Investigation into Photon Emissions as a Side-Channel Leakage in Two Microcontrollers: A Focus on SRAM Blocks

by

Bahareh Ebrahimi Sadrabadi

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2023

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Amr Youssef Professor, Dept. of Information Systems Engineering, Concordia University
Supervisor:	Catherine Gebotys Professor, Dept. of Electrical and Computer Engineering, University of Waterloo
Internal Member:	Vincent Gaudet Professor, Dept. of Electrical and Computer Engineering, University of Waterloo
Internal Member:	Anwar Hasan Professor, Dept. of Electrical and Computer Engineering, University of Waterloo
Internal-External Member:	Alfred Menezes Professor, Dept. of Combinatorics and Optimization, University of Waterloo

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Microcontrollers are extensively utilized across a diverse range of applications. However, with the escalating usage of these devices, the risk to their security and the valuable data they process correspondingly intensifies. These devices could potentially be susceptible to various security threats, with side channel leakage standing out as a notable concern. Among the numerous types of side-channel leakages, photon emissions from active devices emerge as a potentially significant concern. These emissions, a characteristic of all semiconductor devices including microcontrollers, occur during their operation. Depending on the operating point and the internal state of the chip, these emissions can reflect the device's internal operations. Therefore, a malicious individual could potentially exploit these emissions to gain insights into the computations being performed within the device.

This dissertation delves into the investigation of photon emissions from the SRAM blocks of two distinct microcontrollers, utilizing a cost-effective setup. The aim is to extract information from these emissions, analyzing them as potential side-channel leakage points.

In the first segment of the study, a PIC microcontroller variant is investigated. The quiescent photon emissions from the SRAM are examined. A correlation attack was successfully executed on these emissions, which led to the recovery of the AES encryption key. Furthermore, differential analysis was used to examine the location of SRAM bits. The combination of this information with the application of an image processing method, namely the Structural Similarity Index (SSIM), assisted in revealing the content of SRAM cells from photon emission images.

The second segment of this study, for the first time, emphasizes on a RISC-V chip, examining the photon emissions of the SRAM during continuous reading. Probing the photon emissions from the row and column detectors led to the identification of a target word location, which is capable of revealing the AES key. Also, the content of target row was retrieved through the photon emissions originating from the drivers and the SRAM cells themselves. Additionally, the SSIM technique was utilized to determine the address of a targeted word in RISC-V photon emissions which cannot be analyzed through visual inspection.

The insights gained from this research contribute to a deeper understanding of side-channel leakage via photon emissions and demonstrate its potential potency in extracting critical information from digital devices. Moreover, this information significantly contributes to the development of innovative security measures, an aspect becoming increasingly crucial in our progressively digitized world.

Acknowledgements

I would like to take a moment to express my sincere appreciation to everyone who has provided inspiration, encouragement, and support during my PhD research at the University of Waterloo. Their invaluable contributions have been instrumental to the completion of this thesis.

First and foremost, my deepest appreciation goes to my supervisor, Professor Catherine Gebotys. Her invaluable guidance, persistent patience, and insightful feedback have been the cornerstone of this research. Her unwavering support, particularly during challenging periods, played a crucial role in the completion of this dissertation. Furthermore, her consistent positivity and uplifting attitude served as a guiding light throughout this journey. Her mentorship and generous inspiration have left a profound impact on me.

I would also like to extend my sincere gratitude to the members of my defense committee, Professor Vincent Gaudet, Professor Anwar Hasan, Professor Alfred Menezes and Professor Amr Youssef. Their expertise and insights have significantly contributed to enhancing the quality of this dissertation. Their constructive feedback and crucial suggestions have been instrumental in refining this work to its final form. I appreciate the time and effort they invested in reviewing and improving my work.

My previous colleagues in the lab, namely Mustafa Faraj, Haohao Liao, Mahmoud Khalafalla, Mahmoud Elmohr , Karim Amin, deserve special recognition for their support during my research. Our insightful conversations and exchanges of ideas played a significant role in shaping my research.

A heartfelt thank you goes to my friends, whose understanding and encouragement during my moments of crisis were pivotal. Their moral support has played a significant role in the successful completion of this research journey.

Last, but by no means least, I am profoundly grateful to my family, my parents, my husband, and our child, who have provided emotional and financial support throughout this process. Their unwavering belief in me and their prayers for my academic success have been a constant source of strength. To everyone who has played a part in my academic journey, I extend my heartfelt thanks.

Dedication

This work is dedicated to my beloved parents, whose unwavering love and support have always been my strength, to my loving husband, who has been my pillar of support, and to our precious child, whose smiles light up my world. May this be a testament to our shared journey and love.

Table of Contents

List of Figures

List of Tables

List of Listings

List of Abbreviations

ADC Analog to Digital Converter

AES Advanced Encryption Standard

APD Avalanche Photo Diodes

CCD Charge Coupled Devices

CPEA Correlation Photon Emission Attack

DES Data Encryption Standard

DPEA Differential Photonic Emission Analysis

DUT Device Under Test

EM Electromagnetic

EOFM Electro-Optical Frequency Mapping

EOP Electro-Optical Probing

F-PE Field Photon Emission

FIB Focused Ion Beam

GPR General Purpose Registers

GUI Graphical User Interface

IC Integrated Circuit

IDE Integrated Development Environment

InGaAs Indium Gallium Arsenide

IoT Internet of Things

ISA Instruction Set Architecture

LFA Laser Fault Attacks

LLSI Laser Logic State Imaging

LSB Least Significant Bit

LVI Laser-Voltage Imaging

LVP Laser-Voltage Probing

MCP Micro Channel Plates

MOSFET Metal Oxide Semiconductor Field-Effect Transistors

MSE Mean Squared Error

NIR Near InfraRed

PCB Printed Circuit Board

PEM Photon Emission Microscopy

PICA Picosecond Imaging Circuit Analysis

PKC Public-Key Cryptography

PMT Photo Multiplier Tubes

QE Quantum Efficiency

SBOX Substitution-BOX

SFR Special Function Registers

SIL Solid Immersion Lens

SNR Signal-to-Noise Ratio

SPA Simple Power Analysis

SPEA Simple Photonic Emission Analysis

SSIM Structural Similarity Index Measure

SSPD Superconducting Single Photon Detectors

TRE Time Resolved Emission

XOR Exclusive OR

Chapter 1

Introduction

Embedded devices have become an important part of our daily lives, finding use in a diverse range of applications such as credit cards, wireless infrastructure, automated vehicles, the Internet of Things (IoT), healthcare systems, and many more. As these devices continue to be integrated into various aspects of modern society, the importance of safeguarding their security and preventing unauthorized access to sensitive information cannot be overstated. Various attack vectors can be employed to breach these systems, and among the most potent are hardware attacks that exploit physical vulnerabilities within the devices [59]. In these types of attacks, the attacker can passively record unintentional leakages from embedded devices or inject a fault, altering the normal operation of the system.

One such leakage is the photon emission from electronic components, which can yield critical information about the devices' functionality [111]. By analyzing these emissions, attackers can potentially derive cryptographic keys [33] or gain insights into chip functional blocks [66], enabling them to launch more effective fault injection attacks.

This dissertation focuses on the exploration of photon emissions from SRAM blocks and seeks to extract valuable information from these emissions. SRAMs are crucial components in embedded devices, used for storing essential data such as cryptographic keys. Unveiling the contents of SRAM could lead to the disclosure of sensitive information, thereby jeopardizing the entire system's integrity. The investigation of this side channel offers insights into the intensity of these leakages. These findings can be harnessed to analyze photon emissions and uncover critical information, such as secret keys for cryptographic algorithms like AES [33], unlocking secured circuits [83], or pinpointing vital functional blocks [66]. Moreover, the research into photon emissions in data memory components will contribute to enhancing the overall trustworthiness of embedded devices. This information can augment our understanding of the vulnerabilities present in these devices, inform the creation of more potent fault attacks, and assist in the modeling, simulation, and empirical validation of fault injection attacks and their respective countermeasures for embedded systems. Research on photon emissions as a side channel has predominantly relied on high-cost setups [111][33][49]. In contrast, this research utilizes a low-cost setup to investigate the data memory SRAM of a PIC and RISC chip. It has successfully revealed both the AES key and the SRAM content of the chip.

1.1 Thesis Overview

This dissertation investigates photon emission from SRAM blocks in embedded devices, aiming to reveal sensitive information such as cryptographic keys. The flow of the dissertation is as follows:

Chapter 2 provides the background information required for the research, including hardware attacks, photon emission characteristics, and SRAM layout. Relevant research papers on photon emission are also discussed in this chapter.

Chapter 3 outlines the research methodology, objectives, and experimental setup required for recording photon emission. The specifications of the device under test (DUT) and the board used for testing these devices are elaborated upon.

Chapter 4 discusses the recording steps of quiescent photon emission from a PIC microcontroller and the resulting images. Image processing techniques are employed to prepare recorded images for applying various attacks, such as correlation or differential attacks. The results of these attacks are discussed, and image processing measurements are performed to predict SRAM values.

Chapter 5 investigates, for the first time, the photon emissions of memory blocks in a RISC-V chip. Photon emissions of different blocks in memory, such as row and column detectors, are examined. Furthermore, the photon emissions of target rows in SRAM are investigated in an attempt to recover the content values.

In the last chapter, a summary of the work done is presented, along with the contributions related to this research. The limitations of photon emission as a side-channel attack vector and potential future work in this area are also proposed.

Chapter 2

Background

This chapter aims to provide a comprehensive background for the research, setting the stage for a deeper understanding of the investigation into the photon emissions of SRAM blocks as a side channel attack. It begins by introducing the concepts of physical and side channel attacks, which represent significant threats to modern security systems. Following this, the specific topic of photon emissions as a side channel is explained, exploring its origins and characteristics. This discussion offers valuable insights into the nature of this particular attack and sets the context for the main focus of the investigation. To further build the foundation for this research, an overview of SRAM layout and structure is provided. A thorough understanding of these details is crucial for comprehending the data memory blocks that are examined in this study. Next, we introduce the image processing techniques employed throughout the research. These methods play a critical role in analyzing and interpreting the captured photon emissions, enabling researchers to draw meaningful conclusions from the data. Finally, we summarize previous research in the field of photon emission side channels, offering an overview of the current state of knowledge in this area. By reviewing the existing literature, we can identify the gaps that this study seeks to address and establish the context in which the findings should be interpreted. By the end of this chapter, readers will have gained a solid understanding of the key concepts underpinning the research.

2.1 Physical Attack

From a classical perspective, cryptography deals with mathematical theories and algorithms, such as deriving functions that take inputs or plaintext and produce ciphertext with the aid of probable keys that yield computational security. However, cryptographic algorithms and protocols must be implemented in practical systems like embedded devices. With the implementation of cryptographic algorithms, new security problems arise. In embedded devices, not only is the computational security of algorithms important, but also the security of the entire system and electronic device, known as hardware security, needs to be addressed [59]. In hardware security, the characteristics and vulnerabilities of devices are investigated. These features or weaknesses can be exploited by attackers to compromise the integrity of a system. For instance, electronic devices have unintentional leakages that can reveal system operations. This type of information, known as side channel data, is not considered in cryptographic algorithms; however, attackers can exploit such data to perform physical attacks and obtain information about cryptographic algorithms and keys.

Each device can have distinct characteristics, so physical attacks are case-dependent and cannot be generalized, but they are typically more dangerous and effective than classical attacks [107]. Consequently, numerous studies have been conducted to investigate physical attacks.

- **Active attack**: Active attacks intentionally involve direct or indirect interference with the proper functionality of devices. These attacks typically target the computations or operations performed by the device and may either bypass the device's security systems or introduce malfunctions that make the device susceptible to further attacks, such as leaking side-channel information or generating erroneous outputs [106]. Fault injection attacks are a prime example of active attacks, where attackers attempt to inject faults into a device using various methods such as voltage manipulation [90], clock manipulation [15], temperature variation [37], light exposure [101], or electromagnetic waves [78]. By inducing these faults, attackers aim to force the device into erroneous operations, potentially compromising the system's security or revealing sensitive information [131].

- **Passive attack**: Passive attacks, in contrast to active attacks, involve the observation of device characteristics and their leakages in a non-intrusive manner, without interfering with the normal operations of the device. The goal of passive attacks is to collect information that may be of interest to potential attackers. By observing side channel information, an attacker can gain insights into the details of computations or operations performed by the target device. In other words, attackers may carefully monitor leaked data and treat them as effects of potential causes [106]. Some examples of leakage include timing information [85][47][87], power consumption [44][46], electromagnetic emanations [79][4], or any other physical information leakage [107].

Attacks can also be classified based on how they interact with the physical interfaces of devices. As such, three categories of attacks are defined as follows [59]:

- **Invasive attacks**: In invasive attacks, embedded devices' internal layers are disassembled to allow direct access to their components. For example, adversaries may use a connection of wires on the data bus to passively monitor data transfers or employ equipment like Focused Ion Beams (FIB) to access or modify data. Invasive attacks are considered the strongest and most effective types of attacks that can be mounted on crypto devices since they have direct access to vital components of the device. As a result, there are virtually no limitations on what can be performed on these devices [59][100].

- **Semi-invasive attacks**: Semi-invasive attacks are a type of hardware attack in which the chip is de-packaged without physical access to internal components or tampering with the circuit. These attacks are less intrusive than invasive attacks but still involve some degree of tampering with the device. In semi-invasive attacks, passive attacks may aim to read out memory cells without probing read-out memory circuits, while active attacks induce faults in the device with the aid of an electromagnetic field or x-ray beam [59].

- **Non-invasive attacks**: While the previously mentioned attack types require direct access to the crypto devices' chips, non-invasive attacks exploit only externally available data. However, the term ”non-invasive” does not imply that these attacks are passive. There are active non-invasive attacks that create faults in a device without dismantling it. This can be achieved by making clock or power glitches or varying ambient temperature [59].

2.1.1 Side Channel Attack

Side channel attacks are considered one of the most serious threats to the security of hardware devices, ranging from personal computers to small embedded devices such as smart cards and radio frequency identification devices (RFID) [107].

In 1998, Paul Kocher [45] first successfully used power analysis as a side channel attack. Since that time, this area has attracted significant attention. Researchers have investigated side channels from numerous perspectives [131]. A brief overview of the simple, differential, and correlation side channel attacks that will be employed in this research is provided.

In a simple side channel attack (SSCA), the leaked information recorded during an operation of interest, such as cryptographic instructions, is directly used without employing any specific statistical analysis [44]. For example, in power consumption side channels, the value of power changes based on the executed instructions. Thus, repeating instructions show repeating patterns in power consumption traces, and the sequence of instruction patterns can be detected based on the sequence of values in power traces. This information can be used to reveal the key in cryptographic implementations, where the execution sequence depends on the data, such as in DES, RSA, or AES algorithms [44][58]. For instance, by finding the difference in power trace of a device during the execution of multiplication and squaring operations, and locating them when the RSA algorithm is executed, an attacker can break the RSA encryption [45].

In a Simple Power Analysis (SPA) attack, the device's instruction path or key could be revealed. However, it is important to note that some information about the implementation of the device under attack is required for a successful SPA [57]. As simple side channel attacks do not rely on complex statistical techniques, they are generally easier to perform and require less computational effort compared to more advanced side channel attacks. Nevertheless, their effectiveness might be limited against well-protected systems that implement various countermeasures for side channel leakages.

In addition to side channel leakages that are directly related to the sequence of instructions, which are used in simple attacks, there are side channel leakages that correlate with the data values being processed. These variations in leakages are mostly very small and not easily noticeable. However, by employing statistical analysis, it is possible to reveal important information from them, such as the secret key of a cryptographic algorithm [44]. Differential and correlation attacks fall into this group of analyses, which use statistical methods to find the correlation between these recorded leakages and the data values processed in instructions [57].

In differential and correlation attacks, the first step involves recording side channel leakage traces for different plaintext inputs while executing the cryptographic algorithm. Next, a model is proposed to predict the side channel leakage based on input plaintext values and the key. This model is then used to predict the output for the guessed key and the known plaintext input. In the following step, statistical analysis is employed to compare the actual side channel traces with the predicted model for different guessed keys. If the model is accurate, the correct guessed key should have the highest correlation with the actual traces. In a differential attack, the difference of means is used for statistical analysis, while linear correlation, such as Pearson correlation, can be calculated for the correlation attack [20][57][86].

Since the exact time of the output calculation is typically unknown, the statistical analysis must be conducted for each time point within the entire time period in the trace. The highest value for the correct key at a specific time indicates the time of interest for the output calculation [86]. Furthermore, in both differential and correlation attacks, the alignment of the leakage traces is crucial, as the statistical analyses of traces for the same time are compared with each other [57]. Unlike simple analysis, these attacks do not necessitate a thorough understanding of the device implementation or a high Signal-to-Noise Ratio (SNR). However, some knowledge about the cryptographic algorithm is still required [57].

2.1.2 Advanced Encryption Standard Algorithm

In this research, the Advanced Encryption Standard (AES) algorithm has been chosen as the proof of concept for the applied attacks on cryptographic algorithms. A brief overview of the AES algorithm is provided below:

The AES is a widely used symmetric encryption algorithm based on the Rijndael cipher [27] which offers strong resistance against mathematical cryptanalysis [72]. It processes 128-bit data blocks for input plaintext and output ciphertext, and supports key sizes of 128, 192, or 256 bits named AES-128, AES-192, or AES-256. The algorithm comprises a series of repetitive rounds, with the number of rounds being dependent on the key size. Each round encompasses four distinct operations: ByteSubstitution, ShiftRows, MixColumns, and KeyAddition, as depicted in Figure 2.1.

The input plaintext is used as a 4x4 array called the "state," with each element being an 8-bit value. Each round key, denoted as k_i, is derived from the original encryption key K with 128 bit length and is also defined by a 4x4 array. The KeyAddition operation involves an exclusive-or (XOR) of the input with the round key k_i. In the ByteSubstitution step, the byte values in the input are substituted with new values based on a public, predefined S-box table. The ShiftRows transformation involves a cyclic shift of the rows in the input, while the MixColumns operation mixes the columns by multiplying each input state column, treated as a polynomial, with a fixed public array. It should be noted, the first round begins with an extra KeyAddition operation, while the last round omits the MixColumns step [26].

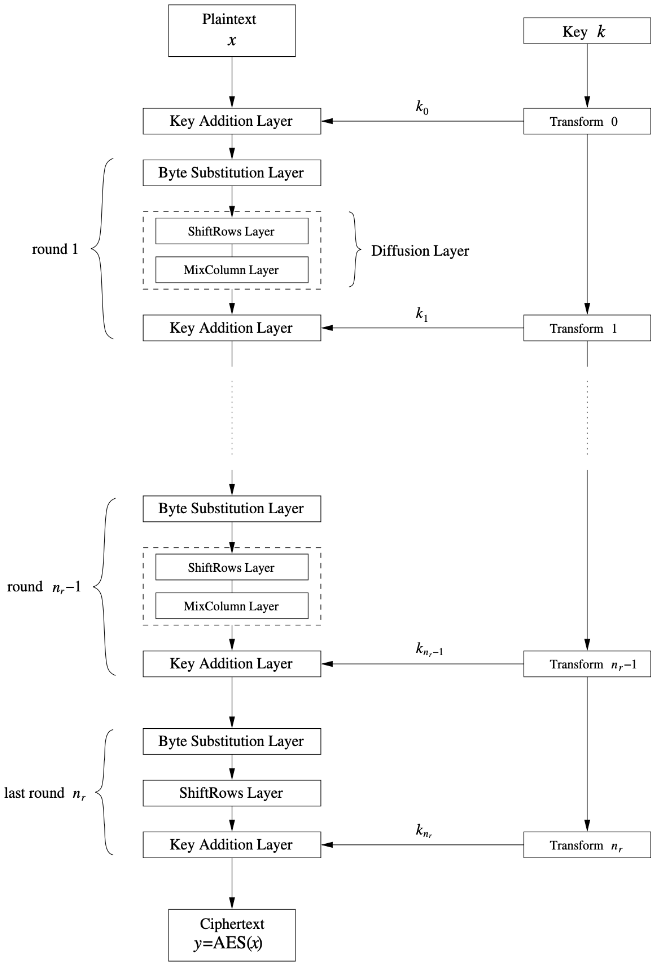


Figure 2.1: AES encryption block diagram from [72].

2.2 Photon Emission

The phenomenon of photon emission from active electronic devices was first discovered in the early nineties [67][24]. These emissions are of an electroluminescent nature, arising solely from the electrical operation of the device without any external stimulus. Since then, researchers have extensively investigated the photon emission properties of active components. Photon Emission Microscopy (PEM) was introduced as a technique for detecting photon emissions in electronic circuits and has emerged as a powerful tool for failure analysis. PEM is considered one of the best methods for identifying the root cause of failures in these circuits [17][16].

Over the past decade, the application of photon emission analysis has also expanded to the field of security [33][66][111]. The light emissions from electronic devices can be exploited as a side-channel to extract sensitive information, enabling powerful attacks on cryptographic systems. In the following sections, we provide an overview of the basic principles and applications of Photon Emission Microscopy.

2.2.1 Basics of Photon Emission

Understanding some basic principles of physics in photon emissions of active devices can be beneficial when working with them as a side-channel. Two main mechanisms define the Electroluminescence of semiconductors in general [17]:

1. Intraband process related to hot-carrier emission: Mobile charge carriers in an electric field acquire kinetic energy. This energy can then be released in the form of light emission, known as Field-Photon Emission (F-PE). In F-PE, the $p-n$ junction is in reverse-bias, resulting in the formation of a depletion region. This depletion region, also referred to as the space charge region, generates a substantial electric field. Charge carriers passing through the depletion region may accelerate in the electric field and gain kinetic energy. Upon relaxation, these carriers produce light emission covering a broad range of wavelengths in the visible to near-infrared spectrum [17][16].

2. Interband recombination emission: Electrons and holes from the conductance and valence bands can recombine with each other. This recombination process releases light and is an interband event since it involves different conductance and valence bands (R-PE). Injecting minority carriers in forward-bias enhances the likelihood of recombination and subsequent light emission. These emissions in silicon are faint and have a Gaussian distribution emission profile with a narrow spectrum [17].

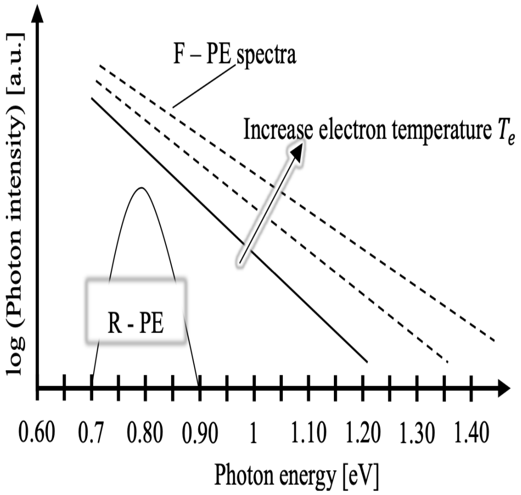


Figure 2.2: Spectral distribution of the two different mechanisms for silicon electroluminescence [16].

Figure 2.2 illustrates the spectral distribution for the two different processes from [16]. There are several light emission events in semiconductors based on these two mechanisms, which can be utilized in various applications. Figure 2.3 illustrates the I-V curve of a $p-n$ junction. It is evident that the current limit for detecting light emissions in a reverse-biased $p-n$ junction is high and occurs in the avalanche region. If the $p-n$ junction exhibits a higher-than-normal current leakage, light emission can be detected at a lower voltage, as demonstrated in figure 2.3. Researchers use the information obtained from PEM in failure analysis to identify leaky currents and problems in the circuit. Hot electrons and thin oxide breakdown are some other examples of light emission events that can be utilized in failure analysis using PEM [17].

The photon emissions of Metal-Oxide-Semiconductor Field-Effect Transistors (MOSFETs), as the most crucial components in integrated circuits, are carefully investigated [110][17][121][38]. The most interesting emissions for MOSFETs in security applications are those in the switching time of the saturated state, as well as quiescent state photon emissions. These emissions depend on the bias point of the MOSFET and can reveal information about the state of the device.

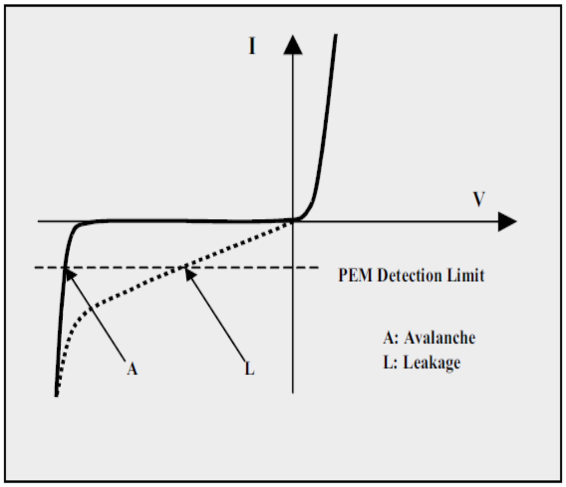


Figure 2.3: I-V curve of a $p-n$ junction [17].

Photon emission in saturated MOS

In the saturation mode of MOSFET transistors, a pinch-off occurs in the inversion layer, leading to the creation of a depletion region. The carriers in the inversion layer gain energy in the electrical field of the depletion region and are accelerated through the area to reach the drain (F-PE). The carriers are then relaxed with photon emissions called hot-carrier luminescence. These photons are emitted from the drain region of the transistor due to the higher electrical field [17][99]. The hot carrier luminescence emissions of interest exhibit a broad spectrum, ranging from 500 nm to 1200 nm, with a peak occurring in the 900-1100 nm range [121].

The intensity of photon emission in saturation depends on several factors, such as the substrate current of the MOSFET [17][93]. The substrate current is initially small. As the substrate current increases and reaches its maximum value during the switching time of MOSFET, the photon emission intensity also increases and can be detected more easily. Figure 2.4 illustrates the change in light intensity with respect to the substrate current from [17]. Consequently, transistors emit enough photons at the time of switching, which detectors can capture. The power supply of the circuit also has an effect on the intensity of photon emissions. As the voltage increases, the intensity of photon emissions increases as well.

Emission levels in NMOS transistors have been observed to be significantly higher than

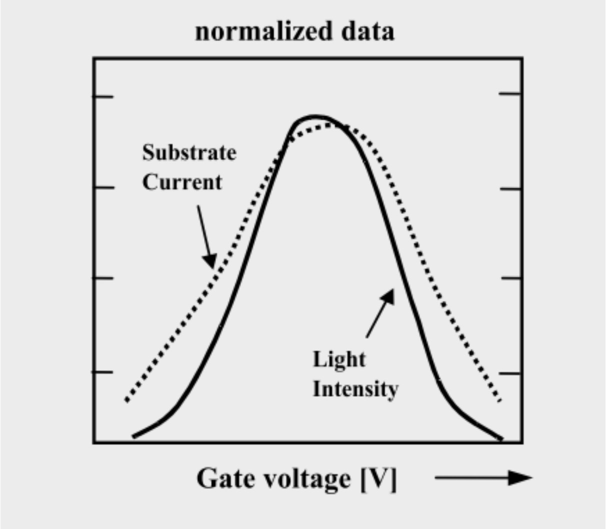


Figure 2.4: Light intensity and substrate current vs the gate voltage of a MOSFET [17].

those in PMOS transistors, primarily due to the higher mobility of electrons compared to holes [108][92][48]. As a result, it is often difficult to distinguish PMOS emissions from the background emissions generated by NMOS transistors, making detection and analysis more challenging [38]. Moreover, photon emissions in the switching state of a transistor from zero to one (0-1) are higher compared to one to zero (1-0) and, consequently, are more likely to be detected [99]. These observations suggest that the level of photon emissions depends on the operation point of the MOSFET, and it can be used as a side-channel to reveal information about circuits. Figure 2.5 shows the photon emission of an inverter at the switching time of transistors from [99].

