KLE TECH

KLE Technological University

Creating Value
Leveraging Knowledge

School
of
Electronics and Communication Engineering

Minor-2 Project Report
on

SIDE CHANNEL ATTACK ANALYSIS

By:

1. **Shreesha Hegde** USN: 01FE21BEC226
2. **Shrinidhi Togaleri** USN: 01FE21BEC136
3. **Nandish** USN: 01FE21BEC303

Semester: VI, 2023-2024

Under the Guidance of

Dr. Nailini Iyer
Prof. Shraddha Hiremath

K.L.E SOCIETY'S
KLE Technological University,
HUBBALLI-580031
2023-24

KLE TECH

SCHOOL OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that project entitled **" SIDE CHANNEL ATTACK ANALYSIS "** is a bonafide work carried out by the student team of **"Shreesha Hegde(01FE21BEC226), Shrinidhi Togaleri (01FE21BEC136), Nandish(01FE21BEC303)"**. The project report has been approved as it satisfies the requirements with respect to the Minor project work prescribed by the university curriculum for BE (VI semester) in School of Electronics and Communication Engineering of KLE Technological University for the academic year 2023-24.

Prof. Shraddha Hiremath	Dr. Suneeta V Budihal	Dr. B. S. Anami
Guide	Head of School	Registrar

External Viva:

Name of Examiners	Signature with date
1. Ramesh Tabib	
2. Dr. Ramkrishna J	

ACKNOWLEDGMENT

We would like to express our gratitude towards our research guide Dr. Nalini Iyer for her continuous support, encouragement, and guidance. We are grateful to her for setting high standards and giving us the freedom necessary for pursuing the project. Our special thanks to research assistant Prof. Shradha B.Hiremath for guiding us throughout the project. Our special thanks to Dr. Ashok Shettar, Vice-Chancellor of KLE Technological University, Hubballi, and Dr. P. G. Tewari, Principal, KLE Technological University, for providing us with an opportunity to undertake this unique course and pursue our desire for research. Finally, we would like to thank all teaching staff, non-teaching staff of the School of Electronics and Communication Engineering for their constant support and motivation for the successful completion of the project and also, we thank all our friends who helped us directly or indirectly in the completion of this project.

-Shrinidhi K T
Shreesha H
Nandish

ABSTRACT

This study investigates differential power analysis (DPA) as a side-channel attack vector against the AES128 algorithm running on the ATXmega128D4-AU microcontroller board, which is widely used in embedded systems. DPA is an advanced technique that exploits small variations in power consumption during cryptographic operations to extract sensitive information such as cryptographic keys and intermediate states. The ATXmega128D4-AU platform was selected because it is prevalent in embedded applications and therefore a suitable target to evaluate the vulnerability of AES128 to DPA. This study uses practical experiments to accurately evaluate the vulnerability of AES128 implementation on ATXmega128D4-AU to DPA attacks. These experiments aim to reveal potential vulnerabilities in cryptographic implementations and explore effective countermeasures. By analyzing power consumption patterns under different scenarios, this study provides valuable insights into the practical feasibility and effectiveness of DPA in real-world environments. We discuss key findings from our experiments to highlight the specific vulnerabilities of AES128 on ATXmega128D4-AU compared to DPA. Furthermore, this study suggests possible mitigations and security improvements to enhance the resilience of embedded systems against such attacks. This work contributes to an improved understanding of side-channel attacks and highlights the importance of implementing robust security measures in embedded cryptographic systems.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

Locks in in side-channel assaults, such as Differential Control Investigation (DPA), on car hardware uncovered basic vulnerabilities with noteworthy real-world suggestions for vehicle security and security. These assaults abuse unintended data spillage, like control utilization vacillations, to infer delicate information such as cryptographic keys utilized to secure vehicle frameworks.

By effectively compromising these frameworks, assailants might possibly pick up unauthorized get to to vehicle controls, compromising security highlights, route frameworks, or indeed immobilizing the vehicle remotely. This postures genuine dangers not as it were to person vehicle proprietors but too to open security at huge. Envision the affect of a noxious on-screen character picking up control over braking frameworks or motor execution through abused cryptographic vulnerabilities.

In tending to these dangers, stages like ChipWhisperer play a pivotal part. ChipWhisperer gives specialized devices and strategies for capturing and analyzing side-channel signals radiated amid cryptographic operations in car gadgets. This capability empowers analysts and industry experts to reenact and distinguish vulnerabilities, subsequently driving progressions in secure equipment plan and cryptographic conventions. By creating more grounded guards against cyber dangers, such as those recognized through DPA assaults, ChipWhisperer contributes specifically to improving the strength and security of vehicles in an progressively associated car environment. This inquire about is significant in keeping up buyer believe and guaranteeing the progressing security of car frameworks around the world.

1.2 Background

1.2.1 Side Channel Attack(SCA)

Rather than directly attacking the software or algorithms of a computer system, a side-channel attack (SCA) is a kind of security exploit that seeks to obtain data from the physical implementation of the system. SCAs take advantage of data that is released while cryptographic algorithms are being executed. This data can include timing details, power usage, electromagnetic leaks, sound, and other tangible characteristics. Attackers may be able to compromise the system's security using the information these leaks give them.

We are primarily concerned with Power Analysis Attacks in our project.

1)Simple Power Analysis(SPA)

2)Correlation Power Analysis(CPA)

3)Differential Power Analysis(DPA)

Simple Power Analysis(SPA)

Simple Power Analysis (SPA) is a side-channel attack technique used to extract sensitive information from cryptographic devices by analyzing power consumption patterns. The power consumption of a cryptographic device during an encryption or decryption process varies depending on the operations being performed. By monitoring these fluctuations, an attacker can derive information about the internal state of the device and potentially reveal secret keys. This attack technique involves collecting power traces by measuring the power consumption of the device as it processes known plaintext or ciphertext. These measurements are analyzed to identify patterns that correlate with specific operations within the cryptographic algorithm. For example, notable power consumption spikes during certain operations such as S-box lookups or arithmetic calculations may indicate key-dependent activity. By correlating these patterns with the known behavior of the algorithm, an attacker can derive parts of the encryption key. To defend against SPAs, cryptographic implementations often employ countermeasures such as constant-time algorithms that ensure all operations take the same amount of time, thereby reducing correlation between power consumption and the data being processed. Randomizing operations and adding noise to the power signal are additional strategies to obfuscate power consumption patterns, making it difficult for an attacker to extract useful information. Other countermeasures include physical shielding to minimize electromagnetic radiation and the use of dual-rail logic in hardware designs that ensure constant power consumption regardless of data value. The goal of these countermeasures is to make it significantly more difficult for an attacker to successfully perform an SPA, thereby improving the security of a cryptographic device. The implementation of these techniques is important to ensure the confidentiality and integrity of cryptographic operations, especially for devices that are not adequately protected against side-channel attacks.

SPA represents a sophisticated method in side-channel attacks that exploits minute variations in the power consumption of a cryptographic device during operations to deduce sensitive information, such as encryption keys. The power consumption model $P(t)$ at any given time t is formulated as:

$$P(t) = P_{base} + \alpha \cdot H(t) + \epsilon(t) \tag{1.1}$$

encompassing P_{base} as the base power consumption, α as a scaling factor linking power to the data processed, $H(t)$ as the hypothetical power model (often derived from characteristics like the Hamming weight of processed data), and $\epsilon(t)$ as the noise component.

To analyze the correlation between the captured power traces $P(t)$ and the hypothetical power model $H(t)$, the Pearson correlation coefficient ρ is employed, calculated as:

$$\rho = \frac{Cov(P, H)}{\sigma_P \cdot \sigma_H} \tag{1.2}$$

where $Cov(P, H)$ denotes the covariance between P and H, and σ_P and σ_H represent their respective standard deviations.

The CW-Lite configuration is integral in SPA, encompassing settings such as gain adjustment, ADC (Analog-to-Digital Converter) configuration for precise sampling, clock synchronization to align with the target device, and trigger settings to commence data capture at optimal points. By leveraging these precise configurations and mathematical principles, SPA effectively discerns power consumption patterns to potentially unveil cryptographic secrets embedded in the device's operations.

Correlation Power Analysis(CPA)

Correlation Power Analysis (CPA) is a sophisticated form of side-channel attack that builds on the principles of Simple Power Analysis (SPA). While SPA derives key-related information by directly examining the power consumption patterns of a cryptographic device, CPA goes a step further and statistically relates power consumption to specific operations or intermediate

values of a cryptographic algorithm. In CPA, an attacker collects multiple power consumption traces from a target device, each corresponding to a different input or plaintext. By carefully correlating the fluctuations in power consumption during the algorithm's execution with the expected values, the attacker can reveal details of the secret key. The method exploits the small variations in power consumption that occur when processing different key bits or intermediate values. Even if a cryptographic implementation uses a constant-time algorithm, aiming to ensure that an operation always takes the same time regardless of the input, CPA can still be effective. This is because CPA is based on statistical analysis and can detect subtle relationships that SPA may miss. CPA therefore poses a significant threat to the security of cryptographic devices. Various countermeasures are used to defend against CPA: Masking hides the relationship between processed data and power consumption by combining the data with random values. Blinding is a technique that uses random values to obfuscate the actual computation.Adding random noise to the power consumption signal is another strategy that makes it difficult for an attacker to associate power consumption with a specific operation. These countermeasures aim to thwart CPA attempts by breaking the connection between power consumption and cryptographic keys.Understanding and mitigating CPA is critical to maintaining the security of cryptosystems in the face of increasingly sophisticated side-channel attacks.

CPA is another pivotal technique in side-channel attacks, adept at exploiting correlations between the power consumption of a cryptographic device and the data processed to uncover sensitive information like encryption keys. The power consumption model $P(t)$ at any time t is represented as:

$$P(t) = P_{\text{base}} + \alpha \cdot D(t) + \epsilon(t) \tag{1.3}$$

where P_{base} denotes the base power consumption, α signifies the scaling factor linking power to the processed data, $D(t)$ represents the data-dependent power consumption, and $\epsilon(t)$ stands for the noise component.

