A Simple and Differential Power Analysis Attack Resistance Circuit for Smart Card Reader Using an Integrated Power Spike Vanisher

Jeffrey Sarmiento
College of Engineering, Architecture and Fine Arts, CpE Department
Batangas State University, Pablo Borbon Main I, Batangas City, Philippines
Email: jeffsarmiento1@gmail.com

ABSTRACT

Contact and contactless smart cards are widely used In modern banking and business transactions. However, one of the most challenging issues that have to be strategically addressed is the security of the data inside the . In embedded system, for example, Simple Power Analysis (SPA) attack and Differential Power Analysis (DPA) attack are the most popular among the many side channel attacks. High frequency operation is due to the fluctuation happening as a result of sequential circuit clocking during the process of encryption operation. These power spikes are then rippled and can be captured using oscilloscope or any power trace capture device. This study proposed new low cost, easy to implement mitigation techniques. Test results showed the difference between the power traces of smart card reader without the proposed mitigation technique and those with mitigation techniques. It was proven that the proposed solution can match the existing solutions and is sometimes better in terms of SPA and DPA resistance.

KEYWORDS*:* SPA, DPA, Voltage Regulator, Encryption, Side Channel Attack

1. INTRODUCTION

An embedded system consists of pre-programming a dedicated short range of functions and is a part of large systems, usually aimed to design a system with minimal end user interaction. Embedded systems and real time operating systems (RTOS) are fast achieving ubiquity, blurring the lines between science fiction and hard reality [1]. A smart card is an embedded system device which contains more information than a magnetic stripe card and it is programmed for different applications. Some cards can contain programming and data to support multiple applications; some are updated to add new applications after they are issued. Smart cards are classified in two different types: contact or contactless. Since smart card contains crucial information, it is a favorite target of computer frauds and identity thieves.

Similarly, the security threats on embedded systems such as smart cards have been an increasing concern of different security experts. Since embedded systems are a widely used technology and most automated devices or equipment are designed using embedded systems, the consequences of exploiting the security vulnerabilities can go beyond mere annoyance to significant societal disruption. A common method used in implementing security on smart card is with cryptography, which is the fundamental building block for securing systems and communications. Smart card uses encryption to hide information it holds. However, any attacker who has an access to the device hardware that is performing cryptographic operation can easily acquire information about the operation by just analyzing the inputs and outputs of embedded system devices. An attacker who is physically close to the device can also measure the power consumed by the device or its EM emissions while it is performing the operation. This kind of attack is widely known as Side Channel Attack (SCA).

Modern devices are implemented using semiconductor logic gates that are constructed out of transistors. Electrons flow across the silicon substrate when charge is applied or removed from a transistor’s gate. The process consumes power and produces electromagnetic radiation. This power consumption may vary depending on the operation performed by the device and can be captured and analyzed using Power Analysis which is a form of SCA [2].

Power Analysis Attacks

The basis of power analysis attacks rests on the analysis of the power consumption of the device while it is performing the encryption operation. Using differential and power analysis of the power consumed by the device, an attacker can learn about the processes that are occurring during the operation to get information that, when combined to the known cryptanalysis techniques, can lead to the recovery of the secret key.

Integrated circuits are built from individual transistors, which act as voltage-controlled switches. Current flows across the transistor substrate when charged is applied to the gate. This current then delivers charge to the gates of other transistors, interconnected wires, and other circuit loads. The motion of electric charge consumes power and produces electromagnetic radiation, both of which are externally detectable. A smart card consists of circuits containing microprocessor, which is mainly based on Complementary Metal Oxide Semiconductor (CMOS) gates. CMOS gates have mainly three power sources: the leakage current in transistors, the short-circuit currents throughout the switching of a gate during simultaneous conduction of NMOS and PMOS and the dynamic power consumption which is due to the charge and discharge of the load capacitance [3].

The circuit shown in Figure 1 shown a component model which is useful to understand how the measurement of power dissipation [4]. Power dissipated by the smartcard can be captured at the ground pin of the smartcard by an oscilloscope connected to the V_{SS} and a small resistor in series between the V_{SS} pin on the card and the true ground. Current moving through R1 creates a time varying voltage that was captured by the oscilloscope.

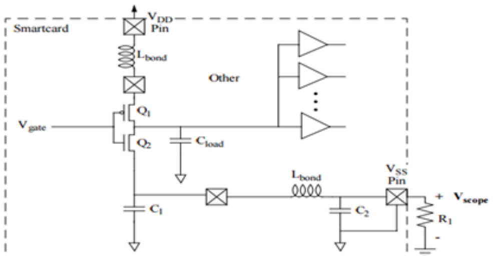


Figure 1. Measuring Power Consumption on Smart Card

The current flows out of the smartcard through a bond wire that acts as an inductor Lbond. The values of the inductor, Lbond, and the capacitors will determine the shape of the power signal that is observed at Vscope.

Information useful to a cryptanalyst is leaked because the amount of current being drawn when the circuit is clocked is directly related to the change of state of Cload or the resulting current drawn by the other gates attached to Cload. On a microprocessor, each clock pulse causes many bit transitions to occur simultaneously. In a typical smartcard microprocessor, a large portion of the power dissipation occurs in the gates attached to internal buses. Experiments showed that activity on the data and address bus is a dominant cause of power consumption changes, which can be observed at Vscope.