Photon emissions in the quiescent state

In addition to hot carrier emissions in saturation, MOSFETs exhibit another form of emission known as Light Emission of Off-State Leakage Current (LEOSLC) [110]. Even when certain transistors within a circuit are off, they still undergo leakage currents, denoted as off-state leakage currents. These currents generate faint photons in the near-infrared region [77]. The intensity of photon emission depends on the leakage current. Given that the leakage current depends on the gate and drain voltages of the transistor, these emissions can reveal information about the circuit and function as a side-channel [110].

As contemporary technology reduces transistor size and threshold voltage, off-state

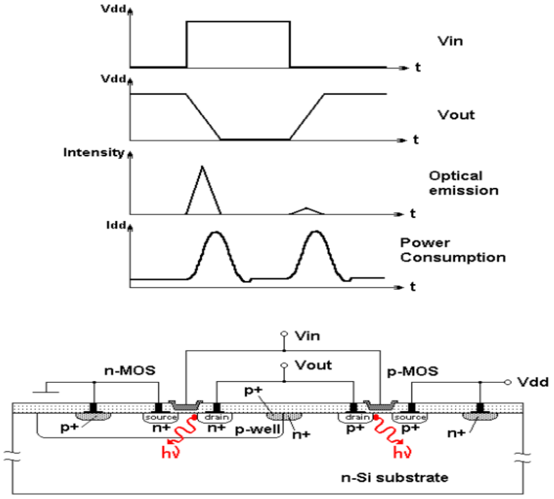


Figure 2.5: Photon emissions from a switching state of inverter and power consumption [99]

leakage currents increase, resulting in higher emission intensities [76]. From 180 nm technology, these emissions become detectable. As technology continues to scale down, the emissions intensify, reaching levels comparable to hot carriers in the saturation state [75].

LEOSLC, also referred to as quiescent state emissions, can be observed in Figure 2.6, which depicts the quiescent emissions in an inverter gate [110]. Figure 2.7 demonstrates the emissions of both the quiescent and switching states of an NMOS transistor within an inverter gate [94]. The peak value of photon emissions during the switching period is higher than that of quiescent photon emissions. Nonetheless, the integrated value of photon emissions in quiescent mode can also be substantial enough to be significant.

2.2.2 Photons Emission Transmission Line

The photons cannot pass through the packaging of the chip, so the chip must be de-packaged in the first step of detecting photon emission. In older technologies, it was possible to record photon emissions from the front side of the chip. However, with the increasing number of interconnect and metal layers in newer technologies, obtaining photon emissions from the front side has become challenging. As a result, in newer technologies, the backside of the chip is de-packaged and used for photon emission investigation [66]. In the backside of the structure, the substrate silicon serves as the only barrier for pho-

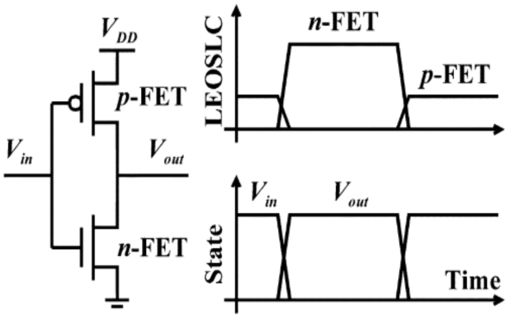


Figure 2.6: Photon emissions from a quiescent state of an inverter gate [110].

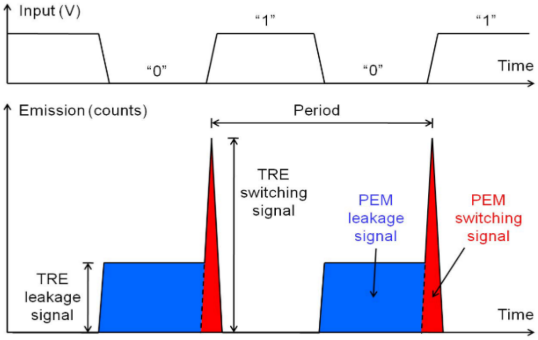


Figure 2.7: A comparison between the quiescent and switching states of an NMOS transistor within an inverter gate [94].

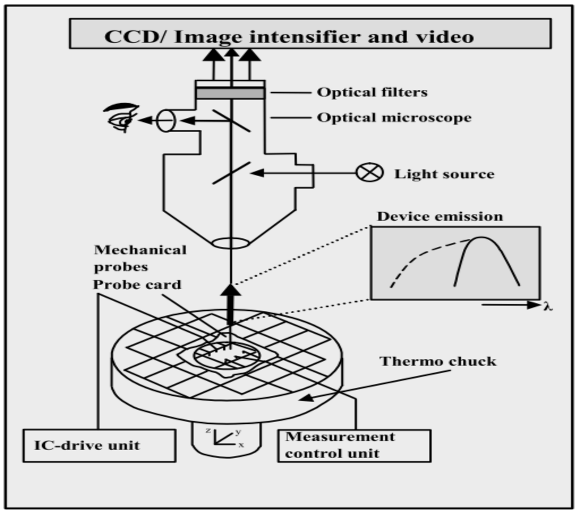


Figure 2.8: A general setup for photon emission analysis based on [17].

tons, offering no additional protection during inspection processes [84]. Furthermore, the interconnects on the front side may cast shadows on emitted photon emissions, leading to significant variability between devices. This variability is undesirable, particularly in certain applications. Thus, even when front-side access is possible, backside investigations are preferred for those specific applications [16].

However, photon emissions with wavelengths shorter than the silicon bandgap will be absorbed by the substrate; consequently, only emissions with wavelengths greater than 1100 nm can pass through the substrate [89][10]. Thinning the substrate of the chip results in less absorption of photons, and consequently, more photons can reach the chip surface [33]. The silicon substrate has no protection against active or passive photon inspection. Thus, such uncovered silicon can be an easy target for an attacker for acquiring access to the on-chip assets.

Figure 2.8 shows a basic setup of most photon emission analysis frameworks. Since the device sizes are very small, a microscope is needed to observe the photon emission of devices with nm spatial resolution. Subsequently, the photon emission should reach a camera in order to be detected [17]. This setup is considered to be a semi-invasive side channel, as it only requires de-packaging the chip but does not involve probing any contacts or making edits.

Detecting photon emissions presents numerous challenges due to various factors. Firstly, not all switching transistors emit light, and when they do, the emitted photons are often faint and insufficient in number for reliable detection [99]. To overcome this issue, the incident of interest must be repeatedly executed, and the corresponding photon emissions recorded. The final emission measurement is obtained by averaging these observations, which in turn improves the signal-to-noise ratio of the recorded image.

Secondly, photon absorption presents another challenge, as it occurs not only within the silicon substrate but also along the transmission line from the chip surface to the detectors in the camera sensor. Approximately, only 5% of the emissions reach the detectors [99]. To enhance the number of photons arriving at the sensor, employing objective lenses and optics in microscopes with higher transmission rates for the specific spectrum range of photons is recommended. Consequently, this approach can effectively reduce the loss of photons during transmission.

Lastly, not all photons reaching the camera are registered by the detectors; only a fraction of them are recorded. The probability that a detector's sensor registers a photon is called Quantum Efficiency (QE) and serves as a characterization factor for the camera [99][17]. Additionally, the detector is subject to dark current noise, which results in lower SNR images. Dark current noise generates a current that persists even in the absence of received photons from the sensor [99]. Selecting a camera with a higher QE for the targeted range of 1100 nm and reduced dark noise leads to better signal quality from photon emissions. The detectors suitable for the intended spectrum and used for photon emission analyses are made from either silicon (Si) or indium gallium arsenide (InGaAs). Silicon detectors exhibit lower dark current noise, but their QE for 1100 nm is significantly low. On the other hand, InGaAs detectors possess a high QE for the desired spectrum, albeit with increased dark current noise. MCT (Mercury Cadmium Telluride) detectors are an alternative option for certain applications, as they possess a broad spectral sensitivity extending up to 2.5 μm. This characteristic makes them highly sensitive to blackbody and heat radiation. However, MCT detectors are known to exhibit significant noise levels, limiting their use to specialized scenarios where these limitations can be managed or tolerated [16][74].

It should be noted that in newer technologies, decreasing the power supply voltage leads to a shift in the photon emission spectrum of switching transistors, pushing it further into the higher IR region [75]. As a result, for smaller transistors, such as those found in 20nm technologies, detectors covering the higher spectrum must be used to ensure improved image resolution [16]. However, new research shows that photon emission can be used for the characterization of advanced technologies such as FinFETs [12].

2.2.3 Different Optical Technique

There are several methods for recording photon emissions with detectors. In the time-integrated method, the photon emissions from each location, a pixel, are integrated over a specific period. Primarily, cameras such as Charge Coupled Devices (CCDs) are utilized for this method. While this approach provides high spatial resolution, it does not offer any information about the temporal variation in photon emission since it aggregates the photon emissions over time. The process of charging the cells in CCDs and the camera itself is time-consuming, which makes achieving a high time resolution unfeasible [16].

In the time-resolved method, vacuum tube-based systems with detectors such as Photo Multiplier Tubes (PMTs), Avalanche Photo Diodes (APDs), and Superconducting Single Photon Detectors (SSPDs) can be used. These detectors can record the intensity of photon emissions from a device with picosecond resolution in time, which is suitable for detecting delays in switching single MOSFETs. The signal provides information about photon emission in time but does not necessarily offer spatial resolution. Using Micro Channel Plates (MCP) can provide spatial resolution [99][16]. The temporal signals of photon emissions can provide valuable information on signal propagation in integrated circuits, which is important for understanding the overall functionality, performance, and potential bottlenecks within the circuit [120][113].

An alternative technique, known as Picosecond Imaging Circuit Analysis (PICA), can be employed to detect photons emitted from switching transistors [117][38][39]. PICA operates on the principle of counting the number of photons and utilizes detectors such as an array of PMTs with a resistive anode for location encoding. This configuration allows for the detection of photons with time-resolved signals in picosecond resolution as well as spatial resolution. Given that the photon emissions from a single switching transistor are quite minimal, the instruction for a specific event must be executed repeatedly. Typically, this requires the switching event to be repeated approximately 10^8 to 10^9 times. As the number of repetitions increases, SNR of the signal improves. However, recording photon emission to acquire a satisfactory signal may take an extended period, potentially lasting several hours. To synchronize the recording of each event, a trigger is necessary to signal the beginning of the event each time. The detection time of the photon is saved for every event and transmitted to a computer. Subsequently, by analyzing the histogram of the number of events at each time, the time signal can be calculated. This observation leads to the conclusion that the signal value at a particular time represents the probability of detecting a photon at that specific moment [116][120]. Initially introduced for failure analysis applications, PICA's sensor exhibited low sensitivity and quantum efficiency (QE) within the spectrum of interest, resulting in lengthy acquisition times for recording. Moreover, the high cost of PICA equipment restricts its utilization to well-funded laboratories [66].

In addition to photon emission microscopy, which analyzes emitted photon emissions from circuits without any external stimulation, there are other optical probing techniques that utilize laser scanning on the circuit and analyze the reflected light to obtain information about the operation points of devices. Some of these techniques include Electro-Optical Frequency Mapping (EOFM), Electro-Optical Probing (EOP), Laser-Voltage Probing (LVP) or Imaging (LVI), and Laser Logic State Imaging (LLSI) [69][41][68][40]. Initially used for debugging circuits and failure analyses, these techniques have recently been applied to security applications as well [18][105][129].

For instance, in EOP and EOFM, a laser beam in the Near-InfraRed (NIR) range is directed at the backside of the device. The amplitude and phase of the reflected light from the laser beam are modulated based on the operation point of the switching time in the transistor. This reflected light is recorded by a detector and sent for analysis. In EOFM, the recorded image is sent to a spectrum analyzer for frequency domain analysis, which provides an activity map of active circuits. On the other hand, in EOP, the recorded image is sent to an oscilloscope and analyzed in the time domain. LVP/LVI employs a different laser beam source compared to EOFM/EOP. In LLSI, the technique is similar to EOFM, with the exception that the supply voltage is modulated to a fixed frequency [14][18].

2.3 SRAM Layout

SRAMs are critical components in microprocessor architectures, commonly used as cache memory in systems due to their speed, affordability, and low power dissipation. SRAM memory retains data until power is disconnected [125]. In embedded devices, SRAM blocks often store crucial information, such as cryptographic keys or AES S-box tables. Accessing the content of these SRAM blocks could expose sensitive data and compromise the security and integrity of the entire system.

This research aims to investigate the photon emissions of SRAM in order to reveal its contents. Several studies have focused on capturing the photon emissions of SRAMs, using the acquired images to either identify the location of SRAMs or expose their contents [66][111]. Such information can be employed for various applications, including security and chip debugging [111]. To effectively examine the photon emission of SRAM, it is essential to have a foundational understanding of its circuit architecture.

The standard architecture of a SRAM cell, which is widely used in Very-large-Scale Integration (VLSI) circuits, consists of six-transistor (6T) cells. Figure 2.9 illustrates the

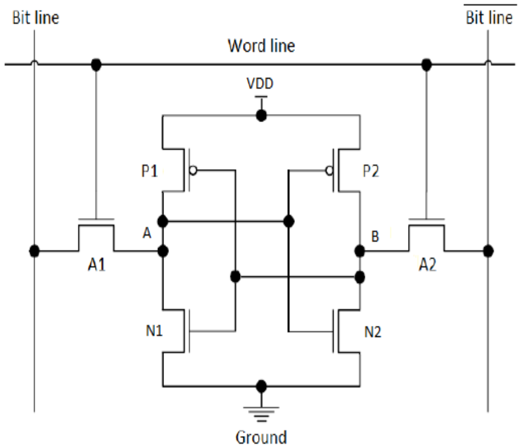


Figure 2.9: Standard architecture of 6T cell of SRAM [9].

circuitry of a 6T cell. The cell is composed of two cross-coupled inverters, which function as feedback and maintain the cell's state, as well as two pass transistors A1 and A2 that connect the cell to Bitline and BitlineN during read/write operations [80].

A SRAM cell operates in three states: idle, read, and write. In the idle state, the cell's word line is deactivated, and the two cross-coupled inverters serve as each other's feedback, holding the values in A and B steady without the need for refreshing. In the read state, the cell's Wordline is activated, and the cell's internal value drives the bit lines. However, changing the Bitline value is slow due to the line's large capacitance, resulting in a slow reading speed. To address this issue and increase operational speed, sense amplifiers are employed during the reading process. These differential amplifiers detect small differences in Bitline and BitlineN and amplify them to full swing. The cells must be strong enough to drive the Bitline during read operations, while ensuring that the Bitline value does not alter the cell values (read stability). In the write state, writing driver circuitry controls the Bitline and BitlineN states, followed by the activation of the corresponding cell's Wordline. The Bitline alters the cell values to new ones. The design must ensure writability, meaning that the Bitlines should be capable of overpowering the cell to update its states [80][125].

A large number of SRAM cells are required in microprocessors, and it is impractical to have each SRAM byte in a single row. Consequently, cells are typically divided into both rows and columns. Row and column decoders select the desired cell. Figure 2.10 displays a portion of SRAM, including a common decoder, sense amplifiers and write drivers.

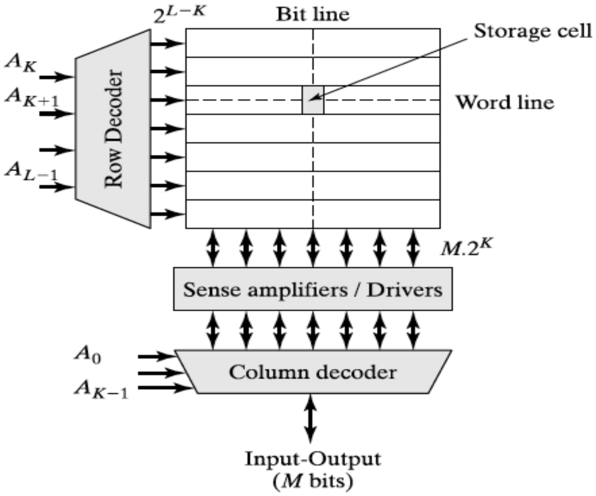


Figure 2.10: Part of SRAM with peripheral circuits [80].

Different placements in the layout of cells lead to variations in specifications such as speed and area. Designers select a specific layout based on the target application. Figure 2.11 displays different layouts of common SRAM cells [9]. Additionally, Figure 2.12 illustrates the layouts of a 4x4 SRAM in some of the most popular configurations. It can be observed that the cells are arranged to share I/O components. These varying layouts result in different photon emissions, primarily due to the distinct transistor locations. Gaining familiarity with these layouts is advantageous when studying photon emission in the SRAM block.

2.4 Image Processing Methods

In this section, various image processing techniques that will be utilized in the subsequent chapters are introduced. These techniques play an important role in the analysis and interpretation of the data obtained during the course of this research.

2.4.1 Mean Squared Error

The Mean Squared Error (MSE) is a widely used metric in image processing that quantifies the difference between two images [34]. It serves as a measure of noise or dissimilarity

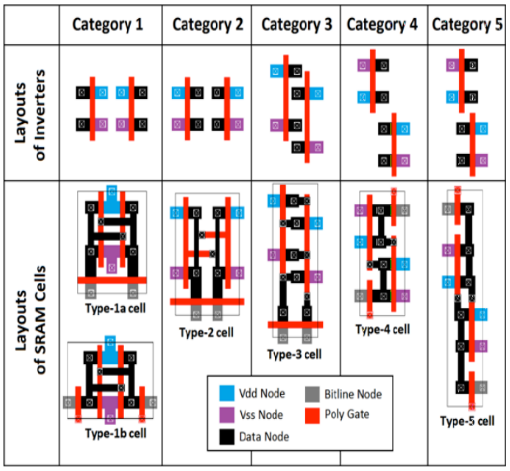


Figure 2.11: Different layouts of common SRAM cells [9].

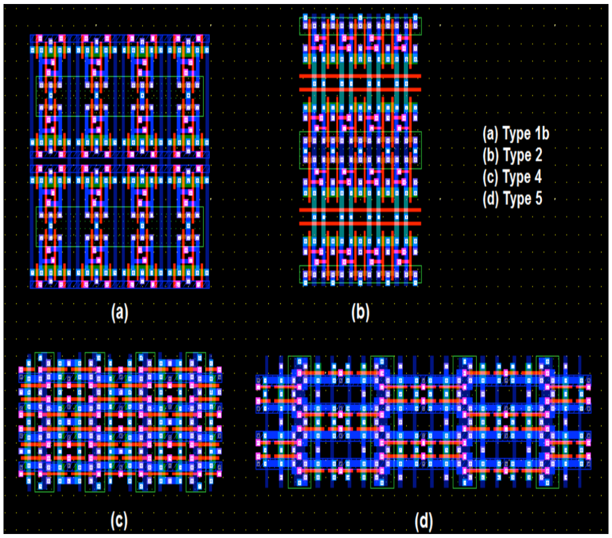


Figure 2.12: Layout of 16B SRAM for some popular typologies [9].

between the images under comparison.

MSE is calculated using equation 2.1, in which R_{xy} represents the reference image and A_{xy} denotes the image being compared against the reference image to determine their dissimilarity. R(x, y) and A(x, y) correspond to the pixel values at position (x, y) in images R_{xy} and A_{xy}, respectively, while M and N represent the dimensions of the images along the x and y axes.

$$MSE(R, A) = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (R(x, y) - A(x, y))^2 \tag{2.1}$$

The differences between the corresponding pixel values of the images, referred to as the error, are calculated. Subsequently, the mean square of the error for all pixels is computed as the MSE. According to the equation, when the intensity of corresponding pixels in both images is identical, the error or noise associated with that pixel is zero for both images. Thus, in the case of two identical images, the error for all pixels is zero, resulting in the minimum MSE value of zero. Therefore, a lower MSE value signifies a smaller difference between the images, indicating that they are more similar. Conversely, a higher MSE value suggests that the difference between corresponding pixels is more significant, which implies greater dissimilarity between the images.

While MSE is widely used in many applications, it has some limitations. The metric relies solely on the difference between individual pixels and does not take into account the structure and overall features of the images. As a result, MSE may not fully capture the perceived similarity between images, as it neglects important aspects of visual quality and similarity.

2.4.2 Structural Similarity Index Measure

The Structural Similarity Index Measure (SSIM) is another method used in image processing to measure the similarity between two images. Unlike the previously mentioned MSE, SSIM does not only rely on pairwise pixel values. Instead, it considers the changes in luminance, contrast, and structural information of the two images, allowing it to better measure their similarity in structure compared to MSE [122].

To calculate SSIM, a window of odd size slides over both images. At each step, the SSIM metric is computed between the corresponding windows of the two images. The final SSIM value is the average of all SSIM values obtained from the sliding window.

The SSIM metric is calculated using equation 2.2:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{2.2}$$

Where x and y represent the two window images derived from the two images being compared, μ_x and μ_y are the mean pixel values of images x and y, σ_x^2 and σ_y^2 are the variances of images x and y, σ_{xy} is the covariance of images x and y, and c_1 and c_2 are constant values to avoid division by zero.

The SSIM value can range from -1 to 1. Images with higher similarity have higher SSIM values; thus, for two identical images, the SSIM value is 1. This method provides a more comprehensive assessment of image similarity than relying on pairwise pixel comparisons alone.

2.4.3 Cross-Correlation

Cross-correlation is a mathematical method widely used in signal and image processing [34]. It can be utilized to evaluate the similarity between two signals as a function of a lag, which is applied to one of them, either in time or space. The cross-correlation between two continuous signals $f(t)$ and $g(t)$ is calculated using equation 2.3:

$$C(\tau) = \int_{-\infty}^{\infty} f(t)g(t+\tau)dt \tag{2.3}$$

Where one of the signals, $g(t)$, is shifted over the other signal, $f(t)$, for different lag values τ. For each value of τ, the correlation between the two functions is calculated for the overlapping region of functions. Since the correlation coefficient calculates the similarity between two signals, the maximum value of the cross-correlation for different lag values indicates the time at which the two signals have maximum similarity. Therefore, cross-correlation can also be employed to detect repeating patterns or find the time or spatial shift between two similar signals. The value of τ associated with the maximum value of cross-correlation indicates the shift value between the signals.

Cross-correlation can also be applied to images for the same applications. The equation for 2D discrete signals, specifically two images with spatial shift, is given by 2.4. In this equation, R_{xy} and A_{xy} represent the two images. The values of d_1 and d_2 indicate the spatial shift in both the x and y directions of A_{xy}, which are in the range of [0,2M-1] and [0,2N-1], respectively, where $M * N$ is the size of the images.

$$C(d_1, d_2) = \sum_{x=1}^{2M-1} \sum_{y=1}^{2N-1} (R(x, y)A(x + d_1, y + d_2)) \tag{2.4}$$

2.5 Research with Photon Emissions in Security

Photon emission microscopy has been utilized for an extended period for failure analysis in electronic devices [112][103]. However, in the last decade, it has garnered attention for its applicability in security applications and its ability to reveal information about devices through side channels. This section reviews various studies that utilize photon emission side channels for security attacks. The analysis underscores the rising significance of this approach in detecting vulnerabilities and securing sensitive data in electronic systems.

Ferrigno et al. [33] pioneered the use of photon emissions as a side-channel in 2008. In their study, they focused on the backside photon emissions from an outdated 0.8 μm thinned PIC16F84A microcontroller. To capture these emissions, they employed a machine called Optica, which was based on the PICA technique. The researchers recorded the photon emissions of switching transistors during the execution of an XOR instruction on the microcontroller and attempted to recover the result of the instruction. To do this, they used a constant number as a key, which was XOR with a state value stored in an SRAM. The outcome was then stored in the SRAM. By gathering photon emissions for each clock cycle and comparing them to the code, they successfully recovered the result of XOR from photon emissions. Due to the low quantum efficiency of the detector, the photon emissions of the chip were recorded for an extended period of 12 hours, ensuring sufficient photon emissions were detected. To achieve this, the desired code was executed continuously in a loop. A trigger pulse was sent to the detectors at the end of each loop to synchronize the code and PICA for the start of each iteration. To improve photon emission measurements, the working voltage and frequency of the chip were set higher than standard. This groundbreaking work laid the foundation for future research in photon emission side-channel attacks.

In the paper by Ferrigno et al. [33], the experiments conducted utilized the costly PICA method and special sample preparation with ASAP [1], requiring an extended recording time of 12 hours. Skorobogatov [99] proposed a more affordable approach to recover data from memory blocks in a microcontroller. The author initially compared the specifications of various camera sensors and ultimately selected four cost-effective cameras with PMT, APD, and CCD sensors capable of capturing photon emissions. PMT and APD cameras were considerably more expensive than CCD cameras; however, they possessed time-resolved capabilities, while CCD cameras relied on photon emission collection during exposure time. Skorobogatov [99] used a 0.9 μm PIC16F628 microcontroller for the test, operating it at a higher than standard power supply but still within the working range. The chip was de-packaged for front-side observation, and simple instructions typically found in secure microcontrollers were executed in a continuous loop. The PMT camera required one hour of acquisition to obtain photon emissions due to its high dark noise and low sensitivity in the NIR region. Photon emission signals collected from the PMT were compared with power traces, revealing a strong correlation between the two during clock signal transitions, where both exhibited peaks. In contrast, APD sensors could not achieve satisfactory signals even after two hours of acquisition, despite their higher cost compared to PMT sensors. The CCD camera, however, successfully captured quality photon emission from the die within 30 minutes of exposure time. Subsequently, Skorobogatov [99] attempted to extract memory block data using the CCD camera. Instructions related to reading EEPROM contents were executed in a continuous loop, and photon emissions were recorded for a 5-minute exposure time. The data in the EEPROM was easily recoverable, and the same process was applied to the XOR of two values and reading and writing of SRAM. The author managed to recover data from the collected photon emissions of switching transistors. Although the photon emissions from the SRAM memory cell were not visible, emissions from address decoders and bus drivers could be utilized. To assess backside photon emissions, de-packaging was performed for a photon emission test. However, achieving the same signal-to-noise ratio for backside images as front-side images necessitated a tenfold longer exposure time. Additionally, more sensitive objectives and optical sensors for wavelengths greater than 1100 nm were required. The paper also examined photon emissions from a 0.5 μm microcontroller, which demonstrated an order of three less intensity from the front side due to the increased presence of metals.

