CHAPTER – 6
ATTACKING AND COUNTER ATTACKING THROUGH ELECTRO MAGNETIC ANALYSIS
6.0 ATTACKING AND COUNTER ATTACKING THROUGH ELECTRO MAGNETIC ANALYSIS

6.1 ATTACKING THROUGH ELECTRO MAGNETIC ANALYSIS

6.1.1 Attacking through Electro Magnetic Analysis – Overview

In the Electro Magnetic Analysis (EMA) attacks, the device under attack emits different amounts of Electro Magnetic emission during the computation of the encryption algorithm depending on the instructions and the data being executed.

6.1.1.1 Classification of Electro Magnetic Analysis attacks

The EMA attacks can be classified as Simple Electro Magnetic Analysis (SEMA) attacks and Differential Electro Magnetic Analysis (DEMA) attacks. In a SEMA attack, an adversary is in a position to extract compromising information from a single EM(Electromagnetic sample). If a computation makes use of conditional branches based on secret information, then on a compromising EM signal, this can be observed as relative shifts in the distances between major computational structures. In some cases, these shifts may be sufficient to reveal the branch taken, which in turn confirms the value of the secret information.

Differential Electro Magnetic Analysis (DEMA) involves hypothesizing a secret key, taking a large number of measurement of EM traces, dividing these traces into two partitions according to the intermediate results, averaging each partition to remove noise, and finally computing the differential trace which is the difference between the average of the two partitions.

6.1.1.2 Origin of Electro Magnetic Emanations:

To comprehend the origin of electromagnetic emissions, it is necessary to know the Maxwell’s equations. Four equations form a complete description of electric and magnetic fields and their interaction. The first equation is Gauss’s law for
electricity which says that electric field diverges from electric charge. The second is Gauss’s law for magnetism which says that there are no isolated magnetic poles. The third equation is Faraday’s law of induction which says that electric fields are produced by changing magnetic fields. The last one is Ampere’s law which says that circulating magnetic fields are produced by changing electric fields and by displacement currents in dielectric.

\[ \varepsilon_0 \oint E \cdot ds = q \]  \hspace{1cm} (1)

\[ \oint B \cdot ds = 0 \]  \hspace{1cm} (2)

\[ \oint E \cdot dl = \frac{d\Phi_B}{dt} \]  \hspace{1cm} (3)

\[ \oint B \cdot dl = \mu_0 (\varepsilon_0 \frac{d\Phi_E}{dt} + i) \]  \hspace{1cm} (4)

Where,

E= Electric Field Strength, \( \frac{V}{m^2} \)

B= Magnetic Flux Density, Tesla or N / A . m

\( \varepsilon_0 = 8.85418782 \times 10^{-12} \frac{F}{m} \), Permittivity of a vacuum

\( \mu_0 = 4\pi \times 10^{-7} \frac{H}{m} \), Permeability of a vacuum

The second and fourth equations clearly explain the reason for release of electromagnetic emanations from an embedded system. The changing current flowing in a closed loop produces changing magnetic field which in turn produces changing electric field so on and so forth.

6.1.1.3 Relationship between Electro Magnetic Wave to Maxwell’s Equations

We assume that at some distance away from the source of Electro Magnetic (EM) waves, there is no charge density \( \rho \) and no current density \( J \). For that region of space, the microscopic Maxwell’s equations becomes (in SI units)
\[ \nabla \cdot \mathbf{B} = 0, \quad \nabla \cdot \mathbf{E} = 0, \]

and

\[ \nabla \times \mathbf{B} = \frac{1}{c^2} \frac{\partial \mathbf{E}}{\partial t}, \quad \nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}. \]

Applying to the last Maxwell equation the following relation, known from vector analysis and valid for any (differentiable) vector field,

\[ \nabla \times (\nabla \times \mathbf{E}) = \nabla (\nabla \cdot \mathbf{E}) - \nabla^2 \mathbf{E} \]

and \( \mathbf{E} \) satisfies the wave equation,

\[ \nabla^2 \mathbf{E} = \frac{\partial (\nabla \times \mathbf{B})}{\partial t} = \frac{1}{c^2} \frac{\partial^2 \mathbf{E}}{\partial t^2}. \]

Note that the displacement current (time derivative of \( \mathbf{E} \)) is essential in this equation. If it were absent (zero), the field \( \mathbf{E} \) would be a static, time-independent electric field and there would be no waves. In the very same way, this wave equation can be proved for \( \mathbf{B} \) as

\[ \nabla^2 \mathbf{B} = \frac{1}{c^2} \frac{\partial^2 \mathbf{B}}{\partial t^2}. \]

From the above equations we can observe that \( \mathbf{E} \) and \( \mathbf{B} \) are related by the third and fourth Maxwell’s equation, which express the fact that a displacement current causes a magnetic field, and a changing magnetic field causes an electric field respectively. So, a time-dependent electric field that is not associated with a time-dependent magnetic field cannot exist and conversely.

The circuits that cause these fields are mainly of two types. They are Time variant electric circuits and Time variant magnetic circuits. Of these numerous
emanations, those induced by data processing operations carry the most compromising information. In CMOS devices, ideally, current only flows when there is a change in the logic state of a device. In addition, all data processing is typically controlled by a “square-wave” shaped clock. Each clock edge triggers a short sequence of state changing events and corresponding currents in the data processing units.

6.1.1.4 Types of Electro Magnetic Emanations:

There are two broad categories of Electro Magnetic emanations which include direct emanations, un-international emanations. Direct Emanations result from intentional current flows. Many of these consist of short bursts of current with sharp rising edges which result in emanations observable over a wide frequency band. Often, components at the higher frequencies prove more useful to the attacker due to overwhelming noise and interference prevalent in the lower frequency bands. In complex circuits, isolating direct emanations can be difficult and may require use of tiny field probes positioned very close to the signal source and/or special filters so as to minimize interference from other signal sources; getting good results may necessitate having to de-capsulate the chip packaging.