Simple power model

In this model, the variable (t) denotes time, and n(t) is a normal distributed random variable used to represent the noise. The power consumption of the single gate represented by (a) is denoted by the function **f(a,t)**. To simplify the power model of the power consumption, it will be the function as shown in Eq. (1). [4]

$$Plos = \sum g\, f(a,t) + n(t) \qquad (1)$$

The function ***f(a,t)*** is not yet known; it will be considered as random variable from an unknown probability distribution. Using Central Limit Theorem, if all ***f (a,t)*** are randomly and independently drawn, then the ***P_{los} (t)*** is normally distributed. The information gathered in this model can be used in DPA by dividing the power measurements in two or more difference between these sets in order to verify the prediction.

Hamming weight model

This model is proposed to express the relationship between power consumption and the hamming weight of data being manipulated at a given point in time. This power consumption is due to the vast amount of power consumed by the bus on the microprocessor compared to any single feature on the chip. This relationship can be expressed as shown in Eq. (2).

$$P_{los} = dH(I) + n \qquad (2)$$

P_{los} ***(t)*** is the power consumption, **I** is the value of data being manipulated, and **H** is a function that calculates the hamming weight. The noise is represented by the variable (n) and also the variation from one clock cycle to another, as the command being executed by the CPU change.

Hamming-distance model

The Hamming-distance model counts the number 1 0 and 0 1 transitions that occur in the cryptographic device while executing the cryptographic algorithm. The number of transitions that occurred describes the power consumption of the cryptographic device at a particular time interval [5].

Simple power analysis

The basis for Simple Power Analysis (SPA) is the visual representation of the power consumption of a unit with an encryption while performing an operation. Interpretation of the collected power consumption measurement during the cryptographic operation is the main technique used in simple power analysis. SPA can gain essential information like the device's operation and key materials used in cryptographic operation [6].

The attacker can directly observe systems power consumption. The amount of power consumed varies depending on the microprocessor instruction performed. Since SPA can reveal the sequence of instruction-executed, breaking cryptographic implementations, from which the execution path depends on the data being processed, can be easily done.

The attacker that uses SPA could can the waveforms of the device and store the data using a digital oscilloscope and later process the information to extract the secret key. Figure 2 depicts the waveform captured during the operation in an encryption device [3]. By just looking at the captured waveform, the attacker can easily identify the rotations of DES encryption protocol.

Skorobogatov and Kuhn [7] have successfully used SPA in retrieving the private password of the MC68HC908AZ60A microcontroller. This password was needed to retrieve the contents of the microcontroller's memory.

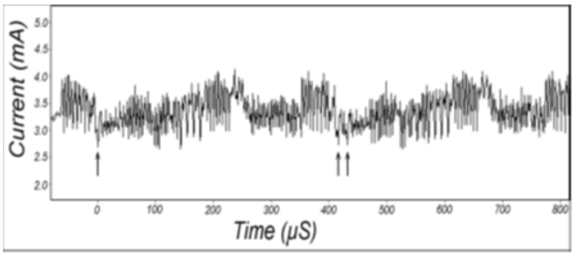


Figure 2. Simple power analysis on DES encryption

Figure 3 shows that by plotting the intensity for all 256 possible values of a password byte, it is possible to determine the out lier, which corresponds to the correct byte.

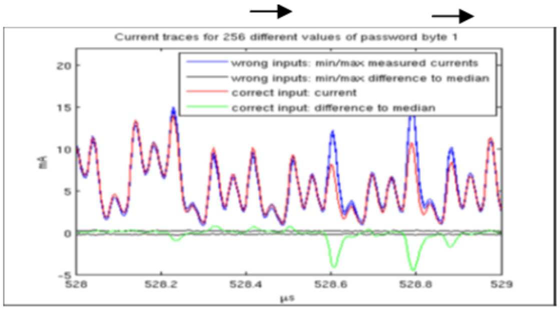


Figure 3. Graph of the current traces for 256 different values of password byte 1

To find the 8 byte long password, the attacker must sequentially try all possible values for the 8 bytes. Thus, for a given byte, all the possible 26 values would be sent to the microcontroller. The correct value can be precisely determined by analyzing the resulting intensity after each possible value.

Differential power analysis

Another way to break the encryption is through Differential Power Analysis (DPA). DPA does not focus only on visual representation, but also on statistical analysis and error-correction statistical methods to obtain essential information about the cryptographic operation. It generally consists of two stages: data collection and data analysis that make extensive use of statistical functions for noise filtering as well as for gaining additional information about the processes that the unit is performing [6].

DPA uses statistical methods to find small variations that may be overshadowed by noise or measurement errors. It also exploits information obtained from the physical implementation of a cryptosystem. To perform differential Power Analysis, an attacker executes a DPA attack for random plaintext values with the same key. The plaintext value is denoted by I_i , where i is from 1 to the maximum number of plain-text. For each plaintext input, the power consumption curve is measured in discrete time. The power trace is the power consumption while processing the cryptographic algorithm. Considering applied cryptographic algorithms and effects upon the secret key, a selection function is chosen. Therefore, one target bit is determined, which becomes the value of isolated bit. The particular bit depends on some bits of the secret key in evidence.