CPA focuses on correlating the power consumption $P(t)$ with the processed data $D(t)$, typically captured during cryptographic operations. The correlation coefficient ρ in CPA is computed using:

$$\rho = \frac{Cov(P, D)}{\sigma_P \cdot \sigma_D} \tag{1.4}$$

where $Cov(P, D)$ is the covariance between P and D, and σ_P and σ_D are their respective standard deviations.

Essential to CPA is the configuration of parameters such as gain adjustment, ADC setup for precise sampling, clock synchronization with the target device, and trigger settings to initiate data capture at strategic moments. By meticulously configuring these parameters and applying rigorous mathematical analysis, CPA effectively identifies correlations between power consumption and processed data, thereby potentially revealing cryptographic keys hidden within the device's operational profile.

Differential Power Analysis(DPA)

Differential Power Analysis (DPA) is an advanced and effective side-channel attack technique used in cryptography to reveal hidden information, such as cryptographic keys, by analyzing the power consumption of a device while it is operating. Unlike Simple Power Analysis (SPA), which directly examines power consumption patterns, DPA involves a more complex statistical analysis of multiple power consumption traces. These traces are collected as the cryptographic device processes different sets of inputs or actions. By comparing these traces, DPA exploits small, often subtle, variations in power consumption that occur due to variations in the data being processed, such as: B. Intermediate values during encryption or decryption. The central idea behind DPA is to find correlations between these performance variations and the hypothetical intermediate values that the cryptographic algorithm operates on. To perform a

DPA attack, an attacker first collects a large number of power consumption traces as the device performs cryptographic operations on known plaintext or ciphertext. These traces are statistically analyzed to identify patterns and correlations that reveal information about the intermediate states of the algorithm. For example, in AES encryption, certain operations such as S-box lookups and key additions can cause noticeable performance fluctuations. By hypothesizing possible values for these intermediate states and comparing them to the observed power consumption, an attacker can gradually derive the correct value and reconstruct the secret key. The effectiveness of DPA lies in its ability to use statistical techniques to amplify small, otherwise imperceptible differences in power consumption, making it a formidable threat even against implementations that are resistant to simple attacks such as SPA. Countermeasures against DPA include masking, which uses random values to obscure the relationship between data and power consumption, or adding noise to the power signal to make correlations harder to detect. Implementing constant-time algorithms, which ensure that operations always take the same time regardless of the data, can also mitigate some of the risks.

Despite these defenses, DPA remains a significant issue in the development and implementation of secure cryptosystems, highlighting the need to continually develop countermeasures to protect sensitive information against increasingly sophisticated attacks.

Note:- The Mathematical Analysis of DPA will be continued in Chapter 2.

1.2.2 Difference of Mean(DoM)

In the context of analyzing side-channel attacks, specifically differential electromagnetic analysis (DEMA) targeting AES128 encryption on the target ATXmega128D4-AU board, "difference of means" refers to a statistical measure used to detect variations in electromagnetic radiation that correlate with different states or behaviors of the cryptographic algorithm. During AES128 encryption, internal data-dependent operations such as S-box lookups, substitution layers, and key schedules cause subtle variations in electromagnetic radiation. These variations can be detected and analyzed using highly sensitive electromagnetic sensors or probes. The "difference of means" technique first classifies electromagnetic radiation traces into two distinct groups based on certain conditions or hypotheses related to the encryption process. For example, one group may correspond to traces where a particular bit or byte of the encryption key or plaintext is hypothetically in one state (0 or 1), and the other group may correspond to the opposite state. The average value of the electromagnetic emissions (often normalized or adjusted for a reference noise) is then calculated for each group. The difference between these averages is an indication of how different the electromagnetic emissions are between the two hypothetical states. In practice, this means that if the average difference is statistically significant and can be observed consistently across multiple cryptographic operations, then the electromagnetic emissions exhibit a recognizable pattern associated with the underlying cryptographic operations. This statistical correlation can be used in side-channel attacks to derive information about encryption keys or plaintext, facilitating the extraction of sensitive cryptographic data through careful analysis of the electromagnetic emissions. Overall, the DEMA average difference serves as a powerful tool in side-channel attack analysis, allowing researchers to exploit subtle variations in the electromagnetic emissions emitted during cryptographic operations to derive important details about the execution of the AES128 algorithm on the target ATXmega128D4.AU board.

1.3 Objectives

Understanding the Cryptographic Cryptanalysis Difference of Mean (DoM) Attacks:
The "Difference of Means" (DoM) attack is a sophisticated cryptographic attack method that targets certain algorithms such as block ciphers and hash functions. It exploits statistical patterns in the output of these algorithms when dealing with plaintext pairs that differ by one bit. By calculating the difference between the mean values of the outputs corresponding to these pairs, the attacker looks for deviations from the expected random or uniform distribution. These differences can indicate weaknesses in the algorithm design, potentially leaking information about the internal state or secret key. In a successful attack scenario, an attacker can deduce the key bits or significantly weaken the security guarantees provided by the cryptographic primitive. To protect against DoM attacks, cryptographic algorithms must be designed with robustness in mind to statistical analysis, ensuring that outputs remain indistinguishable from random even under targeted distinct plaintext inputs. Regular testing and scanning is essential to
identify and mitigate these vulnerabilities before they can be exploited in real-world applications.

Experimental Setup for Capturing Power Traces in Side-Channel Power Attacks Using ChipWhisperer Lite:
The experimental setup for capturing power traces with side-channel power attacks using ChipWhisperer Lite aims to study the vulnerability of cryptographic devices by analyzing their power consumption patterns during operation. The setup includes several key components: the ChipWhisperer Lite hardware, the target device (e.g. , a microcontroller or FPGA), and the software required for data acquisition and analysis. ChipWhisperer Lite is connected to the target device, which is programmed to perform cryptographic operations such as encryption and decryption. During these operations, ChipWhisperer Lite records the current trace, i.e. , the power consumption fluctuations that correlate with the internal processing of the device. Careful analysis of these power traces makes it possible to extract sensitive information, such as private keys, from information loss due to power consumption. This setup provides a controlled environment for performing side-channel attacks, enabling researchers to understand vulnerabilities in cryptographic implementations and develop more robust defenses against such attacks. The process involves precise synchronization, noise reduction techniques, and advanced analytical al-
gorithms to correlate captured performance traces with the cryptographic operations performed.

Preprocessing and Analyzing Power Traces for Differential Power Analysis (DPA) on AES-128:
Differential Power Analysis (DPA) is a powerful side-channel attack technique used to extract cryptographic keys by analyzing the power consumption traces of devices performing cryptographic operations. Applying DPA to identify correlations with AES-128 key bits requires several preprocessing and analysis steps. First, power consumption traces must be captured as the device performs multiple cryptographic operations with different plaintexts. Preprocessing includes aligning the traces to account for temporal misalignment, filtering noise to improve signal quality, and normalizing the traces to reduce baseline fluctuations. After preprocessing, statistical techniques such as correlation analysis are used to correlate the operation of specific key bits with power consumption variations during the operation of the AES algorithm. Special emphasis is placed on the computation of S-boxes and key schedules. By comparing the measured power curve with a hypothetical power consumption model (based

on guessed key bits), an attacker can identify correlation coefficient peaks that reveal the correct key bits. This process is iterative and requires careful analysis, often using advanced techniques such as Principal Component Analysis (PCA) and machine learning to improve the effectiveness of the attack. Successful DPA execution can effectively compromise the security of AES-128, demonstrating the need for strong countermeasures in cryptographic implementations.

Validation of AES-128 Key Recovery via Differential Power Analysis (DPA) Attack on Automotive Systems:
Validating successful AES-128 key recovery via a Differential Power Analysis (DPA) attack on an automotive system requires several critical steps to ensure accuracy and reliability of the results. First, the validation process begins with detailed analysis of power consumption traces captured during cryptographic operations performed by the automotive system. These traces are subjected to statistical analysis to identify correlations between power consumption and intermediate key-dependent values processed by the AES algorithm. Successful key recovery is indicated by peaks in the correlation values at specific points that correspond to the correct key bytes. To verify the integrity of the recovered key, it is important to validate that the key successfully decrypts or encrypts the test data with the expected results. Additionally, the validation process includes a thorough assessment of noise and environmental factors that may affect the current waveform to ensure that any observed correlations are indeed due to key-dependent processes and not artifacts from external disturbances. Repeating the attack under different conditions and on multiple instances of the same system further strengthens the validation, demonstrating the robustness and consistency of the DPA attack. Finally, comparing the recovered key with a known-good key conclusively confirms the success of the attack, highlighting vulnerabilities in the AES-128 implementation in the analyzed automotive system.

1.4 Literature survey

Remote Monitoring Systems of Unsafe Software Execution using QR Code-based Power Consumption Profile for IoT Edge Devices [1]
:-
- The paper centers on the significance of observing blunders in a framework where different edge gadgets work together . This observing is pivotal to anticipate blunders from spreading to other gadgets or causing system-wide disappointments.
- Conventional mistake discovery in implanted frameworks with constrained execution capabilities can be challenging. To address this, the paper proposes utilizing control utilization information to get it the state of edge gadgets and recognize mistakes based on this information. The server deciphers control utilization information to distinguish mistakes utilizing different calculations .
- A key perspective of the proposed framework is the utilize of QR codes for information transmission between the edge gadgets, portal, and server. The edge gadgets transmit control utilization information to diminish the stack on the implanted frameworks, whereas the door and server communicate utilizing QR codes to gather this information. This guarantees productive blunder location and control of edge gadgets .
- The design utilizes a isolated control meter and communication gadget to overcome challenges such as communication mistakes and organize over-burden in IoT gadgets. By utilizing QR codes for information transmission and light communication through cameras, the framework optimizes information trade and blunder assurance forms .
- The usage of the proposed design includes utilizing 'chip-whisperer' for measuring edges and information, as well as 'raspberry pi' for the server usage. This setup effectively illustrates

information transmission, blunder assurance, and negligible extra stack on the edge gadgets, displaying the adequacy of the created framework .

