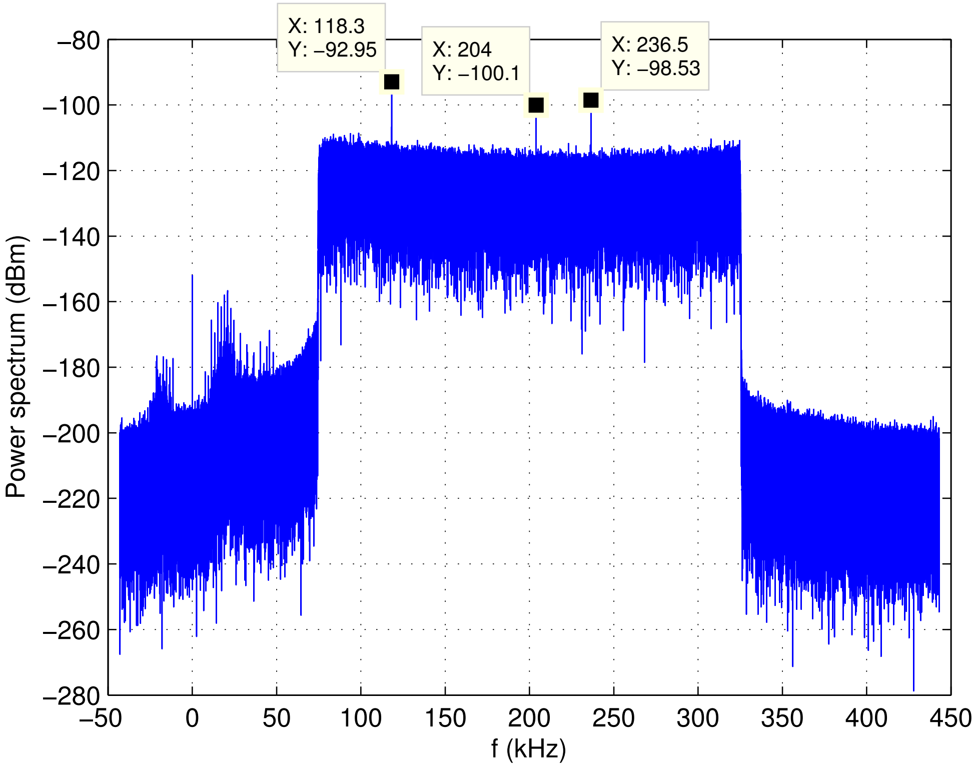


Figure 4.2: Power spectrum of signals created by setup shown in Figure 4.3. The center frequency was at 200 kHz.

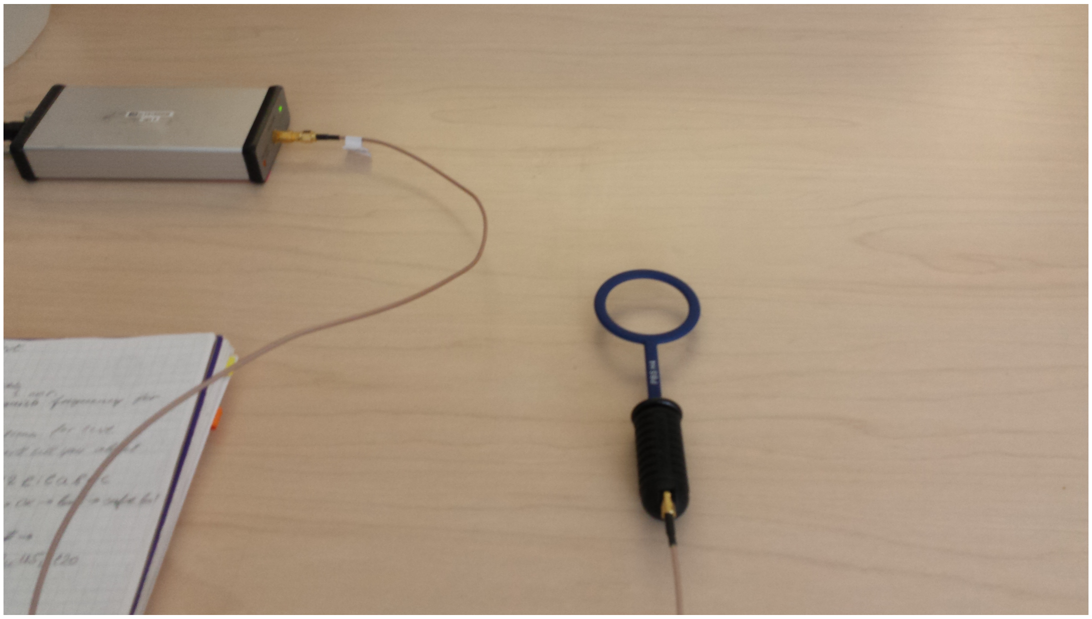


Figure 4.3: The setup for measurements when laptop from Figure 4.1 was taken out of the room.