Unintentional Emanations are due to increased miniaturization and complexity of modern CMOS devices results in electrical and electromagnetic coupling between components in close proximity. Such couplings, while inconsequential from the perspective of a circuit designer, provide a rich source of compromising emanations to the attacker. These emanations manifest themselves as modulations of carrier signals generated, present or “introduced” within the device. One strong source of carrier signals is the harmonic-rich “square-wave” clock signal propagated throughout the device. Other sources include communication related signals. Some of
the ways in which modulation occurs include Amplitude Modulation (AM) and Angle Modulation (FM or Phase Modulation).

6.1.1.5 Identification of probes for sensing EMA

Chip-scale electromagnetic analysis requires very small probes, similar in dimension to the chip areas to be isolated. The standard layout of a smart card chip shows functional blocks of a few hundred microns (CPU, crypto processor). This defines an upper bound for the probe size.

Several experiments are conducted using different kinds of probes which include, hard disk heads, integrated inductors and magnetic loops to determine the EM signals and it was proved that solenoid based probes are the best suited as they produce clean EM Signal due to the reason that the solenoids are made of a coiled copper wire of outer diameters varying between 150 and 500 microns. An example is shown in [Fig: 6.1].

![Figure 6.1 Probe for Electromagnetic Emanations](image)

Simple dipole antennas are well suited for the reception of narrow-band signals, where a good estimate for the frequency of interest is known and the signal has a bandwidth of not more than about a tenth of a frequency. The directional gain of dipoles can be increased by up to about 12 dB with the addition of director and reflector dipoles around the receiving dipole. This construction is known as a Yagi-
Uda antenna, and forms – usually with a folded reception dipole – the most common VHF/UHF household TV antenna.

Dipoles and Yagi antennas tuned to an exact frequency are not necessarily the best choice for compromising emanations experiments though. Most forms of compromising emanations are broadband signals, which means that the lower and upper frequency limit of information carrying emanations can differ by a factor of two or more. Several broadband antenna types have been developed, which offer reasonably constant impedance over a wide frequency range.

Yagi antennas are nevertheless an excellent choice for actual attacks in circumstances where VHF/UHF frequency with the highest information content is known precisely, the bandwidth is not much higher than 1/10 of the center frequency and the attacker has the time to construct an antenna for a particular eavesdropping target. Where compactness of the antenna is not a major concern, entire arrays of Yagi antennas can be connected together to increase the effective aperture. This might be feasible, for example, if the eavesdropper can operate behind a number of large windows from a nearby building.

Broadband antennas, on the other hand, have a good impedance match over a wide frequency range, but lack good directional gain. They are best suited for laboratory work, where the emanations of a device have to be characterized for a threat assessment or for the preparation of an eavesdropping operation. Some compact examples can be seen in [Fig: 6.2].

The first approach for constructing a broadband antenna is a dipole with very thick wires, for example, shaped as cylinders or cones. A dipole is an LC oscillator, whose frequency selectivity (quality factor) depends on the L/C ratio. Thick dipoles
have larger capacitance and lower inductance; the resulting low L/C ratio makes them less frequency selective.

Figure 6.2 Examples of different broadband antenna types

The antennas shown in Figure 6.2 include log-periodic antenna (200–1000 MHz), discone (200–1300 MHz), active monopole (100 Hz–30 MHz), bi-conical antenna (30–300 MHz), and active ferrite loop (H-field, 100 Hz–30 MHz with four different ferrite rods).

An implementation of this idea is the bi-conical antenna (30–300 MHz) commonly used for VHF EMC field-strength measurements. The second approach is the careful combination of a number of dipoles of varying length to cover the entire desired band, leading to logarithmic-periodic antenna, which is commonly used for EMC field-strength measurements in the lower UHF range (200–1000 MHz). It consists of two metal rods, to which in alternating polarity a series of dipoles are connected. The entire antenna has a triangular shape as the length of a dipole is proportional to its distance from the triangle’s tip, which points in the direction of maximum gain. The gain factor of the antenna depends on the periodicity τ, the length
ratio of neighboring dipoles, and it is typically about 3–6 dB (for $0.60 < \tau < 0.85$) better than that of a single dipole.

The third approach is horn antennas. They smooth the impedance mismatch between a transmission line and free space by gradually extending the geometry of the transmission line until its impedance approaches to free space. This avoids the reflection of energy caused by any abrupt change of impedance. The discone antenna is an example that combines the principles of a horn antenna with that of a broadband dipole. It is widely used as an omnidirectional reception antenna for receivers that work over large parts of the UHF spectrum. The ground shield of a coaxial cable is connected to a metallic cone with an angle of $60^\circ$ and a length $l = 0.35c/f_l$, where $f_l$ is the lowest supported frequency. The inner conductor is connected to a metal disc above the cone, whose diameter is 70% of the maximum diameter of the cone. Such a discone antenna provides a SWR < 2 to a 50 cable over a frequency range from $f_l$ to $10f_l$.

The fourth approach is the active antenna. Instead of relying on the inductance and capacitance of a dipole matching the impedance of the transmission line, a monopole much shorter than the wavelength is used to probe the electric field strength. An amplifier circuit with high input impedance (e.g., 10 M) is connected directly to the base of the monopole. It converts the high-impedance voltage appearing on the antenna rod into a 50 output impedance signal suitable for transmission via a coaxial cable.