The paper by Di et al. [29] explores the application of failure analysis techniques for recording time-resolved photon emissions from an FPGA executing a portion of the Data Encryption Standard (DES) cipher algorithm. By applying differential analysis to the collected signals, the authors demonstrated the feasibility of revealing a related subkey. The study investigates the potential of using traditional failure analysis methods in cryptographic applications and highlights the security risks that may arise when such techniques are applied to sensitive components in cryptographic devices, such as microcontrollers and secure memory. The authors used an Actel Proasic3 A3PE600 FPGA in flash technology with $0.13\mu m$ technology, de-packaging the backside for investigation. The attack focused on the first SBOX operation of the DES algorithm in the first iteration executed within the FPGA chip. In this implementation of the DES algorithm, the input should initially be set to a zero value and subsequently changed to a new value as the encryption process progresses. The paper analyzed the photon emissions of the device recorded with a PICA system, utilizing the Time Resolved Emission (TRE) technique and the expensive Hamamatsu Tri-PHEMOS, which had been previously used in failure analyses [35][43]. The study recorded 64 plots for different input plaintexts, displaying the number of photons as a function of time. The plots showed variations based on the input, prompting the authors to apply differential analysis on the plots concerning the chosen bit at the SBOX output. The results indicated that the differential attack was successful for only one bit. However, the authors demonstrated the possibility of finding a subkey by using the time-resolved plots of all bits. Furthermore, the paper employed a laser stimulation technique in failure analysis to induce a current flow. By leveraging laser stimulation, the authors improved the effectiveness of power consumption side-channel attacks.

Nedospasov et al [66] developed an automated methodology for functional analysis of an AVR chip, enabling a more efficient identification of different functional blocks within the chip. The method involved writing several hundred subroutine codes on the chip, with each experiment executing some distinct subroutines. The photon emissions during chip execution were captured using a silicon-based charge-coupled device (Si-CCD). By analyzing the differences in these photon emission patterns, the locations of various functional elements within the chip could be revealed. The backside of an Atmel ATMega328p chip with a substrate thickness of 50 μm was used as the device under test. By examining the photon emission patterns, the authors successfully identified the locations of various functional elements within the chip, including SRAM addresses, bit layout within each byte, the Z status flag and specific areas of execution logic responsible for fetching opcodes from program memory. The ability to determine the locations of functional elements within the chip can significantly reduce the need for exhaustive search during fault injection-based security attacks, thus simplifying the process and increasing the efficiency of these attacks.

Schlosser et al. [88] employed spatial and temporal traces of photon emissions from row access in SRAM during the Substitution-box (SBOX) operation. Utilizing Simple Photonic Emission Analysis (SPEA), the researchers successfully recovered the AES key. They conducted experiments on two microcontroller models, the AVR ATMega328P and the AVR XMega128A1. The chips were decapsulated from the backside, and the substrate was thinned to enhance SNR of photon emissions. Two detectors were used to capture photon emissions, obtaining both spatial and temporal photon emission tracks. The Silicon Charge-Coupled Device (Si-CCD) camera provided information about spatial photon emissions, while the secondary detector, an Indium Gallium Arsenide/Indium Phosphide Avalanche Photo Diode (InGaAs/InP APD), was employed for temporal measurements. The research focused on computing only the first AddRoundKey and SubBytes operation for the initial iteration of AES. To locate the row addresses in SRAM, row drivers, and the SBOX element contained within the SRAM, the authors initially recorded photon emissions using the same techniques described in [66]. Utilizing the spatial information obtained from the Si-CCD camera, the InGaAs/InP APD detector was employed to record the temporal photon emission measurements of row drivers for a specific row related to some of the SBOX elements. The 256 time-resolved traces of the specific row driver for all 256 available plaintext values were recorded, allowing researchers to monitor the row access time for all traces. Based on the plaintext values that reached the box numbers in that row, the number of key candidates sets decreased, and they were ultimately able to recover the key for the first iteration. It is noteworthy that the recording time for each trace varied between the microcontrollers: 90 seconds for the ATMega328P and over two hours for the XMega128A1.

The same methodology and setup employed in a previous study [88] were adapted to utilize Differential Photonic Emission Analysis (DPEA) in [51] for recovering the AES key. The investigation focused on the temporal switching photon emissions of driving inverters in the ATmega328 during the execution of the first AddRoundKey and SubBytes operation of the initial round. Temporal photon emissions of driving inverters were recorded for 256 different plaintext inputs, and DPEA was subsequently applied to the data. For the statistical analysis of DPEA on the first byte, both the Difference of Means and Pearson correlation coefficient were utilized. Using Pearson correlation analysis, the key could not be directly distinguished; however, they were able to recover a single bit of the Sbox and reduce the set of possible keys to a range where brute force became applicable. Ultimately, this approach led to the discovery of the AES key. However, employing the Difference of Means analysis enabled the direct identification of the key.

In [36], the photon emission of SRAM was investigated to gather information about SRAM characterization and to use this information for launching an edit using FIB on the SRAM PUF. The authors successfully created a physical clone of the SRAM PUF implementation. To record the SRAM photon emissions, the high-end Hamamatsu Phemos was employed on a backside-thinned Atmel ATmega328P chip. The chip was thinned to 20 μm for improved signal quality, and the photon emission was recorded with a 300-second integration time.

Researchers predominantly investigate the photon emission of microcontrollers; however, Tajik et al. [115] have explored emission analysis of a Complex Programmable Logic Device (CPLD). They identify the emission fingerprint of each primitive and locate basic logic primitives for hardware implementations. A Max V CPLD was depackaged from the backside and thinned to approximately 30 μm using a specialized Ultratec ASAP-1 polishing machine. The photon emission was recorded with time integration ranging between 20 to 120 seconds, utilizing a Hamamatsu PHEMOS 1000.

In their research, Stellari et al. [111] investigated the photon emissions from a 64 MB SRAM test chip using 14 nm SOI technology. They employed both time-integrated and time-resolved methods to study SRAM functionality and reveal memory content. By recording photon emissions from various memory cells using an InGaAs camera over a 5-minute period, the authors observed dominant photon emissions from activated rows and identified the location of the Wordline driver. Additionally, they utilized a 2D imaging PICA camera to record time-resolved emissions of SRAM during read operations. This data provided insight into the sequence of events during a read operation. To monitor changes in SRAM content, Stellari et al. studied photon emissions from SRAM in both read and quiescent states for the first time. To capture quiescent-state emissions, the SRAM was filled with all ones, and a 10-minute recording was taken without activating any Wordlines. They then changed the first row and a middle position within the SRAM to zeros, and recorded photon emissions using the same procedure. Although the researchers could partially detect changes using differential analysis, they were unable to pinpoint the exact locations, and the content of SRAM remained hidden. However, when they repeated the process by capturing emissions during a read operation, where a Wordline was activated, the images showed an improved signal-to-noise ratio. The difference image revealed the exact location of changes, and by comparing the brightness of SRAM locations with a reference image and knowing the content of the read row, the authors successfully determined the changing content of the SRAM.

Couch et al. [25] investigated the idle state photon emission of SRAM cells within a 220 nm process FPGA. The chip was decapsulated from the backside and thinned to 30 μm using an Ultratec ASAP-1 machine. A low-cost setup consisting of two InGaAs cameras and a Silicon CCD camera was employed to examine the BRAM photon emission. The InGaAs cameras were utilized to investigate through the chip and locate the BRAM block, while the CCD camera was responsible for recording photon emissions. Photon emissions from the BRAM were recorded for several minutes while continually reading from the SRAM. To capture the photon emissions of the SRAM in its idle state, the integration time was set to 8 hours, resulting in a lower SNR. The paper compares the photon emissions obtained using both methods.

Faraj et al. [32] introduced a low-cost setup to investigate quiescent photon emissions of SRAM memory blocks in embedded systems. To facilitate this, the clock was frozen during the recording of the quiescent photon emission. The photon emissions of two embedded devices were investigated with a brief 0.5-second integration time. For the PIC16F687, an overvoltage was utilized, which revealed the SRAM value. However, the voltage for the ARM Cortex-M0 was increased, yet remained within the operating range. The photon emissions of SRAM were observed, and through differential analysis, the data dependency of quiescent photon emissions were detected.

Photon emission techniques boast a wide range of applications beyond security. For example, they have been employed to detect hardware trojans and identify malicious alterations in circuits [104][130], as well as to locate defects in integrated circuits [19]. Furthermore, recent studies have demonstrated the effectiveness of photon emission for characterizing and debugging modern designs such as ReRAMs [109] and other cutting-edge technologies [119]. These advancements highlight the versatility and potential of photon emission techniques in addressing diverse challenges in the field of electronics.

Several research studies have utilized various probing techniques to reveal the contents of registers or memories for security applications [53][55][114][42][23]. For instance, Rahman et al. [83] employed Electro-Optical Frequency Mapping (EOFM) probing to uncover the register values of a 28 nm locked flash-based FPGA using a PHEMOS-1000 machine. They successfully retrieved the obfuscation keys stored in a register, effectively unlocking the circuit.

Researchers [49] employed optic probing technique of LLSI to obtain a snapshot of a hardware state within a single clock cycle, revealing the logical state of registers. The device under test was an Intel Cyclone IV FPGA, a 60 nm technology, which was decapsulated from the backside and thinned to $25\mu m$. The Hamamatsu PHEMOS-1000 device was used for this investigation. By employing these techniques, they were able to capture snapshots of the target register with the key stored in it. Although the content could be recognized manually and visually, they utilized image processing techniques such as filtering and cross-correlations to automate the process of revealing register content. The known location of a register cell was cut and compared with known snapshots of register cells for values 0 and 1 with the aid of cross-correlation. In the process of obtaining register snapshots, it is essential that the content is not altered, either by freezing the clock or by not changing the register values.

2.6 Summary

This chapter provides the background information necessary for investigating photon emissions as a side channel and reviews previous research in this area. Photon emission is a crucial side channel attacks, which can potentially compromise the security of embedded devices and reveal sensitive information.

Table 2.1 and 2.2 present a summary of the research mentioned in this field. Many of pertinent studies have employed high-end equipment for preparing the device under test and recording photon emissions [36][115], including tools like PHEMOS [43] and ASAP-1 [1]. There's a notable gap in comprehension when it comes to low-cost setups and the photon emissions captured using these alternatives [32][99]. Exploring photon emissions recorded from low-cost setups could provide more insight into the strength of this side channel and make this type of analysis more accessible to a wider range of researchers.

Additionally, most research has focused on switching photon emissions [36][115][51][88], with limited work on exploring quiescent photon emissions in embedded devices [32][25]. Recording switching photon emissions requires the execution of the target instruction many times, a feature that may not be feasible for many applications. This highlights the potential benefits of investigating quiescent photon emissions, which could offer new insights and attack vectors. Investigating quiescent photon emission of SRAMs, which are essential components in embedded devices, using a low-cost setup and assessing its potential for launching powerful attacks can address some of these gaps.

The resulting images of photon emissions require specific post-processing techniques that are not well-addressed in the literature [81]. Developing and refining these techniques could improve the effectiveness of photon emission analysis in revealing sensitive information. Furthermore, no research has been conducted on the photon emissions of embedded devices on RISC-V chips so far. Investigating this emerging platform could provide valuable insights into its potential vulnerabilities and contribute to the development of more secure devices. This research aims to address these gaps by exploring low-cost setups as employed in [32], investigating quiescent photon emissions, refining post-processing techniques, and examining a RISC-V chip. In the following chapter, the methodology and experimental setup employed to achieve the research objectives will be illustrated.

‘

Table 2.1: A summary of selected research studies on embedded security using PEM

Research paper	DUT	Switching or Quiescent	Method of recording	Location	Special note
Ferrigno [33]	0.8 μm PIC16F84 A	Switching	Time Resolved using Optical	SRAM, possibly sense amplifier	12 hour of recording
Skorobogatov [99]	0.9μm PIC16F628	Switching	both Time resolve and integration	EEPROM and SRAM value from detector, drivers	Use APD, PMT, CCD sensors
Di [29]	0.130 μm Actel ProAsic A3PE600 FPGA	Switching	Time resolve -Use PHEMOS and laser stimulation	The implemented area for cipher algorithm	applied Differential analyze on special implemented DES
Nedospasov [66]	0.38 μm ATmega328p	Switching	Time integration with Si-CCD	different functional blocks	Analyze difference in PEM
Schlosser [88]	0.35 μm ATmega328p	Switching	Time resolve with InGaAs/InP APD and integration with Si-CCD	Memory row drivers of SRAM	Use SPEA on AES with temporal signal
Kramer [51]	0.35μm ATmega328p	Switching	Time resolve with InGaAs/InP APD and integration with Si-CCD	Driving inverters of SRAM	Use DPEA on AES with temporal signal

Table 2.2: Continuous summary of selected research studies on embedded security using PEM

Research paper	DUT	Switching or Quiescent	Method of recording	Location	Special note
Helfmeier [36]	0.38 μm ATmega328P	Switching	integration time- Use PHEMOS	SRAM PUF	Use FIB
Tajik[115]	Altera Max V CPLD	Switching	Integration time- Use PHEMOS	basic logic primitives	identify the emission fingerprint of different block
Stellari [111]	14 nm SRAM test chip	both Switching and Quiescent	both time-integrated with InGaAs camera and time-resolved with PICA	SRAM block	locate the change in SRAM content in Switching mode
Couch [25]	0.22 μm FPGA	both Switching and Quiescent	Time integration with Si-CCD	BRAM storage	8 hour of recording
Faraj [32]	0.45 μm PIC16F687	Quiescent	Time integration with InGaAs camera	SRAM storage	Use a low-cost setup
This work [30]	0.45 μm PIC16F687 and 0.18 μm FE310-G002	both Switching and Quiescent	Time integration with InGaAs camera	SRAM storage	Use DPEA,CPEA and image processing to reveal the content using the [32] setup.

Chapter 3

Methodology and Setup

This chapter provides a detailed description of the research methodology. It begins by outlining the research objectives and continues with the approach taken to fulfill these objectives. Following this, the chapter details the experimental setup and the necessary equipment for conducting a cost-effective experiment. It goes on to elaborate on the specifications of the device selected for the experiments and introduces the terminology that will be used throughout this dissertation. The chapter concludes by summarizing the key points discussed.

3.1 Methodologies

The main objective of this work is to investigate the photon emission of data memories in chips in a low-cost setup and explore the information that could leak from them, as well as their impacts on security. One of the targets of the study is to determine whether the photon emissions of SRAM contents can be used in a low-cost attack where visual inspection of the emissions cannot reveal the data value stored at a particular address in the SRAM. In certain embedded processors with advanced technologies, the objectives may not offer sufficient zoom to identify emissions from individual transistors, or the objectives with higher zoom may need to be placed too close to the device's backside surface, making it impossible to focus.

The SRAM rows may typically contain photon emissions of n-words interleaved in both horizontal and vertical directions. If an attacker can acquire a quiescent photon emission image of the SRAM during clock cycles, they may be able to launch a Simple Photon Emission Attack (SPEA), Differential Photon Emission Attack (DPEA) or correlation Photon

Emission Attack (CPEA) on AES. Additionally, if the attacker can characterize the photon emission of the data memory, they may be able to directly determine the contents of an arbitrary address that was recently written to in the SRAM.

To investigate the aforementioned objectives, a DUT was selected, which was the PIC16F687 microcontroller. The whole SRAM content of this device emits photons during overvoltage, and its quiescent photon emissions can also be captured. This feature of the device makes it useful for investigating the possible attacks discussed earlier. The initial phase of the investigation involved capturing the quiescent photon emissions of the SRAM for different values. Subsequently, image processing techniques were utilized to identify and extract the SRAM block area. Various methods were then evaluated for accurately aligning the SRAM block images. In the final stage, the aligned photon emissions within the SRAM block were exploited to execute SPEA, DPEA, CPEA, or to apply image processing techniques to discern a 0 or 1 bit value.

In the subsequent step, the FE310-G00 chip was selected as the next device under test to investigate the photon emission of the data memory of a chip with the RISC-V standard Instruction Set Architecture (ISA) for the first time. The photon emissions of the memory block, as well as its row and column detectors, were studied. Additionally, the photon emission of the targeted row in the SRAM was examined to determine if the attacks on the PIC device were also applicable to the RISC-V chip.

The focus of this work was on investigating the photon emission of memory blocks in two different devices using different zoom levels. Low zoom photon emissions were used for cases where visual inspection was not possible, while high zoom was used to obtain more detailed information about the photon emission of the memory block and to confirm the findings from the low zoom level. Moreover, different image processing algorithms were applied to test the applicability of their use in memory readout analysis and show their effectiveness.

In the following section, the experimental setup needed for recording photon emission and the equipment will be discussed, followed by a discussion on the specifications of two devices under test and the boards needed for their work.

3.2 Experiment Setup

Our in-house experimental setup [32] of the equipment and their connections for photon emission microscopy is presented in Figure 3.1. Initially, the DUT must be prepared so that its photon emissions can be accessed. Subsequently, the DUT is placed under a microscope,

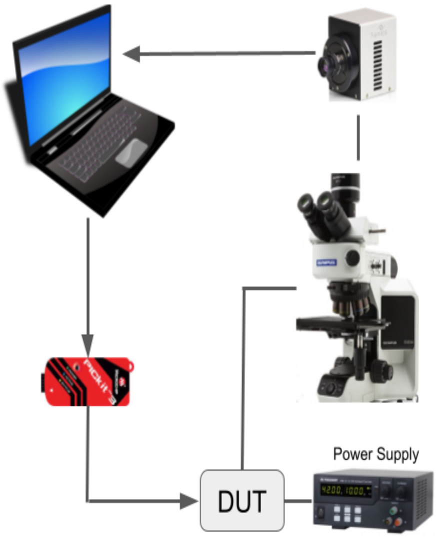


Figure 3.1: Experimental Setup for Recording photon emission.

which is used to magnify and capture photon emissions. A digital camera is mounted on a specific microscope to record the photon emissions, and the camera sends the captured images live to a computer for further analysis and processing. Additionally, the DUT must be connected to a power supply to gradually change the voltage and observe the changes in photon emissions. To modify the program within the DUT and examine the variations in photon emission with different programs, the chip must be connected to a computer, and new code needs to be uploaded to it.

This section provides a more detailed account of the experimental equipment used in the study. It also elaborates on the limitations and problems encountered while working with the equipment. The subsection includes information about the microscope, camera, and preparation equipment used for backside IC processing.

3.2.1 Microscope

The microscope plays a crucial role in photon emission microscopy experiments by magnifying and transmitting the photon emission for the digital camera. Hence, it is essential to have a microscope with excellent transmission and performance in the peak region of photon emissions, which is typically around 1100 nm.

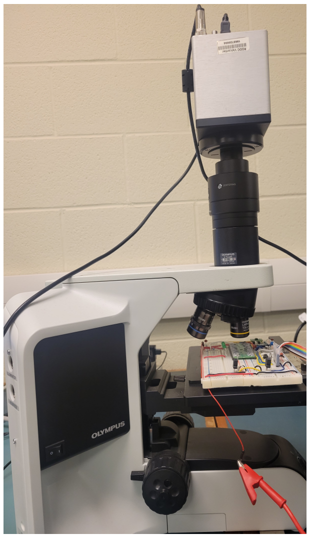


Figure 3.2: Olympus microscope and XEVA camera setup for Photon Emission Microscopy.

The light BX3M [70] series microscope from Olympus was chosen due to its superior transmission performance for IR wavelengths. An image of the microscope with a camera mounted on it can be seen in Figure 3.2. However, it is important to note that this microscope is not motorized, and the focus and settings need to be adjusted manually. Additionally, the microscope has a nosepiece that can provide up to five different objectives, allowing for flexibility in magnification.

In addition to the microscope itself, the objectives and other optical elements in the path of photon emission also have an effect on the transmission rate. Two Olympus lenses are utilized in our experiments: one with 10x magnification and another with 50x magnification. These lenses are IR-optimized and specifically designed for inspecting internal structures in silicon wafers [71]. The lenses have optimal transmission in the infrared region of 700-1300 nm wavelengths. transmission rate of the microscope in the 1100 nm is 82% with the 10x lens and 76% for the 50x lens. To connect the objectives to the eyepiece or camera, a tube is required. In the experiments, a U-TLUIR tube is utilized that has a 95% transmission at 1100 nm and is specific for IR observation [32][71].

As demonstrated in the work by Wegerhoff et al. [124], the refractive index of different wavelengths is not the same. This phenomenon results in a blue sky. However, in lenses and imaging, this characteristic is undesired because it causes different wavelengths to focus on different points, leading to chromatic aberration. Chromatic aberration causes color fringing at edges and blurriness, resulting in different focal points [124]. Figure

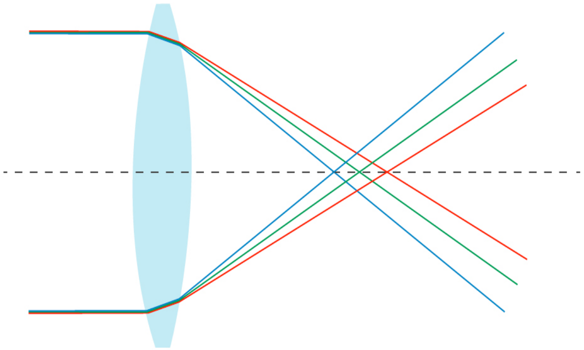


Figure 3.3: Chromatic aberration in a lens [13].

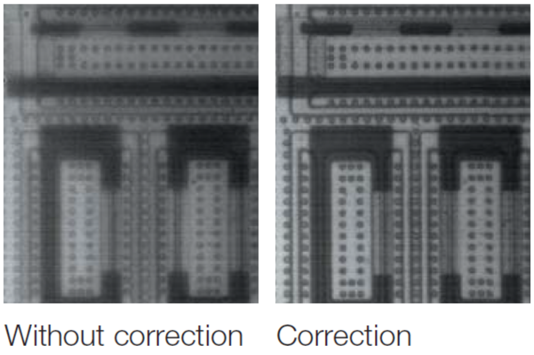


Figure 3.4: An image exhibiting chromatic aberration alongside its correction using IR objectives [71].

3.3 demonstrates this phenomenon in lenses with different wavelengths. Plan Achromatic lenses are used to address chromatic aberration, which can correct a long range of visible light through the InfraRed and produce an image without color fringing. Figure 3.4 shows an image with chromatic aberration and its correction [71].

For photon emission microscopy, no light is required to observe photon emission. This is because the faint photon emissions are captured, and illumination can hinder the detection of photons. Therefore, the microscope used in the experiments does not have a built-in light source. However, before conducting the investigation on the chip, it's crucial to first identify the structure and the location of different blocks within it. This can be accomplished by illuminating the chip and capturing images of its various locations. For this purpose, a light source that can penetrate through the silicon and sketch the structure

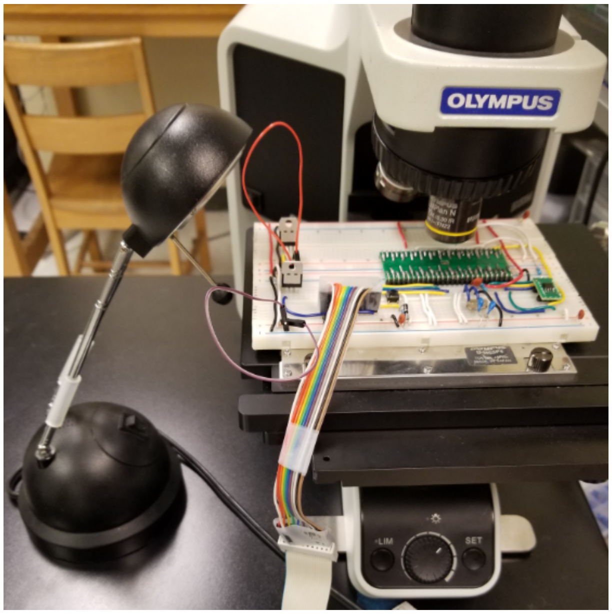


Figure 3.5: Illumination of the microscope with a halogen lamp.

of the device is required. Since silicon is transparent for wavelengths equal to or larger than 1100 nm, a light source within this range can be used. A halogen light is an excellent choice for this task, as it emits light in the IR region, which is suitable for this purpose. By illuminating the chip with this light, the different locations and their corresponding structures can be recorded, which is vital for subsequent analyses. Figure 3.5 showcases the halogen lamp used to illuminate and image the structure of the wafer.

One of the challenges associated with microscopes is the potential for spatial shifts during the acquisition of a large sequence of images. This shift is negligible in a small sequence but becomes more significant with increasing acquisition time. Consequently, these shifts can result in misalignment of the photon emissions, making it difficult to analyze some images accurately. This is a common problem in time-lapse microscopy and has been reported in other studies that utilized sequential microscope images. The drift is believed to occur due to fluctuations in the axial position of the microscope focal plane, which can be caused by temperature variation, gravity, or vibration [2]. Moreover, this particular microscope does not have a clip or a fixing mechanism to hold the DUT securely in place under the lens. This can make it difficult to prevent any movement or displacement, especially when the programmer for the chip is being connected or disconnected to flash new code. To address these issues, various alignment algorithms are used to make the

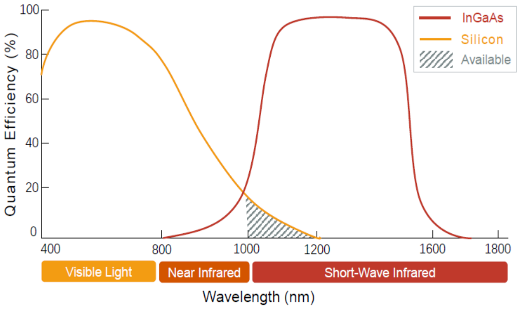


Figure 3.6: Comparison of quantum efficiency in Si and InGaAs camera [56].

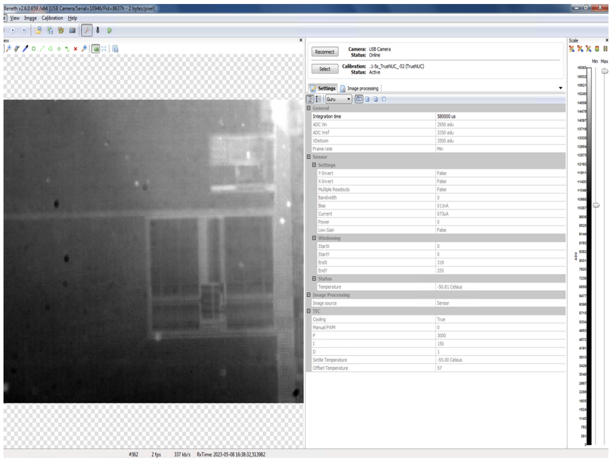
images more aligned. These algorithms will be discussed in more detail in the next chapter 4.

3.2.2 Camera

The camera utilized for detecting and recording photon emissions should exhibit high quantum efficiency at the desired wavelength of 1100 nm. Two potential detector options for this application are InGaAs and Si cameras. InGaAs cameras are more appropriate due to their superior quantum efficiency in the interested area compared to Si cameras. Figure 3.6 provides a comparison of quantum efficiency between InGaAs and silicon cameras in the SWIR region [56]. The graph shows that the InGaAs camera has extended sensitivity from the NIR region to SWIR and better QE compared to the Si camera for 1100 nm. InGaAs sensors also have low power consumption and reliable performance at room temperature. However, these cameras are generally more expensive and have lower resolution compared to silicon cameras [56]. Moreover, they have higher dark current noise [32].

The Xenics XEVA-1.7-320 TE3 camera was used as the digital camera for photon emission microscopy. This is a SWIR camera with an InGaAs sensor detector, where the sensor resolution is 325*256 pixels [127]. Reducing the temperature of the InGAAS sensor results in less production of dark current noise and better images, so the InGAAS camera has a three step T3 cool-down system that can cool the camera down to a minimum of 50 degrees below ambient temperature, resulting in less dark current noise.