Using the selection function, one can compute for the values of target bit, given ciphertext and key. The power traces of samples are captured into two power traces that are equivalent to zero and power traces that is equivalent to 1. The average power trace 1 will be slightly higher at the point of correlation. If the key guess is correct, the average trace for 0 will be slightly lower. If the key guess is incorrect, the power traces will be equal to the correct bit value with probability P = ½ , yielding average traces that are approximately equal.

The differential trace computed is the difference between the two average power traces. The differential traces should approach to zero if there is an incorrect guess of key. Otherwise, the differential traces should approach the target bit's power contribution at the correlated samples.

To perform Differential Power Analysis on DES and 3DES implementation on smart card, the inner function of this algorithm must be studied rigorously. The key observation on this kind of attack is to know the 6-bit key of the DES like the xored bit on the state before applying the s-box. Using the existing information one can simply apply a simulation to predict the output of the s- box as seen in Figure 4 [6].

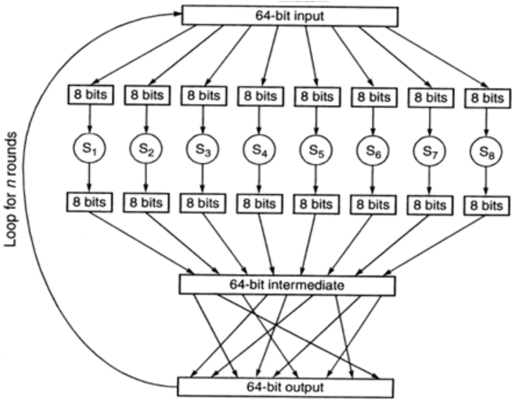


Figure 4. Data Encryption Standard

Inside a single s-box is a set of operations that are used to create a cyphertext. The attacker does not necessarily need to know the cyphetext at all; just a plaintext which is the known data during the transaction is used to initiate the attack.

Each guess will give a power consumption curve that can be partitioned into two sets: 1 set where the computed bit is "1" and another where the computed bit is "0". After getting the average of each set, it is necesassary to get the difference of the averages of the two sets. The whole process is depicted in Figures 5a and 5b.

Whenever the guess is correct, the leak can be clearly seen in the captured power consumption as compared to the power curves when the guess is wrong.

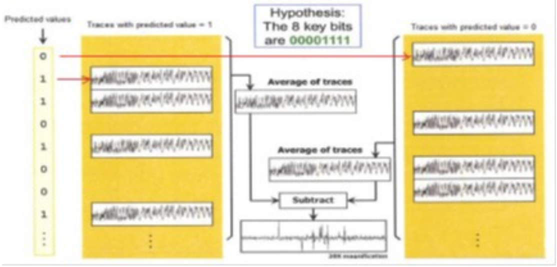


Figure 5a. DPA Evaluation Process with Correct Guess

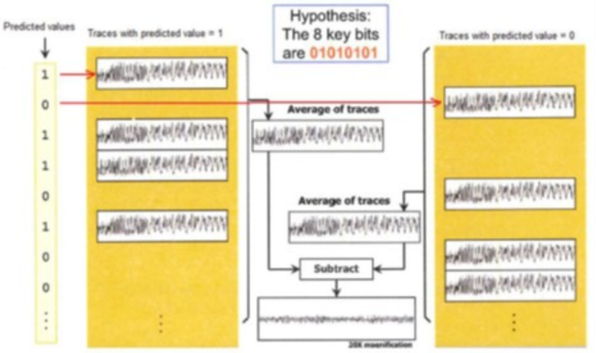


Figure 5b. DPA Evaluation Process with incorrect Guess

Objectives of the Study

The study generally focused on the integration of a protection circuit against simple and differential power analysis attacks on smart card reader. Specifically, the study aimed to propose mitigation techniques to protect the smart card reader from power analysis attacks. The study also identified devices used in the testing the proposed mitigation technique and also aimed to show proofs that the proposed solution is effective in mitigating power analysis attacks. A comparison of the proposed solution compare and other existing solutions.

2. MATERIALS AND METHODS

Smart card security using encryption

The first part of the study dealt with the security implementation of embedded system devices, specifically smart cards (Figure 5) This was done by reviewing previous researches that dealt with different smart card security features and divulged different encryption methods applied to secure the information inside the smart cards.

This included important information on how the cryptography was implemented in smart card, the basic information about the cryptographic process and the overall structures of the cryptography.

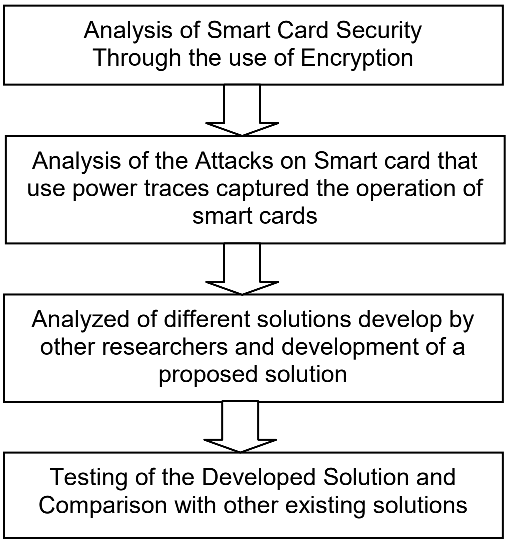

Analysis of Smart Card Security Through the use of Encryption
Analysis of the Attacks on Smart card that use power traces captured the operation of smart cards
Analyzed of different solutions develop by other researchers and development of a proposed solution
Testing of the Developed Solution and Comparison with other existing solutions

Figure 6. Research Flow

The implementation of AES and 3 DES under the synchronous encryption algorithm was highlighted in this part since it is a common encryption method used in most embedded system devices. The anatomy of these two types of algorithm was studied rigorously to understand its implementation and how it can be broken using the existing cryptanalysis and power analysis. On the other hand, the implementation of RSA method was also studied since it is the most common encryption method used under the asynchronous encryption method.