Active antennas are the only compact antennas available for sensitive field-strength measurements in the 100 Hz–30 MHz range. Depending on whether a metallic rod or a ferrite core loop is connected to the amplifier, an active antenna can measure either E- or H-field strength, a distinction that is of particular interest in the
frequencies below the VHF range, where an eavesdropper might well be located in the near-field of an emitting device. The active E- and H-field antenna that is part of the Dynamic Sciences R-1150-10A Portable Antenna Kit that is being used is a two-stage zero-gain amplifier using two n-channel JFET transistors (2N5397 and MPF820). It features two separate amplifiers, one with 10 M input impedance for connection of the E field monopole (1 m), the other with 200 k input impedance for connection with one of four interchangeable ferrite loops (100 Hz–50 kHz, 50 kHz–1.5 MHz, 1.5–10 MHz, 10–30 MHz).

6.1.2 Previous work related to Attacking through Electro Magnetic Analysis

The basic premise of these attacks is that they attempt to measure the electromagnetic radiation emitted by a device to reveal sensitive information. Successful deployment of these attacks against a single chip would require intimate knowledge of its layout, so as to isolate the region around which electromagnetic radiation measurements must be performed.

Electromagnetic analysis attacks are classified into two types. They are Simple Electromagnetic Analysis (SEMA) and Differential Electromagnetic Analysis (DEMA). In a SEMA attack, an attacker is able to extract compromising information from a single EM sample. If a computation makes use of conditional branches based on secret information, then on a compromising EM signal, this can be observed as relative shifts in the distances between major computational structures. In some cases, these shifts may be sufficient to reveal the branch taken, which in turn confirms the value of the secret information. This is analogous to what has already been demonstrated for power sample by Kocher, 1999 [35]. Thus conditional statements in the code could provide valuable opportunities for both SPA (Simple power analysis) and SEMA. The interesting case is where SEMA attacks are successful in extracting
information on when SPA attacks fail. This is possible if an EM signal for some instruction leaks more information than the power side-channel.

**Wim Van Eck, 1996 [50]** presented a method to attack a video display unit and the possible counter attacks were discussed. To prove that eavesdropping is feasible in a practical situation, a simple experiment was carried. The equipment (dipole antenna, TV receiver, and synchronization oscillators) was put in a car, which was placed in the car park of a building in which a word processor was being used. An attempt was then made to copy the information from this word processor's video unit by taking photographs of the screen of the receiving television set.

**Dakshi Agarwal et al., 2006 [10]** suggested a systematic investigation of the leakage of compromising information via electromagnetic (EM) emanations from chip cards and other devices. This information leakage differs substantially from and is more powerful than the leakage from other conventional side-channels such as timing and power.

EM emanations are shown to consist a multiplicity of compromising signals, each leaking somewhat different information. The experimental results confirm that these signals could individually contain enough leakage to break cryptographic implementations and to defeat countermeasures against other side-channels such as power. Using techniques from Signal Detection Theory, they showed that generalized and far more devastating attacks can be constructed from an effective pooling of leakages from multiple signals derived from EM emanations. The magnitude of EM exposure demands a leakage assessment methodology whose correctness can be rigorously proved. They defined a model that completely and quantitatively bounds the information leaked from multiple EM side-channel signals in CMOS devices and use that to develop a practical assessment methodology for devices such as chip cards.
Eric Peeters, et al., 2006 [14] considered CMOS inverter to conduct the EM attack. Most chips are designed in CMOS technology. The CMOS technology is certainly the most widely used in current digital design applications. They started with a simple gate, namely the inverter which is the nucleus of all CMOS IC's. Static CMOS gates have three distinct dissipation sources. The first one is due to the leakage currents in transistors. Its contribution to the overall dissipation is in general very small. The second one is due to the so-called direct path current": there exists a short period during the switching of a gate while NMOS and PMOS are conducting simultaneously.

Finally, the most important dissipation (and most relevant from a side-channel point of view) is due to the charge of the load capacitance. This capacitance is composed from different parasitic capacitances (junctions, gates...) and the wiring capacitance (interconnections). In CMOS devices, when measuring the power consumption (either at the ground pin or at the power pin), the highest peak will therefore appear during the charge of this capacitance. During the discharge, the only current we can measure is the direct path current. They simulated and measured a simple CMOS gate to support this assumption.

E. De Mulder et al., 2005 [13] conducted Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem. They focused on presenting simple (SEMA) and differential (DEMA) electromagnetic analysis attacks on an FPGA implementation of an elliptic curve processor. Elliptic curve cryptography is a public key cryptosystem that is becoming increasingly popular.

Kerstin Zangl et. al., 2004 [33] wrote a program that could determine the exact key out of one round of the AES (Advanced Encryption Standards). This is done by measuring electromagnetic radiation that occurs when the AES runs on a chip.
and then the data is analyzed by the correlation coefficient. They have explained a method using which the secret key is measured out of one round of AES with the help of EM measurements. After a short introduction of the SCA (side channel analysis) and the AES, he directly started with the attack.

**Jonas karlsson, 2003 [22]** proposed a thesis on TEMPEST attacks using a simple radio receiver. He proved that there exists a TEMPEST technique that is cheap and relatively simple but poses a security risk. He proved TEMPTEST with facts from literature studies and an experiment. Today there is only one way to protect you against TEMPEST attacks and that is by metal shielding. This is expensive and home users have the option but not often the resources to finance this type of protection.

The methods presented in the literature do not take account any non-linearity’s that exists in the electromagnetic emanations. **Subba Rao et al., 2010 [30]** have presented an experimental setup using which EMA is captured for many sample of inputs fed to the encryption algorithm and they have shown that secrecy can be revealed by observing the inputs and outputs related to a sample. A simple EMA probe has been used as shown in the [Figure 5.1].