Optimization Technique for Deep Learning Methodology on Power Side Channel Attacks [2]

:-

Understanding Profound Learning for Side Channel Assaults:
- Profound Learning is utilized to discover mystery codes in Side Channel Assaults by analyzing designs and measurements . - Differential Profound Learning Investigation (DDLA) has been compelling in uncovering mystery keys utilizing these measurements .
Affect of Preparing with Redress Names:
- Preparing deep learning models with the proper names makes a difference in accomplishing lower misfortune and higher exactness levels, driving to superior execution .
Progressions in Profound Learning Procedures:
- Different progressed designs like MLP, CNN, LSTM, and stacked Auto-Encoders have been connected in profiling strategies for side channel assaults, appearing advance within the field .
- Modern calculations and preparing techniques have been proposed to oversee challenges in profound learning-based Side Channel Assaults, just like the tall learning costs and broad retraining requirements .
Presenting Shared Layers for Moved forward Execution:
- Shared layers have been presented within the organize structure to improve memory administration and generally execution in parallel setups . - This procedure has altogether quickened assaults, making them up to 134 times more successful compared to past strategies when connected to datasets like ASCAD and ChipWhisperer-Lite .

Fault Attack Detection in AES by Monitoring Power Side-Channel Statistics [3]

:-

- Differential Blame Examination (DFA) could be a strategy to get it crypto-algorithms by making deficiencies amid encryption.
- The investigate presents a CMOS-based system for identifying clock-glitch assaults utilizing control side-channel measurements.
- The approach includes checking control side-channel spillage and utilizing bit thickness estimation to create a measurable show for discovery.
- Execution incorporates utilizing CMOS current-mode Gilbert Gaussian Circuit-based Gaussian parts for KDE.
- The think about centers on AES-128, which is actualized on an ARM Microcontroller by ST Microelectronics.
- ChipWhisperer-lite board was utilized for propelling clock-glitch assaults and capturing control side-channel follows for assessment.
- The research illustrates real-time factual show overhauling employing a sliding window approach.
- The proposed CMOS-based mixed-signal system is outlined at a 45nm innovation hub, giving productive discovery with customizable parameters such as Part SD and LH T hres.
- The normal control utilization of the proposed plan is around 210 W at a 2 MHz inspecting recurrence.
- The strategy emphasizes the significance of parameter programming for improving discovery viability.

Improved DPA Attack Method on AES Encryption [4]

:-

Side channel attacks are a new technology that focuses on device performance losses such as

energy, time, and radiation. These attacks help to discover encryption keys by analyzing the leakage. Differential Power Analysis (DPA) is a side channel attack technique that compares the peaks of the curves to see if the key is correct. This method is often used to break security protocols by analyzing the power consumption fluctuations. A research paper mentions an improvement in DPA attacks against AES-128 encryption. By fixing the plaintext data and forcing the correlation to approach a high value of 1, the signal-to-noise ratio (SNR) is improved. This improvement allows the new method to be used to mount a successful DPA attack. The results of this research provide valuable insights and guidance to researchers interested in strengthening encryption techniques and improving security measures against side-channel attacks. Understanding and refining DPA techniques can help researchers better protect sensitive data from potential compromise.

Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA) [5]

:-

The research report focuses on demonstrating two major techniques, Differential Power Analysis (DPA) and Correlation Power Analysis (CPA), for performing power analysis attacks against an AES-128-S box based on the Arduino Uno microcontroller. The authors implement a Difference of Means attack for DPA and build a power model using the Hamming weight power model method for CPA.Rephrase

These target the AddRoundKey and SubBytes functions of the AES-128 algorithm and extract the full 16-byte encryption key by analyzing the power consumption pattern during encryption operations. Experimental results show that both DPA and CPA attacks are effective against the Arduino Uno. However, it is found that the results obtained by CPA are easier to interpret analytically compared to DPA. The contribution of this paper is a comprehensive comparison of the applicability of DPA and CPA techniques against power analysis attacks. Moreover, the authors provide a detailed methodology that allows the reader to reproduce these attacks on their own hardware and understand how the attacks are performed, specifically targeting the AES-128 algorithm. Overall, this work highlights the vulnerability of cryptosystems, especially the AES-128-S-Box, to power analysis attacks such as DPA and CPA, and emphasizes the importance of implementing countermeasures to protect against such threats in real-world scenarios.

Efficient Implementation of Masked AES on Side-Channel Attack Standard Evaluation Board [6]

:-

The research study described an AES-128 smart card implementation that uses a masking technique to fend off Differential Power Analysis (DPA) assaults. The solution aimed to eliminate the relationship between power consumption and the hamming weight of sensitive data, hence offering resilience against first-order DPA assaults. The suggested approach successfully secures the data while using little memory and clock cycles, making it simple to implement in software. The application and masking algorithm of the smart card were shown to be effective based on the testing findings obtained on the Side-Channel Attack Standard Evaluation Board (SASEBO-W).

Hardware Software Co-Simulation of an AES-128 based Data Encryption in Image Processing Systems for the Internet of Things Environment [7]

:-

The study paper addresses many encryption methods for security, including RSA, DES, and AES. It investigates the use of lightweight cryptography as an IoT security solution. The study also discusses picture encryption in wireless sensor networks using the AES algorithm. The

implementation of AES on FPGA for effective encryption is also mentioned in the study. It explores the importance of hardware-software co-design applications in encryption procedures. The literature also emphasizes the design of Rijndael (AES) as an enhanced encryption standard. The study also discusses AES-based picture encryption methods for a variety of uses, such as satellite systems. It talks about how AES has been modified for use in picture cryptosystems and how important it is for safe communication.

Vulnerability of Advanced Encryption Standard algorithm to Differential Power Analysis attacks implemented on ATmega-128 microcontroller [8]

:-

This study looks into how susceptible a microcontroller crypto-device's Advanced Encryption Standard (AES) algorithm is to Differential Power Analysis (DPA) attacks.
Side channel attacks, such as DPA, use physical properties of cryptography hardware, including power consumption, to crack secret keys.
The investigation collected 1000 power traces for DPA analysis using the ChipWhisperer capture hardware Rev2 tool.
After encrypting 1000 plaintexts with the same key, the study successfully recovered the 128-bit secret key of the AES implementation by monitoring power consumption during encryption processes.
The findings highlight how crucial it is to design cryptographic algorithms securely in gadgets such as smartcards, ASICs, and FPGAs in order to guard against side-channel attacks.

Interceptive Side Channel Attack on AES-128 Wireless Communications for IoT Applications [9]

:-

In the study report, a wireless interceptive Side-Channel Attack (SCA) method for IoT wireless communications AES-128 encryption decryption is introduced. The suggested method entails utilizing Correlation Electromagnetic Analysis (CEMA) to get the secret key from the encrypted communication channel set up between two Arduino boards with ATmega processors. Recognizing modules that generate notable electromagnetic (EM) signals during encryption and evaluating the AES-128 algorithm's resilience to CEMA-based attacks are the essential elements of the interceptive SCA approach. Through studies, the researchers discovered that during the encryption process, EM signal leakage happen at particular modules such FLASH memory, data bus, and SRAM, making it possible to successfully retrieve the secret key from EM traces.

Improved Power/EM Side-Channel Attack Resistance of 128-Bit AES Engines With Random Fast Voltage Dithering [10]

:-

The study article focuses on using a method known as random fast voltage dithering (RFVD) to increase the security of 128-bit Advanced Encryption Standard (AES) engines. In order to withstand power and electromagnetic (EM) side-channel attacks (SCA), the study presents the idea of an integrated voltage regulator (IVR) with bond-wire inductors and an on-chip all-digital clock modulation (ADCM) circuit to implement RFVD. The RFVD technique successfully reduces the impact of local and global supply noises by causing random shifts in clock edges and random fluctuations in the AES input supply. This makes it more difficult for attackers to decode sensitive data.

Side Channel Attack Countermeasure for Low Power Devices with AES Encryption [11]

:-

The Internet of Things (IoT) frequently uses low-power devices, which frequently lack adequate security safeguards to safeguard sensitive data. The study article compares and analyzes defenses against Side Channel Attacks (SCA) in low-power devices that use 128-AES encryption. It is noted that algorithm-based countermeasures are more suited to safeguard low-power devices from SCAs. A customized countermeasure based on byte logic is proposed as a result of testing to evaluate the efficacy of countermeasures against Correlation Power Analysis (CPA) attacks in low-power devices. To assess the effectiveness of the suggested byte logic-based countermeasure in safeguarding low-power devices, it is compared with traditional countermeasures of the same kind.

Research on AES Cryptographic ChipElectromagnetic Attack Based on Deep Transfer Learning [12]

:-

This research report emphasizes electromagnetic radiation detection as the main test method and focuses on studying side-channel threats using FPGA cipher chips and the AES-128 cryptographic algorithm. By giving the training model beginning weights, transfer learning is used to address the problems of labor-intensive training and huge sample gathering. This method increases the speed and accuracy of important side-channel attacks based on deep learning while enabling the use of more training data. The study team successfully constructed an attack model that obtained a 77.13 percent recovery rate for the nibble key by aligning the AES-128 plaintext and keys and gathering matching electromagnetic data. This represents a significant improvement over direct training.

Attacking AES Implementations Using Correlation Power Analysis on ZYBO Zynq-7000 SoC Board [13]

:-

The study focuses on two popular side channel attacks that are still in use today: Differential Power Analysis (DPA) and Correlation Power Analysis (CPA). It talks about executing the CPA attack on AES-128 implementations in hardware and software by using a modified ZYBO board. The researchers present the outcomes of their experiments in which they used the modified ZYBO device to attack AES implementations. The writers offer thorough explanations of how to carry out CPA attacks against AES-128, highlighting the significance of hardware and software security in cryptographic systems. Overall, the literature review in the research highlights how susceptible AES implementations are to CPA attacks and stresses how crucial it is to protect cryptographic systems against these side-channel attacks in order to guarantee the confidentiality and integrity of data.