Power analysis attacks on smart card

The study analyzed the anatomy of the simple power analysis and differential power analysis and the different theories behind this kind of attack.

The simple power analysis is only used to break the DES encryption; there was an only minimal discussion about this kind of analysis. On the other hand differential power analysis uses power consumption and statistical methods in breaking the secret key that an encryption algorithm is using. Thus, there is needed for an intensive analysis as to how the power consumption can reveal the necessary information to break the encryption. In analyzing the power consumption, the study analyze different power models used to identify the bit, comprising the waves captured using the device called oscilloscope. The information gathered research was used to formulate a possible solution to avoid or mitigate power analysis attack. The knowledge as to how the power consumption of the device was captured and analyzed was the basis on the development of proposed solution to mitigate power analysis attack.

Design, Development and Testing Stages

Figure 6 shows the step by step process used in the study during the design and development stages. The researcher studied the causes of the power spikes on the electronic devices including the smart cards. This was made possible by conducting a research on different electronic devices and their operations and power consumption during the operations.

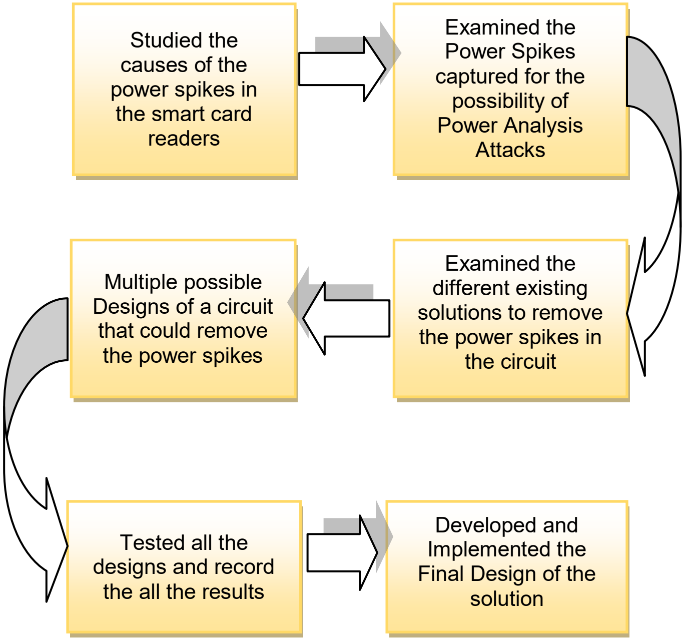

Studied the causes of the power spikes in the smart card readers
Examined the Power Spikes captured for the possibility of Power Analysis Attacks
Examined the different existing solutions to remove the power spikes in the circuit
Multiple possible Designs of a circuit that could remove the power spikes
Tested all the designs and record the all the results
Developed and Implemented the Final Design of the solution

Figure 7. Design and Development Flow of the solution

The smart card reader was tested the power spikes/ traces during the operation of the smart card. The captured power traces were then analyzed for the possibility of power analysis attacks. The analysis was based on the existing attacks on smart cards. Since power spikes in electronic circuits are not new, the next step in the design was studying different solutions made to reduce or remove power spikes. The knowledge gained on the previous step was utilized to create multiple possible designs that could reduce the power spikes produced by the circuit.

The final step was performed along with the testing since each of the designs was tested and compared to get the best design that can be applied in the circuit. The systematic development and testing flow is shown in figure 7.

The first step in the development and testing as to run the original smart card reader and smart card. The initial power traces were captured and recorded. The designs formulated during the design stage were applied on the original smart card readers. The researcher ran the smart card reader with the implemented designs power; captured and recorded the powers traces, and repeated the steps until all the designs were tested.