The Camera sums the photon emission of each pixel over a period of time (integration time). The integrated photon value is then detected by the detection sensor, amplified, and



Xeneth v2.6.0.659 /x64 [USB Camera/Serial=10946/Pid=8637h - 2 bytes/pixel]

Camera: USB Camera
Status: Online

Calibration: .1-5s_TrueNUC_-52 (TrueNUC)
Status: Active

General	
Integration time	580000 us
ADC Vin	2950 adu
ADC Vref	3350 adu
VDetcom	3500 adu
Frame rate	Min
Sensor	
Settings	
Y-Invert	False
X-Invert	False
Multiple Readouts	False
Bandwidth	0
Bias	011nA
Current	073uA
Power	0
Low Gain	False
Windowing	
StartX	0
StartY	0
EndX	319
EndY	255
Status	
Temperature	-50.81 Celsius
Image Processing	
Image source	Sensor
TEC	
Cooling	True
Manual PWM	0
P	3000
I	150
D	1
Settle Temperature	-55.00 Celsius
Offset Temperature	57

#362 2 fps 337 kb/s RxTime: 2023-05-08 16:38:32,513982

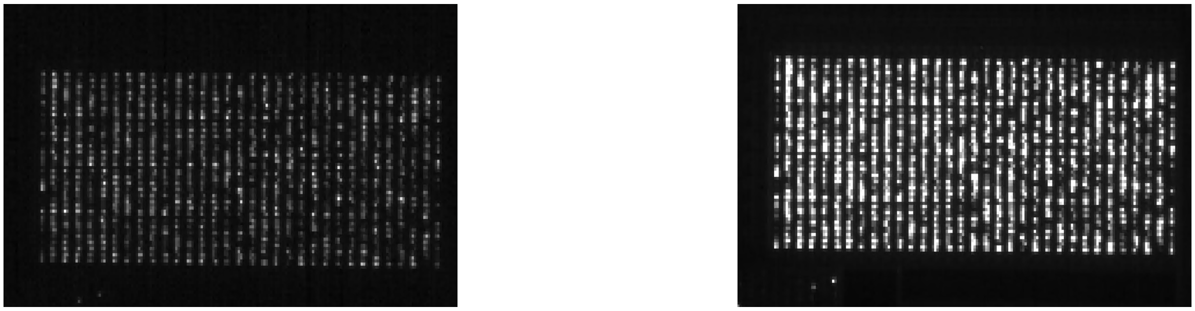
Figure 3.7: Screenshot of the Xeneth software, utilized as the camera's GUI.

quantized with a 12-bit Analog to Digital Converter (ADC). The resulting pixel intensity levels are then sent to a computer through a USB connection. The camera is operated through a Graphical User Interface (GUI) called Xeneth, which allows users to view the camera image and adjust settings such as integration time. The GUI also provides access to some image processing algorithms and real-time analysis capabilities. Figure 3.7 illustrates the camera's GUI.

In the context of improving image quality, several configurations of the camera can be used. Some of the important features that can impact the quality of the image are as follows:

- **Integration Time**: In photon emission microscopy, the integration time is a crucial parameter that determines the duration for which the camera integrates the photons emitted from each pixel. A longer integration time results in more photons being accumulated, thereby improving the image quality by providing greater detail. However, an increase in integration time also leads to a higher level of dark current noise, which can distort the image. In addition, if the integration time is excessively long, the capacitor associated with the detection filter may become saturated, resulting in a completely white image. This may necessitate the selection of a shorter integration time to avoid overexposure. As a result, the image captured may have less detail due to the shorter integration time. Therefore, it is essential to find the optimal integration time for each experiment.

  The Xenics XEVA-1.7-320 TE3 camera used in this study has a maximum integration time of 10 seconds in its highest gain setup. However, the integration time used in the



(a) Time integration of 0.1 S

(b) time integration of 1 S

Figure 3.8: A comparison of photon emission images captured with two distinct time integration periods.

(a) ADC V_{IN}=2650

(b) ADC V_{IN}=2950

Figure 3.9: A comparison of photon emission images captured with two distinct ADC V_{IN}.

experiment was limited to 5 seconds. Figure 3.8 demonstrates the effect of integration time on the photon emission from SRAM at two different integration times.

- **ADC** V_{IN}: This feature adjusts the central point of the input of the ADC, resulting in a shift of the histogram to the left or right. As a result, the image becomes darker or lighter, respectively [126]. Figure 3.9 shows the photon emission of $SRAM$ at different values of ADC V_{IN}.

- **ADC** V_{REF}: This feature determines half of the window width of the ADC input, which is the range of variation for the photon intensity. Choosing a very small value for ADC V_{REF} would limit the range of the ADC and result in a very black and white image. On the other hand, a high value for ADC V_{REF} would result in a grayscale image. This feature also affects the effective gain of the camera; a higher value for ADC V_{REF} results in a higher gain [128][126].

- **VDETCOM**: This feature sets the voltage of the detector substrate filter, which is used for biasing the sensor for detecting photon emissions. A higher value of VDETCOM leads to higher dark noise, but it also results in a lower (faster) response time [128][126].
- **Bw**: The bandwidth feature in the camera, adjusts the capacitors in amplifiers to control the bandwidth. This adjustment can lead to a change in the gain of the amplifier and noise levels [126].
- **Calibration Pack**: The camera software includes calibration packs that can correct for non-linearities in the images, such as offset correction, gain correction, and bad pixel replacement.

  The camera possesses an inherent light offset, which generates a base level of light even in dark conditions when there is no external light source. The calibration pack is primarily used to correct this issue. Additionally, the detector pixels in the camera do not respond linearly to light, resulting in varied gain for each pixel. The calibration pack is also necessary to correct this non-uniformity and produce an image with a consistent response. Bad pixels are pixels that are consistently dark or bright, or unresponsive to light, differing from their neighboring pixels. The calibration packs can reduce the number of such pixels. Moreover, these packs can be recalibrated based on the specific environment to produce better images [128].

The best camera settings for each DUT and objective are different. The process of selecting these settings is crucial in obtaining accurate and high-quality results in photon emission microscopy experiments. After experimenting with different calibration packs and adjusting various camera features, the optimal camera settings are chosen for each DUT and objective. The selected camera settings are subsequently applied during the experiment to record photon emissions. Careful selection of optimal camera settings can lead to improved image contrast and reduced noise. Moreover, it helps to minimize any potential image distortions that could compromise the accuracy of the analysis.

3.2.3 Sample Preparation

To capture photon emissions from a chip, a series of preparation procedures are necessary. Initially, the packaging materials of the sample chip should be removed, and the silicon die

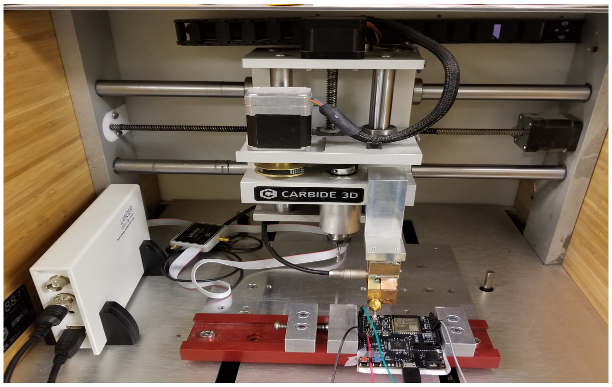


Figure 3.10: Our CNC machine deployed for sample preparation.

should be exposed so that the photon emission can be transmitted through. As the front side of chips usually contains metals and interconnects that make it difficult to reach the photon emission, the backside of the chip is typically the best option for photon emission microscopy.

The chip preparation steps used for the DUT were based on a CNC-based methodology developed in our lab, which is commonly used for preparing samples for various hardware security applications such as EM or laser fault injection [54][6][31], as well as photon emission microscopy [32]. This method is modeled after UltraTec's ASAP-1 procedure [118] and utilizes an in-house CNC machine. The Carbide 3D Nomad 883 Desktop CNC machine is used for sample preparation and is controlled by its GUI, Carbide Motion. The GUI allows for manual or automatic movement of the machine in any direction or location in the XYZ plane [21]. To perform the depackaging process, different milling bits are used, and the machine moves in the desired direction with the help of the GUI. Figure 3.10 illustrates the CNC machine used in our study for performing the depackaging process.

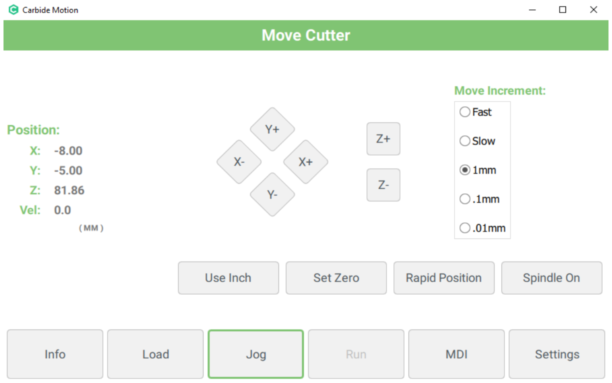
The initial step in preparing a chip for photon emission microscopy is to decapsulate the backside of the chip until the heat sink copper is exposed. To accomplish this, a mill is used to drill the area of interest. The same process is then repeated on the copper until it is completely removed, exposing the silicon die. Care must be taken during this process to avoid damaging the wiring and connections on the chip [118]. It is important to perform this task gradually and with precision to ensure the integrity of the chip.

The subsequent step in the chip preparation process for photon emission microscopy is to polish the substrate until it achieves a scratch-free, mirror-like surface. This polishing process comprises three stages: two pre-polishing phases followed by a final polishing stage. The first pre-polishing stage utilizes a coarse diamond with a wooden bit drill, followed

(a) Before Sample preparation

(b) After Sample preparation

Figure 3.11: The PIC16F687 chip, shown before and after the completion of preparation steps.



Carbide Motion

Move Cutter

Position:
X: -8.00
Y: -5.00
Z: 81.86
Vel: 0.0
(MM)

Move Increment:
○ Fast
○ Slow
● 1mm
○ .1mm
○ .01mm

Figure 3.12: A screenshot showcasing the user interface of the Carbide Motion software.

by a fine-grain diamond in the second stage. The final stage uses Colloidal Silica and a polishing bit to make the surface shiny, ensuring effective transfer of photon emission from the substrate [118]. It is important to perform the polishing process carefully and precisely to ensure that the surface is uniform, as any inconsistencies could potentially interfere with the photon emission microscopy analysis [5][32]. The result of this process is a high-quality substrate surface that is ready for experimentation. Figure 3.11 depicts images of PIC16F687 DUT before and after completing the preparation steps.

The GUI used for the CNC machine is capable of performing both manual and automatic drilling processes. A Gerber code can be used to provide instructions for each milling step of the machine. Running the code allows the machine to complete the task automatically. The Carbide Motion GUI, as shown in Figure 3.12, is used to control the CNC machine during the milling process.

The use of specialized machines, such as the ASAP-1 [118], can perform all the necessary sample preparation steps for photon emission microscopy. However, such machines come at a higher cost compared to the CNC machine setup utilized in our study. It is worth noting that the polishing technique employed in our study also results in some degree of IC thinning. To investigate photon emissions from a thinned chip, a PIC16F687 chip was thinned in partnership with an industry collaborator. The results of this investigation will be discussed in the next chapter, along with the decapsulated chip prepared in our lab.

3.3 Devices Under Test

In this study, we examined the photon emission from the data memories of two chips. This section presents specific details about these chips and their associated working boards.

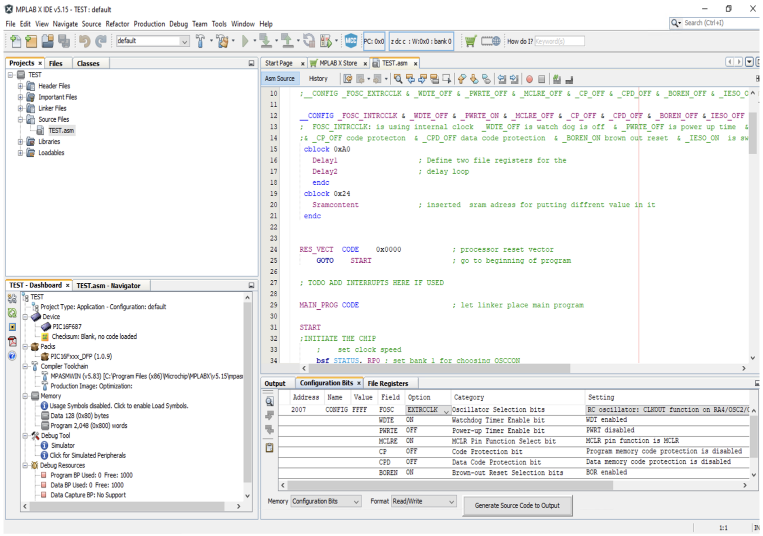
3.3.1 PIC16F687 Specification

The PIC16F687 microcontroller [61] was chosen as the first chip for investigating photon emission. It is an 8-bit microcontroller designed by Microchip, based on the Harvard architecture with a two-stage pipeline. In the first instruction cycle, the instruction is fetched, and in the next cycle, it is executed. Normally, instructions are executed in one instruction cycle.

The PIC16F687 microcontroller has a program memory of 3.5KB and data memory of 384 bytes, which are divided into 128 byte SRAM bytes and 256 byte EEPROM. The data memory is partitioned into four banks, each containing General Purpose Registers (GPR) and Special Function Registers (SFR). The general purpose registers are the 128 byte SRAM data memory. GPRs are used for storing any data, while SFRs control specific functions of the CPU or peripheral blocks [62].

The access addresses for GPRs are 0x20 to 0x7F in bank 1 and 0xA0 to 0xBF in bank 2. The status register of the chip has two bits that determine which bank will be accessed at any given time. GPRs can be accessed directly by providing the address or indirectly through the File Select Register (FSR). The INF register is not a physical register but is used in instructions to access the data memory address saved in the special register of FSR [62].

The PIC16F687 microcontroller is available in various package types, including PDIP, SOIC, and QFN. For this study, the Plastic Dual In-Line Package (PDIP) was chosen due



TEST
Project Type: Application - Configuration: default
Device
PIC16F687
Checksum: Blank, no code loaded
Packs
PIC16Fxxx_DFP (1.0.9)
Compiler Toolchain
MPASMWIN (v5.83) [C:\Program Files (x86)\Microchip\MPLABX\v5.15\mpas
Production Image: Optimization:
Memory
Usage Symbols disabled. Click to enable Load Symbols.
Data 128 (0x80) bytes
Program 2,048 (0x800) words
Debug Tool
Simulator
Click for Simulated Peripherals
Debug Resources
Program BP Used: 0 Free: 1000
Data BP Used: 0 Free: 1000
Data Capture BP: No Support

```
;__CONFIG _FOSC_EXTRCCLK & _WDTE_OFF & _PWRTE_OFF & _MCLRE_OFF & _CP_OFF & _CPD_OFF & _BOREN_OFF & _IESO_O

__CONFIG _FOSC_INTRCCLK & _WDTE_OFF & _PWRTE_ON & _MCLRE_OFF & _CP_OFF & _CPD_OFF & _BOREN_OFF &_IESO_OFF
;  FOSC_INTRCCLK: is using internal clock  _WDTE_OFF is watch dog is off  & _PWRTE_OFF is power up time  &
;& _CP_OFF code protecton  & _CPD_OFF data code protection  & _BOREN_ON brown out reset  & _IESO_ON  is sw
 cblock 0xA0
   Delay1                  ; Define two file registers for the
   Delay2                  ; delay loop
   endc
 cblock 0x24
   Sramcontent             ; inserted  sram adress for putting diffrent value in it
 endc


RES_VECT  CODE    0x0000            ; processor reset vector
    GOTO    START                   ; go to beginning of program

; TODO ADD INTERRUPTS HERE IF USED

MAIN_PROG CODE                      ; let linker place main program

START
;INITIATE THE CHIP
    ;    set clock speed
    bsf STATUS, RP0 ; set bank 1 for choosing OSCCON
```

Address	Name	Value	Field	Option	Category	Setting
2007	CONFIG	FFFF	FOSC	EXTRCCLK	Oscillator Selection bits	RC oscillator: CLKOUT function on RA4/OSC2/C
			WDTE	ON	Watchdog Timer Enable bit	WDT enabled
			PWRTE	OFF	Power-up Timer Enable bit	PWRT disabled
			MCLRE	ON	MCLR Pin Function Select bit	MCLR pin function is MCLR
			CP	OFF	Code Protection bit	Program memory code protection is disabled
			CPD	OFF	Data Code Protection bit	Data memory code protection is disabled
			BOREN	ON	Brown-out Reset Selection bits	BOR enabled

Memory: Configuration Bits
Format: Read/Write

Figure 3.13: A screenshot of the MPLab Integrated Development Environment (IDE).

to its simplicity in depackaging and ease of use in target boards. The chip has 20 leads and is built using a 450 nm process. It has an operating voltage range of 2V to 5.5V and includes 18 general-purpose I/O pins, along with several integrated peripheral blocks such as a 10-bit ADC, timer, comparator, and more. The clock source can be generated internally with a selection of several clock frequencies or externally.

PIC microcontrollers support an Integrated Development Environment (IDE) called MPLAB® IDE Software [65]. The software is an application that operates in the Windows environment and can be used for high-level source code debugging and programming [64]. For the experiment on the PIC16F687, the codes were written in MPLab IDE software in assembly language. It was possible to simulate the code in MPLab IDE and verify the SRAM content of the chip before investigating its photon emission. Figure 3.13 shows a screenshot of the MPLab IDE.

The PICkit3 in-circuit debugger/programmer was used to program the code from MPLab IDE to the chip [63]. It connects to a computer through USB on one side and uses a 6-pin header to connect to the chip on the other side. A universal target board was used to mount the PIC16F687 for experimentation. The board has connections for the programmer, an on-board regulated power supply, and LEDs and switches. Figure 3.14 shows the depackaged PIC16F687 mounted on the universal board, with the PICkit3 connected for programming.

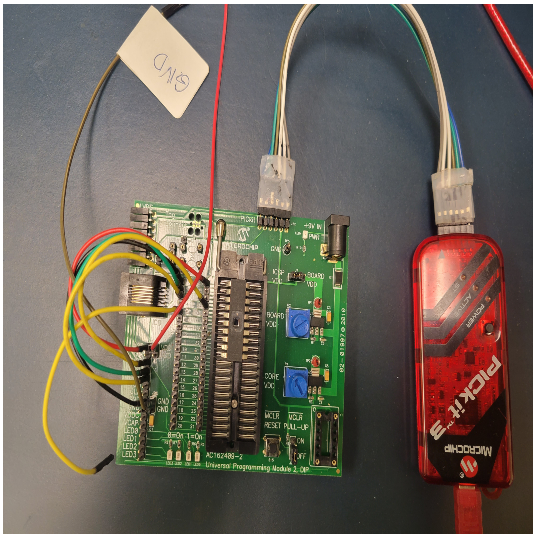


Figure 3.14: The PIC16F687, shown alongside the Universal board and PICkit3 programmer used for programming.

3.3.2 FE310-G00 Specification

The second Integrated Circuit (IC) selected for the investigation of photon emission is the FE310-G002 with a RISC-V core. This System-on-Chip (SoC) is part of the Freedom E300 platform and boasts a 32-bit E31 Core that is designed to support the RV32IMAC ISA options. The core features a high-performance, single-issue, in-order execution pipeline with a five-stage design, capable of reaching a peak sustainable execution rate of one instruction per clock cycle [96][97].

The FE310-G002 includes a General Purpose Input/Output Controller (GPIO) and various flexible I/O peripherals, as well as a clock generation and an Always-ON (AON) block that includes a programmable Power Management Unit (PMU). The internal clock can be generated from an on-chip trimmable oscillator or Phase-Locked Loop (PLL), or an external oscillator can also be used. The IC necessitates the utilization of two specialized power rails, which supply 1.8 V to the core logic and 3.3 V to the I/O pads and the always-on block, as reported in [97] and [96]. The memory architecture of the chip includes 16 KiB of Data Tightly Integrated Memory (DTIM) and a 16 KiB 2-way set-associative L1 Instruction Cache (I-Cache) [96][97]. The FE310-G002 utilizes off-chip Flash memory, which is connected to the Serial Peripheral Interface (SPI) and is controlled by the on-chip dedicated Quad-SPI flash controller.

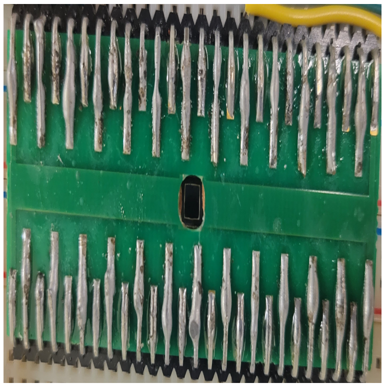


Figure 3.15: The PCB, used for mounting the depackaged RISC-V chip.

The FE310-G002 is manufactured using the TSMC CL018G 180nm process and is packaged in a 48-lead Quad Flat No-leads (QFN) package, which is an industry-standard [96][97]. To prepare the IC for photon emission investigation, it decapsulated from the back side. A custom-designed PCB board was created to mount the depackaged chip and enable easy connection to all of its pins. Figure 3.15 illustrates the prepared chip with its Printed Circuit Board (PCB). The schematic diagram necessary for the proper functioning of the IC is illustrated in Figure 3.16 based on [98]. To maintain the voltage at the nominal value, each of the two power supplies utilizes a voltage regulator. In order to program and debug the IC, a Segger J-Link base [91]is required, which serves as a bridge between USB and the chip. The U1 is utilized as the on-board Flash memory. A crystal oscillator is also included in case the chip uses an external clock source. Additionally, an LED is incorporated for testing purposes; for instance, if a particular address in the data memory has the expected value, the LED will begin blinking. Figure 3.17 presents the DUT on a breadboard.

SiFive Inc provides the Freedom E SDK, a development environment that allows users to compile source code using command line tools. The SDK is available as a public GitHub repository and supports the development of software for various SiFive Core Complexes, SoCs, and emulation environments. It offers direct support for Linux, including builds of the RISC-V toolchain. For the experiments in this study, we used the Freedom E SDK to compile the source code for the chip, using command line tools in a Linux operating system running on VirtualBox [98][95].

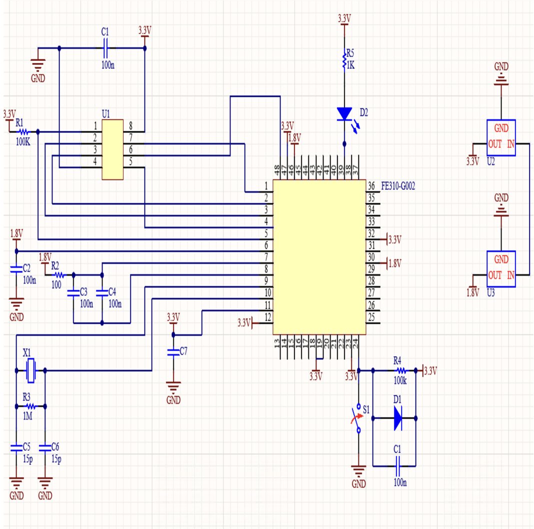


Figure 3.16: The RISC-V schematic designed for testing procedures.

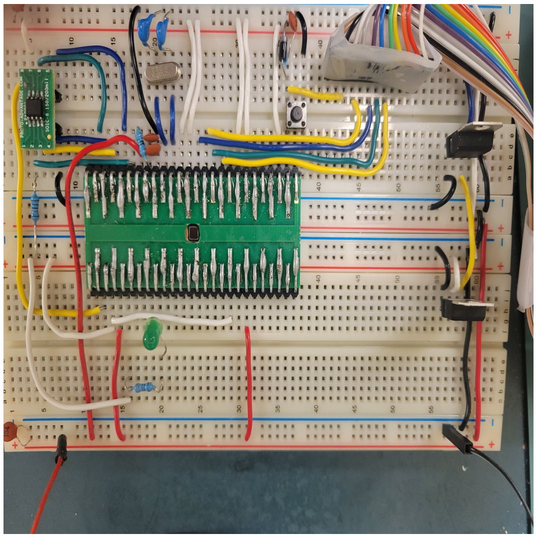


Figure 3.17: The RISC-V DUT board prepared for testing.

3.4 Terminology

The following section presents the terminology used in the dissertation. V_{DD} represents the supply voltage used to power the DUT. When targeting a specific address in data memory, the row that the target word is located in is denoted by R_i, and the column of the target word is denoted by C_j. TW_{ij} represents the target word located in row i and column j. In a fixed row, there are j number of words (columns), and each word contains n bits. The x bit of the j word in a row is denoted by W_j^x, where the first bit and row start from zero.

Table 3.1: Terminology used in the thesis

V_{DD}	Supply voltage of the DUT
R_i	Target word located in row i
C_j	Target word located in column j
TW_{ij}	target word located in row i and column j
W_j^x	bit x of word j in a row

3.5 Summary

In summary, our experimental setup included a high-transmission microscope in the IR range, a SWIR camera with good quantum efficiency, equipment for processing the backside of ICs, and two devices under test, a PIC16F687 microcontroller and a RISC-V chip. The equipment is low cost [32], amounting to approximately 40K CAD, in comparison to industry standards such as PHEMOS, which costs over 2M Euros [29]. The development of image processing techniques and methodology for advancing low-cost PEMs allows for the extension of the use of these side channels, making them accessible to those with limited funding.

Chapter 4

Investigating Photon Emission of SRAM block in PIC16F687

This chapter delves into an examination of the quiescent photon emission originating from the SRAM of the PIC16F687 chip. The focus lies on discerning whether any valuable information can be extracted from these emissions while storing different values in the chip's memory. The chip features 128-byte general-purpose registers, functioning as accessible SRAM data memory, which serve as the core of this investigation.

Initially, the photon emission of the SRAM is examined to establish whether it is possible to locate each 128-byte GPR and its corresponding bits. Subsequently, the photon emission of a specific word is analyzed for different stored values, checking for identifiable patterns. For launching differential or correlation attacks on photon emission, it is necessary to have completely aligned images. Thus, image processing techniques are employed to align the images and prepare them for potential attacks. Under a 10x objective, the photon emissions of the SRAM do not visually reveal the content of the data. Consequently, different attack methods such as differential or correlation attacks are applied to the photon emission of the SRAM under a 10x objective to ascertain if any information can be gleaned. Image processing measures are then applied to test the possibility of revealing the bit values. In summary, this chapter delves into the investigation of the quiescent photon emission of the SRAM of the PIC16F687 chip, exploring various techniques, including differential and correlation attacks, as well as image processing methods, to extract potential information.