### 6.1.3 Problem Definition

The methods that could be used for sensing EMA emitted due to the execution of instructions contained in a program which is meant for undertaking RSA encryption are required. The reveling of secrecy built into an encryption algorithm based on EMA radiation requires conducting many experiments for collecting EMA data for different input situations which include data such as MAC code, KEY value, Type of algorithm used etc., In all the methods defined in the literature, one or two experiments are conducted just to prove the concept. Few experiments will not precisely expose the information that has been encapsulated into an encryption
algorithm. Many experiments are needed to accurately assess the secrecy contained in crypto server by exploring the type of execution undertaken by the encryption program.

One of the most important issue that has not been discussed in the literature is the way EMA is sensed and converted into data, meaning the way the EMA is represented in terms of data. EMA is emitted in a stream on a continuous basis. A set of EMA measurements together represent a single execution unlike other kinds of side channel attacks.

It is important that most effective EMA probing system that is simple and accurate is to be selected and the same is to be used for continuous probing and generating the streamed data which is stored in a data base along with other operating data. The data base can be called as knowledge base which can be analyzed for a set of operating conditions and reveal the secrecy of the encryption algorithm.

Experimental models thus are required for creating a Knowledge base which contains data collected out of experimenting by varying operating conditions and with continuous streaming of EMA and probing the same with accurate method and convert the same into data equivalent. The data base can be queried for a particular operating conditions and the secrecy used for undertaking the encryption is revealed.

6.1.4 Comparison of existing attacking methods – Electro Magnetic Analysis

As said in the problem definition, it is important to select a most important probing method as it is the main source used for attacking crypto server system. A comparison of the methods proposed in the literature is made which is shown in the [Table 6.1].
<table>
<thead>
<tr>
<th>Serial Number of the Method</th>
<th>Author</th>
<th>Year</th>
<th>Method</th>
<th>Accuracy</th>
<th>Complexity</th>
<th>Speed</th>
<th>Experimentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Kocher</td>
<td>1999</td>
<td>Single EMA simple</td>
<td>Less</td>
<td>Less</td>
<td>High</td>
<td>Less</td>
</tr>
<tr>
<td>2.</td>
<td>Wim Van Eck</td>
<td>1996</td>
<td>Use of simple antenna</td>
<td>Med</td>
<td>High</td>
<td>High</td>
<td>Less</td>
</tr>
<tr>
<td>3.</td>
<td>Dakshi Agarwal</td>
<td>2006</td>
<td>Theoretical signal detection theory</td>
<td>Less</td>
<td>High</td>
<td>Less</td>
<td>Less</td>
</tr>
<tr>
<td>4.</td>
<td>Eric Peters</td>
<td>2006</td>
<td>CMOS inverter</td>
<td>Med</td>
<td>High</td>
<td>High</td>
<td>Less</td>
</tr>
<tr>
<td>5.</td>
<td>E. De Mulder</td>
<td>2005</td>
<td>Simple EMA probing</td>
<td>High</td>
<td>Less</td>
<td>High</td>
<td>Less</td>
</tr>
<tr>
<td>6.</td>
<td>Kerstin Zangl</td>
<td>2004</td>
<td>One round AES, Theoretical probing</td>
<td>Less</td>
<td>Less</td>
<td>High</td>
<td>Less</td>
</tr>
<tr>
<td>7.</td>
<td>Jonas karlsson</td>
<td>2003</td>
<td>Use of a Radio receiver</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Less</td>
</tr>
<tr>
<td>8.</td>
<td>Subba Rao</td>
<td>2010</td>
<td>Simple probe with experimental models</td>
<td>High</td>
<td>Less</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

**Table 6.1 Comparative Analysis of EMA probing system**

The methods shown in the [Table: 6.1] are generally theoretical and complex and uses just one experiment except for the recommendation of Subba Rao et. al. These methods generally are not accurate and cannot be used for sensing EMA radiated by a Crypto server. The method proposed by Subba Rao et. al., uses a simple probes, undertakes continuous EMA streaming and uses an experimental model using which huge data base can be created. The method presented by Subba Rao et. al., is accurate, less complex, achieves high speed in streaming and completely based on experimental models which are used for carrying further investigation on attacking through EMA for revealing the secrecy built into the crypto servers.

**6.1.5 Investigation and findings related to Attacking through Electro Magnetic Analysis**

**6.1.5.1 Attacking through Electro Magnetic Analysis using experimental models and results**

As explained earlier in Chapter 2.0, a Crypto server is connected to the embedded system that monitors and controls the safety critical system. Crypto server
is used for authentication purposes to enable the user to start, stop and change the operating conditions that should be used by the embedded system to monitor and control the safety critical system. The ES software is developed using RSA algorithm with a key length of 128 bits. The authentication is implemented through a MAC number and PIN number. As such any encryption algorithm and key of any size can be used for developing the Encryption algorithm. The ES software as such is developed on the HOST and moved to the crypto server and make it run through pushing a reset button.

The main basis of attacking the crypto server is through the development of a Knowledge base. Experiments are conducted for acquiring the data related to Crypto server system that has been built in to the embedded system that monitors and control the temperatures within the safety critical system.

An experimental setup has been invented and implemented [Fig: 6.3] for sensing the EMA radiation. While encryption is in progress, EMA radiation is emitted and the same is sensed through the EMA probe shown in figure 6.1 which is simple coil based organizational setup. The probe releases a signal that is amplified and the same is converted to data through A/D converter.

The data which is proportional to the EMA radiation is read by the Attacking server which is another embedded application. The Attacking server communicate the same to the HOST through RS 232C Interface. The application running on the HOST intermittently stores EMA data sensed at different time intervals.

A knowledge base is created through the experimental model shown in [Fig: 6.3]. The MAC, PIN, Algorithm and the key are supplied by a PC connected to the crypto server. Crypto server undertakes encryption by executing the instructions. EMA is radiated when instructions are executed. The radiated EMA is sensed by a
sensor and converted to digital and fed to the attacking server. The encrypted output is captured by attacking server at the end of completion of encryption process.