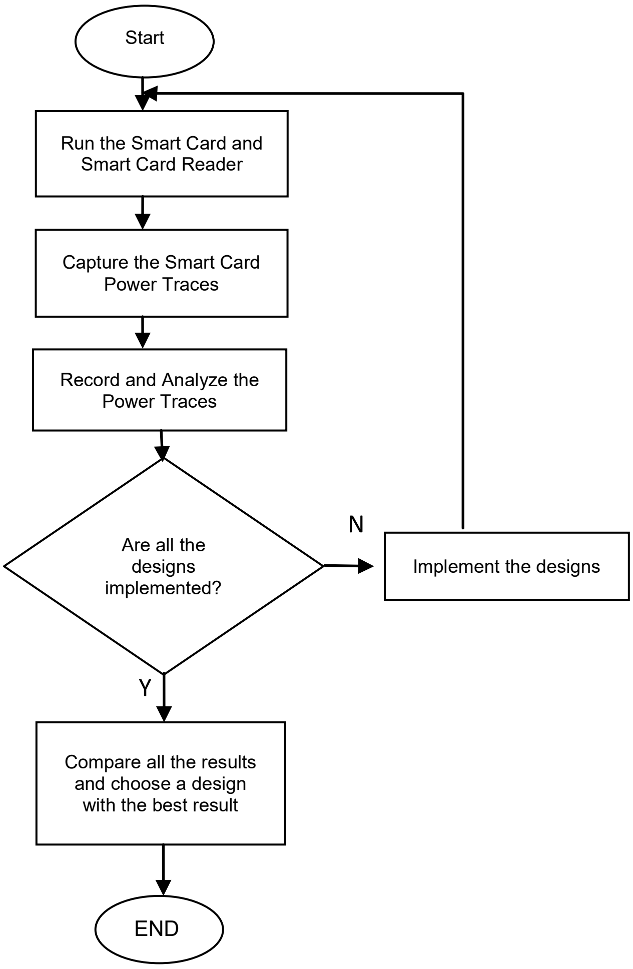

Start
Run the Smart Card and Smart Card Reader
Capture the Smart Card Power Traces
Record and Analyze the Power Traces
Are all the designs implemented?
N
Implement the designs
Y
Compare all the results and choose a design with the best result
END

Figure 8. Testing Flow

After all the designs were tested, all the results were compared to identify the designs that generated better and acceptable results.

3. RESULTS AND DISCUSSION

Mitigation Technique for smart card security

To perform power analysis attack, the capturing device must be connected to the ground end of the smart card reader. The idea brought out the concept of how to mitigate the attack. Since power analysis attack is dependent on the power spikes read at the ground, the mitigation was to add an additional circuit before the current flowing from the smart card reader reaches the true ground.

The mitigation was designed to remove power spikes produced by the smart card during the process of encryption. In this way, the power analysis attack is possible since no power traces are read on the capturing device.

The additional circuit was based on the existing voltage regulator design. By adding some electronic device, there were no power spikes that can be observe on the normal operation of the device, as well as during the encryption process.

Devices used to Test the Effectiveness of the Mitigation Technique

To ensure that the solution was efficient and effective, there were few testing devices needed. During the course of the research, one of the main problems that the researcher met was the device to be used in the testing of the mitigation technique. The first device used was a siglent SDS1102CML oscilloscope but during the testing itself, it did not give an exact value since zooming the power traces was impossible for this device.

The researcher also considered the DIY oscilloscope using Arduino Uno microcontroller and a Processing software. The testing showed power spikes on the device but not the spikes needed to perform the power analysis attack. The researcher also tried to devise a probe for the DIY oscilloscope with 1x frequency ; but the device was useless for the research.

The third device was the NI myDAQ, since it can be used to capture almost all the things that can be measured in an electronic device. The device served its purpose and became useful during the testing of the mitigation circuit.

Along with myDAQ, a software was also used to easily capture and record the power traces in the device. The first software the researcher used was elvismx oscilloscope, but like the first oscilloscope the spikes could not be zoomed out. The second software was the LAbview also made by National Instrument. The software was found to be complete with all the needed sub-application to capture and record power traces.

Test Result of the mitigation techniques

During the test, the smart card produced ripple power spikes during its normal operation even without reading any smart, as shown in Figure 9. The waveform graph was composed of amplitude**,** which is the voltage spike captured on the smart card reader, and the time when the spikes happened.

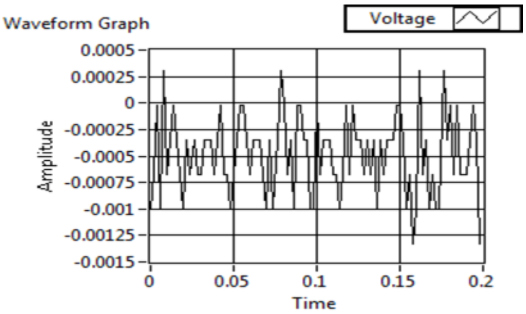


Figure 9. Power spikes during the normal operation of the reader 100 samples

There were 100 samples captured during the experiment, and the voltage, though below 0V, clearly depicted the power spikes happening during the operations of the smart card. Figure 10 also shows captured spikes, but this time with 300 samples.

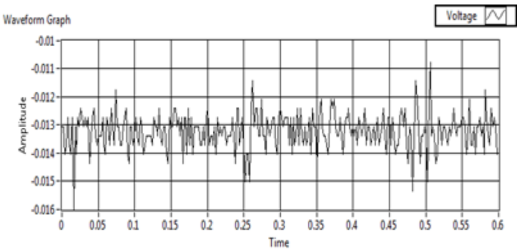


Figure 10. Power spikes during the normal operation of the reader 300 samples

On the second experiment, the power spikes with 300 samples were captured and showed much different power levels with clear distinction of encryption operations happening while reading the content of the card. This is shown in Figure 11.

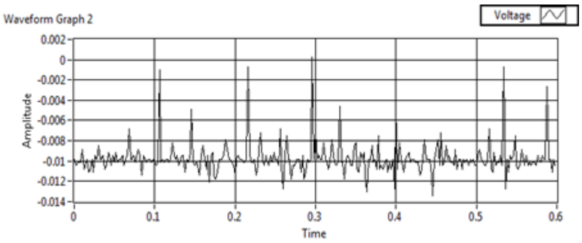


Figure 11. Power spikes while reading the content of the smart card

As the figure clearly depicts that the operation was repeatedly done as seen in the timeline 0.1 to 0.2, 0.3 to 0.4 and 0.5 to 0.6. These sample power spikes clearly depicted the possibility of SPA and DPA.