4.1.2 Spectrum Analyzer, Laptop with Software for the Spectrum Analyzer, and Laptop for Running Cache Hit/Miss Program

Next measurement was performed when the testing laptop was turned on and only the operating system (OS) was running (Figure 4.4).

In Figure 4.5, we see the power spectrum for this case. All frequencies that are different from the frequencies in Figure 4.2, except the central frequency (peak is at 204 kHz), and signal's peak power is greater than -100 dBm are marked in Figure 4.4. There are 118.8 kHz (-96.58-dBm peak power), 152.6 kHz (-90.79-dBm peak power), 272.5 kHz (-94.98-dBm peak power), 277.9 kHz (-97.19-dBm peak power), and 305.3 kHz (-96.37-dBm peak power). There are also several peaks which have peak powers less or equal than -100 dBm, but greater than -103 dBm. These peaks locate at frequencies: between 101.7 and

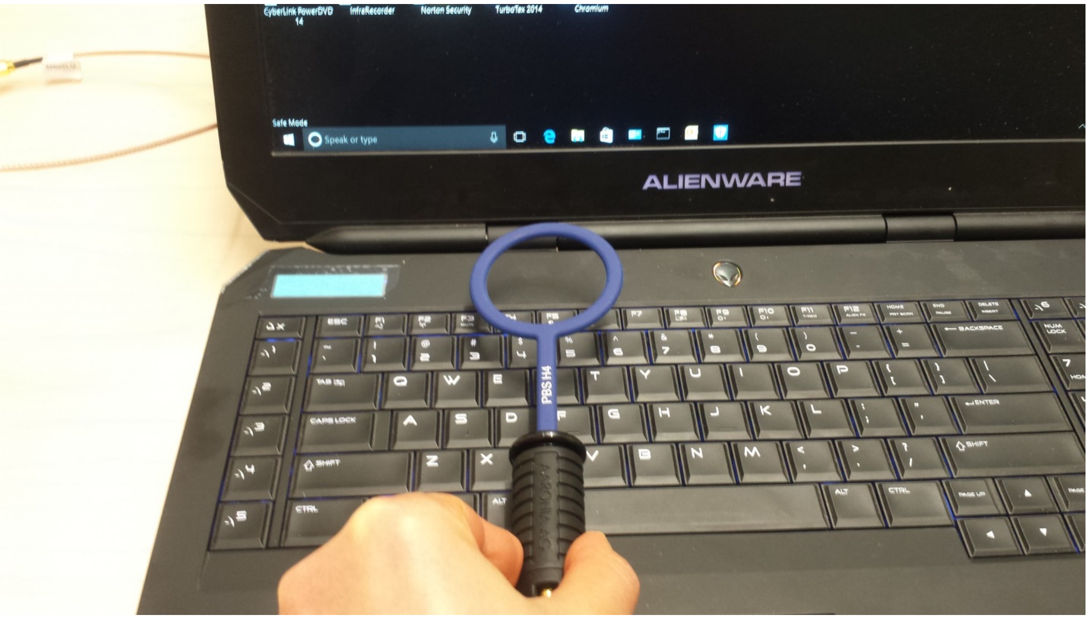


Figure 4.4: The setup for measurements when laptop from Figure 4.1 was idle.

104 kHz with values of the peak powers between -103 and -100.6 dBm, 206.9 kHz (-102-dBm peak power), 237.6 kHz (-102.5-dBm peak power), and 292.9 kHz (-101.7-dBm peak power). The origins of theses frequencies is unknown.

4.2 Cache Hit/Miss Program's EM Radiation

Several measurements when the cache hit/miss program was creating frequencies of 175, 180, 185, 650 kHz, and 1.65 MHz were made. The program was running for 10 min. The centered frequencies were 200 kHz for "program's frequencies" (1/T, see detailed explanation in Section 2.2) 175, 180, and 185 kHz, 700 kHz for "program's frequency" 650 kHz, and 1.7 MHz for "program frequency" 1.65 MHz.