**Figure 6.3** Creating knowledge base for Electro Magnetic Analysis

Attacking server keeps measuring EMA at different points in time throughout the process of undertaking encryption. Attacking server makes available the Encrypted output and the EMA measurements to PC. At PC, a data base is created using all the inputted data and the captured output. The data base thus created forms the knowledge base. [Table: 6.2] show some sample entries created in to the knowledge base.

Several experiments have been carried and data is collected from nearly 1000 experiments has been created. Analytics are carried on the data base to determine the PIN and MAC pairs that have highest support and confidence. [Table: 6.3] shows some sample calculations for some of the entries contained in the Knowledge base.
Support value is calculated based on the number of records in which the same MAC, PIN. Encrypted output and Algorithm is present over the number of records contained in the data base. Confidence value is calculated based on the number of records containing the same MAC, PIN, Encrypted output, and the Algorithm having the same standard deviation computed out of the Charge Data with variation allowed up to 10%. From these records the MAC and the PIN numbers are selected that have the confidence and the support more than the threshold value that can be fixed by the analyst which also can be changed from time to time.

<table>
<thead>
<tr>
<th>Mac Number</th>
<th>PIN Number</th>
<th>Key</th>
<th>Algorithm</th>
<th>Encrypted output</th>
</tr>
</thead>
<tbody>
<tr>
<td>987654321</td>
<td>1234</td>
<td>128</td>
<td>RSA</td>
<td>4321123456789</td>
</tr>
</tbody>
</table>

Sample number | Time (Micro Seconds) | Charge (Columbus) |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>22</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>19</td>
</tr>
</tbody>
</table>

**Table 6.2** Sample entries in the Knowledge base

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Mac Number</th>
<th>PIN Number</th>
<th>Algorithms</th>
<th>Key Value</th>
<th>Encrypted output</th>
<th>Standard deviation in the charge emitted</th>
<th>Support(%)</th>
<th>Confidence(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9876543210</td>
<td>1234</td>
<td>RSA</td>
<td>128</td>
<td>01234567894321</td>
<td>1.1</td>
<td>23</td>
<td>87</td>
</tr>
<tr>
<td>2</td>
<td>9876542301</td>
<td>2341</td>
<td>RSA</td>
<td>128</td>
<td>10324567891432</td>
<td>1.2</td>
<td>37</td>
<td>43</td>
</tr>
<tr>
<td>3</td>
<td>9876512345</td>
<td>4321</td>
<td>RSA</td>
<td>128</td>
<td>54321567891234</td>
<td>0.9</td>
<td>22</td>
<td>89</td>
</tr>
</tbody>
</table>

**Table 6.3** Analytics using data base
Thus, most probable MAC and PIN with which the Crypto system can be attacked could be determined by conducting the analytics on the database created. The most likely data will have highest confidence and support values.

6.1.5.2 Experimenting for attacking through EMA Analysis

The most probable MAC and PIN are selected from the database. The attacking of the Crypto server is experimented by way of connecting a smart card and a matrix keyboard to the Crypto server as shown in [Fig: 6.4].

![Experimental setup for attacking through EMA Analysis](image)

**Figure 6.4 Experimental setup for attacking through EMA Analysis**

The user swipes the smart card having the same MAC number that has been queried from the database and also enters the same PIN through KEYBOARD that has been selected from the database. Encrypted output is collected by Attacking Server. Attacking Server also captures the EMA radiated at different points in time while the process of encryption is in progress [Table: 6.4].
<table>
<thead>
<tr>
<th>S.NO</th>
<th>TIME (micro-seconds)</th>
<th>CHARGE (coulombs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>21</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>20</td>
</tr>
</tbody>
</table>

Table 6.4 Experimental results – Attacking through EMA analysis

Both the encrypted output and the EMA measurements are sent to PC. AT PC query is made to collect EMA measurements at different points in time for the matching MAC, PIN and encrypted output. Correlation coefficient is calculated between the measured EMA readings and the stored EMA readings. If they are positively correlated then the PIN and the MAC that is used to attack, reveal the secrecy. Correlation between the EMA data stored in the data base and the EMA data collected from experimenting is computed using the equation

\[
\rho = \frac{\sum x y - \frac{\sum x \sum y}{N}}{\sqrt{\left(\sum x^2 - \frac{(\sum x)^2}{N}\right) \left(\sum y^2 - \frac{(\sum y)^2}{N}\right)}}
\]

When the correlation between the sensed and queried data is positive, it reveals to saying that they belong to the same header data thus revealing the secrecy of the data used for carrying the encryption. The secrecy of the crypto server gets revealed when the correlation coefficient computed for different samples is consistent across all the samples for the same set of sensed data and it could be concluded that the header data is related to the sensed data thus revealing the secrecy [Table: 6.5].
From the table it could be seen that the correlation coefficient which is calculated considering EMA measurement acquired through experimenting and the data enquired from the data base produces considered correlation coefficients, thus revealing that the header data which include MAC, PIN, KEY, ALGO and the encrypted output are the ones used by the crypto server. It could be concluded that correlation coefficient values which are computed using the EMA data and the data stored in the data base for different samples of data acquired are consistent.