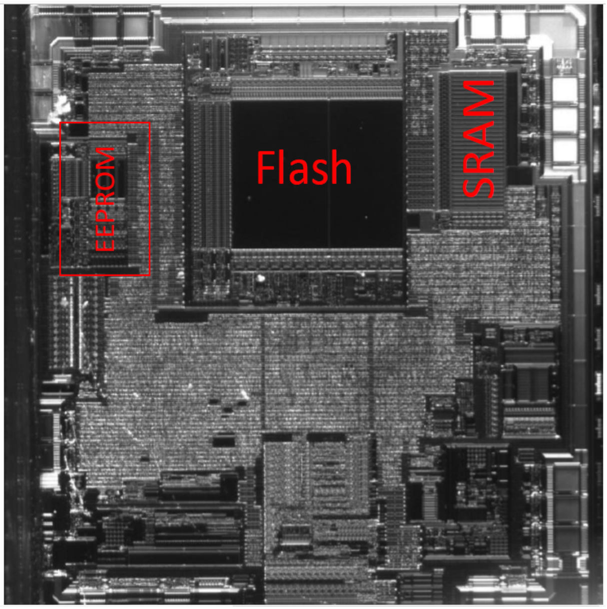


Figure 4.1: A die photo of the chip, highlighting the locations of various blocks [6].

4.1 Basic Investigation of Photon Emission of SRAM

Figure 4.1 presents the backside view of the PIC16F687 microcontroller, highlighting its various structures [6]. The figure also specifically emphasizes the SRAM block, which is the focus of the photon emission investigation.

The initial step in observing the quiescent photon emission from the SRAM block involves programming the chip with a simple piece of code, referred to as Code 1. In this code, the content of all bits in the general-purpose registers is set to one. Subsequently, the chip executes an infinite loop that does not require access to the SRAM. It is during this infinite loop that the quiescent photon emissions of the SRAM will be observed. At this point, the chip does not access the SRAM, but instead continuously runs a loop without performing any operations. As a result, the photon emissions observed from the SRAM block are not attributable to the switching transistors. They are associated with the SRAM's quiescent photon emission.

The photon emissions from the PIC board were initially observed when connected to a power supply at a nominal voltage of 2V. The chip also operated with its internal clock at a frequency of 8 Mhz. The SRAM block was observed using 10x objectives with a 0.1-second integration time. At nominal voltages, no photon emissions were visible from the

SRAM block. Therefore, in the subsequent step, the chip's voltage gradually increased, which caused several parts of the SRAM to begin illuminating. Eventually, at a voltage of approximately 11V, the entire SRAM block clearly emitted light. Figure 4.2 displays the photon emission of the SRAM, captured using a 10x objective at a power supply voltage of 11V and a 0.1-second integration time. For a more detailed examination of the SRAM's photon emissions, the emissions were observed using a 50x objective, as depicted in Figure 4.3. Using a 50x objective allows for the observation of only a small fraction of the SRAM at a time, but it provides more detailed information.

```

    bcf STATUS, RP1
    bcf STATUS, RP0
    movlw 0x20          ;start of GPR address
    movwf FSR       ;indirect address
 ;; in WRITE-B0 THE SRAM address FROM 0X20 TO 0X7FH (96 BYTE general registers) will be written all with 1 value
WRITE_B0:
    movlw b'11111111'       ; value all 1 for byte
    movwf INDF
    incf FSR, 1             ; move to next byte address
    btfss FSR, 7           ;if the 8th bit is set skip next instruction, so when fsr=ox80h (end of general register)
    goto WRITE_B0

    bcf STATUS, RP1         ;select Bank2
    bsf STATUS, RP0
    movlw 0xA0
    movwf FSR
 ;;  ;; in WRITE-B1 THE SRAM address FROM 0XA0 TO 0XBFH (32 BYTE general registers) will be written all with 1 value
WRITE_B1:
    movlw b'11111111'       ; value all 1 for byte
    movwf INDF
    incf FSR, 1
    btfss FSR, 6
    goto WRITE_B1
;Finish writing in SRAM

LOOP:
    NOP
    goto LOOP
 END
```

Listing 4.1: Part of the code number 1 related to write to SRAM for observing quiescent photon emission of PIC16F687 chip

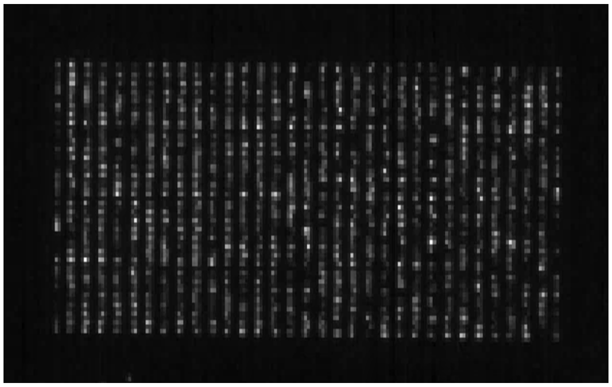


Figure 4.2: SRAM lite-up with 11v voltage and 0.1s integration time

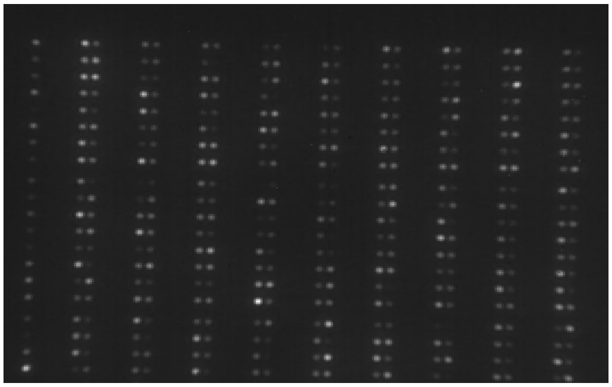


Figure 4.3: A section of the SRAM captured using a 50x objective, with 11V voltage and 5s integration time.

An alternative method for capturing quiescent photon emissions involves operating the chip with an external clock and then halting it at the desired clock cycle time [32]. The photon emissions were recorded using this method with both 10x and 50x objectives. By comparing the resulting images to those obtained with the previous method in Figure 4.2 and 4.3, it was observed that the photon emissions from both approaches were identical. Therefore, throughout the experiments in this chapter, the first approach will be employed. This method involves capturing the photon emissions from the SRAM while it is engaged in a loop of non-operational tasks.

4.1.1 Location of Bytes

In the previous step, the quiescent photon emission of the SRAM was recorded while all accessible words in the SRAM were set to the same value, with all bits filled with one (FF value stored in each word). In this section, a specific word is selected as the target. The value stored in this target word is changed to zero, while all other words continue to retain the value FF. The quiescent photon emission of the SRAM is then recorded. The objective of this step is to observe any changes in the photon emission of the SRAM block compared to the previous photon emission, where the target word held a value of FF. This will help to uncover any information related to the location of that target word.

The final part of the previous code has been modified, as shown in Code 2, so that one target word in the SRAM has a value of zero. The code then enters an infinite loop with no operations, during which the photon emissions from the SRAM are recorded using a 10x objective. Initially, the first accessible word in the SRAM at address 0x20 is selected as the target word.

```

; changing  values  from 1111111 to 00000000 at some specific address of Sram Content in sram like ox20

 bcf STATUS, RP1
 bcf STATUS, RP0
 movlw b'00000000'
 movwf  Sramcontent   ;0x20 now
 LOOP:
    NOP
    goto LOOP
 END
```

Listing 4.2: Part of the modified code number 2 related to changing only one byte for observing quiescent photon emission for different target addresses

Upon comparing the two photon emission images, it was observed that the photon emission of one row was brighter in the image where the target word was changed to zero, as compared to the same row in the other image. Additionally, the photon emission of this specific row was brighter than other rows within the same image. Figure 4.4 displays the photon emission when only the target word content is changed to zero for different addresses. The first image depicts the photon emission of the SRAM when there is no target word and all the words have an FF value. The brighter row, as can be seen in the figures, can be identified as the location of the targeted word.

Using this method, the location of the targeted word in the physical row of the SRAM could be determined by identifying the row with a brighter photon emission. This procedure was repeated for all 128 accessible word addresses in the SRAM, and their corresponding photon emissions were recorded. This enabled the identification of each word's location. Table 4.1 shows the location of the address of target words in the physical row of the SRAM after the experiment was conducted.

Table 4.1: Location of address of SRAM in relating physical row

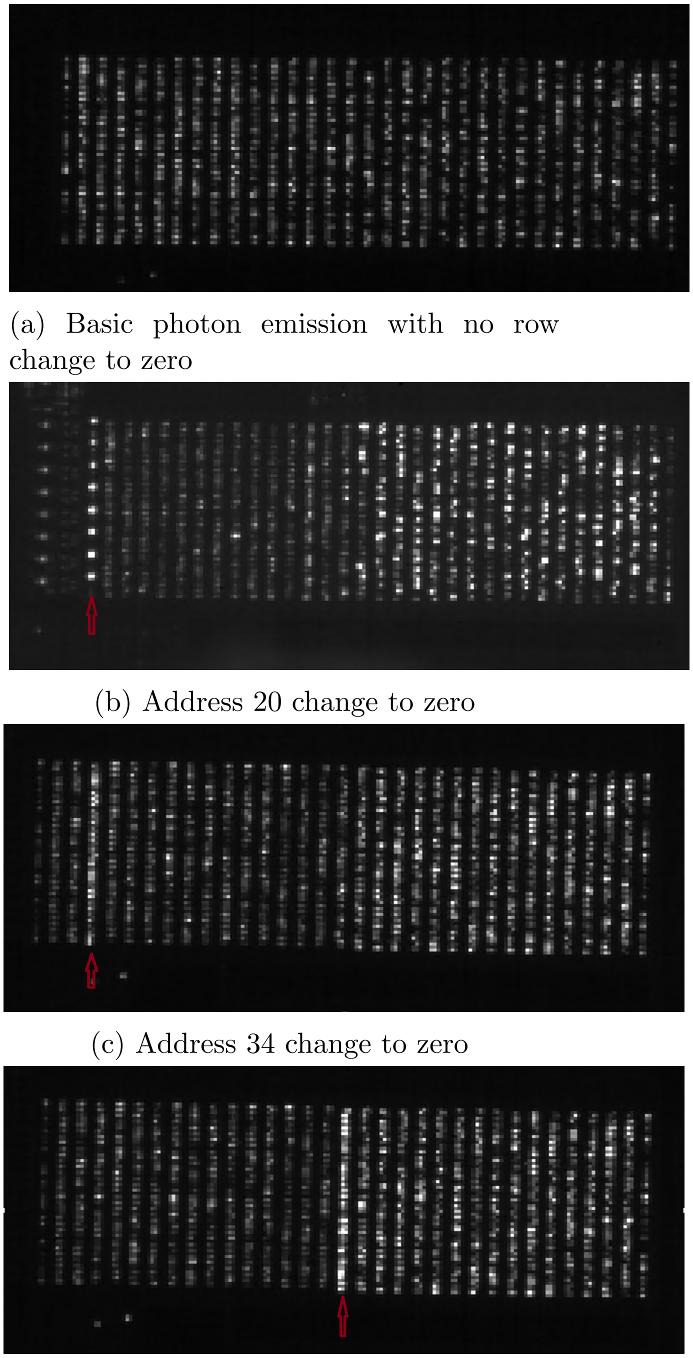
Row number	Byte address	Row number	Byte address
1	0x20-23	10	0x64-6B
2	0x24-2B	11	0x6C-73
3	0x2C-33	12	0x74-7B
4	0x34-3B	13	0x7C-7F 0xA0-A3
5	0x3C-43	14	0xA4-AB
6	0x44-4B	15	0xAC-B3
7	0x4C-53	16	0xB4-BB
8	0x54-5B	17	0xBC-BF
9	0x5C-63	-	-

Upon targeting the first four consecutive words, it was observed that the first row emitted brighter photons. This pattern was also noticed when the next eight consecutive words were targeted, with the second row showing brighter photon emission. This trend continued for the other rows with the following sets of eight consecutive words. Previously, as stated in [32], it was believed that each row in this chip contained only four bytes. However, with the new findings regarding the location of bytes, we now understand that each row, except for the first, contains eight bytes.

It's important to note that for the observation of the recorded photon emissions, we utilized Fiji [3], an open-source image processing package. Fiji enables viewing the recorded images in a sequence, similar to a video, which significantly simplifies the process of distinguishing changes in the images.

4.1.2 Placement of Bits Inside a Row

The subsequent objective is to discern the precise placement of bits within a given row. To accomplish this, a specific row is selected as the target, and the content of its bits is altered



(a) Basic photon emission with no row change to zero

(b) Address 20 change to zero

(c) Address 34 change to zero

(d) Address BC change to zero

Figure 4.4: Photon emissions from SRAM corresponding to a specific row with zero value.

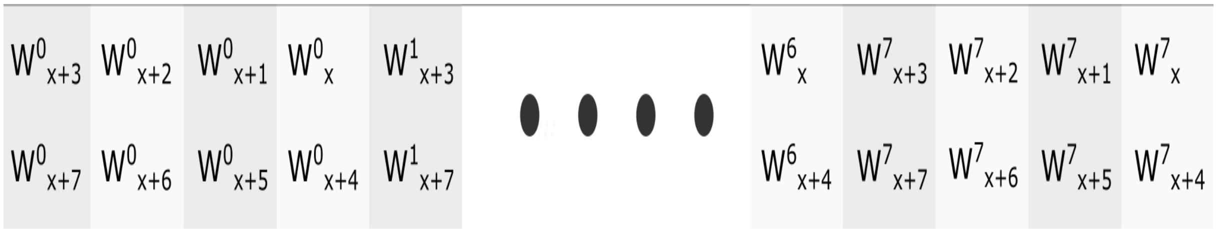


Figure 4.5: The location of bits within a single row.

for every word within that row. The photon emissions are recorded for each change in bit value, facilitating an investigation into the location of these changes. More specifically, the photon emissions for both potential bit values (0 and 1) are analyzed to gain a better understanding of the bit placement within the row.

For this task, row number two, denoted as R_2, was chosen as the target row to identify the placement of bits within it. As per table 4.1, word addresses from 0x24 to 0x2C are located within R_2. In the initial step, the first word address situated in the row was chosen as the target word. Using code number 2, employed in the previous section, the content of one bit of the target word was changed to zero each time, and the photon emissions of the SRAM were subsequently recorded. Given the difficulty of visually discerning changes in a single bit in photon emissions with a 10x objective, the photon emission of the row was captured using a 50x objective. However, this higher magnification only allows for observation of half of the row at a time. Thus, the photon emission of the row was recorded in two stages, requiring a slight adjustment of the chip to cover the entire row.

The same procedure was replicated for the remaining seven words in R_2, with the respective photon emissions being recorded. A thorough examination and comparison of all photon emission images, along with their corresponding known bit values, allowed for an investigation into the exact bit locations within this row. Figure 4.5 illustrates the location of 64 bits within one row. As can be seen, the most significant bits (W_i^7) are arranged from right to left, followed by (W_i^6), (W_i^5), and so forth. Notably, every pair of bits is situated relatively close to each other, resulting in their photon emissions converging at the same location under the 50x objective lens.

4.1.3 Patterns For Each Bits with 50x Objectives

With the understanding of bit locations in a row, the subsequent goal is to ascertain whether a photon emission pattern based on the value stored in a bit can be recognized.

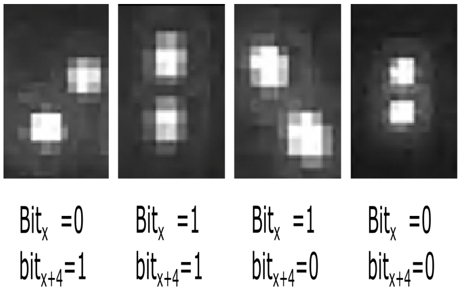


Figure 4.6: Photon emission pattern of two bits located at the same position.

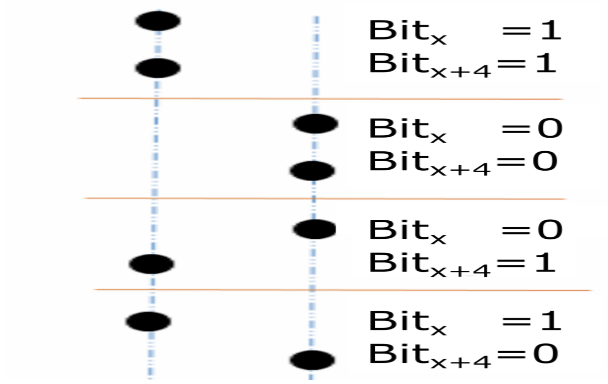


Figure 4.7: The pattern and location of photon emissions from two bits at the same position.

To accomplish this, photon emission images of two bits located at the same position, storing four distinct values of 00, 01, 10, and 11, were captured each time.

In row number two R_2, the first two words situated at the same location (C_0 and C_4) were selected as target words for this experiment. Utilizing a modified version of code 2, called code 3, the least significant bit of target words was altered each time to encompass all four possible values, and their corresponding photon emissions were recorded each time. By comparing the photon emissions, a pattern is observed based on the content of the two bits. Figure 4.6 displays the four distinct patterns of photon emissions related to the two-bit value.

The same process was repeated for the other bits of the target words C_0 and C_4, and subsequently for other words. A similar pattern was observed for other pairs of bits as well. It was determined that when both bits have the same value of 0 or 1, their pattern is identical; however, upon closer examination, it was revealed that the location of the

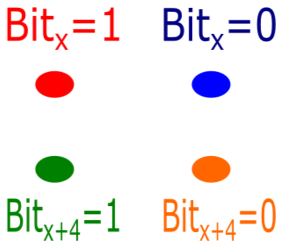


Figure 4.8: Possible photon emissions from two bits with differing values.

illuminated areas is not the same. Figure 4.7 illustrates the pattern of photon emissions for two bits based on their value, along with the location of the patterns. Figure 4.8 displays the possible photon emissions associated with each bit. Photon emissions corresponding to each case are depicted in different colors.

```
;only two bits at the same location change  for observing quiescent
   photon emission for ; Moving the changing values from 1111111 to
   1111110 at two addresses located at the same place.

bcf STATUS, RP1
bcf STATUS, RP0
movlw b'1111110'
movwf  Sramcontent   ;0x24 now
movlw b'1111111'
movwf  Sramcontent1   ;0x28 now
```

Listing 4.3: Part of the code number 3 for change 2 bit of target words with different value

4.2 Prepossessing of Photon Emission Images

The information obtained thus far has enabled the identification of the physical locations of general-purpose registers and their corresponding bits within the SRAM. Moreover, the values stored in the SRAM block have been determined by observing the quiescent photon emission pattern using a 50x objective lens.

In the next step, the photon emission of the SRAM will be analyzed using a 10x objective, where it is not possible to visually recognize photon emission patterns related to bit values. The objective is to apply various analyses on images of SRAM photon emission and attempt to uncover any information about the data saved in it. The images display the photon emission of SRAM with varying values stored in the target word. However, to conduct these analyses on the images, some preprocessing must be performed. Some image processing techniques are utilized to prepare the images for further analysis.

In photon emission microscopy, it is common to observe variations in intensity for identical scenarios captured at different time points. Despite having the same underlying structure, these images may display different illumination or lighting conditions. For example, when comparing photon emissions recorded from an SRAM with a fixed value at two distinct time intervals, the overall pattern and structure remain consistent, but the distribution of intensity values varies. This variability in intensity can be attributed to fluctuations in photon emission from CMOS transistors, as mentioned in the background chapter 2.

Certain image processing techniques are sensitive to these intensity variations and may not perform optimally. For instance, techniques like cross-correlation, which directly compares pixel intensities between two images, require a more normalized distribution of intensity values. Otherwise, even if the structures of two images are identical, the technique may fail to detect the similarity due to significant intensity variations.

To mitigate the effect of non-uniform intensity distributions, photon emission images should be normalized. By employing z-score normalization, as shown in equation 4.1, all images will share the same distribution, which is more suitable for applying image processing techniques.

$$I_{normalized} = \frac{I - \mu_I}{\sigma_I} \tag{4.1}$$

Here, $I_{normalized}$ denotes the normalized image, I is the original image, μ_I is the mean pixel intensity value of the original image, and σ_I is the standard deviation of pixel intensity values in the original image.

In addition to fluctuations, the process of recording photon emissions is subject to a significant amount of noise and interference. As a result, it is typically recommended to repeat the photon emission recording procedure under the same conditions multiple times. This generates a series of identical images. In theory, these multiple images should contain the same information, but with varying noise levels. By obtaining a set of images with different noise levels, averaging can be used to mitigate the impact of noise. This process involves calculating the mean of the pixels in the same spatial location and setting that as the final value for the pixel. In this research, for each different value of the target word, a sequence of 10 images is recorded. During the analysis, both the average of the sequence images and a single recorded image are utilized.

4.2.1 Alignment Issue

During each stage of recording the photon emission with a different value stored in the target word, the stored value needs to be updated in the code. After making the necessary modifications, the code will be flashed onto the chip using a PICkit 3 programmer. However, the PICkit 3 is unable to connect to the universal board when it has an overvoltage of 11V (necessary for observing photon emissions) due to its internal circuitry. As a result, the chip must first be disconnected from the power supply before being connected to the PICkit 3 programmer. Once programming is completed, the PIC universal board will be disconnected from the PICkit 3 board and reconnected to a power supply with an overvoltage of 11V to enable photon emission recording.

Connecting and disconnecting the board from the PICkit3 may cause some spatial shift to the chip. Furthermore, as mentioned in the previous chapter, recording the sequence of images with the microscope causes additional spatial shifts. Despite securely fastening the PIC universal board to the microscope base, it was not possible to completely avoid the spatial shift that occurs during the recording of the photon emission images. Due to this spatial shift, the analysis methods cannot be applied to the image sets, as they require applying to the same location in each image. Therefore, further analysis of the PEM image sets is not possible without first addressing the alignment issue.

First, several existing tools were used in an attempt to align the captured images, but the results were not promising. For instance, the free software DeepSkyStacker, which is commonly used by astronomy photographers to process pictures taken with CCD astronomy cameras, was utilized. This software can align images of the sky by detecting the locations of stars and performing alignment based on star locations, which are typically perceived as bright spots in the image [28]. This software was used since the characteristics of captured images in our experiment are similar to captured images using the CCD astronomy cameras. Unfortunately, the software was unable to align images properly since it could not detect bright enough pixels to treat them as anchors for the alignment purpose.

Additionally, several publicly available MATLAB toolboxes were used to perform spatial alignment on the captured images, but all attempts were unsuccessful. We believe that there are differences between natural images and the captured photon emission images, which make utilized alignment approaches fail. Specifically, the intensity range of the captured images is much wider than that of typical 8-bit images, and the textures found in our captured images are blurry, making it challenging to achieve accurate alignment. Therefore, an attempt was made to align the captured images. Several image processing techniques were used and compared at different stages. An in-house method was developed, utilizing the techniques that led to the best alignment for the images for this purpose.

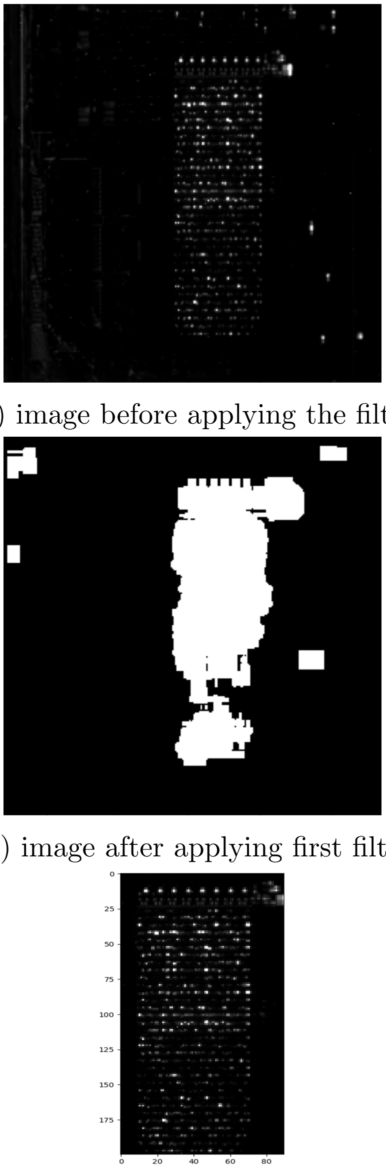
As an initial step for aligning images, a threshold filter is applied to ignore pixels with intensity values lower than a specified threshold, setting them to zero. This process removes pixels around the SRAM with low intensity. Other filters, such as Wiener or Gaussian filters, did not work effectively for photon emission images, as they caused the images to become more blurry and lose small but important information about photon emissions.

In order to make the alignment process faster, it is more efficient to focus on the SRAM block instead of the entire image. Therefore, the next step in the alignment process is to detect the SRAM block location and crop it from the whole acquired image. This will increase both the speed and accuracy of the spatial alignment of SRAM photon emission images. For precise cropping of the SRAM image, two methods showed the most favorable outcomes. These were selected from a range of approaches that were tested. These two methods were then employed.

In the first step, a spatial filter with a specific window size is applied to detect large blocks in the image. A sliding filter with a small size, such as 5 or 10, is used to identify signal activity within each window. If the signal activity inside the window is lower than a threshold, the pixels within the window are set to zero to reduce speckle noises and low signal activities, which are common artifacts of the photon emission acquisition procedure. Figure 4.9a shows the image before applying the filter, and Figure 4.9b shows the image after applying the filter, where the locations with detected activity using the filter are highlighted. Since several activity locations can be detected other than the SRAM, only blocks with high signal activity and approximate size of the SRAM are retained after filtering, denoting the approximate location of the SRAM block.

The coordinates detected for the SRAM in these steps are often smaller than the actual SRAM dimensions. This results in only partial SRAM detection, which lacks accuracy. Therefore, a second filter is used to detect the SRAM location more accurately. A window filter with the size of the SRAM block is chosen and slides around the coordinates obtained from the previous step. The energy level of each window is calculated in each step. When the window completely covers the SRAM block, the energy level should be at its maximum level. Thus, the coordinates related to the highest energy level are then used as the SRAM location and employed to crop the SRAM from the whole image. Figure 4.9c displays the result of the final filtering. With the SRAM block cropped, it becomes easier to align the SRAM for further analysis.

The cross-correlation value between two images with similar content is maximized when they are aligned and have the same value at the same coordinate [102]. The recorded images of photon emissions are not identical due to the presence of noise and variations in photon



(a) image before applying the filter

(b) image after applying first filter

(c) Final crop SRAM image

Figure 4.9: The steps involved in detecting and cropping the SRAM area within a photon emission image.

emission pattern values. However, some parts of the SRAM are mostly similar. Therefore, it may be possible to determine the spatial shift of an unaligned image with respect to the reference image by applying cross-correlation to these similar locations in both images.

To do so, a part of the cropped SRAM images with nearly similar photon emissions is selected. One image from the entire set is arbitrarily chosen as the reference image, denoted as R_{xy}. Other images should be aligned with respect to the reference image. In each step, one of these unaligned cropped SRAM images is chosen as the second image, A_{xy}, and the cross-correlation is calculated between the selected part of the reference image and the second image. The spatial number that corresponds to the maximum value of the cross-correlation between the two images provides the spatial shift between them. The second image is then shifted in that spatial direction to be aligned with the reference image. This process is repeated for all unaligned SRAM images. By utilizing this approach, the images in our experiments were better aligned, and the attacks could be applied to them.

It should be noted that the cropped images have been subjected to filtering, where intensities lower than a threshold value are reduced to zero. Additionally, intensity normalization has been applied to these images to achieve a better distribution. Other analysis methods, such as Mean Squared Error and Peak Signal-to-Noise Ratio (PSNR), have also been used for determining the spatial shift. However, the cross-correlation method yielded better alignment results.