SIDE CHANNEL ANALYSIS - A DEMONSTRATIVE APPROACH ON A 128-BIT AES ALGORITHM [14]

:-

Side channel analysis is the study of unintentional signals that are released during a device's functioning and have the potential to reveal private data. Many studies have been conducted on power analysis attacks on circuits, especially after Differential Power Analysis was introduced and shown to be more successful than Simple Power Analysis. To improve security measures, researchers have created variants of power analysis approaches, such as correlation power analysis utilizing Pearson's Correlation Coefficient. Although side channel assaults are intended to be mitigated by proposed defenses like the Montgomery Ladder Method and Random Splitting Operation, attackers continue to develop inventive ways to get around security measures. The outsourcing of various circuit components worldwide, which compromises integrity for speed and quality, has resulted in a rise in security threats as a result of the globalization of circuit production.

Software Implementation of CRA and TRA to Recover the AES-128 Key using Side-Channel Signals with Python3 [15]

:-

The study describes the software-enabled recovery of the AES-128 key from an unidentified system using two side-channel radio attacks. The two attacks that are being used are the Template Radio Attack (TRA) and the Correlation Radio Attack (CRA). These attacks are constructed on a Linux-based machine with Python3, making use of the algorithm's Hamming-weight model and Probability Density Functions. The measure of partial guessing entropy is used to assess the results. The CPU is used to execute the software, demonstrating how these radio attacks can be used in real-world recovery situations.

1.5 Problem statement

Side Channel attack analysis of AES128 algorithm on ATXmega128D4-AU target board and perform Differential electromagnetic analysis.

Chapter 2

System design

In this chapter, we list out the interfaces.

2.1 Differential Power Analysis(DPA)

2.1.1 Mathematical Analysis DPA

Differential Power Analysis (DPA)

Differential Power Analysis (DPA) is an advanced cryptanalytic technique used to extract cryptographic keys by analyzing minute fluctuations in power consumption during cryptographic operations. Imagine a scenario where an attacker targets the first byte (byte 0) of a secret key in AES encryption. To execute DPA, the attacker systematically hypothesizes different values for byte 0, ranging from 0x00 to 0xFF. For each guessed value k, the attacker calculates a hypothetical intermediate value L using the AES Substitution Box (S-box):

$$L = S\_box[P \oplus k] \tag{2.1}$$

where P represents the plaintext byte.
During the encryption process, the attacker measures and records power consumption traces generated by the device. These traces are then categorized into two distinct groups based on a specific bit b of the hypothetical intermediate value L: Group 1 comprises traces where the bit b is set, while Group 0 consists of traces where it is not set.
Next, the attacker computes the average power consumption for each group:

$$one\_avg = \frac{1}{|P_1|} \sum_{T \in P_1} T \tag{2.2}$$

$$zero\_avg = \frac{1}{|P_0|} \sum_{T \in P_0} T \tag{2.3}$$

where $|P_1|$ and $|P_0|$ denote the number of traces in Group 1 and Group 0, respectively, and T represents individual power traces.
The core of the DPA technique lies in calculating the differential trace $diff\_trace$, which reveals the difference between one_avg and $zero\_avg$:

$$diff\_trace = one\_avg - zero\_avg \tag{2.4}$$

By analyzing these differential traces across all guessed values k, the attacker identifies the key byte k that produces the maximum differential value. This key byte is highly likely to correspond to the correct value of byte 0 of the secret key. Through this meticulous process of

exploiting subtle power variations, DPA demonstrates its effectiveness in compromising cryptographic implementations.
This example underscores the critical importance of implementing robust countermeasures to mitigate such vulnerabilities. Protecting against DPA involves techniques such as randomizing power consumption patterns, adding noise to power measurements, or employing algorithms that minimize leakage of information through power channels. By understanding and addressing these vulnerabilities, cryptographic systems can better safeguard sensitive information from sophisticated attacks like DPA.

2.2 Advanced Encryption Standard(AES)128

AES (Advanced Encryption Standard) 128 is a widely used symmetric encryption algorithm known for its high security and efficiency in protecting sensitive data in various applications. The basis of AES is the use of a secret key that can be 128, 192, or 256 bits long. In particular, AES 128 uses a 128-bit key. This key is very important as it controls both the encryption and decryption processes. Therefore, it is important to keep it secure and secret. The AES 128 encryption process operates on blocks of data that are uniformly 128 bits (16 bytes) in size. To protect data, AES uses a series of complex encryption operations made up of multiple rounds. Each round consists of different transformations applied to the data block and the encryption key. AES 128 contains 10 rounds of these transformations, including operations such as permuting, rearranging, and shuffling the data bits. These operations are carefully designed to ensure that the encrypted data remains resistant to a wide range of encryption attacks. At the heart of AES is its ability to ensure confidentiality through these complex rounds of transformations. During encryption, each block of data undergoes a series of permutations using substitution boxes (S-boxes), in which each byte of the block is permuted according to predefined rules. This is followed by a permutation step, in which the positions of the bytes in the block are rearranged based on a specific matrix. Additionally, a mixing operation called the MixColumns step further improves data spreading, ensuring that local changes in the plaintext do not lead to significant changes in the entire ciphertext.

Mathematical Analysis AES 128

1. Key Expansion:
The key expansion process involves generating a series of round keys from the original key. Each round key is derived from the previous round key using a key schedule function. The key schedule function involves various operations such as substitution, rotation, and XOR. Mathematically, the key expansion process can be represented by a function K that takes the original 128-bit key K_0 and produces a series of round keys $K_1, K_2, \ldots, K_{10}$:

$$K(K_0) \rightarrow \{K_1, K_2, \ldots, K_{10}\} \tag{2.5}$$

2. Initial Round:
In the initial round, the plaintext block is XORed with the first round key. Mathematically, this can be represented as:

$$C_0 = P \oplus K_0 \tag{2.6}$$

where P is the plaintext block and C_0 is the intermediate ciphertext after the initial round.
3. Rounds:
AES-128 consists of 10 rounds, each involving four main operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey.

1. **SubBytes:** The SubBytes operation involves substituting each byte of the block with a corresponding value from a substitution table (S-box). Mathematically, this can be represented as:

$$S(P) = \{S(P_{i,j})\} \tag{2.7}$$

where $P_{i,j}$ represents the byte at row i and column j of the plaintext block P, and $S(\cdot)$ is the substitution function.

ShiftRows: The ShiftRows operation involves cyclically shifting the rows of the block. Mathematically, this can be represented as:

$$\begin{bmatrix} C_{0,0} & C_{0,1} & C_{0,2} & C_{0,3} \\ C_{1,0} & C_{1,1} & C_{1,2} & C_{1,3} \\ C_{2,0} & C_{2,1} & C_{2,2} & C_{2,3} \\ C_{3,0} & C_{3,1} & C_{3,2} & C_{3,3} \end{bmatrix} = \begin{bmatrix} P_{0,0} & P_{0,1} & P_{0,2} & P_{0,3} \\ P_{1,1} & P_{1,2} & P_{1,3} & P_{1,0} \\ P_{2,2} & P_{2,3} & P_{2,0} & P_{2,1} \\ P_{3,3} & P_{3,0} & P_{3,1} & P_{3,2} \end{bmatrix} \tag{2.8}$$

3. **MixColumns:** The MixColumns operation involves multiplying each column of the block by a fixed polynomial modulo $x^4 + 1$, followed by modular reduction. Mathematically, this can be represented as a matrix multiplication:

$$\begin{bmatrix} C_{0,0} & C_{0,1} & C_{0,2} & C_{0,3} \\ C_{1,0} & C_{1,1} & C_{1,2} & C_{1,3} \\ C_{2,0} & C_{2,1} & C_{2,2} & C_{2,3} \\ C_{3,0} & C_{3,1} & C_{3,2} & C_{3,3} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} P_{0,0} & P_{0,1} & P_{0,2} & P_{0,3} \\ P_{1,0} & P_{1,1} & P_{1,2} & P_{1,3} \\ P_{2,0} & P_{2,1} & P_{2,2} & P_{2,3} \\ P_{3,0} & P_{3,1} & P_{3,2} & P_{3,3} \end{bmatrix} \tag{2.9}$$

4. **AddRoundKey:** The AddRoundKey operation involves XORing the round key with the block. Mathematically, this can be represented as:

$$[C_i = C_{i-1} \oplus K_i,] \tag{2.10}$$

where C_i is the intermediate ciphertext after round i and K_i is the round key for round i.

4. **Final Round:** The final round is similar to the other rounds but lacks the MixColumns operation.
5. **Output:** After the final round, the resulting ciphertext block is the encrypted form of the plaintext block.

2.3 Functional block diagram

Figure 2.1 depicts a standard DPA attack setup. This configuration uses a target board that has the AES128 cryptographic algorithm loaded on it. The powertraces collecting device on the capture board measures the power consumption traces during specific encryption operations using an ADC. The data can be instantly transferred from the capture device to the PC for additional analysis using the USB interface. Hence, we ought to be able to obtain the power consumption traces in a hassle-free, modular manner.