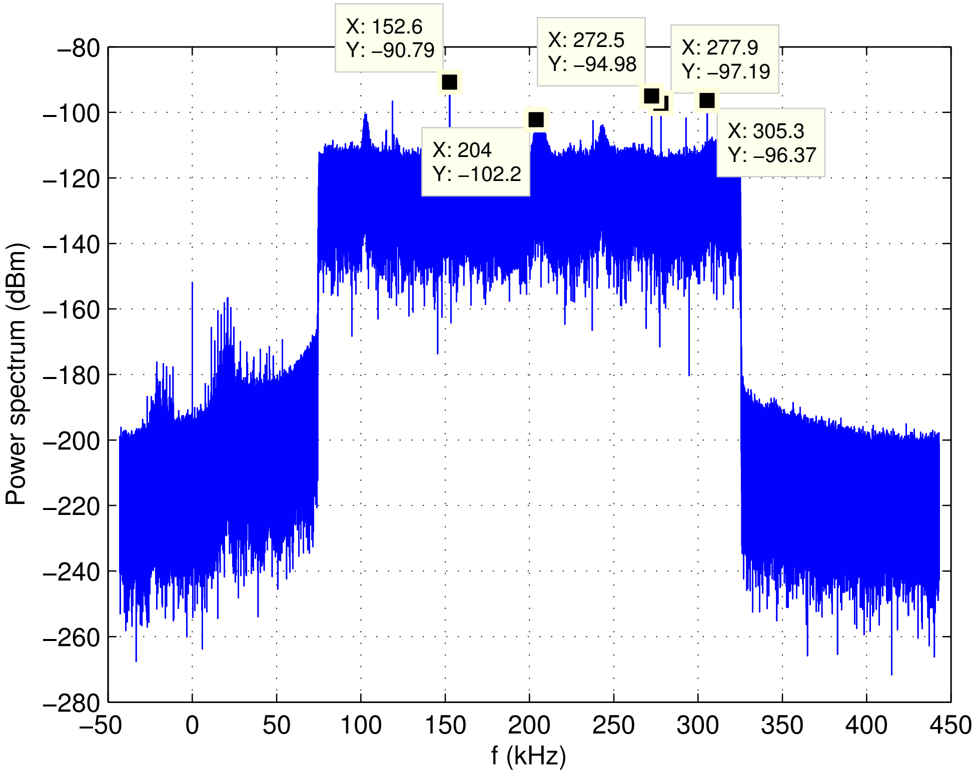


Figure 4.5: Power spectrum of signals when the testing laptop was idle. The center frequency was at 200 kHz.

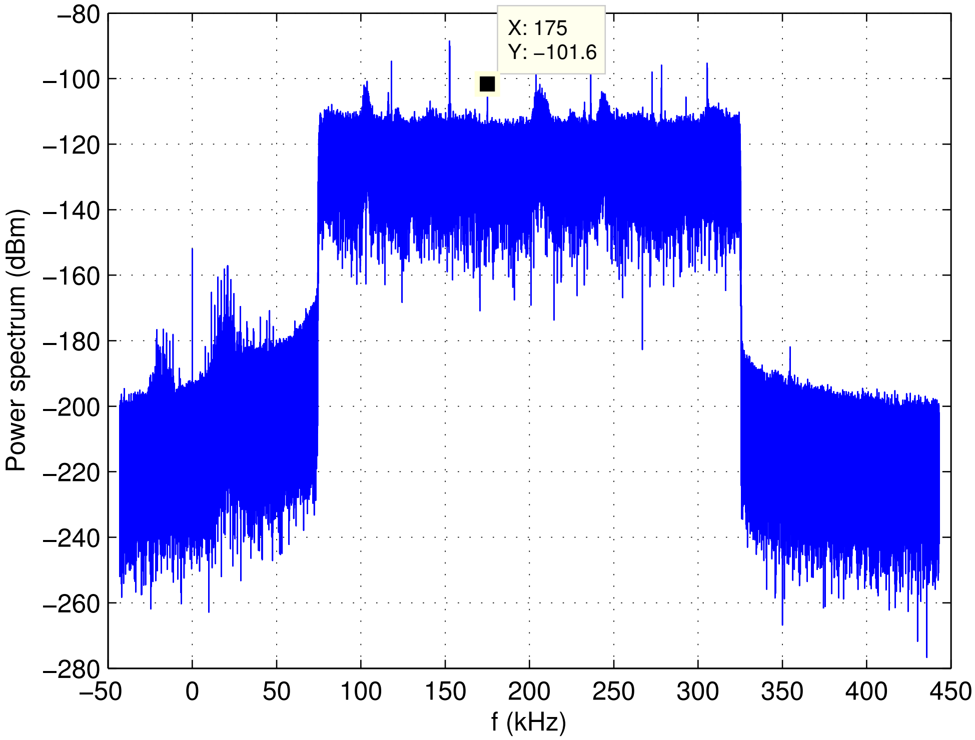


Figure 4.6: Power spectrum of signals when testing laptop was running LDL1/LDL2 instructions at frequency of 175 kHz and performing the cache hit/miss. The center frequency was at 200 kHz.

4.2.1 Center Frequency 200 kHz

4.2.1.1 Program's Frequency 175 kHz

In Figure 4.6, the power spectrum of the signals when the testing laptop was running LDL1/LDL2 instructions at frequency of 175 kHz and performing the cache hit/miss is presented. The center frequency was 200 kHz. Comparing Figures 4.5 and 4.6, we see a new peak with the value of the power of -101.6 dBm at frequency 175 kHz. It is exactly the program's frequency.