The SPA and DPA are powerful attacks in which even the contactless smart card are vulnerable. Figure 12 shows the sample power spikes of the NFC reader, a reader used by contactless smart card manufactured by ACS Corporation.

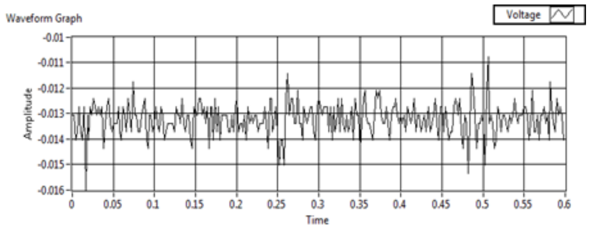


Figure 12. Power spikes of NFC reader without smart card detected

ACS smart card reader only reads mifare classics smart card that uses cipher 1 as its encryption. The algorithm used in this card is depicted in the captured power spikes as shown in Figure 16. The power spikes in timeline 0.1 until the middle of 0.25 and 0.3 clearly show the amount of power spikes during the reading of contactless smart card. Compared to contact smart card, power spikes here are too obvious that these do not need to use DPA anymore.

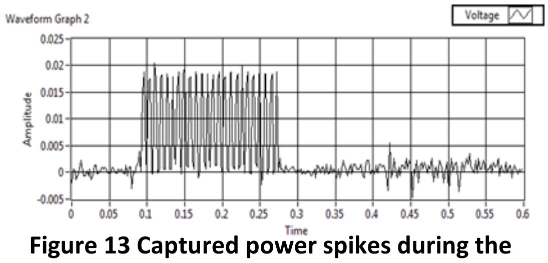


Figure 13 Captured power spikes during the reading of mifare contactless smart card

The Linear regulator was initially designed to improve stability, accuracy, transient response, and to lower the output impedance. The original design would simply regulate the amount of voltage and current flowing through the circuit. All linear regulators have difficulty in handling spikes, but can be tweaked to efficiently remove the spikes without degrading the quality of signal flowing into it. To remove the spikes in the circuit, a filter capacitor was added on both input and output of the circuit.

The role of the filter capacitor is to filter out the range of frequency present in the circuit. Since the power spikes are also frequencies, filter capacitors can be used to filter them out. The input filter capacitor is intended to even the power spikes before they enter the regulator. The output filter capacitor is optional since it is just used to maintain low output impedance at high frequency. The output capacitor is also used to minimize the generated noise and residual signals. This signal plays which an important role in hiding the power traces made during the operation of the device thus, there is no need to minimize it but instead amplify and add more of this in the circuit.

To ensure that the right amount of frequency was filtered in the input filter capacitor, the design employed the formula, as shown in Eq. (3).

$$Xc = 1/2\pi fc \qquad (3)$$

whereas, Xc is the filter capacitance, f is the operating frequency of the device, and c is the capacitor value. Using the formula, the design came up with the value of 0.1μF 10v filter capacitor. The value was expected to reduce the spike generated during the smart card reader operation. The circuit design can be seen in Figure 14.

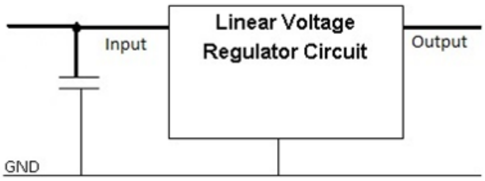
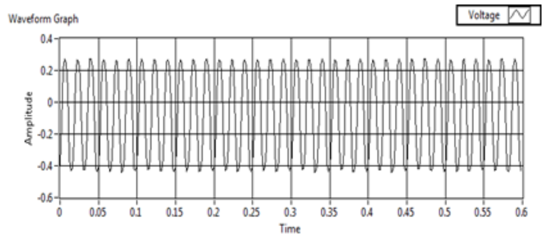


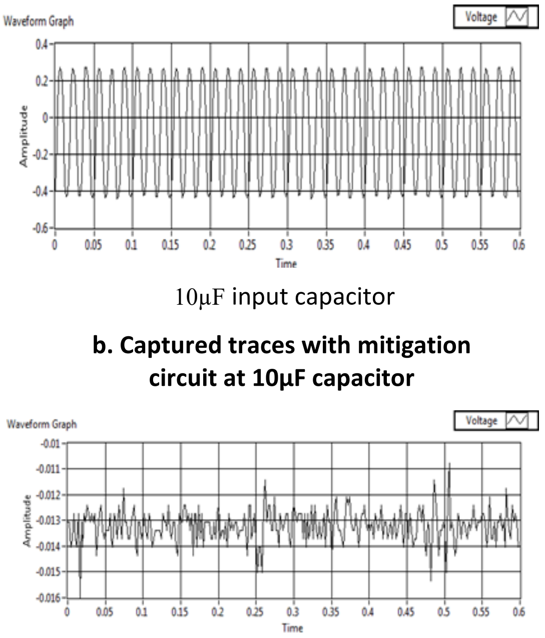
Figure 14. Linear regulators with filter capacitor

The amount of capacitor clearly reduces the presence of spike as shown in Figure 14.