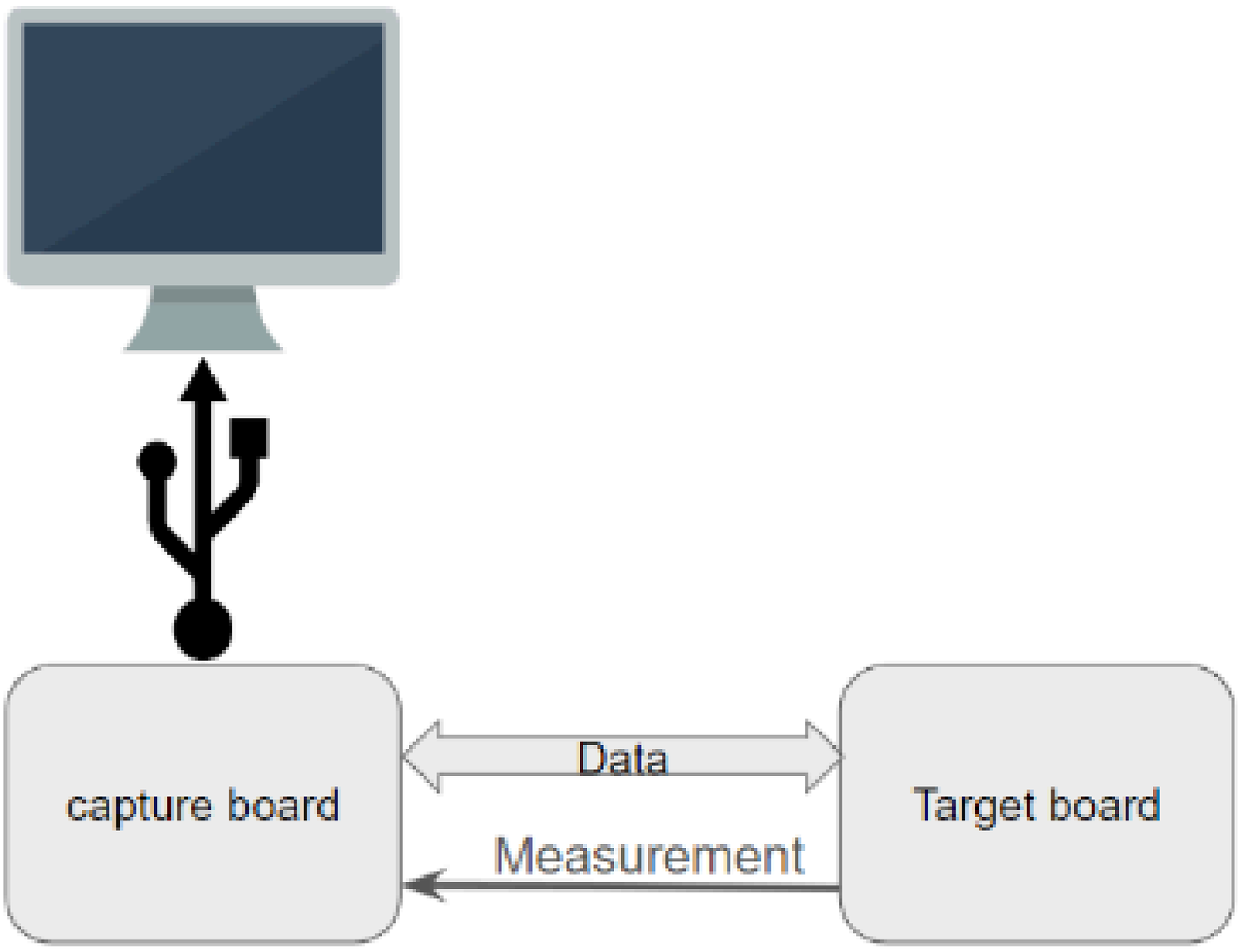

Figure 2.1: Functional block diagram

Chapter 3

Implementation details

3.1 Specifications and system architecture

3.1.1 ChipWhisperer

A comprehensive open source toolchain for researching side channel attacks on embedded systems and confirming these devices' side channel resistance is called ChipWhisperer. Specifically, ChipWhisperer concentrates on voltage and clock glitching attacks, which momentarily interrupt a device's power or clock to produce unexpected behavior (such skipping a password check). Power analysis, on the other hand, leverages information disclosed by a device's power usage to execute an attack. For this reason, they have a variety of hardware settings, including as the ChipWhisperer Lite, Husky, Nano, Pro, and others. These setups vary from one another in terms of speed, triggering ports, accuracy of measurements, and compatibility with target boards. In our instance, ChipWhisperer Lite is our main concern. The hardware components of the toolchain are packaged together in a single unit and include SMA cables, a USB, a target board, a capture board, and a 20-pin FRC. With the aid of github, we may download and install the software because it is opensource.

Target board

The ATxmega128D4-AU microcontroller from Atmel (now Microchip Technology) provides a flexible solution for embedded systems that require powerful processing capabilities and extensive peripheral support in Figure 3.1 . It features a powerful 8/16-bit AVR core running at up to 32 MIPS with 128 KB Flash memory for program storage and 8 KB SRAM for data management. The microcontroller integrates multiple communication interfaces, including

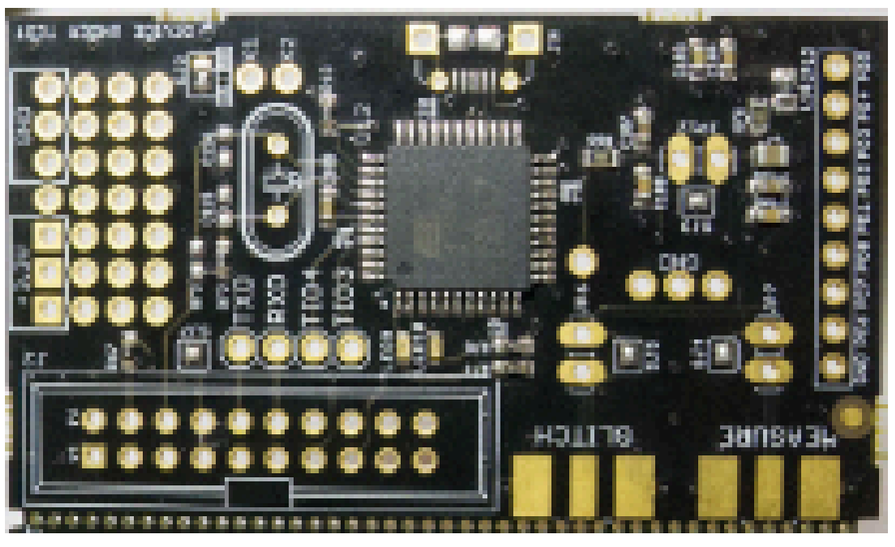

Figure 3.1: Target Board

feature	range
Target Device	ATXmega128D4-AU
Target Architecture	8-bit Harvard
Vcc	3.3V
Programming	PDI
Hardware Crypto	No
Availability	ChipWhisperer-Lite 1-part/2-part
Shunt	49.9 ohms

Table 3.1: Specifications

full-speed USB 2. 0, CAN and LIN, as well as up to 8 USART/UART, 4 SPI and 2 TWI modules for flexible connectivity options. It includes advanced peripherals such as 12-bit ADCs and DACs, multiple 16-bit timers/counters, and real-time counters (RTCs) for precision timing applications. Power management options include various sleep modes to minimize power consumption, improving its suitability for battery-powered applications. The ATxmega128D4-AU is packaged in a 44-pin TQFP format and supports in-system programming and debugging via JTAG and PDI interfaces, making it a comprehensive choice for various embedded system designs.

Capture Board

A hardware tool designed specifically for side-channel power analysis and glitching assaults on embedded devices is the ChipWhisperer Lite capture board. It was created by NewAE Technology Inc. and has high-speed analog-to-digital converters (ADCs) to record fluctuations in microcontroller power consumption and electromagnetic emissions. The board has capabilities including external trigger synchronization and USB interface for control and data transfer. It is mostly used in hardware security testing and security research to find flaws and retrieve private data, including cryptographic keys, from target devices. The Figure 3.2 shows the hardware structure of the Capture Board.

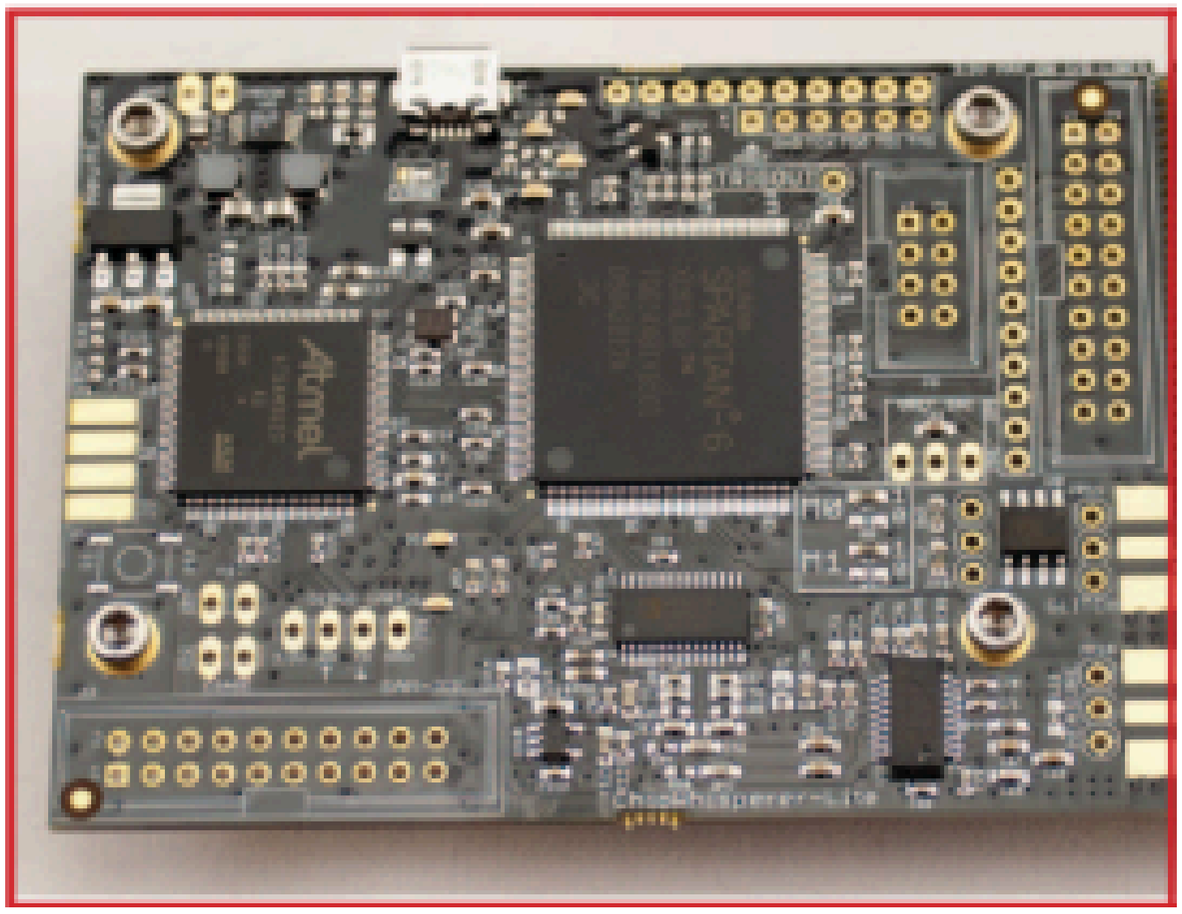

Figure 3.2: Capture Board

Highlights

- Can be clocked at both the same clock speed as the target and 4 times faster.
- Has a 10-bit 105MS/s ADC for capturing power traces.
- Can be configured for synchronous capture and glitch architecture, which greatly improves performance over a typical asynchronous oscilloscope setup.
- Can generate clock and voltage faults via FPGA-based pulse generation.
- Has an integrated XMEGA (PDI), AVR (ISP), and STM32F (UART Serial) bootloader.