<table>
<thead>
<tr>
<th>Mac Number</th>
<th>PIN Number</th>
<th>Key</th>
<th>Algorithm</th>
<th>Encrypted output</th>
</tr>
</thead>
<tbody>
<tr>
<td>987654321</td>
<td>1234</td>
<td>128</td>
<td>RSA</td>
<td>4321123456789</td>
</tr>
<tr>
<td>Sample number</td>
<td>Time (Micro Seconds)</td>
<td>Charge Measured (Columbus)</td>
<td>Charge Fetched (Columbus)</td>
<td>Correlation coefficient</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>35</td>
<td>33</td>
<td>0.9666</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>22</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>26</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>18</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>33</td>
<td>33</td>
<td>0.9898</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>21</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>29</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>22</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>32</td>
<td>31</td>
<td>0.99</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>21</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>28</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>19</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

**Table 6.5** Correlation coefficients calculated for several samples for the same header data

### 6.1.5.3 Simulating the Attacking through Electro Magnetic Analysis and results

Experimental model developed through specially developed embedded systems could be used to carry experimentation manually and it is difficult to carry higher level of experimentation. A simulation model is required using which the experimentation can be carried either automatically generating the data or manually inputting the data with ease. Many simulation systems have been tried to simulate the
experimental model and none of the simulation software available could support such a simulation required. A new software has been designed and developed for simulating the experimental model the architecture of which is shown in the [Fig: 6.5].

![Architecture](image)

**Figure 6.5** Architecture – Simulating Software – Attacking through EMA

At PC, encryption is undertaken using known MAC, PIN and KEY. The EMA radiated at different points in time is also calculated based on the EMA data made available by the manufacture for executing any of the instructions. The encrypted output stored in the data base is also fetched and compared with the computed encrypted output. The simulator undertakes several of the experiments automatically and the results obtained from the data base and computed are shown in [Table: 6.6].
<table>
<thead>
<tr>
<th>Mac Number</th>
<th>PIN Number</th>
<th>Key</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>987654321</td>
<td>1234</td>
<td>128</td>
<td>RSA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sample number</th>
<th>Time (Micro Seconds)</th>
<th>Charge Measured (Columbus)</th>
<th>Computed Encrypted Output</th>
<th>Fetched Encrypted Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>35</td>
<td>4321987654321</td>
<td>4321987654321</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>33</td>
<td>4321987654321</td>
<td>4321987654321</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>29</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>32</td>
<td>4321987654321</td>
<td>4321987654321</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>19</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6.6 Simulation Results – Attacking through EMA

6.2 COUNTER ATTACKING THE ELECTRO MAGNETIC ANALYSIS ATTACKS

6.2.1 Counter Attacking Electro Magnetic Analysis Attacks – overview

Counter attacking EMA can be undertaken through modifications to Embedded Hardware and Software. Countering the EMA attacks can be achieved making changes to Cryptography software. Counter measures such as nonlinear key updates can help prevent attackers from being able to correlate power traces with encryption operations. Using Key-Use-Counters shall prevent attackers collecting large samples of data which is necessary to perform the attack. Countering the EMA attacks can also be achieved through making changes to Hardware. Many types of modifications to the Hardware can be carried so that it becomes difficult to investigate the secrecy built into the crypto server by utilizing the EMA dissipations. Some of the modifications that can be carried to the hardware are as below:

1. Adding a metal layer to the chip, to contain the radiation, and placing an active grid on top of the chip to introduce more noise into the EM field, blurring the emanations.
2. Radiation can also be reduced by shrinking the technology, and using smaller transistors in the construction of the chip.

3. Adding photosensitive circuitry to the chip, so that, the chip will cease to function when exposed to light, would complicate the de-capsulation process, as well as the acquisition phase.

All these measures will reduce the leakage of useful information via the EM side-channel, which will greatly increase the amount of samples needed to perform a successful attack, possibly making the attack infeasible. An attacker with infinite samples however would still be able to perform an EMA attack on the reduced signal.

Since EMA requires the attacker to know the exact amount of charge radiated while executing different types of instructions. Inserting more number of dummy instructions which are of different types into the encryption algorithm make irregular patterns of EMA discharges. An even more effective measure would be to introduce random clock-cycles, which would mean the EM traces were not synchronized, and calculating average and differential traces would be far more difficult.

**Attacking strategies**

Many strategies which are either hardware or software based have been proposed to combat side-channel attacks through EMA, among which some general strategies prescribed include the following:

- De-correlate the output traces on individual runs (e.g., by introducing random timing shifts and wait states, inserting dummy instructions, randomization of the execution of operations, etc.)

- Replace critical assembler instructions with those instructions which are hard to analyze, or re-engineer the critical circuitry which performs arithmetic operations or memory transfers
- Make algorithmic changes to the cryptographic primitives, so that attacks are provably inefficient on the obtained implementation, e.g., masking data and key with random mask generated at each run.

The resistance level of the countermeasures may depend on the value of data and the power of adversaries. Evaluating the resistance level should be done at least from the three angles which include adversary’s power (including knowledge, resources and skills), the power of attack (which is closely related to the state-of-the-art) and the effectiveness of countermeasures’. It appears that a combination of hardware and software countermeasures yields a very good security/cost ratio.

It is found that algorithmic techniques are the most versatile, all-pervasive, and may be the most powerful. Also, in many contexts they are the cheapest to put in place. So for the better resistance level, we have divided our counter attacking method into software based and hardware based.

The counter attacking through software includes introducing dummy instructions, and randomization of the instruction execution sequence, randomization of instruction set execution and/or register usage. The method of introducing a random key and execution of dummy instructions for execution has been found to be a more powerful.

On the hardware level, the countermeasures usually include generation of unintentional emanations, clock randomization etc. Generation of unintentional emanations has been proved to be most effective method.

6.2.2 Previous work related to Counter Attacking – Electro Magnetic Analysis

In literature, many of the counter measures are proposed to counter EM analysis attacks. Wim Van Eck-1996 [50] presented a method to attack a video
display unit and the possible counter attacks he discussed includes, decreasing radiation level, increasing noise level, cryptographic display and shielding. All of these had their own disadvantage due to the presence of several unexpected EM leakages. A comprehensive EM vulnerability assessment has to be an integral part of any effort to develop countermeasures against EM attacks on specific implementations. Such countermeasures fall into two broad categories namely signal strength reduction and signal information reduction.