1μF input capacitor

a. Captured traces with mitigation circuit at 1μF capacitor



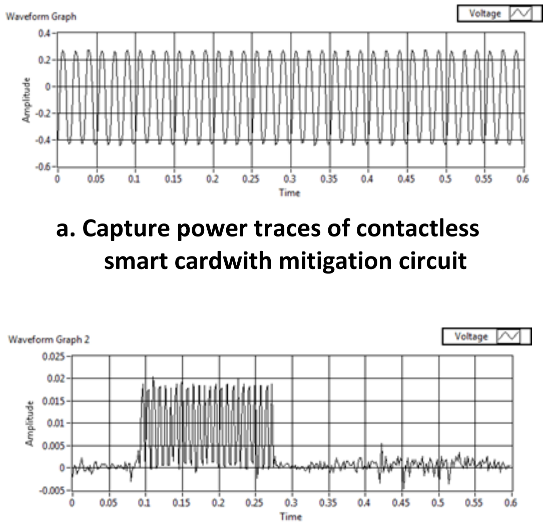
10μF input capacitor

b. Captured traces with mitigation circuit at 10μF capacitor

c. Captured traces without the Mitigation circuit

Figure 15. LDR with 1μF and 10μF Input filter Capacitor

The filter capacitor was unable to eliminate wide-band, which caused few small spikes, occasionally seen in the power traces. Even increasing the size of the input filter capacitor had no effect on this rise time. Compared to the original circuit without the mitigation circuit, there was a clearer view of the power spikes removed by the circuit. The same power spike can be seen in contactless smart card reader when the mitigation circuit was added to the original circuit, as shown in Figure 16.



a. Capture power traces of contactless smart cardwith mitigation circuit

b. Capture power traces of contactless smart card without mitigation circuit

To further test the circuit design, a ferrite bead was added to the design and the sample power traces captured showed a slight difference in the wavelength of the frequency, thus giving an almost similar power trace with the circuit without ferrite bead. This is shown in Figure 17.

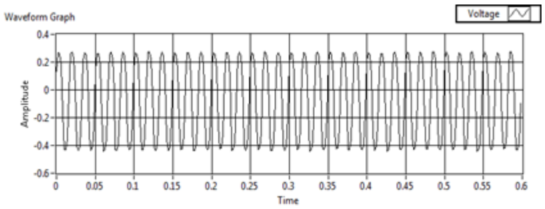


Figure 16. Power traces of circuit with input filter capacitor and ferrite beads

The traces were the same on contactless smart card reader which can be seen on Figure 17.

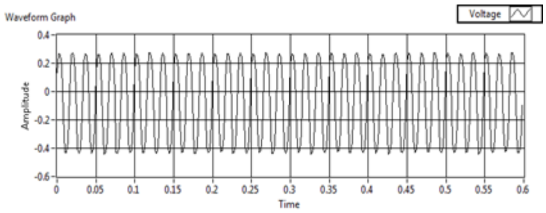
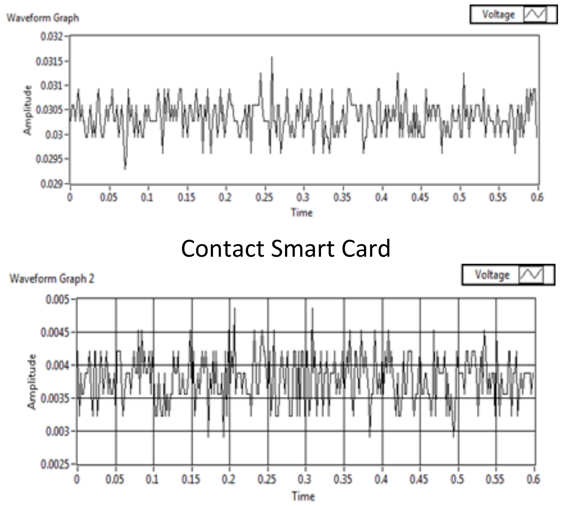


Figure 17 Power traces of circuit with input filter capacitor and ferrite beads on contactless smart card

The original design should have an output filter capacitor to reduce noise gain and flatten the output voltage. But during the test of the circuit, this output capacitor regained the spikes and instead of removing noise from the circuit, propagated and amplified it. This may cause an attack vulnerability in the circuit. The power traces was shown in Figure 18.

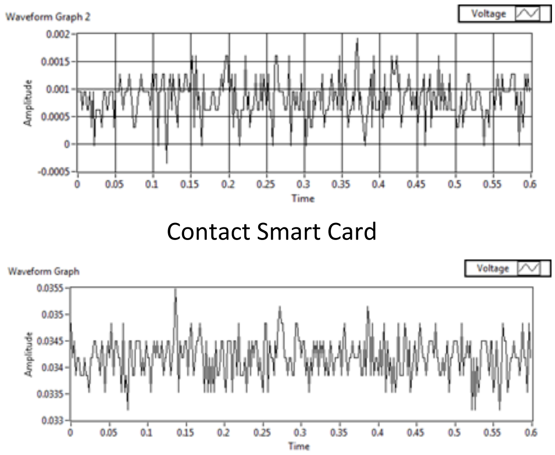


Contact Smart Card

Contactless Smart Card

Figure 18. Power traces of the circuit with output filter capacitor

Even the help of ferrite bead on the output did not help in reducing the noise and power spikes, as shown in Figure 20.