Visit ChipWhisperer Lite Specifications for the whole specification.

Note: Throughout our project we'll be using ChipWhisperer Lite 2-part version(cw1173), which is almost same as ChipWhisperer lite.

3.2 Algorithm

The main attacking algorithm is as follows

Step 1: Trace Capturing

The first step in the procedure is to record the cryptographic device's power usage while it encrypts data using AES. Every trace shows the amount of power used for a single AES encryption operation over time. The plaintext data to be encrypted, the fixed key for AES encryption, and power measuring equipment to track power usage during the encryption are the inputs for this stage. One encrypted plaintext input is represented by each power trace in the output, which is a collection of power traces. This is an important step since these power traces contain information that leaks from the power usage of the device. This information can be deciphered through analysis to provide the secret key used for AES encryption.

Step 2: Hypothetical Leakage Model

The next stage is to define the leakage model, which connects the power usage to the intermediate values during the AES encryption process. Using this model, fictitious power consumption estimates for certain important assumptions are produced. The inputs are a function that mimics the nonlinear substitution stage of the AES algorithm, known as the SBox operation. The fictitious leakage numbers based on the plaintext data and the key estimate are the output. We can create expected power consumption numbers for various key estimates using this model, which is essential since we can compare them to the actual measured traces.

Step 3: Key Byte Guessing Loop

In this phase, we estimate the power consumption for each guess by iterating over all possible values (0 to 255) for each byte of the AES key. The range of potential values for a single key byte (0 to 255) and the plaintext data used in the trace capturing are the inputs. The estimated power consumption figures for each major estimate are the output. This step is important because it allows us to identify which estimate most closely fits the actual measured power consumption later on by speculating on the power usage for each potential key byte.

Step 4: Trace Grouping Based on Hypothetical Leakage

We classify the power traces for each key estimate into two groups according to the value of a particular bit in the theoretical leakage model. Traces with a bit of 1 will be in one group, and traces with a bit of 0 will be in the other. The real power traces that were recorded and the estimated leakage values for the current key guess are the inputs. Two sets of power traces are produced as an output: one set for traces with the hypothetical bit set to 1 and another set for traces with it set to 0. By grouping traces together in this way, we can compare the patterns of power consumption when the bit is set to 1 and when it is set to 0, which will help us determine which key byte is accurate.

Step 5: Average Trace Calculation

The average power usage trace for each of the two sets of traces—one with the hypothetical bit set to 1 and the other to 0—is then determined. The two sets of traces that were acquired in the preceding stage serve as the inputs. Two average power traces—one for each group—are the result. The average traces smooth out noise and highlight the variations brought about by the key-dependent activities. They also reflect the normal power consumption pattern for each fictitious bit value.

Step 6: Difference Calculation

Next, we determine the absolute difference between the two groups' average traces. Determine the difference's greatest value at each time point in the trace. The two average power traces from the preceding phase serve as the inputs. The output for the current key guess is the largest absolute difference value. The largest difference shows how closely the real power usage fits the theoretical leakage model (for the present key guess). A greater discrepancy indicates a more plausible key guess.

Step 7: Best Key Byte Identification

The goal of this stage is to determine which key byte guess yields the highest maximum difference value. This estimate is thought to be the most likely value for the key's current byte. The inputs consist of all key guesses' maximum difference values. The most likely value for the current key byte is the output. The recovery of the complete AES key results from this step's reduction of the range of values that can be assigned to each key byte.

Step 8: Full Key Recovery

Lastly, we carry out the same procedure again using the full 16 bytes of the AES key. For every byte of the key, the most likely value will be produced for each iteration. The inputs consist of the raw power traces and plaintext data, as well as the range of values that can be assigned to each key byte (0 to 255). The entire 16-byte AES key is what is produced. The effectiveness of the DPA attack is demonstrated by recovering the complete AES key by combining the most likely values for each key byte.

3.3 Flowchart

The primary flow of a program is defined, encompassing the loading of algorithms, the creation of plaintexts, encryption, recording power traces, and the DPA attack model. For every step-by-step process, input and output are shown and defined. Using standard symbols and conventions, create the flowchart and connect each sub-step to the appropriate input and output nodes. The flowchart has been examined and enhanced to ensure that it accurately represents the main program flow. putting the flowchart into practice and testing the program to ensure that it runs well and adheres to project requirements.
The procedures for carrying out a Differential Power Analysis (DPA) attack with the ChipWhisperer Lite kit are shown in the Figure 3.3 which is supplied here. This is how the procedure is described:

Start:
The beginning of the DPA attack procedure.

Load Crypt Algorithm with Key: The cryptographic algorithm is loaded onto the target board along with the secret key.

Generate Plaintext: A plaintext message is generated, which will be encrypted for N Times.

Encrypt: The plaintext is encrypted using the cryptographic algorithm and key.

Take Power Trace: The power consumption during the encryption is recorded to capture the power trace.

DPA Attack: The collected power traces are analyzed using DPA techniques to find patterns correlated with the secret key.

Key Recovery: The final step is to recover the secret key based on the analysis of the power traces.

End: The conclusion of the DPA attack process.

This flowchart is crucial for understanding the sequence of actions in a DPA attack, which involves analyzing variations in power consumption to uncover secret keys in cryptographic hardware.

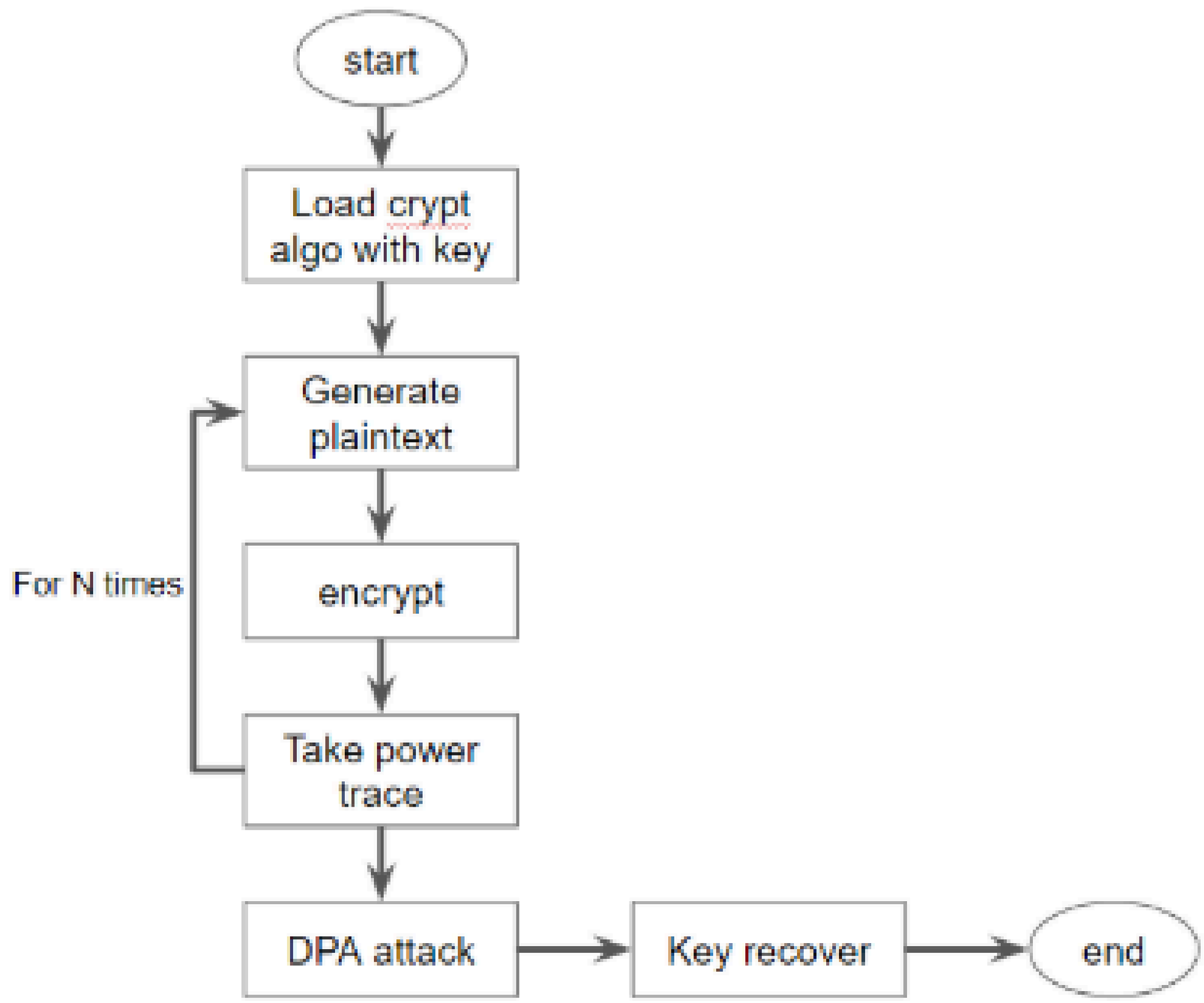

Figure 3.3: Flowchart

Chapter 4

Results and discussions

4.1 Result Analysis

This chapter focuses on the results obtained and their analysis. Following figures will provide output at various intermediate steps.