4.3 Investigating Photon Emissions for Different Value Store in SRAM 10x Objectives

The previous sections have emphasized that any change in an SRAM bit value prompts a modification in the corresponding photon emission pattern. This, in turn, influences the pixel intensity at the bit's location. Therefore, it might be possible to analyze these variations in image intensities and extract information from these images, even when the visual changes are not perceptible to the naked eye. The goal is to ascertain the feasibility of launching attacks on these photon emission images to potentially extract sensitive information from SRAM. In the following section, correlation and differential analysis will be investigated.

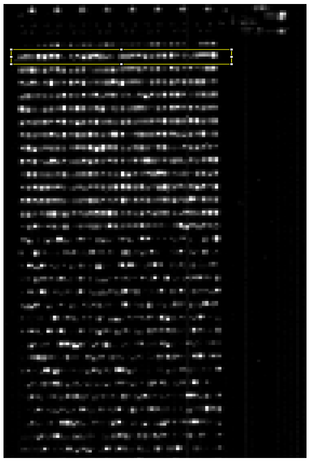


Figure 4.10: Photon emission from SRAM holding 0x4A in the target word, showcasing the selected area of interest.

4.3.1 AES Key Attack Correlation Attack

By changing the value of the target word, the intensity of certain pixels associated with that word will also change. This might affect the total intensity within the target row. Consequently, a correlation could exist between the sum of the intensities of the target row pixels and the bit changes within that row. As such, a correlation attack could be conducted on the photon emissions images of an SRAM while it executes the first Key Addition operation of the AES algorithm.

The primary goal is to perform a known-plaintext attack and attempt to identify the AES key, based on the subsequent photon emissions. In this context, it is assumed that the known plaintext values are exclusively OR'ed with a fixed key, and the resulting output is stored in the target word. For this analysis, the key is assumed to have a value of zero. The aim is to determine the feasibility of discovering this key by analyzing the photon emissions from the SRAM.

For recording the photon emissions associated with this attack, an accessible address of the SRAM was chosen as the target word. The first word in row number two, having the address 0x24, was selected as this target word (TW_{20}). Consequently, the row containing the target word is designated as R_2. Figure 4.10 illustrates the photon emission image from the SRAM, with a target word value of 0x4A. The area of interest is highlighted in this figure.

In order to capture all potential photon emissions associated with the target word, it's necessary to record the photon emissions for all 256 possible values of the word. In the first set of images (image Set 1) to be analyzed, the value of the target word was altered to include all possible values, while all other accessible words in the SRAM remained at a constant value of 255. The SRAM's quiescent photon emission was recorded for each possible value of the target word, from 0 to 255, using a 10x objective and 1-second integration time. For each value, ten consecutive images were captured and used for averaging, following the previously mentioned preprocessing techniques. After the acquisition of all 2560 images, preprocessing steps such as z-score normalization and alignment procedures were carried out to prepare the images for subsequent analysis.

In a typical correlation attack, the Hamming weight of the expected output can serve as a possible model for predicting the side channel. Consequently, the correlation between the actual side channel trace and the predicted Hamming weight of the possible output is calculated. The highest correlation coefficient should indicate the correct key. In this attack, considering that all other bits in R_2 have a value of 1, and the intensity of a bit with a value of zero is higher, the count of zero bits is used instead of the count of bits with a value of 1. The correlation attack was conducted between the sum of all pixel intensities of the target row R_2, which contains the target word TW_{20}, and the number of zeros in the expected output. This output is obtained by performing an exclusive OR operation between the known plaintext and the guessed key.

A section of the image associated with R_2 was chosen as the area of interest, and the intensities of all its linked pixels were summed. The expected output is derived from exclusive OR operations between the plaintext, which can vary from 0 to 255 - representing all potential changing values of the SRAM, and a guessed key that can also range from 0 to 255. The Pearson correlation was used in the analysis to compare the sum of intensities for the target row and the count of zero bits for the expected output values. The highest correlation coefficient reveals the correct key. Fig. 4.11 shows the correlation coefficient results for all the guessed keys. The highest correlation coefficient, standing at 0.62, corresponds to the key value of zero, accurately identifying the correct key.

The previous plot showcases the correlation coefficient results for all the 2560 recorded images, in which 10 sequential images were captured for each unique value stored in the target word. The correlation coefficient was also calculated using just a single image from the set of 10. These results are consistent with those from the previous plot but exhibit a slightly lower correlation coefficient of 0.61 for the correct key, which is in line with expectations.

In the correlation attack, the analysis involved all 256 possible cases. However, in the next step, the number of input plaintexts was decreased, and the analysis was replicated

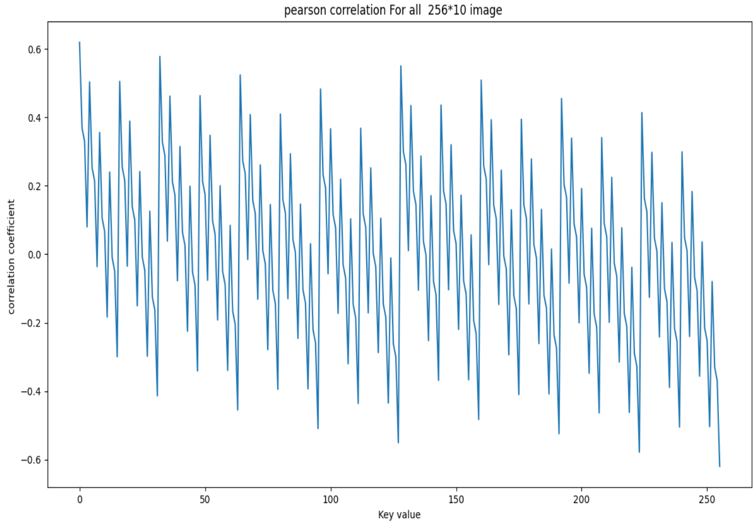


Figure 4.11: The correlation coefficient plot representing all the guessed keys for image set 1.

with fewer images. Observations indicated that with a reduced number of plaintexts - between 128 and 256 - the key=0 still had the highest coefficient. Yet, when the number of plaintexts was diminished further, from 128 down to 32, the highest correlation coefficient corresponded to both the key=0 and another key. When fewer than 32 plaintexts were used, the number of images proved insufficient for the attack.

The first scenario, using image set 1, involved changing the target word value across all 256 possible values. During this process, all the other bits in the row maintained a constant value of 255. As addressed in previous sections, bits associated with one word are located far apart. Consequently, when changing the bits of a target word, their changing photon emissions do not overlap due to this distance. To increase the complexity of the scenario and modify bits closer to one another, a second set of images (image set 2) was produced. Here, instead of altering the 8-bit value of the target word W_0, its 4 lowest bits (W_0^0 to W_0^3) and their corresponding bits in the same location (W_4^0 to W_4^3) were changed. Photon emission from the SRAM was recorded for all 256 possible values of these 8 bits. The goal is to assess whether a correlation attack can be successful under these conditions, where 2 bits located at the same place are changing, and their photon emissions mutually influence each other.

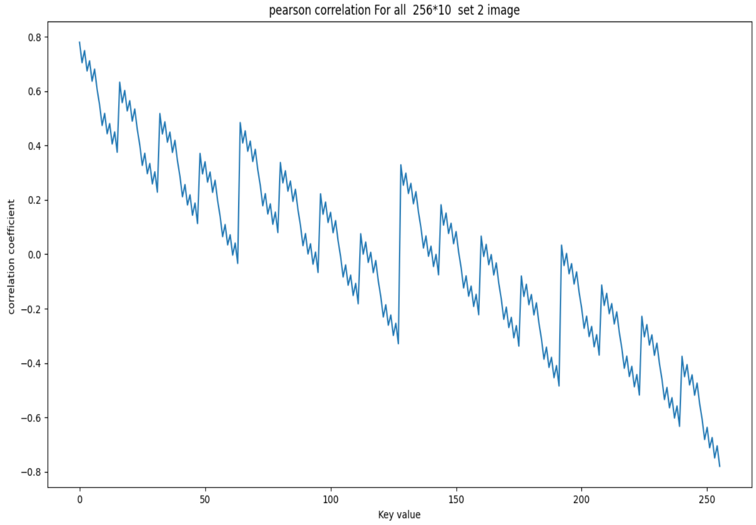
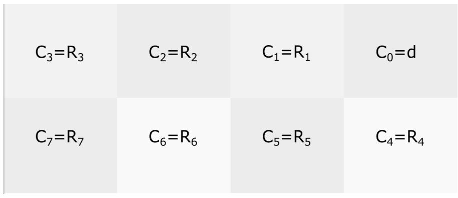


Figure 4.12: The correlation coefficient plot representing all the guessed keys for image set 2.

The image set 2 was pre-processed and readied for analysis. The same correlation attack procedure used in the first scenario was then applied to this second image set. Figure 4.12 illustrates the Pearson correlation coefficients for various key guesses associated with the second image set. The highest value corresponds to the correct key of zero. Hence, the correlation attack proved successful in scenario 2, even when the bits at the same location were subject to change and not held constant. During the photon emissions recording for image set 2, adjustments were made to the camera settings to obtain higher-quality images. Despite the increased complexity of the attack in this scenario, it's noteworthy that the correlation coefficient for the correct key within this set was higher, reaching a value of 0.78.

In an attempt to further elevate the complexity of the analysis, a third scenario (image set 3) was devised. Figure 4.13 illustrates the positioning of the words and the changes associated with them. In this case, the value of the target word (C_0) was altered in each step, to include values ranging from 0 to 255. However, the values of the other seven words (C_1 to C_7) in the target row were not constant and varied randomly with each iteration.

In every step, the target word C_0 would take on a different value 'd', with fresh random values assigned to C_1 through C_7. To temper the impact of the photon emissions from C_1



$C_3=R_3$	$C_2=R_2$	$C_1=R_1$	$C_0=d$
$C_7=R_7$	$C_6=R_6$	$C_5=R_5$	$C_4=R_4$

Figure 4.13: Positioning of the words and the changes associated with image set 3.

to C_7, an additional image was captured during each step. This time, C_0 was assigned a value of 0, while the same random values were maintained for C_1 to C_7. The final photon emission image pertaining to that value was acquired by subtracting the photon emission image, where the target word C_0 held a value of 'd', from the photon emission image, where the target word C_0 had the value 0. In both images, the values of C_1 to C_7 remained the same. The process of recording photon emissions with varying values of 'd' for C_0 was repeated, but with different random numbers for C_1 to C_7 compared to the previous step. The photon emissions from the SRAM were captured using a 10x objective and an integration time of 1 second.

After performing the required pre-processing steps on the images, a correlation attack was conducted on this image set. The Pearson correlation coefficients for all key guesses are depicted in Figure 4.14. As is evident, the correlation attack was successful even in this final, more complex scenario where all words in the row were subject to change. It's important to highlight that the experiments for image sets 1 to 3 were conducted at different address locations and on different chips to assess redundancy. Thus, the attack proved successful across varied locations and chips.

4.3.2 Differential Analysis

In the initial step towards revealing information stored in a target word, the key for known plaintext was successfully determined. The subsequent step involved investigating the possibility of discerning the value of each bit stored in a target word from photon emission images. To analyze photon emission at the bit level, the location of each bit for the target word needed to be identified.

Leveraging 50x objectives, it became feasible to pinpoint the position of every individual bit. Additionally, the locations of words within a row could be determined even with a 10x objective. The main aim was to ascertain the practicability of identifying each bit's location within a row using a 10x objective. This assessment focused on whether such

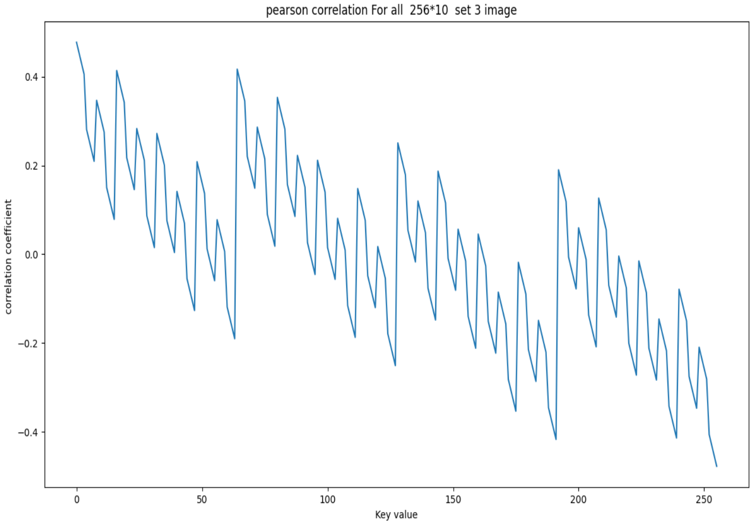


Figure 4.14: The correlation coefficient plot representing all the guessed keys for image set 3.

identification could be achieved by analyzing changes in image intensity, even when these alterations are not visibly discernible to the eye.

Since the photon emission at each bit location varies depending on the bit value, the bit location in the image can be inferred by applying a difference of means based on each bit's value. To validate this possibility, the image sets 1 from the first scenario were chosen for initial evaluation using the difference of means.

In a standard differential attack, the output for each known plaintext, combined with a guessed key, is computed. The traces are subsequently categorized based on the value of the output bit into two groups: zero and one. The difference of means for the traces pertaining to these two groups is then calculated. If the guessed key was accurate, noticeable peaks should emerge in the final plot of the difference of means. This is because, if the key guess was incorrect, the calculated output would also be incorrect, which would result in traces being categorized randomly and the difference of means becoming noise. Applying this principle to our evaluation, it anticipates that computing the difference of means for the correct key (key=0) may allow us to identify the location of target bits within the target word. This would be reflected in the difference of means plot, which should display peaks at these target bit locations.

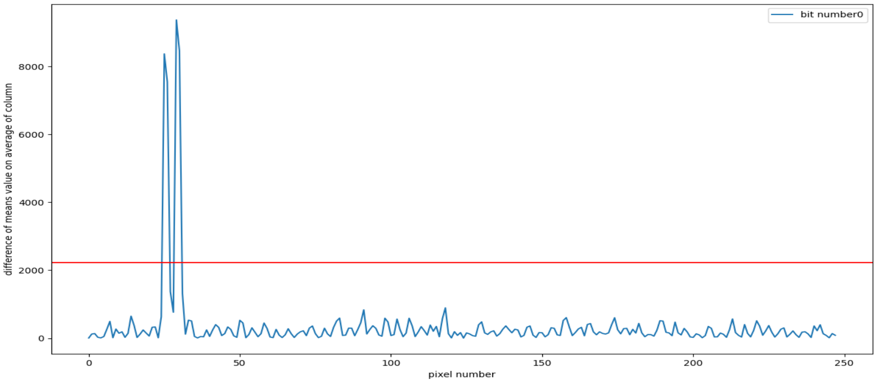


Figure 4.15: The absolute difference of means trace for bit 0 of BUA within image set 1, with the red line representing a 2*σ value.

In the initial step, the difference of means analysis was applied to image set 1, using the correct key=0. Images were categorized into two groups according to the value of each specific bit in the target word. Images with a bit value of 0 were allocated to the zero group, while those with a bit value of 1 were placed in the one group. For each bit, the difference of means between the two groups was calculated. Peaks in the difference of mean trace for each bit indicated the location of that particular bit.

The difference of means was applied on two-dimensional images. To display the plot in a trace, the two-dimensional matrix of the image was converted into a one-dimensional vector. In this case, the area of interest in the photon emission of the image consisted of 4x62 pixels, which was converted into a single vector of size 248. Every four pixels with the same Y-coordinate were placed next to each other, followed by the pixels of the next Y-coordinate. This resulted in some traces having two closely spaced peaks, representing pixels located near each other in the x-direction.

Figure 4.15 displays the trace for the absolute difference of mean on bit 0. The red line represents 2*σ value, indicating that peak values are significant. The standard deviation of each pixel for the difference of means value for different keys was calculated. It is evident that the peak is only present at the location related to the place of bit 0, with other locations exhibiting small values as expected.

Figure 4.16 illustrates the eight traces for the absolute difference of mean for all eight bits combined in a single plot. The peaks indicate the location of each bit in the row associated with the address 0x24 of SRAM, as anticipated. The locations identified through this analysis are consistent with the bit locations previously determined using a 50x objective lens. This demonstrates the effectiveness of the proposed method in determining the positions of individual bits within the memory row, even when using a lower magnification, such as a 10x objective lens.

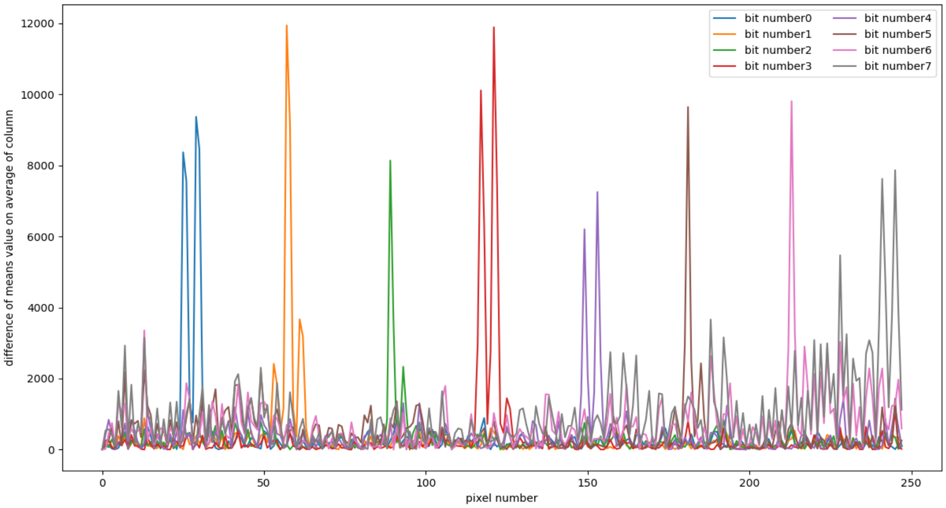


Figure 4.16: The absolute difference of means trace for all 8 bits of BUA within image set1.

Alternative methods for plotting the trace exist, such as selecting only one pixel with the same Y-coordinate instead of using all pixels in the image. For instance, choosing the maximum intensity pixel or averaging the four pixels. The new plot also displays the peaks, albeit with less detail (Figure 4.17).

The same process can be repeated for all the other 7 words in the same row, and the locations of all bits within the row can be revealed using a 10x objective lens. This demonstrates the scalability and robustness of the proposed method, as it can be applied to any target words in memory.

In the next step, difference analysis was performed on the more complex scenario 2 images. In this case, bits located in the same position changed simultaneously, resulting in photon emissions at a single location being influenced by two different bits at a time. The difference of means for each bit in this scenario was calculated. Figure 4.18 presents eight distinct plots, each displaying the absolute difference of mean derived from averaging four

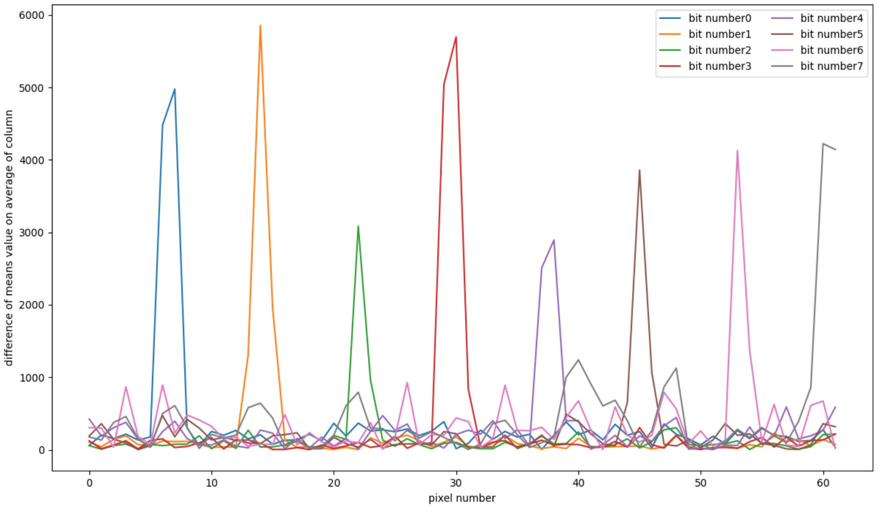
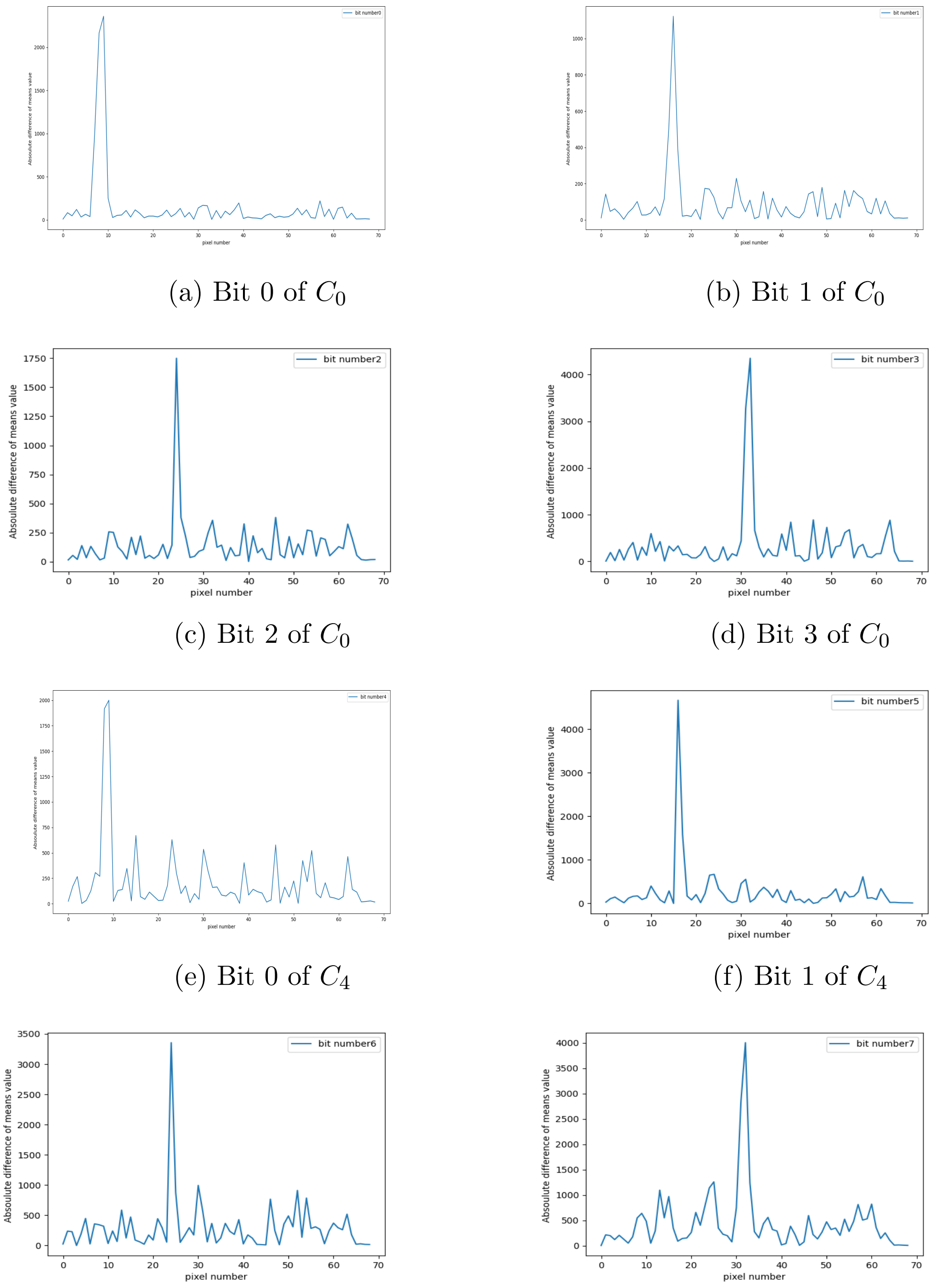


Figure 4.17: The absolute difference of means for all 8 bits, derived from averaging four pixels within a column.

pixels within a column for all eight bits. It can be observed that every two bits are located at nearly the same position, as expected. This analysis demonstrates that even when two bits with the same value change simultaneously, the location of the target bit can still be accurately determined. Figure 4.19 shows the difference of means plot for two bits located in the same position in a single plot to highlight this finding.

The difference analysis was also applied to image set 3, where the other 7 words in the row changed randomly along with the target word value. The analysis was not successful in this case. One of the reasons for this outcome is that in image set 3, with each change in the bits b^i of the target word, all the surrounding bits of the interested bit also changed, and their photon emissions had some effect on the photon emission of b^i. This made it difficult to categorize images based solely on the changes in one bit. On the other hand, since in image set 3 the photon emission of all the surrounding locations of the interested bit changed as well, it became crucial to ensure that all bits were completely aligned and that there was no misalignment, even by a single pixel. This factor was not as stringent for the previous image data sets. The very small misalignments in the images caused the analysis to fail in this case.



(a) Bit 0 of C_0

(b) Bit 1 of C_0

(c) Bit 2 of C_0

(d) Bit 3 of C_0

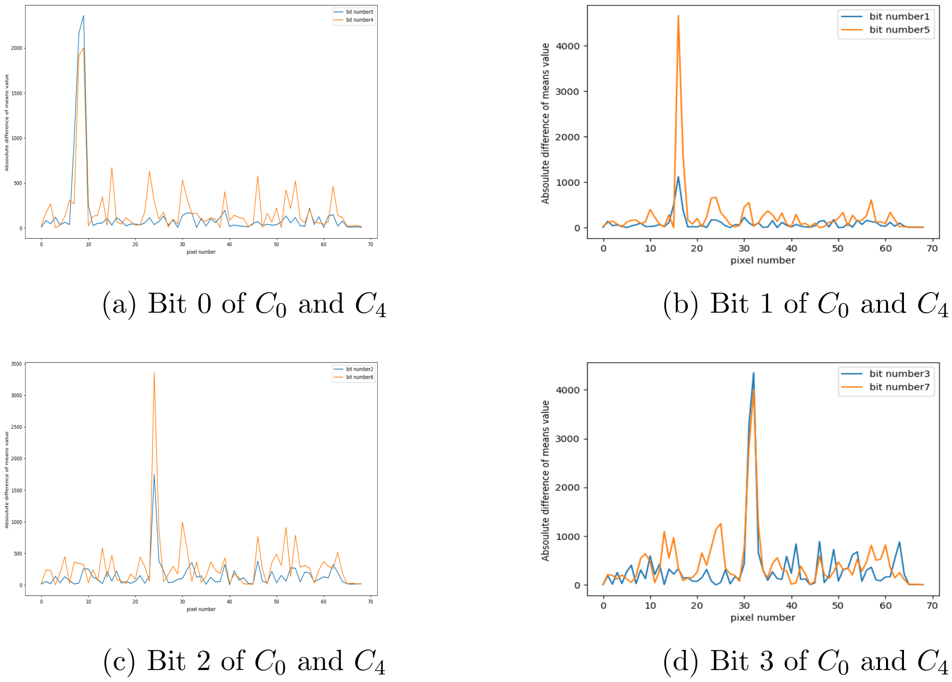
(e) Bit 0 of C_4

(f) Bit 1 of C_4

(g) Bit 2 of C_4

(h) Bit 3 of C_4

Figure 4.18: The absolute difference of means trace for target bits within image set 2.