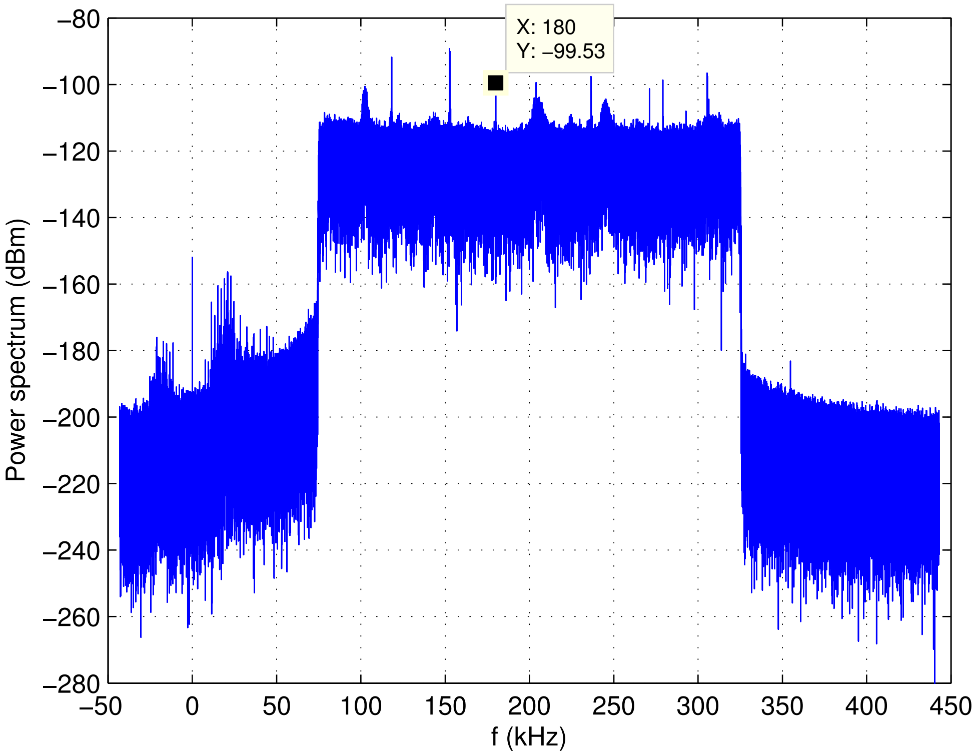


Figure 4.7: Power spectrum of signals when testing laptop was running LDL1/LDL2 instructions at frequency of 180 kHz and performing the cache hit/miss. The center frequency was at 200 kHz.

4.2.1.2 Program's Frequency 180 kHz

Next measurements of the EM leakage were performed at the program's frequency of 180 kHz, but with the same center frequency (200 kHz). In Figure 4.7, the power spectrum of this leakage is presented. As we see from Figure 4.7, there is no peak at 175 kHz, but there is a peak with power of -99.53 dBm at 180 kHz. It is one more additional piece of evidence that I am capturing the program's frequency.

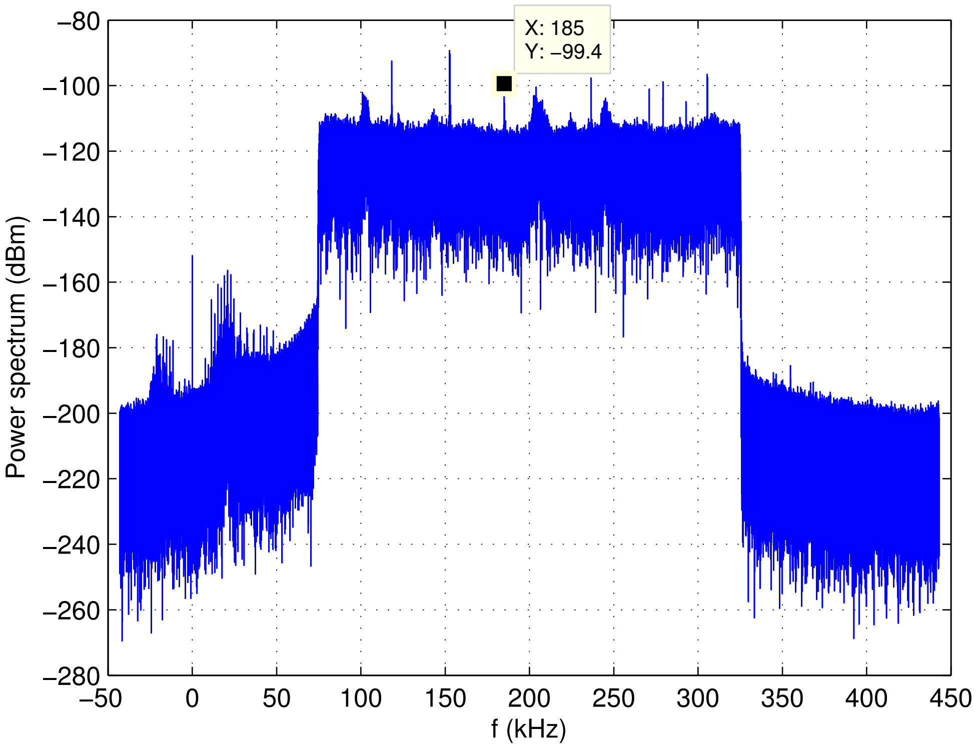


Figure 4.8: Power spectrum of signals when testing laptop was running LDL1/LDL2 instructions at frequency of 185 kHz and performing the cache hit/miss. The center frequency was at 200 kHz.