Techniques for signal strength reduction include circuit redesign to reduce unintentional emanations and the use of shielding and physically secured zones to reduce the strength of compromising signals available to an adversary relative to ambient thermal noise. Techniques for signal information reduction rely on the use of randomization and/or frequent key refreshing within the computation so as to substantially reduce the effectiveness of statistical attacks using the available signals.

**Eric Peters, et al., 2006** [14] proposed a common countermeasure to be used in the devices using CMOS technology i.e., to pre-charge the buses with random values. The leakages cannot be predicted if the buses are pre-charged with random values instead of all zeroes. Even more effective measure would be to introduce random clock-cycles, which would mean that the EM traces were not synchronized and calculating average and differential traces would be far more difficult.

**E. De Mulder, et al., 2005** [13] had conducted SEMA and DEMA attacks and has shown that it is possible to find key bits by making more measurements and using correlation analysis. Their attacks show that an electromagnetic attack is a realistic threat for a broad range of cryptographic hardware implementations. They opined that further work is necessary to optimize these attacks using more sophisticated antennas and signal processing techniques. On the other hand, they have recommended that
system designers and cryptographers should jointly develop, implement and evaluate additional countermeasures against side channel attacks which include frequent key updates and various masking and de-correlation approaches.

Kerstin Zangl, 2004 [33] wrote a program that could determine the exact key out of one round of the AES. This is done by a measurement of the electromagnetic radiation that occurs when the AES runs on a chip and then the data is analyzed by the correlation coefficient. In this work he had explained how to measure the secret key out of a one round AES with the help of EM measurements. After a short introduction of the SCA and the AES he directly started with the attack.

Jonas Karlsson, 2003 [22] presented a thesis on TEMPEST - Attacks using a simple radio receiver. In his thesis he proved that there exists a TEMPEST technique that is cheap and relatively simple but has with it some level of security risk. He proved this with facts from literature studies and an experiment that he conducted. There is only one way to protect against these types of attacks and that’s shielding. There is no other way known today that can prevent the radio signals from an attacker. The signals need to be shielded. One can shield specific equipment or an entire building. This is usually done by expensive metal. But these kinds of solutions are expensive and are only used by agencies and big companies.

Subba Rao et al., 2012 [31] have proposed a knowledge base that stores EMA data along with known input, secrecy in terms of algorithm and key length, and the encrypted output generated. The attacking is undertaken by way searching for the EMA data that is associated with the input data fed into crypto system. The counter attacking method included the querying the data base for the MAC and PIN number that has the highest confidence and support and use the same for attacking. The counter attacking is undertaken by using hardware measures. A counter attacking
method has been presented that creates additional field near the crypto server so that the value of the charge emitted is different from what is actually emitted.

6.2.3 Problem definition

The counter attacking methods presented in the literature are not consistent. They do not produce the same counter attacking measure every time an experiment is conducted. The counter attacking method proposed must be effective which can counter any kind of attack from the side channel. Several experiments are to be conducted to determine the effectiveness of a counter attacking method. Experimental models whether hardware based or software simulation based are to be used for conducting more number of experiments. The analysis of experimental results shall help determining the effectiveness of counter attacking method.

Several counter attacking methods are to be investigated to find the counter attacking method that best suits an attacking method. The best counter attacking method has to be selected and the same has to be implemented into Crypto server system. Experiments are to be conducted to find how good the selected counter attacking system is in terms of non-revealing of secrecy information and operational data by way of conducting many number of experiments.

Experimental models which are Embedded Systems driven or simulation based must be used so that several experiments can be conducted to find whether the counter attacking method has been effective. The data base is queried and the operational data used for building the secrecy within an embedded system has to be determined. Operating data is measured after enforcing the counter attacking method and the results are compared with the results obtained from the data base. If the results are different it can be concluded that the counter attacking system is most effective. Thus the problem is to find the most effective, accurate and less complex counter
attacking method that is amenable for huge experimentation for estimation of the accuracy of the counter attacking method.

6.2.4 Comparison of Counter Attacking Mechanisms – EMA Analysis

[Table: 6.7] shows the comparison between different types of counter attacking methods. The method proposed by Subba Rao et. al., is found to be most accurate, less complex and the process can be implemented at a fast rate. The method as such supports conducting several experiments for checking the accuracy of the counter attacking method.

<table>
<thead>
<tr>
<th>Serial Number of the Method</th>
<th>Author</th>
<th>Year</th>
<th>Method</th>
<th>Accuracy</th>
<th>Complexity</th>
<th>Speed</th>
<th>Experimentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>Wim Van Eck</td>
<td>1996</td>
<td>Decreasing radiation level, increasing noise level, cryptographic display and shielding</td>
<td>Less</td>
<td>High</td>
<td>Less</td>
<td>Less</td>
</tr>
<tr>
<td>10.</td>
<td>Eric Peters</td>
<td>2006</td>
<td>pre-charge the buses with random values</td>
<td>Less</td>
<td>High</td>
<td>Less</td>
<td>Less</td>
</tr>
<tr>
<td>14.</td>
<td>Subba Rao</td>
<td>2013</td>
<td>Creation of Additional Magnetic Field</td>
<td>High</td>
<td>Less</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Table 6.7 Comparative Analysis – Counter attacking methods – EMA Attacks

6.2.5 Investigation and findings related to Counter attacking the Electro Magnetic Analysis Attacks

6.2.5.1 Counter Attacking the Electro Magnetic Analysis through experimental models and results

An experimental setup to find the effectiveness and accuracy of Counter attacking EMA attacks has been developed and implemented as shown in [Fig: 6.6]. PIN and MAC codes are selected from the data base based on correlation coefficient.
The selected MAC code is inputted through swiping a smart card and the selected PIN is inputted through the Keyboard. While encryption is in progress, EMA radiation is emitted and the same is sensed through the EMA probe. The probe releases a signal that is amplified and the same is converted to data through A/D converter.