(a) Bit 0 of C_0 and C_4

(b) Bit 1 of C_0 and C_4

(c) Bit 2 of C_0 and C_4

(d) Bit 3 of C_0 and C_4

Figure 4.19: The absolute difference of mean values for each pair of bits located at the same position within image set 2.

4.4 Revealing the Value of a Bit Using SSIM

In the previous section, it was demonstrated that unknown bit values could be revealed based on the visible photon emission patterns associated with different bit values when captured using 50x objective lenses. In this section, the goal is to investigate whether it is possible to reveal bit values where the patterns are not visible to the eye by analyzing the images of photon emission captured using 10x objective lenses.

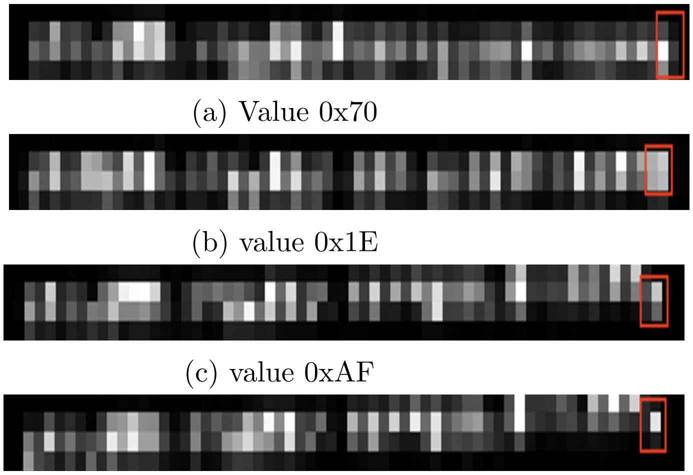
The location of each bit in an SRAM row was determined through the use of difference of mean analysis in the previous section 4.3.2. By analyzing the intensity variations in photon emission images corresponding to each bit's location, and utilizing image processing techniques, it might be possible to distinguish between images with differing values. This process could thereby facilitate the determination of bit values stored in memory. It should be emphasized that these images were captured employing a 10x objective lens.

Figure 4.20 displays the photon emission of the second row for four different values in the target word, with a highlight on the location of bit 7. This visual representation helps to illustrate the variations in photon emission associated with different values stored in the target word. Moreover, it can be observed that although the value of bit 7 for both 4.20a and 4.20b are the same, their photon emission patterns are not easily distinguishable by the eye. This emphasizes the importance of using image processing techniques and analysis to reveal sensitive information such as the content of individual bits within the memory, even when working with lower magnification images captured using 10x objective lenses.

During the initial phase of the analysis, the simpler Image Set 1 was utilized. To begin, for each specific bit, two template images were created based on images of bits with known values. These templates represented the photon emission patterns associated with the binary values of zero and one for a specific bit. Following this procedure, the unknown value of the target bit could be determined by comparing the image at the corresponding bit location with the corresponding template images.

To construct templates for each bit in the target word, images from Set 1 were first sorted into two categories, zero and one, corresponding to the value of the respective bit. For the zero-value template of each bit, the images in the zero category were averaged, and the area related to target bit location was extracted from the average image to create the zero template. The same procedure was applied to generate the one-value template, using all the images in the one category for that bit. Figure 4.21 displays the two templates for the one and zero values of bit 7 at address 0x24 in the SRAM. These templates were created by averaging all 1280 images available for each category.

Utilizing these templates, the unknown value of a bit in the target word could poten-



(a) Value 0x70

(b) value 0x1E

(c) value 0xAF

(d) value 0xEB

Figure 4.20: Photon emissions from the second row displaying differing values in C_0, highlighting the photon emission from bit 7.

(a) Template for bit value 0

(b) Template for bit value 1

Figure 4.21: Photon emissions of the template for bit 7 within image set 1.

tially be predicted by comparing the similarity between these templates and the image at the location of the unknown bit. Appropriate image comparison techniques, if implemented correctly, could potentially reveal the original bit values stored in the memory. Hence, in the subsequent phase, the area corresponding to each of the eight bits in the target word was selected from every image in Set 1. This area was then compared with its two respective templates. The template that exhibited the greatest similarity to the selected area in the image was predicted to represent the value of the bit in that image.

To compare the similarity between images, the Structural Similarity Index (SSIM) technique was employed. A part of the image corresponding to the bit of interest was compared with the two templates using SSIM method. The template yielding a higher SSIM value, when compared with the photon emission image, defined the value of that particular bit. Applying this approach, the bit values of the target word could be predicted with an average accuracy of 97.86%. In certain instances, for specific bits, the prediction accuracy reached 100%, underscoring the effectiveness of the method even when images were captured using 10x objective lenses.

In the next stage, the process of generating templates for each bit value was tweaked; instead of using the average of all 1280 images corresponding to a bit value, a single image representing each bit value was used as a template. The process of comparing the photon emission images with these templates was repeated, utilizing the SSIM method once again. This revised approach successfully revealed the bit content in SRAM with 94.32% accuracy percentage, indicating the robustness of this method even when employing a more simplified template. Other image similarity measurement techniques, such as Mean Squared Error (MSE), cross-correlation, and Pearson correlation, were also used for comparison purposes. However, the SSIM technique had the best success rate for predicting the unknown bit value of the target word. Table 4.2 provides a comparison of different methods for the correct prediction of unknown bits for both approaches to creating templates. For the average template, all available 1280 images were averaged. Conversely, for the single image template, only one image was selected from the available 1280 images to serve as the template.

In another variation of the approach, the templates generated for one bit were also used for the other bits of the target row. For instance, the template generated for bit 3 was used as the template for all the bits in the target word. Employing the SSIM method, the bit values were deciphered with an accuracy of around 80% in these cases. This further demonstrates the effectiveness of this method, even when a single bit template is generalized for all the bits. This finding demonstrates that lower magnification images can still be utilized to reveal sensitive information, like finding the content of a bit, through photon emission analysis and image processing techniques.

Table 4.2: Percentage of correctly revealed cell values using different image measurement techniques, utilizing both average and single image for templates.

Method	Average image	single image
SSIM	97.87	94.32
MSE	97	79
Pearson Correlation	84.86	77
Cross Correlation	52.75	57.63

Upon applying the SSIM method to Image Sets 2 and 3, there was a decrease in the accuracy of predicting the unknown bit values compared to Image Set 1, resulting in the inability to accurately reveal the bit values. This decrease in accuracy is likely due to similar issues that affected the efficacy of the differential analysis on Image Set 3.

In conclusion, the SSIM method managed to achieve high prediction accuracy for deciphering unknown bit values in the image set 1. However, its performance faltered for image sets 2 and 3 due to added complexities introduced in these sets, such as precise alignment issues. A more detailed examination and potential optimization of the image processing techniques may be necessary to improve prediction accuracy in scenarios with increased complexity.

4.5 Experiment with Industrial Thinning

The photon emissions recorded in the previous steps were from a PIC microcontroller that was de-packaged using our in-house CNC machine without thinning the chip. It is known that thinning the chip can result in less photon emission being absorbed in the substrate, thereby increasing the SNR of the recorded photon emissions. As such, in the next step, a thinned microcontroller was used for recording photon emissions. The chip was sent to one of our lab partners, who kindly thinned it using industrial machines. The goal was to repeat the process used for the previous unthinned chip, this time with the thinned chip, and compare the results. The recording of photon emissions for data set 3 began, where one target word changed through all its possible 256 values from 0 to 255, while the other words in the row changed randomly. Unfortunately, the two available chips stopped working unexpectedly in the middle of recording photon emissions, and it was not possible to complete the experiment.

4.6 Summary

This chapter investigated the quiescent photon emission of an SRAM block within a PIC16F687 chip using a low-cost setup. Spatially-resolved images were recorded with a time integration of approximately one second. Initially, the physical location of bytes within the entire SRAM and the bitmap within one row were examined using the recorded quiescent photon emission. A similar investigation was previously conducted on an AVR chip using switching photon emissions [66].

The patterns of quiescent photon emissions for different values of the SRAM cell were discernible to the naked eye with a brief integration time of one second. The approach mirrored that of [32], but with updated pattern corrections. In contrast,[25] was able to identify the pattern of quiescent photon emissions after eight hours of recording. Moreover, the switching photon emission pattern of SRAM cells for different chips was previously investigated visually using expensive devices [36][111].

In previous studies, the patterns and contents of SRAM cells were revealed only when they were visually discernible [32][25][36]. However, in this research, the SSIM image processing metric was employed to reveal the SRAM content when the photon emissions were not visible to the naked eye. This approach achieved a 97.86% accuracy rate.

A Pearson correlation attack was previously conducted [51] using temporal switching photon emissions on several bits of inverter drivers, but not the SRAM cells themselves. The attack successfully reduced the number of possible keys to approximately 2^{48}, making brute force a viable option. In contrast, this chapter demonstrates that a correlation attack on the sum of intensities for a target row could reveal the AES key directly. This attack was successful even when all other bytes in the row were randomly changing.

Difference of mean analysis has been previously applied to temporal switching photon emissions to recover part or all of the key [29][51]. Moreover, difference analysis has been employed to reduce background noise from the switching photon emissions in several studies [32][25][66], aiding in identifying changes in SRAM cells. In previous research, [111] was able to identify the location of changes in SRAM using switching photon emission. In this chapter, difference of mean analysis on quiescent photon emission is utilized to identify the location of individual SRAM cells when such locations cannot be visually distinguished.

Chapter 5

Investigating Photon Emission of Memory Blocks in the FE310-G002 RISC-V Chip

In this chapter, the photon emissions of the data memory in a chip with the RISC-V ISA are investigated for the first time. The investigation is conducted on the FE310-G002 RISC-V chip, with the primary goal of evaluating the feasibility of extracting information from its photon emissions. Given the limited knowledge we had about the location of the data memory block and the chip's photon emissions, a step-by-step experimental procedure is carried out on the chip. Based on the results derived from analyzing the photon emission of each experimental phase, the details of the next phase are determined. Unlike the previous chapter 4, this section examines the switching photon emissions from SRAM during its continuous access. Additionally, the photon emissions from components other than SRAM cells, such as column/row detectors, are also explored.

This chapter discusses the procedures employed to capture and analyze the photon emission patterns of memory blocks within the FE310-G002 chip, as well as the implications these patterns have on the device's security.

5.1 Investigating Photon Emission of the Entire Chip

To gain an initial understanding of the location of different structures within the chip, a backside image of the chip with illumination was used. Figure 5.1 shows a backside

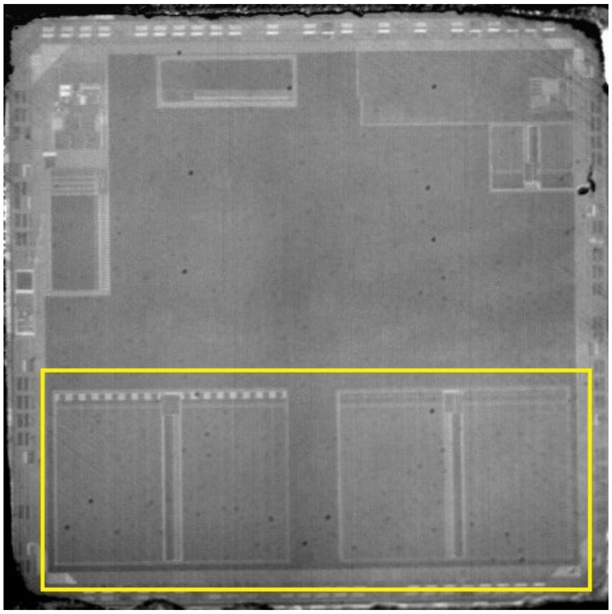


Figure 5.1: Backside image of the FE310-G002 RISC-V chip, with the hypothesized memory blocks highlighted.

image of the silicon die of the chip, captured using the MHAB-100W-IR illuminator [5]. The highlighted blocks in the figure are hypothesized to represent the 16 KiB 2-way set-associative L1 Instruction Cache and the 16 KiB data memory block, which are the blocks of interest for photon emission investigation. To confirm the hypothesis that the highlighted blocks are related to memory and instruction cache blocks, the photon emissions of these blocks will be analyzed in the next session under various scenarios in which the chip accesses the data memory.

In the initial phase of the experiment, the photon emission of the entire chip was examined under nominal voltage conditions while executing a simple code. The primary objective of this phase was to identify whether any chip components exhibited photon emissions under nominal voltage. To examine the chip in nominal voltage condition, it was supplied with voltage of 1.8V for the logic core (VDD) and 3.3V for the analog portion (AVDD). The chip also employed its default clock frequency, which consisted of an internal trimmable high-frequency ring oscillator operating at 13.8 MHz. During the experiment, the chip executed a code designed to set all bits in the data memory block to one, followed by an infinite loop of NOP (no-operation instruction). A segment of the code used for photon emission investigation of the chip in nominal voltage can be found in Code Listing

1. Photon emissions of the chip while executing the infinite NOP loop were captured using a 10x objective lens and a 1-second integration time. Upon examining the recorded images, it was observed that under nominal voltage conditions, only a small region on the upper surface of the chip exhibited photon emissions.

```
"li x27,0x80000000\n"     //Define DATA Memory Base
"li x26,0x80004000\n"     //Define end of DATA Memory
"li x25,0x80000000\n"     //DATA Memory Pointer initialized with the base
"li x24,0xFFFFFFFF\n"     //Data word with all 1s
"LOOP:\n"                //Loop Label
"sw x24,0(x25)\n"         //Store data to the data Memory word
"addi x25, x25, 4\n"      //Increase the data Memory address by 4, for
                            //next word
"bne x25,x26,LOOP\n"      //keep in loop until counter is 0

"WHILE_1:\n"                  //Infinite loop
"NOP\n"       //nop
"j WHILE_1\n"
```

Listing 5.1: Part of code number 1 for RISC-V chip experiment

In the next phase of the experiment, the logic core voltage (VDD) gradually increased, and the changes in photon emission of the entire chip were observed at varying voltage levels. The objective of this phase was to determine whether other locations on the chip, particularly the hypothesized memory blocks, would emit photons at higher voltages. To increase the logic core voltage from the nominal voltage, the VDD of the chip was disconnected from the voltage regulator (1.8V) and connected directly to a power supply instead. The voltage VDD was progressively increased, while the photon emission from different locations on the chip was recorded using a 10x objective and a 5-second integration time.

Observing the recorded image, it was revealed that as the digital voltage core of the chip increased from nominal value, additional locations on the chip began to exhibit photon emissions. At a voltage of 2V, the upper portions of the block on the right side started emitting photons, while no visible emissions were observed in the left block. As the voltage continued to increase, the photon emission of the right block became more distinct, and at 3.8V, its photon emission was clearly visible. Figure 5.2 illustrates the overall chip photon emission while Code 1 was running with a logic core voltage of 3.8V and an integration time of 5 seconds. Since the lens allowed for the viewing of only a small section of the chip, the chip was slightly shifted after each observation to cover all areas and finally various locations on the chip were stitched together to create the figure.

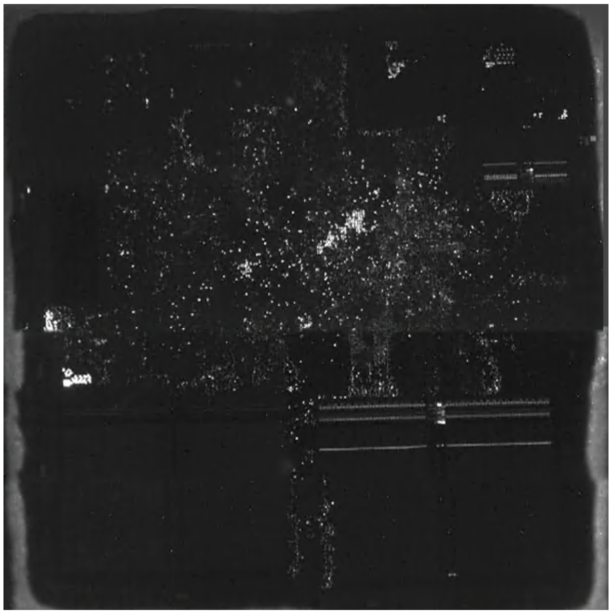


Figure 5.2: Photon emission across the entire chip, captured while utilizing Code 1.

5.2 Photon Emission of Memory Blocks

The subsequent phase of the photon emission experiment focused on observing the photon emission of the hypothesized memory blocks while executing different instructions in an infinite loop for each test. The objective of this phase was to identify any changes in the photon emission of the observed blocks due to these varying instructions and to gather pertinent information about the target blocks in order to verify our assumptions that these blocks are related to memory and instruction cache blocks. To this end, the FE310-G002 RISC-V chip was subjected to various code scenarios, each running an infinite loop with distinct actions performed within it. These actions included loading data into registers, reading data from data memory, storing information in data memory, or simply executing no-operation instructions. During the execution of each code on the chip, the photon emission of the corresponding blocks was recorded.

The analysis of the recorded photon images demonstrated that when the infinite loop involved load/store operations performed on the data memory, both the left-side and right-side blocks emitted photons. In contrast, when the loop did not involve data memory usage and only executed operations such as loading into registers, no photon emissions were detected from the left-side block. This observation suggests that the left-side block is likely

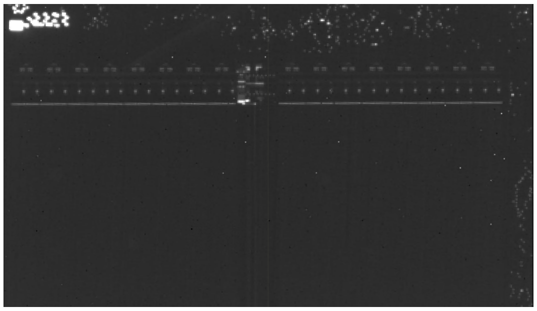


Figure 5.3: Photon emissions captured in the upper section of the data memory block.

associated with the 16 KiB data memory and exhibits photon emissions when the instructions involve memory access. On the other hand, the right-side blocks, which consistently emitted photons across all scenarios, might be linked to the 16 KiB Instruction Cache. Furthermore, it can be reasonably concluded that the phenomenon of block illumination, observed when the chip continuously executes load or store operations on the data memory block within an infinite loop, is primarily attributed to the switching activity occurring in the transistors. Figure 5.3 depicts the photon emissions of the upper part of the data memory block when the code repeatedly loads a data memory address into a register. The photon emission was recorded with a voltage of 3.8V and an integration time of 5 seconds. Due to the limited field of view of the microscope, the photon emissions of the blocks were captured using a 10x objective lens in two steps, and the images were then combined to provide a comprehensive view of the upper side of the block. As can be seen in Figure 5.3, the data memory consists of two sides, with some areas in the data memory clearly illuminated.

To further investigate the left-side blocks and validate the hypothesis that they represent the 16 KiB data memory blocks, the photon emissions of these blocks were captured while targeting different word addresses in the data memory. This was accomplished using Code 2, a segment of which is displayed in Code Listing 2. In this code, a word in the data memory was targeted. The content of the data memory, starting from the target word to 15 words after it, was filled with the value "0xFFFFFFFF". Within the infinite loop, the value of the targeted word was continuously loaded into a register. The photon emissions of the blocks were recorded using a 10x objective lens and an integration time of 5 seconds for each different targeted word address.

To conduct the experiments, the first word of the data memory at address 0x80000000 (TW_{00}) was selected as the initial target word, and its corresponding photon emission was captured. Following this, the target address was incremented by four to target the subsequent word (TW_{01}), and the photon emission for the new address was recorded. This procedure was conducted repeatedly to document the photon emissions associated with targeting consecutive words within the data memory.

```
"li x20,0x80000000\n"      //DATA RAM Pointer initialized with the base
"li x21,0xFFFFFFFF\n"      //Data  word All 1s
"sw x21,0(x20)\n"          //store data in one row
"sw x21,4(x20)\n"
"sw x21,8(x20)\n"
"sw x21,12(x20)\n"
"sw x21,16(x20)\n"
"sw x21,20(x20)\n"
"sw x21,24(x20)\n"
"sw x21,28(x20)\n"
"sw x21,32(x20)\n"
"sw x21,36(x20)\n"
"sw x21,40(x20)\n"
"sw x21,44(x20)\n"
"sw x21,48(x20)\n"
"sw x21,52(x20)\n"
"sw x21,56(x20)\n"
"sw x21,60(x20)\n"

"WHILE_1:\n"                    //Infinite loop
"lw x22,0(x20)\n"
"j WHILE_1\n"
```

Listing 5.2: Part of code number 2 for investigating the photon emission of data memory at different addresses

Upon recording the photon emissions of the left blocks using Code 2 while targeting different memory addresses, it was observed that the emissions from certain locations varied depending on the accessed address. This observation confirmed the hypothesis that the left blocks represent the 16 KiB data memory blocks. Furthermore, for the first 16 consecutive words, a single line within the block was illuminated. However, for the subsequent 16 words, the location of the lit line shifted slightly lower, with the same pattern continuing for the next set of 16 words. Thus, it can be concluded that the illuminated line corresponds to the location of the targeted word address in the data memory, where each line comprises 16 words or 64 bytes. When a word in memory is targeted, all rows containing the target word will light up. Consequently, for 16 consecutive words located in one row, the location of the lit-up row remains constant, and then it moves to the location of the next row for the following 16 words.

Upon further examination of the photon emissions for all 16 consecutive words in a

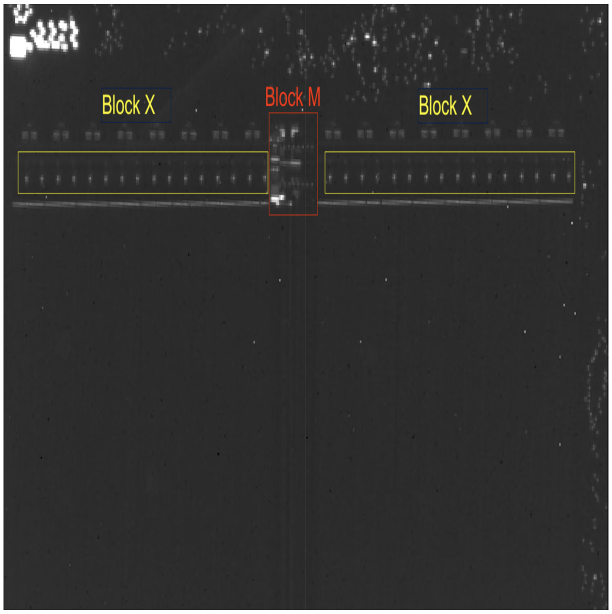
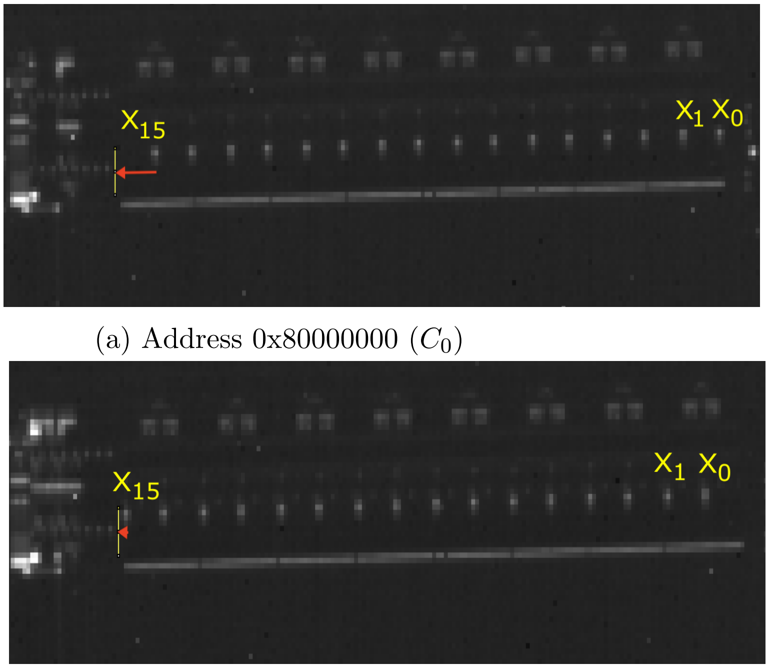


Figure 5.4: Photon emission from the data memory block, pinpointing the locations of changes for different word addresses within a row.

single row of the data memory, it was observed that the photon emissions from certain locations in the upper level of the memory changed for each word address. Figure 5.4 presents the photon emission of the upper side of the data memory block, highlighting the locations where the photon emission varied for different word addresses within a fixed row. One of the highlighted locations is denoted as Block X, which consists of 32 smaller subblocks named X_0 to X_{31}. By comparing the photon emissions of different target words in a row, it was observed that the positions of each smaller subblock differ for the 16 distinct words within the same row. Figure 5.5 displays the photon emission from subblocks X_0 to X_{15} for two different addresses within a row, captured using a 10x objective lens. The change in position for the smaller subblock X_{15} for two addresses is highlighted in the figure. Based on the observation of photon emissions in block X, it can be concluded that each of the 32 subblocks X_i can be associated with a single bit in the 32-bit target word. For different target words in the same row, the column position of the target word differs, resulting in a corresponding shift in the location of photon emissions related to each subblock X_i.

The observation of recorded images also revealed that, apart from Block X, there is a noticeable change in the photon emission patterns of another block, referred to as Block



(a) Address 0x80000000 (C_0)

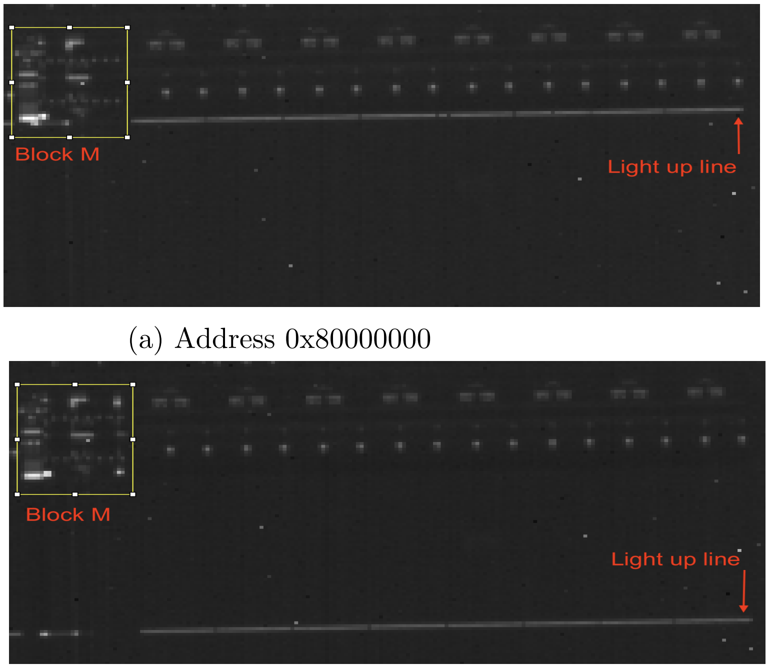
(b) Address 0x8000003C (C_{16})

Figure 5.5: photon emission from subblocks X_0 to X_{15} for a target word at two distinct addresses within a row.

M. It is possible that Blocks M and X are associated with the column detectors and decoding circuitry within the data memory. Further investigations will be carried out to examine these blocks and ascertain their specific roles.