4.2.1.3 Program's Frequency 185 kHz

In this Section, the power spectrum of the signals when the testing laptop was running LDL1/LDL2 instructions at frequency of 185 kHz is shown. The center frequency is 200 kHz. As can be seen in Figure 4.8, the peak power of -99.4 dBm is at 185 kHz and there are no peaks at 175 and 180 kHz. This confirms that the cache hit/miss program EM leakage has been detected.

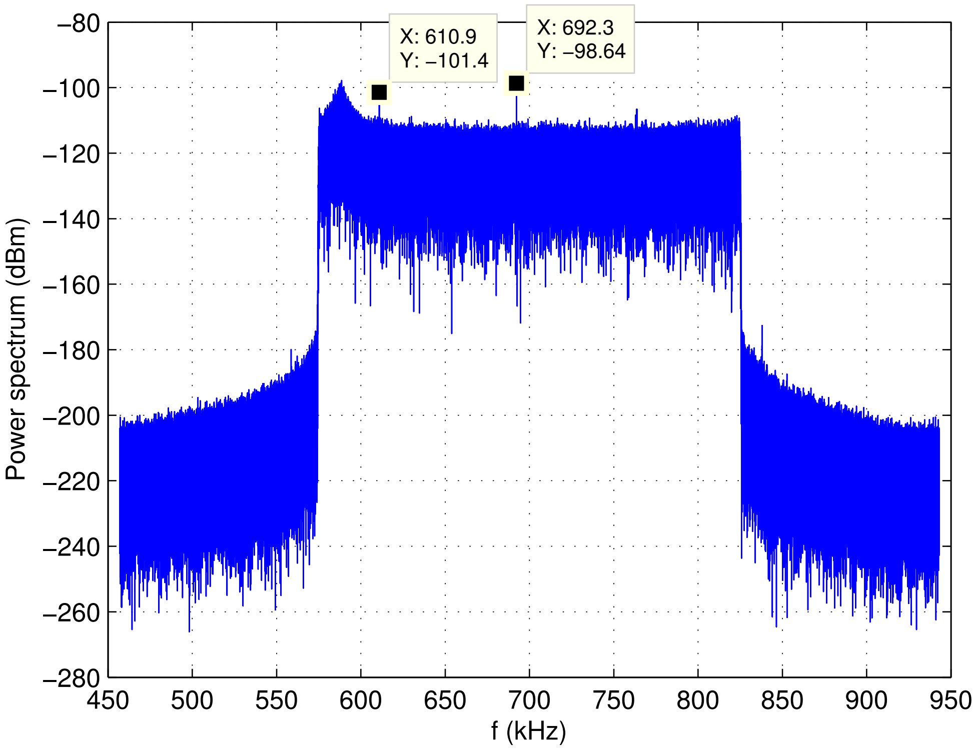


Figure 4.9: Power spectrum of signals when testing laptop was idle. The center frequency was at 700 kHz.

4.2.2 Center Frequency 700 kHz

4.2.2.1 The Testing Laptop Idle

For an addition experiment, the center frequency is 700 kHz. In order to distinguish the signals which related to the cache hit/miss program from other signals, I measured the EM signals from the testing laptop when only the OS was running. In Figure 4.9, the power spectrum of these signals is shown. There are two peaks in Figure 4.9. One is with -101.4-dBm peak power at 610.9 kHz. Its origin is unknown. The testing peak is with -98.64-dBm peak power at 692.3 kHz related to the center frequency.