![Diagram of hardware circuit](image)

**Figure 6.6 Counter Attacking the EMA based attacking**

The Counter attacking is implemented by means of generating unilateral emanations through the hardware circuit interfaced to the target Crypto server. The hardware circuit is designed with D/A converter, an EMF Generator and an EMA probe. Due to these unintentional unilateral emanations, the EMA radiation sensed by the EMA probe that is connected to the attacking server is completely different from the actual radiation emitted by the target crypto server during encryption process. The results of the operation carried are shown in the [Table: 6.7].
6.2.5.2 Simulating Counter Attacking Electro Magnetic Analysis Attacks through experimental models and results

Hardware based experimental model requires complex manual effort for conducting experiments and creation of a data base. General hardware pilot models are counter checked through software based simulations and vice versa. Several simulators which includes **TOPVIEW, PROTIUS, MATLAB, LABVIEW** have been tried. It has been found that the existing simulation tools are not quite effective to build simulated experimental models. Special software has been developed to simulate the Counter attacking of EMA attacks. **[Figure 6.8]** shows the software architecture that simulates the way the counter attacking method can be implemented and the effectiveness of the same can be measured.

<table>
<thead>
<tr>
<th>Sample Number</th>
<th>Time in Milli seconds</th>
<th>Counter Charge</th>
<th>Sensed Charge</th>
<th>Total Charge</th>
<th>Searched Charge from the data base</th>
<th>Correlation coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>35</td>
<td>35</td>
<td>70</td>
<td>32</td>
<td>-0.966</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>22</td>
<td>22</td>
<td>44</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>26</td>
<td>26</td>
<td>52</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>18</td>
<td>18</td>
<td>36</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>33</td>
<td>33</td>
<td>66</td>
<td>33</td>
<td>-0.987</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>20</td>
<td>21</td>
<td>41</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>24</td>
<td>29</td>
<td>53</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>16</td>
<td>22</td>
<td>38</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>30</td>
<td>32</td>
<td>62</td>
<td>31</td>
<td>-0.993</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>18</td>
<td>21</td>
<td>39</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>20</td>
<td>28</td>
<td>48</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>14</td>
<td>19</td>
<td>33</td>
<td>26</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 6.7** Experimental results – Counter Attacking through EMA

A repository of radiation that will be induced at different point in times is maintained in a data base for a set of input parameters. The cumulative EMA that will
be radiated when certain numbers of instructions are executed till a point in time is estimated. A varying magnetic field is generated and added to the computed EMA. The EMA estimated and retrieved from the repository is tabulated for many number of experiments conducted at different points in time. Time is taken as one of the parameters to compute the charge based on the Input parameters. The correlation between the measured and queried EMA charges is computed for different samples as many as we fix as target. The correlation between the queried EMA and the generated EMA is computed and found to be negative. Table 6.8 implies that the attacking that is enforced has been quite accurate and effective. The main issue is incorporating a model with the simulation software using which EMA is computed based on amount of EMA radiated when each of the instruction is executed. The data as such is supplied by the manufacture of the Microcontroller.
**Figure 6.8** Software Architecture for simulating – EMA Counter Attacking

<table>
<thead>
<tr>
<th>Input data</th>
<th>KEY</th>
<th>ALGORITHM</th>
<th>OUTPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTACK</td>
<td>123</td>
<td>RSA</td>
<td>KCATTA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sample Number</th>
<th>Time in Milli seconds</th>
<th>Counter Charge</th>
<th>Sensed Charge</th>
<th>Total Charge</th>
<th>Searched Charge from the data base</th>
<th>Correlation coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample 1</td>
<td>10</td>
<td>35</td>
<td>35</td>
<td>70</td>
<td>32</td>
<td>-0.966</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>22</td>
<td>22</td>
<td>44</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>26</td>
<td>26</td>
<td>52</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>18</td>
<td>18</td>
<td>36</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Sample 2</td>
<td>10</td>
<td>33</td>
<td>33</td>
<td>66</td>
<td>33</td>
<td>-0.987</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>20</td>
<td>21</td>
<td>41</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>24</td>
<td>29</td>
<td>53</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>16</td>
<td>22</td>
<td>38</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>Sample 3</td>
<td>10</td>
<td>30</td>
<td>32</td>
<td>62</td>
<td>31</td>
<td>-0.993</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>18</td>
<td>21</td>
<td>39</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>20</td>
<td>28</td>
<td>48</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>14</td>
<td>19</td>
<td>33</td>
<td>26</td>
<td></td>
</tr>
</tbody>
</table>

Table 6.8 Simulation results – Counter Attacking through Counting

### 6.3 CONCLUSIONS

Attacking using the EMA measurement and correlating the charge radiated is one of the most severe form of attacks. The assessment requires that many experiments are to be conducted. Experimental models are to be used for collection of the data and storing the same in a database. The experiments can be repeated for more number of times so that consistency of the EMA radiated can be measured. Electronic probes can sense the amount of charge emitted. The charge emitted will vary from instruction to instruction and therefore, is not feasible to measure EMA instruction wise. Instead EMA can be measured at specific periods of time. Several EMA measurements at different times for the same sample gives us the basis of computing the correlation coefficient. Hardware based counter attacking through creation of electromagnetic field around the crypto server gives most accurate counter
attacking method. Experimental models are required to show the effectiveness of a counter attacking method. The counter attacking method that uses the creation of extra magnetic field around the crypto server is found to be most accurate.