Configurations
The Figure 4.1, shows the implementation of the S-box that AES uses in it. At the first round of substitution, it will uses the full original key and we just exploit this.
Using this S-box we will derive hypothetical leakage data of 2500 various plaintext inputs considering 1 byte at a time. For a total of 256 key guesses for a given byte we passed it to this s box and got a hypothetical power consumption trace. Based on the LSB bit of S-box output, we segregated it as 0 valued key or 1 valued key. 5000 samples were considered for a givn 128bit plaintext. Notably for n bit key, bruteforce method of password breaking requires (2^n) attempts .
which means for 128 bit key 2^{128}= 340 trillion trillion trillion attempts but our method decreases this to 256(n/8) i.e. 256 x 128/8 =4096 attempts would be enough. All we need is enough plaintext input vs power consumption traces.

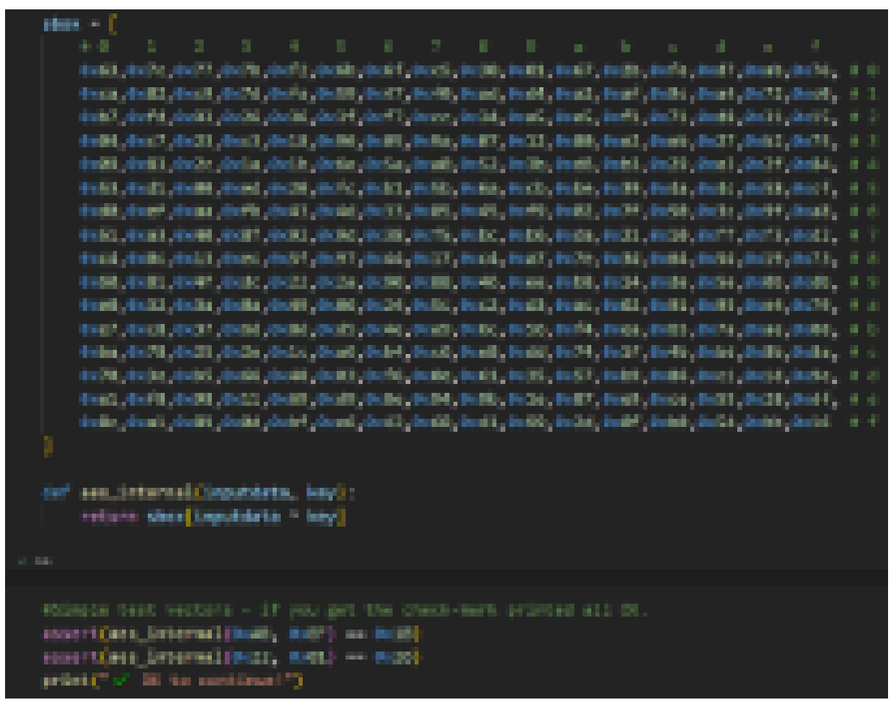

Figure 4.1: S-box Implementation

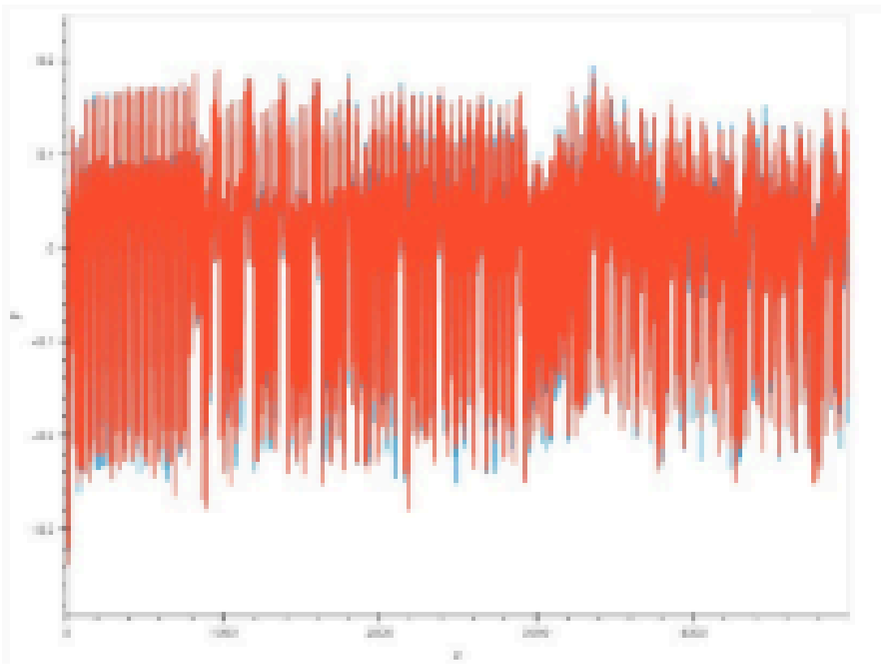

Figure 4.2: Power Traces

The Figure 4.2 explains the about power consumption of crypt algorithm looks like for a given plaintext key pair. In our implementation we have taken power traces for 2500 of such plaintext inputs with a given key. So the resulting trace array consisits 2500 x 5000 array. We may extend it to more number of samples per trace while we configure the scope.

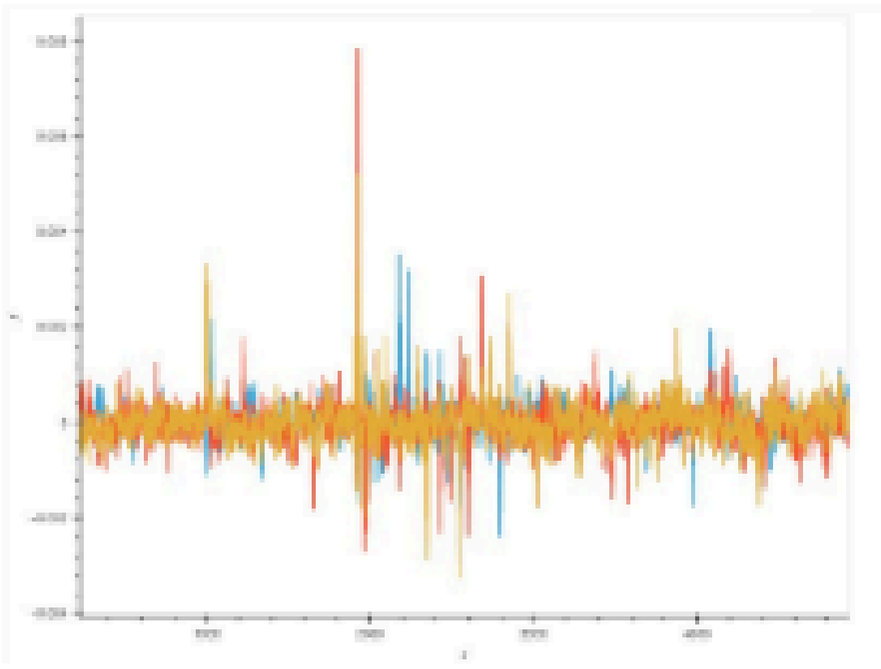

Figure 4.3: Difference of Means

The Figure 4.3 explains about the plot of difference of means for the key guesses 7e,2c,2d. this clearly shows a large peak for the keybyte 0x7e.since we haven't taken absolute value of differences of means, plot is in both + y axis and - y axis. in nutshell for a given byte of key, for nth key guess dom = mean(0trace[n])-mean(1trace[n]) where 0 trace is group that have the traces corresponds to the plaintexts whose output for keyguess n will result in LSB=0; similarly for 1trace.