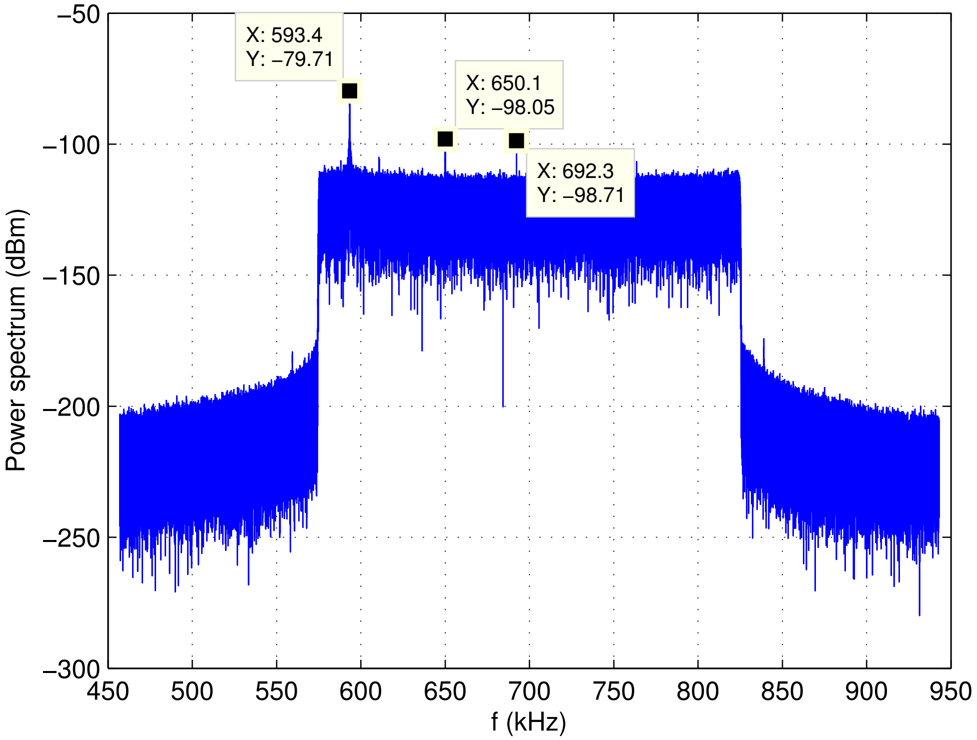


Figure 4.10: Power spectrum of signals when testing laptop was running LDL1/LDL2 instructions at frequency of 650 kHz and performing the cache hit/miss. The center frequency was at 700 kHz.

4.2.2.2 Program's Frequency 650 kHz

After the frequencies under computer idle regime were established, I set up the cache hit/miss program's frequency to be 650 kHz. In Figure 4.10, the power spectrum of the signals for this case is presented. As we can see in Figure 4.10, there are two peaks above the noise in addition to the center frequency peak. One peak is -79.71 dBm at 593.4 kHz. Its origin is unknown. The testing peak is -99.96 dBm at 650 kHz that is the program's frequency.

4.2.3 Center Frequency 1.705 MHz

4.2.3.1 Program's Frequency 1.65 MHz

In order to establish how high the value of the program's frequency can be, the program was run in MHz region. The highest frequency that allows program to run without crashing is 1.65 MHz. From the previous experience (see Sections 4.2.1 and 4.2.2), the program's frequency is very pronounced. Therefore, I skipped the measurements when the testing laptop is idle this time and measured only the EM leakage from the running cache hit/miss program. In Figure 4.11, the power spectrum of the signals when the testing laptop was running LDL1/LDL2 instructions at frequency of 1.65 MHz and performing the cache hit/miss is showed. The center frequency is 1.7 MHz. There are several peaks in Figure 4.11. The center frequency peak is -105 dBm at 1.705 MHz. One more peak near the center peak is -98.41 dBm at 1.708 MHz with unknown origin. The program's peak is -106.2 dBm at 1.651 MHz. The peak at 1.783 MHz is also related to the program, but the meaning of that peak is unknown.

4.2.4 Origin of the EM Leakage

The last question addressed in this thesis is where is the origin of the EM leakage? In Figure 4.12, we see the hardware of the testing laptop. The violet circle corresponds to the location where the signal of the cache hit/miss EM leakage has the maximum amplitude. As we see in Figure 4.12, it is on the left side from the processor. When the antenna moved to the left or right sides from that location, the magnitude of the signal attenuated rapidly. Therefore, the processor is the source which creates the EM leakage during execution of the cache hit/miss program.