Contact Smart Card

Contactless Smart Card

Figure 20 Power traces of the circuit with output filter capacitor and ferrite beads

The test shows that LDO with input filter capacitor and ferrite beads was effective in removing power spikes. The final design is shown in Figure 21.

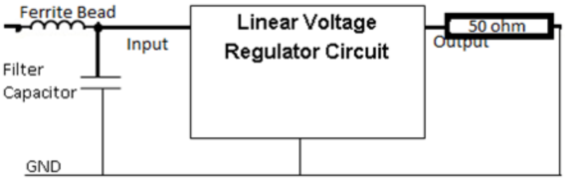


Figure 21 Final Circuit Design

The 50 ohm resistor was added to ensure that changes in voltage happens when the output voltage is grounded.

Comparison of the developed technique to other mitigation techniques

Masking Technique

The developed technique was viable compared to other known mitigation techniques. One of the mitigation techniques used to secure smart card was the AES encryption method. The method, which is called masking of s-box, is masking the intermediate bytes which are executed in an AES mathematical calculation [21].

The research concluded that the masking and other algorithmic countermeasures are not resistant to the first order differential power analysis attack.

The technique used in this paper does not really need to change the algorithmic properties of the device, instead, it just changes the circuit at the negative edge of the device to remove the power traces.

Table 1. The Present Mitigation Technique compared to the Protection Circuit Presented in Different Research

Mitigation Technique	Protection Against		
	SPA Attack?	DPA Attack?	DFA attack?
DPA and DFA protection circuit	No	No	Yes
Masking Techniques	Yes	No	No
Combinational instead of sequential in AES encryption	Yes	Yes	No
The present technique	Yes	Yes	No

Protection Circuit for DPA and DFA

Pei Lou introduced the protection circuit for FPGA, based smart card reader and smart card that uses AES encryption method [18]. The protection was proven to be effective against the attack, but increases the over all power leakage, making it more vulnerable to DPA attack.

The solution presented in this research is also a type of protection circuit but is dedicated to counter SPA and DPA attack. While the protection circuit developed by Pei Lou detects the occurrence of DFA attacks, it consumes more power. The present solution does not need to detect the attack but instead avoids it while maintaining the original power consumption.

Presented in Table 1 is the summary of the protection capability of the mitigation techniques to resist the SPA, DPA and DFA attacks on smart card.

Combinational circuit instead of sequential circuit in AES encryption architecture

The protection made by Vijaya focuses on the architecture of AES encryption. The techniques try to remove a sequential process in the encryption algorithm, and add random delay by using combination design at the first and last rounds of AES encryption, thus producing random power spikes. Analyzing the power traces captured in this device would be impossible, since the power traces did not have direct correlation with the operation performed in the smart card [18].

The present study has a different track compared to the study of Vijaya, since that study concentrated on the hardware implementation rather than the implementation of the encryption algorithm.

4. CONCLUSIONS

After thorough research, design and testing of the circuit and analysis of results, the following conclusions are drawn.

Smart card is vulnerable on side channel attack specially on SPA and DPA attacks. SPA can be easily mitigated by just adding noise to the smart card reader circuit. DFA can also be mitigated if one understands how it is performed. Removing the power traces using few tweaks on the conventional low drop out linear regulator can be use to mitigate the two mentioned attacks.

ACR 122U smart reader, Mifare Smart Card, NI my-DAQ and LAbview are the softwares and devices use in the study.

Based on the power traces captured during the test, it is proven that the developed device can remove the power spikes.

The present solution can match the existing solutions and sometimes are better in terms of SPA and DPA resistance.

5. RECOMMENDATIONS

The researcher recommends that design mitigation techniques for other side channel attacks be tested, as present solution was only tested on ACR122u smart card reader. Future researchers are advised to test the present solution on other smart card reader as the card used in the present study is just a mifare card. The present solution may also be tested in other smart card.

REFERENCES

[1] GoodWill, "Defending against side channel attacks - PArt I," *IEEE,* 2012.

[2] M. Estefan, E. Oswald and T. Popp, Power Analysis Attacks, Revealing the Secrets of Smart Cards, Springer, 2007.

[3] O. Choudary, "Breaking Smart Card using Power analysis." *IEEE,* 2012.

[4] T. Messerges, E. Dabbish and R. Sloan, "Invetigations of Power Analysis Attacks on Smart Card."

[5] K. Pongaliur, "Securing Sensor nodes against side channel Attacks." 2009.

[6] T. Katashita, S. Hirofumi and H. Yohei, "Side-Channel Attack Standard Evaluation Board," 2012.

[7] S. Skobogative and M. Kuhn, "Power Analysis of the Motorola MC68HC908Az60A".

[8] Card Logic Corp., "Smart Card Security Part 2," *Smart card Basic,* 2010.

[9] Credit Card Association of the Philippines, "Cards of the Future," *TechTarget,* 2015.

[10] K. K. Ajoy and J. M. Hrijoy, "Side Channel Attack and Their Mitigation Techniques," 2013.

[11] P. Kocher, J. Joshuan and J. Benjamin, "Introduction to Differential Power Analysis."