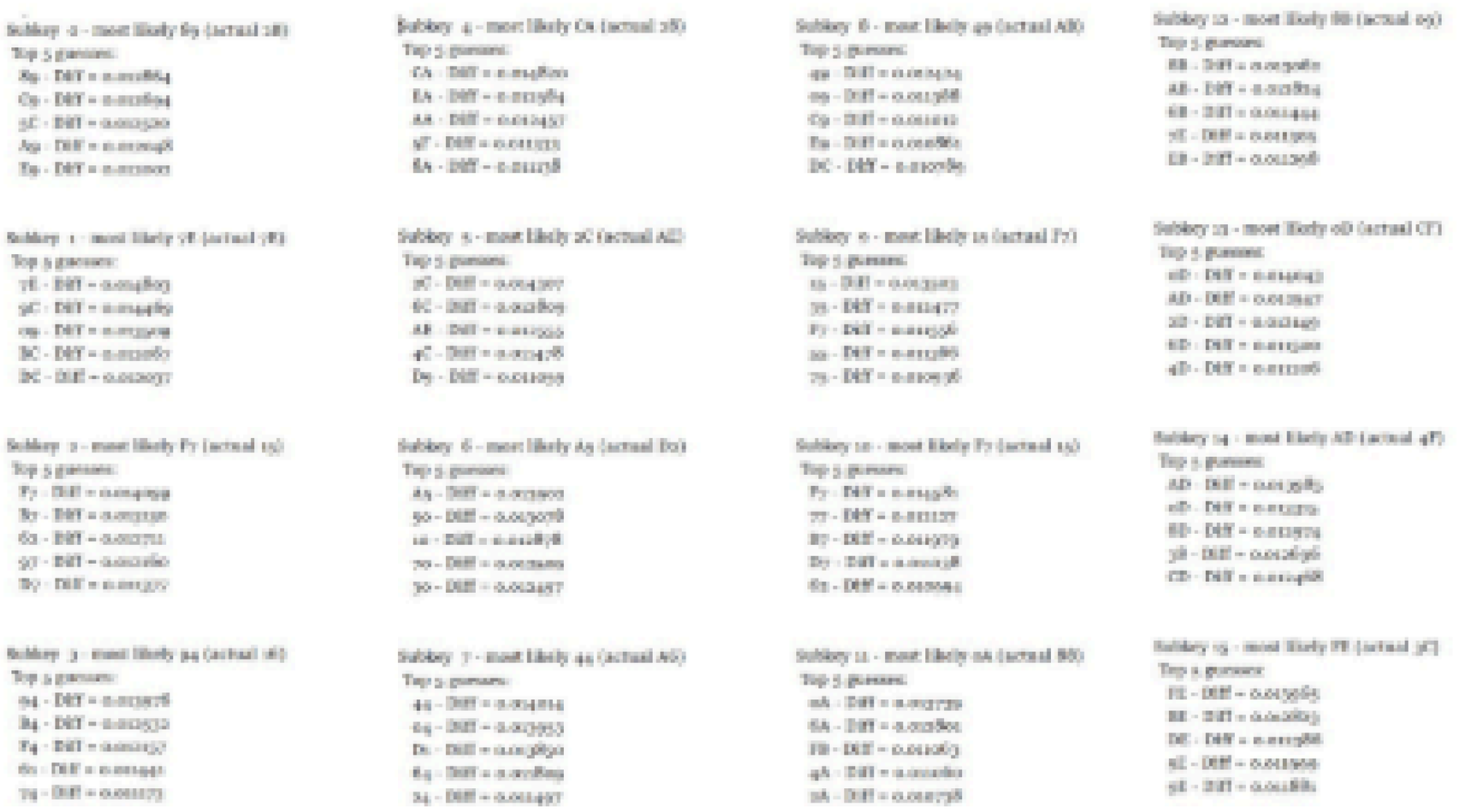

Figure 4.4: Key Recovered

The Figure 4.4 explains about the keys that are recovered from DPA analysis. also it shows top five guesses for a given byte of key.
From figure 4.4 we can see that only one byte of key with its correct position has been recovered with maximum confidence. which means we are able to crack only 12.5 percent of the actual key. this low result my be due to the noise present in the power spectrum, or lesser number of traces or lesser number of samples per trace. But with the help of more number of traces and samples we may able to achive good results.

Chapter 5

Conclusions and future scope

5.1 Conclusion

In conclusion, the Differential Power Analysis (DPA) attack employing the ChipWhisperer Lite kit produced a meager success rate of only 12.5 percent , contrary to early expectations. As part of the project, the cryptographic method and key were loaded, plaintext messages were generated, and then they were encrypted while power traces were being recorded.
Nevertheless, the examination of these traces indicated very weak correlations with the secret key, underscoring the difficulties and intricacies associated with carrying out successful side-channel attacks. In the future, more research and development will be needed to improve DPA defenses and fortify embedded systems' security against similar vulnerabilities.

5.2 Future scope

Based on the problem statement and analysis of the AES128 algorithm implemented on the target board ATXmega128D4-AU using Differential Power Analysis (DPA), here are some possible areas and considerations for the future:
1.Strengthen Security Measures: Investigate and implement countermeasures against DPA attacks. This could include considering techniques such as algorithm masking, hardware-based noise injection, or using advanced crypto implementations that are resistant to side-channel attacks.
2.Hardware Optimization: Investigate hardware modifications or optimizations on the target board to reduce electromagnetic leakage. This may include shielding techniques, layout redesign, or the use of components with lower electromagnetic radiation characteristics.
3.Advanced Side Channel Analysis: Extending the analysis to include other side channel attacks in addition to DPA, such as: B. Simple Electromagnetic Analysis (EMA), Fault Injection Attacks (FIA), or Timing Attacks. Comparing these techniques may provide a more comprehensive assessment of the security of an AES128 implementation.
4.Real World Considerations: Investigate how findings from a controlled laboratory environment translate to real world scenarios. Factors such as environmental conditions, operational variability, and long-term reliability across different usage patterns can significantly impact the effectiveness of countermeasures against side-channel attacks.
5.Benchmarking and Validation: Conduct a benchmarking study to compare the security and performance of the ATXmega128D4-AU board with other microcontroller platforms or cryptographic hardware modules. This may include standardized test frameworks and metrics that allow for objective comparisons.
6.Education and Training Initiatives: Based on the results, develop educational materials or training programs to raise awareness among developers and designers about the importance of

secure implementation practices and the vulnerabilities associated with side-channel attacks.
7.Integration with IoT and Embedded Systems: Investigate how the AES128 implementation on the ATXmega128D4-AU board integrates with IoT and embedded system architectures. In addition to vulnerability to side-channel attacks, resource limitations, power consumption, and secure communication protocols must also be considered.
8.Regulatory and Compliance Considerations: Investigate the impact on compliance with industry standards (e.g. NIST, FIPS) and regulations (e.g. GDPR, HIPAA) related to cryptographic security and data protection. This may include conducting audits or assessments to ensure compliance with security requirements. Each of these future application areas builds upon an initial analysis of the AES128 algorithm on the ATXmega128D4-AU board with DPA to address broader aspects of security, performance, and real-world deployment considerations.

5.2.1 Application in the societal context

In today's digital age, financial transactions are primarily conducted online or through electronic payment systems. The security of these transactions relies heavily on encryption protocols such as AES128 to protect sensitive information such as credit card details, personal identification numbers (PINs), and financial records. How AES128 relates to DPA: AES128 (Advanced Encryption Standard with a 128-bit key) is widely used due to its balanced combination of security and efficiency. However, even robust encryption can be vulnerable to advanced attacks such as DPA. This attack technique uses the power consumption or electromagnetic radiation patterns emitted by the encryption device during encryption to derive the encryption key. Impact of Side-Channel Attacks: Successful side-channel attacks such as DPA against AES128 can compromise the confidentiality of financial transactions. If an attacker can extract the encryption key, they could decrypt intercepted communications, gain unauthorized access to financial accounts, or conduct fraudulent transactions. This could threaten personal financial security and undermine trust in electronic payment systems. Research and Mitigation: Investigating DPA on the ATXmega128D4-AU target board provides insight into practical vulnerabilities of AES128 implementations in real-world scenarios. Understanding these vulnerabilities can enable researchers to develop countermeasures and more secure implementations of cryptographic algorithms. This research will directly contribute to improving the resilience of financial systems against complex cyber threats.

Chapter 6

Refrences

[1] Myeongjin Kang and Daejin Park Quisquater, "Remote Monitoring Systems of Unsafe Software Execution using QR Code-based Power Consumption Profile for IoT Edge Devices". 2021 International Conference on Electronics, Information, and Communication (ICEIC)

[2] Amjed Abbas Ahmed, Mohammad Kamrul Hasan, Nazmus Shaker Nafi, Shayla Islam, Mohammad Siab Nahi, Azana Hafizah Aman's paper is titled " Optimization Technique for Deep Learning Methodology on Power Side Channel Attacks ". 2023 33rd International Telecommunication Networks and Applications Conference (ITNAC)

[3] Ahish Shylendra , Priyesh Shukla , Swarup Bhunia , and Amit Ranjan Trivedi's "Fault Attack Detection in AES by
Monitoring Power Side-Channel Statistics". 21st Int'l Symposium on Quality Electronic Design.

[4] S. Lan "Improved DPA Attack Method on AES Encryption". International Conference on Computer Information Systems and Industrial Applications (CISIA 2015) © 2015. The authors - Published by Atlantis Press

[5] Owen Lo, William J. Buchanan and Douglas Carson (2017) Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA), Journal of Cyber Security Technology, 1:2, 88-107, DOI: 10.1080/23742917.2016.1231523

[6] Massoud Masoumi, PouyaHabibi and Mohammad Jadidi " Efficient Implementation of Masked AES on Side-Channel Attack Standard Evaluation Board"International Conference on Information Society (i-Society 2015).

[7] Kusum Lata and Sandeep Saini " Hardware Software Co-Simulation of an AES-128 based Data Encryption in Image Processing Systems for the Internet of Things Environment" 2020 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS).

[8] Kealeboga Mpalane, Naison Gasela, B.M Esiefarienrhe and H.D Tsague " Vulnerability of Advanced Encryption Standard algorithm to

Differential Power Analysis attacks implemented on ATmega-128 microcontroller" ©2016 IEEE.

[9] Ali Akbar Pammu, Kwen-Siong Chong, Weng-Geng Ho and Bah-Hwee Gwee " Interceptive Side Channel Attack on AES-128 Wireless Communications for IoT Applications" APCCAS 2016.

[10] Arvind Singh, Monodeep Kar, SamuK.Mathew, Anand Rajan, Vivek De and Saibal Mukhopadhyay " Improved Power/EM Side-Channel Attack Resistance of 128-Bit AES Engines With Random Fast Voltage Dithering" IEEE JOURNAL OF SOLID-STATE CIRCUITS © 2018 IEEE.

[11] Ruminot-Ahumada, Nicol´ as; Valencia-Cordero, Claudio; Abarz´ ua-Ortiz, Rodrigo " Side Channel Attack Countermeasure for Low Power Devices with AES Encryption" 2021 IEEE International Conference on Automation/XXIV Congress of the Chilean Association of Automatic Control (ICA-ACCA).

[12] Xiaotong Cui, Hongxin Zhang, Lice Wang "Research on AES Cryptographic ChipElectromagnetic Attack Based on Deep Transfer Learning".

[13] Petr Socha, Jan Brejnik, Matej Bartik "Attacking AES Implementations Using Correlation Power Analysis on ZYBO Zynq-7000 SoC Board". 2018 7th MEDITERRANEAN CONFERENCE ON EMBEDDED COMPUTING
(MECO),11-14JUNE2018,BUDVA,MONTENEGRO

[14] Dr.J.Godwin Ponsam, S.V.Juno Bella Gracia, G.Geetha, Dr.S.Karpagaselvi, M.Safa "SIDE CHANNEL ANALYSIS - A DEMONSTRATIVE APPROACH ON A 128-BIT AES ALGORITHM ". 2020 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS).

[15] Desislava Nikolova, Ivaylo Vladimirov and Zornica Terneva "Software Implementation of CRA and TRA to Recover the AES-128 Key using Side-Channel Signals with Python3 ". ©2020 European Union.