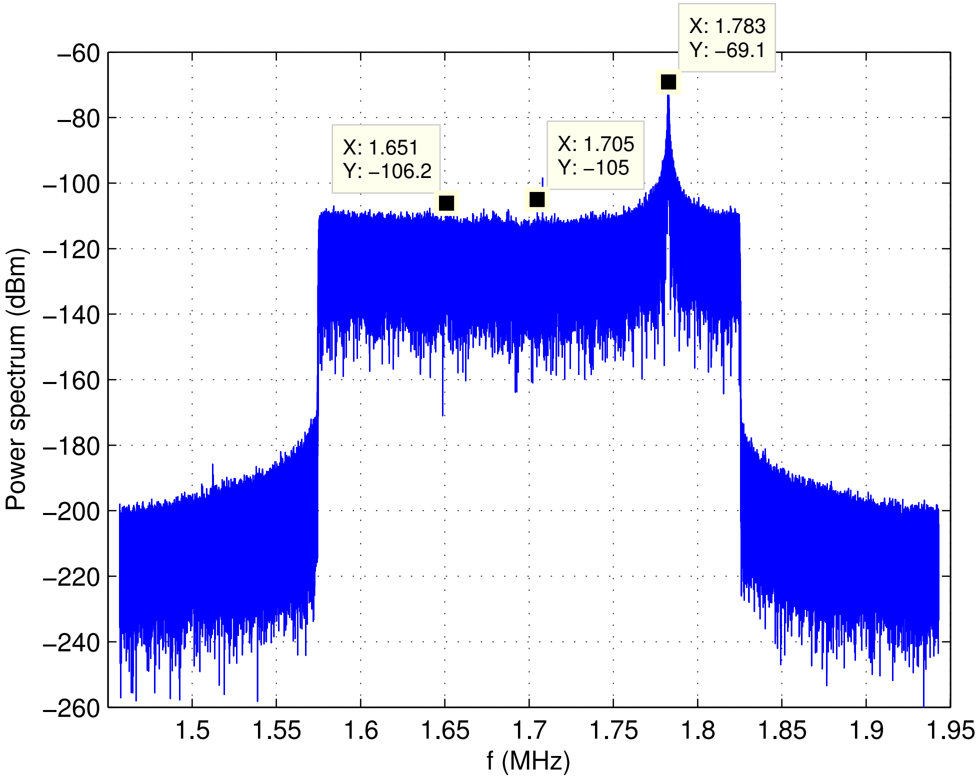


Figure 4.11: Power spectrum of signals when testing laptop was running LDL1/LDL2 instructions at frequency of 1.65 MHz and performing the cache hit/miss. The center frequency was at 1.7 MHz.

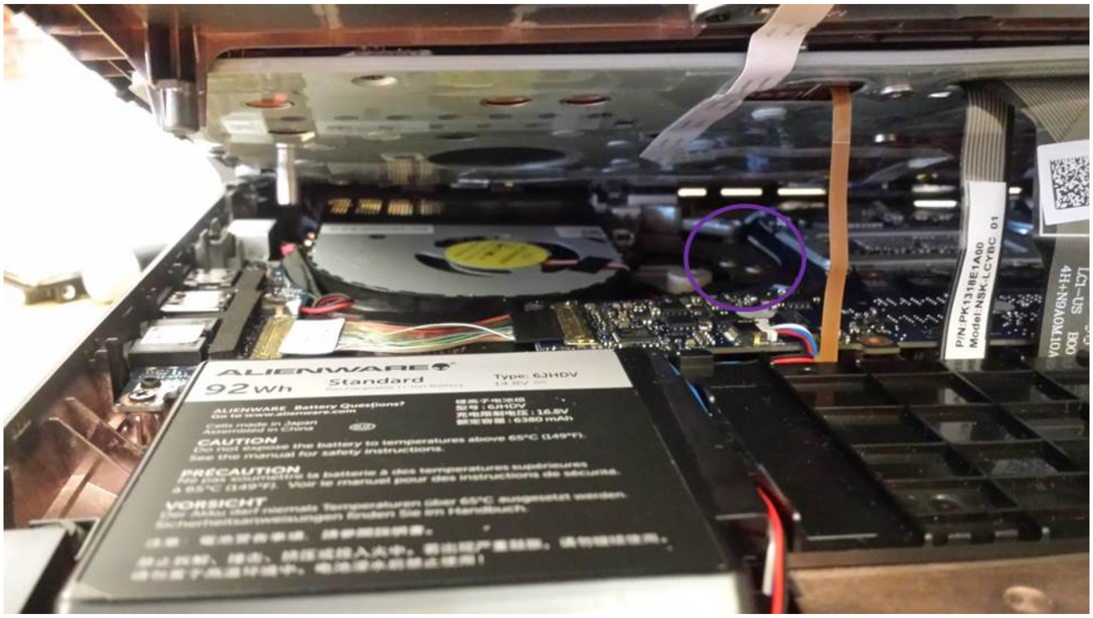


Figure 4.12: Internal hardware of the testing laptop.

Chapter 5

CONCLUSIONS

The possibility of using electromagnetic signals of modern laptops for stealing information from them has been explored. For that purpose, five sets of measurements were made: 1) EM signals from the spectrum analyzer by itself, 2) EM signals of the spectrum analyzer that was fitted by the tracking generator, 3) EM signals from the testing laptop's location in absence of the laptop measured with 50-mm magnetic probe which was connected to the SA, 4) similar to the previous set but the testing laptop was in the room and was turn on, 5) similar to the previous set but the cache hit/miss program was running on the testing laptop which was creating an EM leakage. The cache hit/miss program has two loops: LDL1 and LDL2 with the total period T. Thus, the program was creating 1/T frequency that was possible to measure with the 50-mm magnetic probe connected to the SA. I have determined that the frequency measured is the one that the running program was creating. Therefore, I conclude that it is possible to detect that a program is running on modern laptops by measuring their electromagnetic signals.

It is possible to determine the frequency of a periodic program fairly easily. To determine the actual information content or exchange within the laptop is much harder to accomplish. For this, one needs to lock onto the internal clock and read time series information that is shuffled between registers. This, however, requires a much more sophisticated set up, possibly including specialized hardware. To my knowledge, this has not yet been done. Therefore, it can be considered as topic for future work.

Bibliography

Aciiçmez, O., Ç.K. Koç, and J.-P. Seifert, 2007: On the power of simple branch prediction analysis. *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security*, Singapore, ACM Special Interest Group on Security, Audit, and Control.

Agrawal, D., B. Archambeult, J. Rao, and P. Rohatgi, 2002: The EM side-channel(s). *Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, Redwood Shores, CA, USA, International Association for Cryptologic Research.

Bangerter, E., D. Gullasch, and S. Krenn, 2011: Cache games - bringing access-based cache attacks on AES to practice. *Proceedings of the 32nd IEEE Symposium on Security Privacy*, Oakland, California, USA, IEEE Computer Society Technical Committee on Security Privacy.

Bayrak, A., F. Regazzoni, P. Brisk, F.-X. Standaert, and P. Ienne, 2011: A first step towards automatic application of power analysis countermeasures. *Proceedings of the 48th Design Automation Conference*, San Diego, California, USA, Association for Computing Machinery.

Biham, E., and A. Shamir, 1997: Differential fault analysis of secret key cryptosystems. *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, Santa Barbara, California, USA, International Association for Cryptologic Research.

Callan, R., A. Zajić, and M. Prvulovic, 2014: A practical methodology for measuring the side-channel signal available to the attacker for instruction-level events. *Proceedings of the 47th Annual IEEE/ACM International Symposium on Microarchitecture*, Cambridge, UK, IEEE Computer Society Technical Committee on Microprogramming Microarchitecture.

Chen, J., and G. Venkataramani, 2014: CC-Hunter: Uncovering Covert Timing Channels on Shared Processor Hardware. *Proceedings of the 47th Annual IEEE/ACM International Symposium on Microarchitecture*, Cambridge, UK, IEEE Computer Society Technical Committee on Microprogramming Microarchitecture.

Coppens, B., I. Verbauwhede, K. de Bosschere, and B. de Sutter, 2009: Practical Mitigations for Timing-Based Side-Channel Attacks on Modern x86 Processors. *Proceedings of the 30th IEEE Symposium on Security Privacy*, Oakland, California, USA, IEEE Computer Society Technical Committee on Security Privacy.

Evtyushkin, D., J. Elwell, M. Ozsoy, D. Ponomarev, N. Ghazaleh, and R. Riley, 2014: Iso-x: A flexible architecture for hardwaremanaged isolated execution. *Proceedings of the 47th Annual IEEE/ACM International Symposium on Microarchitecture*, Cambridge, UK, IEEE Computer Society Technical Committee on Microprogramming Microarchitecture.

Gandolfi, K., C. Mourtel, and F. Olivier, 2001: Electromagnetic analysis: concrete results. *Proceedings of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems*, Paris, France, International Association for Cryptologic Research.

Genkin, D., A. Shamir, and E. Tromer, 2017: Acoustic cryptanalysis. *J Cryptol*, **30 (2)**, 392–443.

Giraud, C., 2004: DFA on AES. *Proceedings of the 4th international conference on Advanced Encryption Standard*, Bonn, Germany, US National Institute of Standards and Technology.

Highland, H., 1986: Electromagnetic radiation revisited. *Computers Security*, **5 (2)**, 85–93.

Kocher, P., 1996: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. *Proceedings of the 16th Annual International Cryptology Conference*, Santa Barbara, California, USA, International Association for Cryptologic Research.

Kocher, P., J. Jaffe, and B. Jun, 1999: Differential power analysis: leaking secrets. *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, Santa Barbara, California, USA, International Association for Cryptologic Research.

Sekiguchi, H., and S. Seto, 2013: Study on maximum receivable distance for radiated emission of information technology equipment causing information leakage. *IEEE Transactions on Electromagnetic Compatibility*, **55 (3)**, 547–554.

Tsunoo, Y., E. Tsujihara, K. Minematsu, and H. Miyauchi, 2002: Cryptanalysis of Block Ciphers Implemented on Computers with Cache. *Proceedings of International Symposium on Information Theory and its Applications*, Xian, China, Society of Information Theory and Its Applications.

van Eck, W., 1985: Electromagnetic radiation from video display units: an eavesdropping risk? *Computers Security*, **4 (4)**, 269–286.

Zajić, A., and M. Prvulovic, 2014: Experimental demonstration of electromagnetic information leakage from modern processor-memory systems. *IEEE Trans. Electromagn. Compat.*, **99 (3)**, 1–9.