In the previous step of the experiment, the photon emission of target words in a single row but different columns were investigated. To explore further, the photon emission of target words in the same column but different rows was investigated in the subsequent step. Therefore, the target memory address was incremented by 64 bytes, starting from the initial address of the memory block. As each line in data memory consists of 64 bytes, these new target addresses correspond to the first word (column C_0) of each line. Hence, for all target addresses, only the rows changed while the columns remained constant. The photon emission related to each address was recorded.

Upon comparing the photon emission of these images, it was observed that the location of the lit-up line shifted to a lower position with each new address, which is consistent with the previous finding that the lit-up line is related to the illumination of the row with the



(a) Address 0x80000000

(b) Address 0x80001000

Figure 5.6: Photon emissions from the right side of the data memory block for a target word, contrasting two different row addresses.

target word located in it. Figure 5.6 shows the photon emission of two different addresses captured using a 10x objective lens in the right side of the data memory block.

Furthermore, it was observed that there were alterations not only in the position of the illuminated line but also in the upper region of the data memory blocks, Block M. These alterations in photon emission could be attributed to the row decoder of the data memory and were highlighted in Figure 5.6.

5.3 Investigating Photon Emission of Column and Row Detectors with 50x Lens

By comparing the changes in the location of photon emission in Figures 5.4 and 5.6, it becomes evident that the photon emission of block M is influenced by alterations in both rows and columns of the target word address. In contrast, block X only exhibits modifications due to changes in the columns of the target word address. This finding implies that words in different rows but sharing the same column demonstrate similar photon emissions in block X. As a result, the next step will involve a more in-depth investigation of the photon emissions in these blocks.

To better understand the potential relationship in blocks M and X, their photon emissions for different addresses will be examined using a 50x objective lens. This higher magnification will provide a more comprehensive insight into the row and column detectors within the chip, potentially guiding future research and security measures. During this analysis, the chip will be placed under the 50x objective lens of a microscope, allowing for the observation of block M and some subblocks within X, such as X_{15} and X_{14}.

5.3.1 Exploring Photon Emission of Column/Row Decoder: Reading a Word from Data Memory

In the initial phase of examining blocks M and X with a 50x objective lens, different addresses in the data memory were individually targeted by loading from the respective addresses. The corresponding photon emissions were then recorded. The goal of this phase was to investigate the photon emissions of blocks M and X while accessing words from various rows and columns. This investigation helps to discern any relationships between the targeted word address and the observed emissions.

The experiment was conducted using the previously mentioned Code 2. A single row was chosen, and the addresses of all 16 words within that row were sequentially targeted. Subsequently, addresses for words in various rows were also targeted. At each step, the photon emission associated with each targeted word was recorded. Figure 5.7 illustrates the photon emissions of both block M and a portion of block X (specifically, subblocks X_{15} and X_{14}) when observed through a 50x objective lens for a target address of 0x80002224.

In the first step of analyzing the recorded images from the experiment, the photon emission of subblock X_{15} was examined. Figure 5.8 illustrates the photon emission for subblock X_{15} for two different target words in a row. Subblock X_{15} is highlighted in the figure, and the change in location is depicted by an arrow. The images demonstrate that subblock X_{15} consists of two smaller parts, labeled as H_{15} and L_{15}.

An analysis of the changes in the location of photon emissions of the lower part (L_{15}) for different words in a row revealed that every two consecutive words share the same position. Then, for the next two consecutive words, the location of (L_{15}) photon emissions moves slightly to the left to a new position. In contrast, the location of the other part

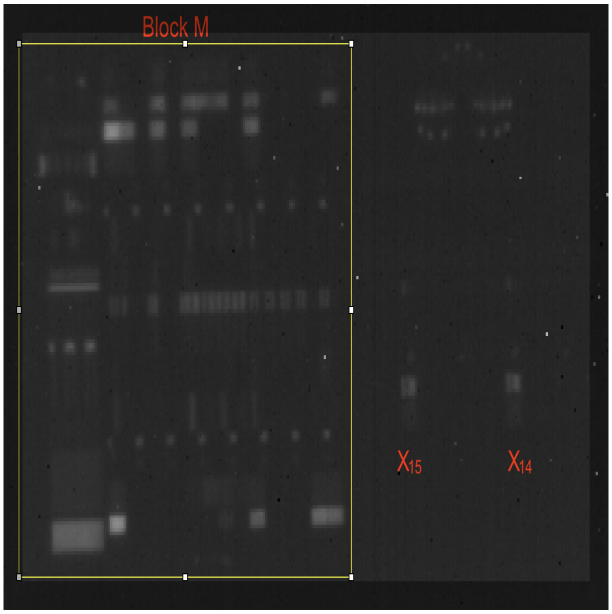
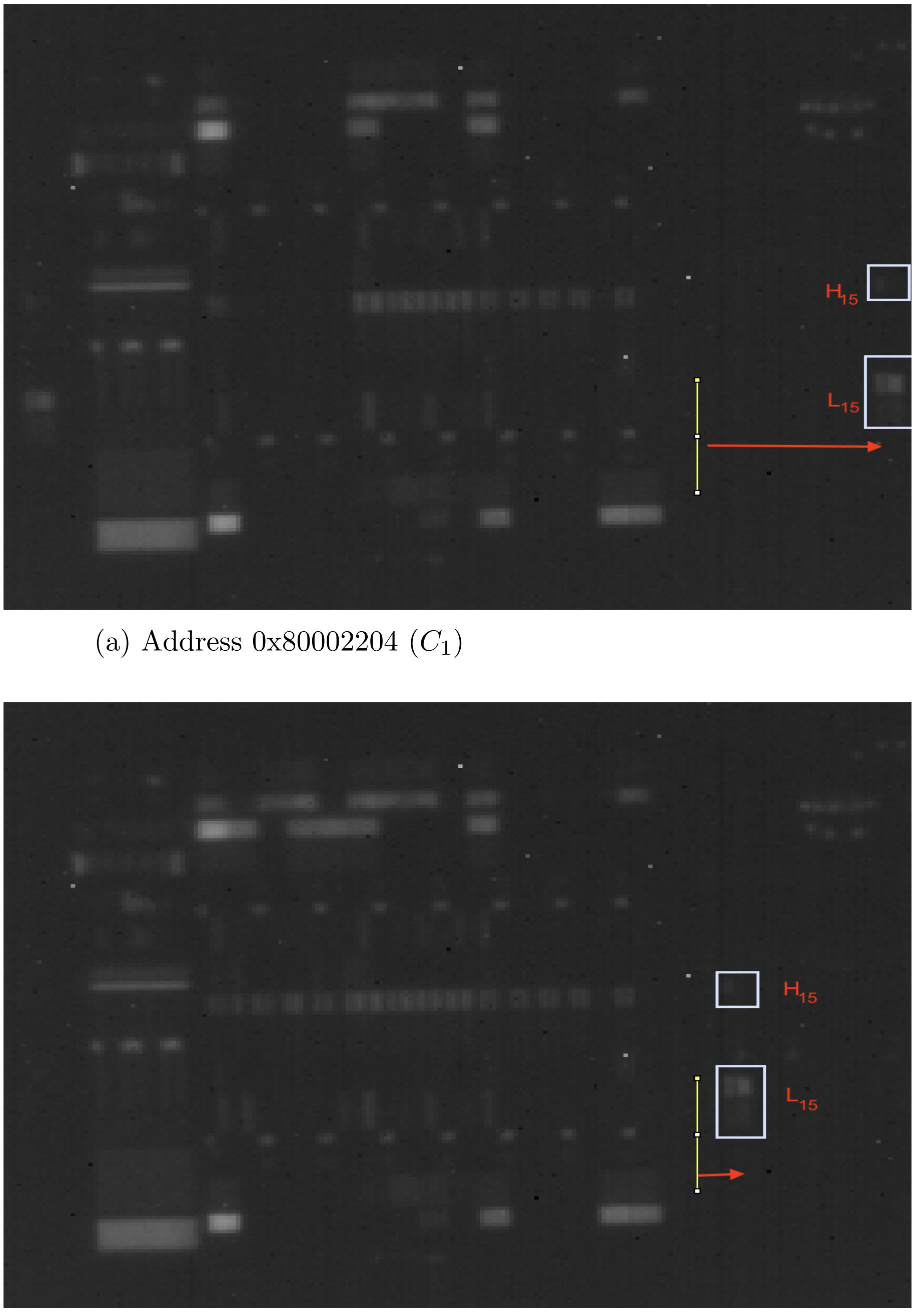


Figure 5.7: Photon emission from block M and subblocks X_{15} and X_{14} for the target address, captured using a 50x objective.

(H_{15}) changes for every different word in the row. However, the photon emissions from the H are not particularly strong and may be challenging to identify, while the L exhibits easily recognizable photon emissions. Thus, by analyzing the photon emissions of L and utilizing the location of the photon emissions, the targeted group of two consecutive words in the row can be determined. Furthermore, by observing the photon emissions of block X for targeted words in different rows but the same column, it is evident that the photon emission of Block X for these target words is similar. This finding is consistent with previous observations that the location and photon emission of Block X differ only for different columns. Figure 5.9 shows the repeating location patterns for subblock X_i for all 16 words in a row.

In the subsequent phase of the analysis of images, the photon emissions from block M were examined. The photon emissions of all words in a fixed row were observed to identify any patterns in the changes of photon emissions when the column changes and the row remains fixed. The locations where the photon emission changed were identified and highlighted in red in Figure 5.10. Analyzing the photon emissions of words located in a row for some other rows revealed the same consistency.

To further understand the phenomenon, the photon emissions of target addresses with



(a) Address 0x80002204 (C_1)

(b) Address 0x80002234 (C_{14})

Figure 5.8: Photon emission from subblock X_{15} for a target word, contrasting two different column addresses, captured using a 50x objective.

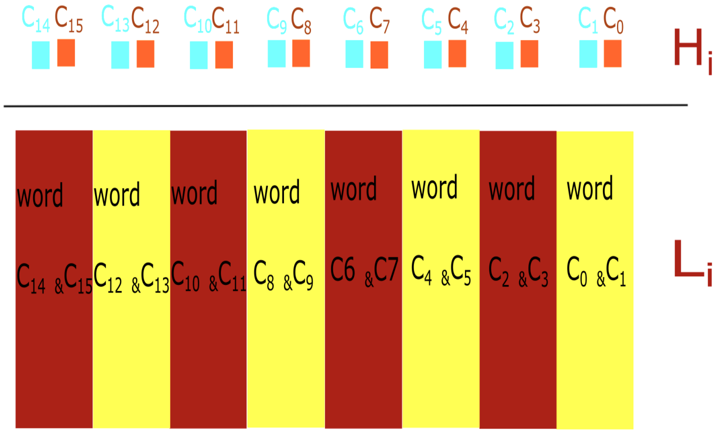


Figure 5.9: The photon emission pattern for subblock X_i, showcasing bit i from all 16 words within a row.

the same column but different rows were analyzed. This was done to identify patterns in the changes of photon emissions when the row changed, and the column remained fixed. The analysis of these images revealed that the photon emission of some blocks changed for words with different rows but a fixed column, which was highlighted in blue in Figure 5.10. To confirm the accuracy of the findings, the same process was repeated for several other columns.

Based on the observations and analysis of the images in Figure 5.10, it can be seen that there is a location labeled block A, which exhibits changes in photon emission only with a change in columns. The photon emissions of block A for two words with different rows but the same column have the same photon emission pattern. On the other hand, the other block labeled as block B display changes only when the row of the target word is altered. blocks C and D, however, show photon emission changes when there is a change in either columns or rows. Therefore, it is possible to identify a pattern for the targeted column by observing the photon emission in Block A, while the observation of photon emissions in Block B may assist in finding the target row.

Observing the photon emission of addresses with different columns confirms the hypothesis for Block A. A discernible pattern for photon emission can be observed in each column of Block A. Based on this pattern, it can confirm which column is targeted. Figure 5.11 displays the pattern for each column. Therefore, if two different addresses have the

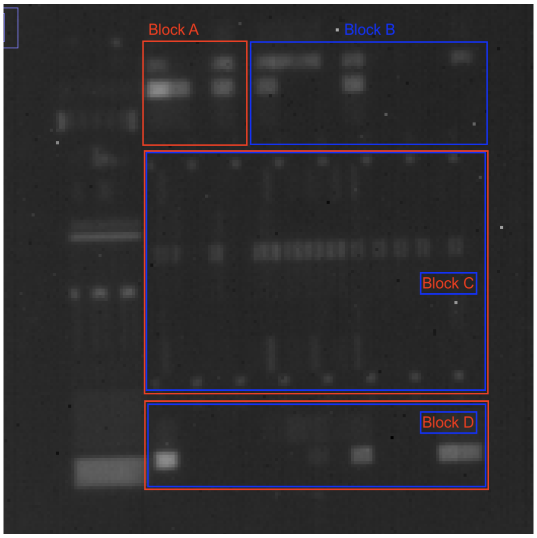


Figure 5.10: Photon emission from Block M for reading a target word, with changes in emission locations highlighted; red indicates the locations of column changes, while blue marks the locations of row changes.

same column, their photon emissions in Block A will be the same, as shown by the pattern in Figure 5.11.

Analyzing the photon emission of consecutive rows in Block B shows that a pattern for the targeted row exists. However, these results show that the row detector in Block B is more complex compared to the column detector in Block A, and it requires a more detailed analysis to determine the targeted row.

Upon observing the photon emissions in Block B, it was found to be composed of three smaller blocks, which are named B_1, B_2, and B_3, as shown in Figure 5.12. The accessible data block address range of the chip is from 0x8000000 to 0x8003FFF, with 256 rows, each containing 64 bytes. Therefore, the row detector changes for every 0x40 address. Upon observing the photon emission of all 256 consecutive rows, the following results were obtained:

- Block B_1 exhibited a total of 8 different patterns, with photon emissions changing for every consecutive row. After the 8th row, the pattern repeated.
- Block B_2 had 8 different patterns, with photon emissions changing after every 8 consecutive rows. After 64 consecutive rows, the pattern repeated.

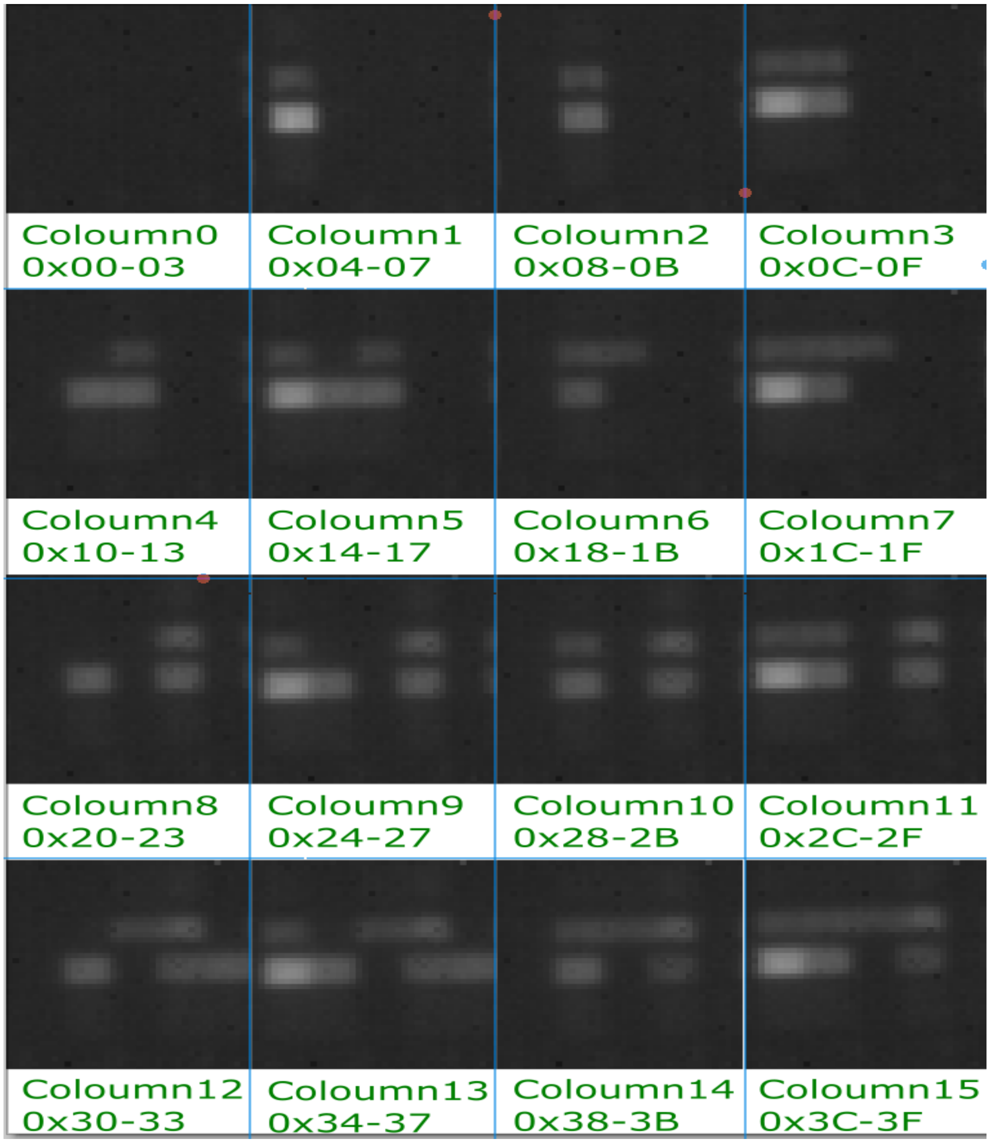


Figure 5.11: Photon emission pattern from block A, differing across various columns.

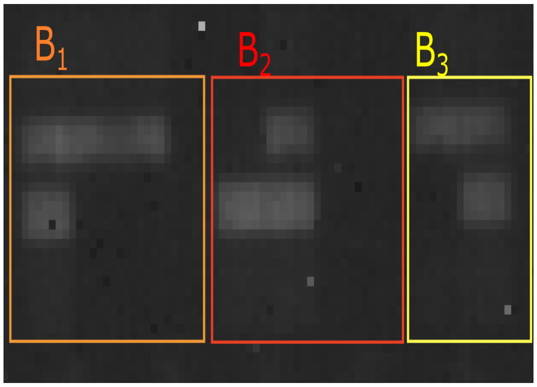


Figure 5.12: Photon emission from block B for the target address, with three smaller sub-blocks within block B distinctly highlighted.

- Block B_3 had 4 different patterns, with photon emissions changing after every 64 consecutive rows, until it reached the end of the accessible range of data memory.

Figure 5.13 illustrates the changes in photon emission for all 256 rows in data block B. This figure provides a visual representation of the repeating patterns of photon emissions observed in Block B, which can be used to identify the targeted row.

Upon analyzing Figure 5.13, it can be observed that all 256 rows can be classified into 4 groups, each with a unique photon emission pattern in Block B_3. Each pattern covers 64 rows. Figure 5.14 illustrates the 4 different patterns for Block B_3 and the memory address range covered by each pattern. Each of these 4 groups can be further divided into 8 smaller sub-groups, each with a distinct photon emission pattern in Block B_2. Figure 5.15 illustrates the photon emission patterns for Block B_2. Finally, each of these sub-groups can be divided into 8 even smaller groups, each containing a single row of memory data in Block B_1. Figure 5.16 shows the photon emission patterns for Block B_1. In the B_1 pattern, it can be observed that the photon emission patterns for five different addresses are identical, making it impossible to distinguish between them. However, these five addresses exhibit unique photon emission patterns in blocks C and D. The distinct photon emission patterns for blocks C and D can be utilized to accurately determine the exact address among the five addresses in question.

This information reveals that by examining the photon emission pattern of blocks A and B using a 50x objective, it is feasible to determine the targeted word whose content is being continuously read in a loop.

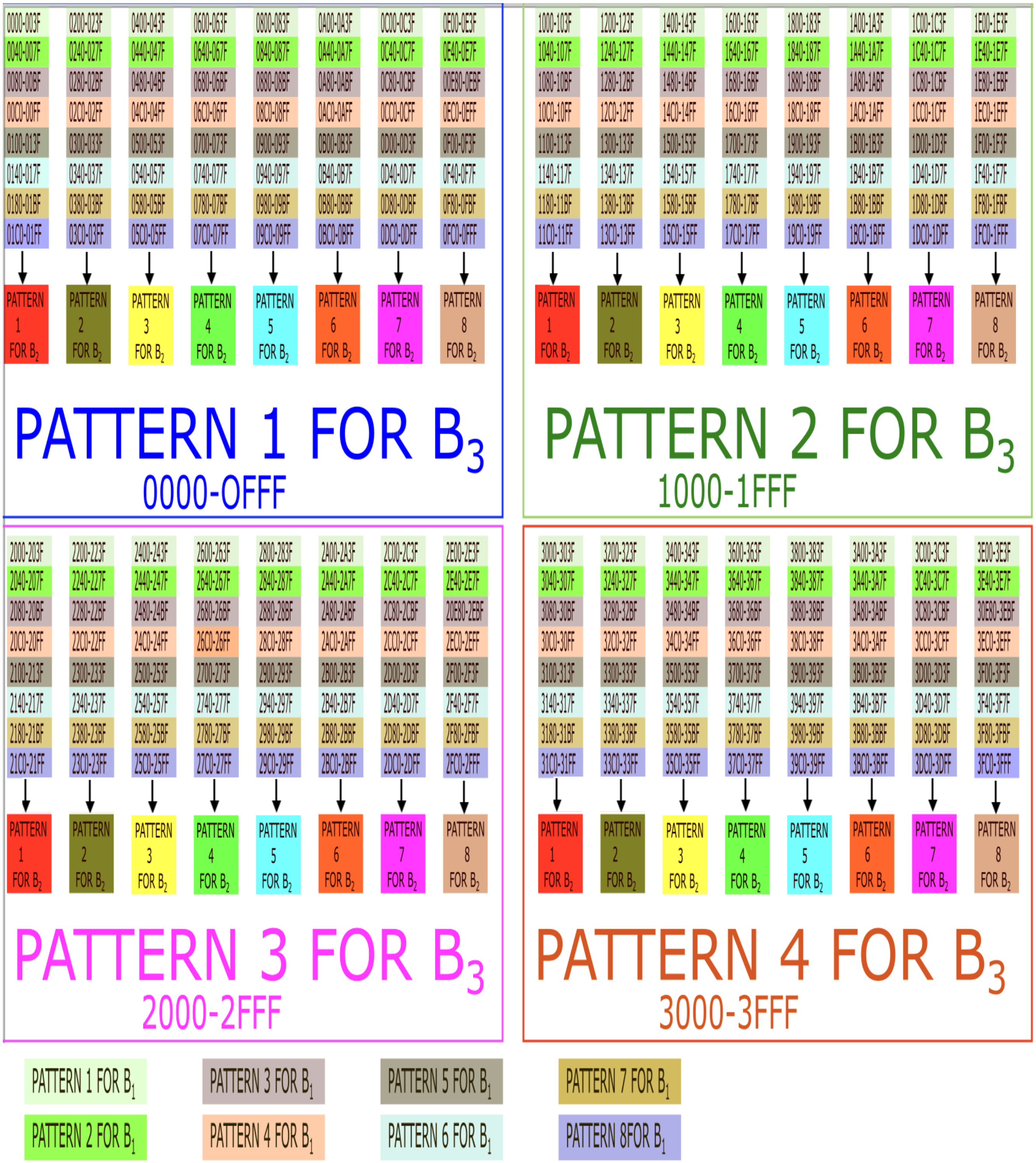


Figure 5.13: Photon emission pattern for block B, encompassing all 256 distinct rows.

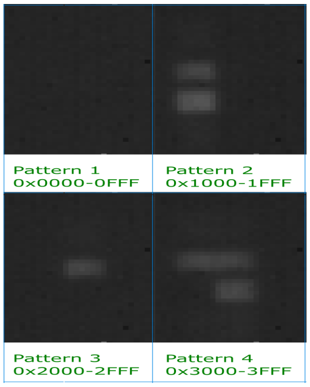


Figure 5.14: Photon emission pattern in B_3, with corresponding addresses illustrated within the pattern.

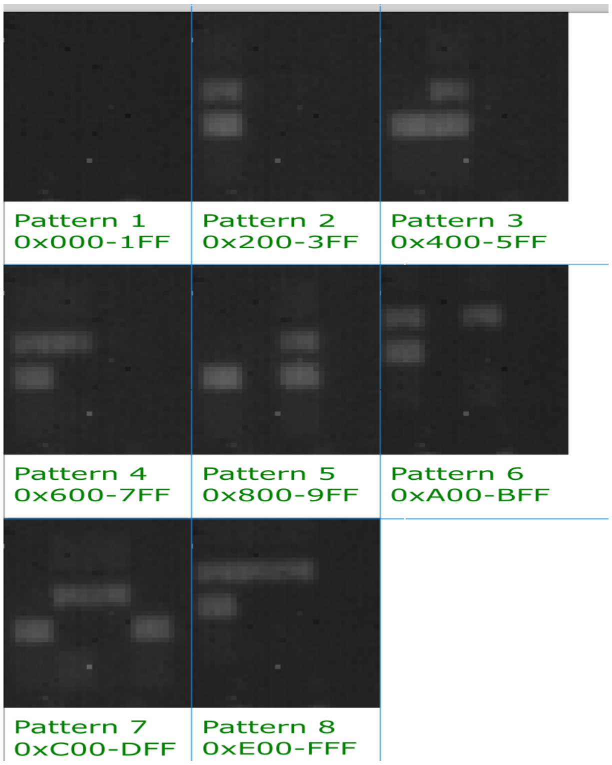


Figure 5.15: Photon emission pattern in B_2, showcasing periodicity as addresses repeat every 0x1000 bytes.

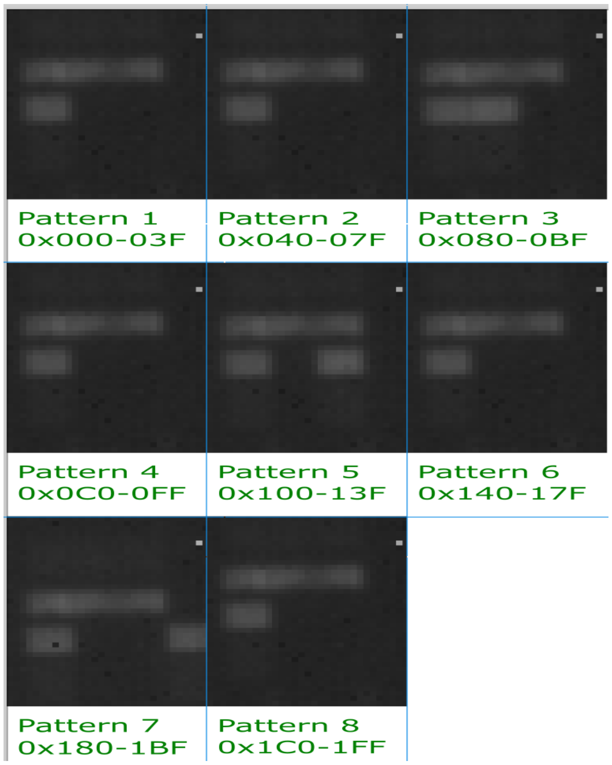


Figure 5.16: Photon emission pattern in B_1, showcasing periodicity as addresses repeat every 0x200 bytes.

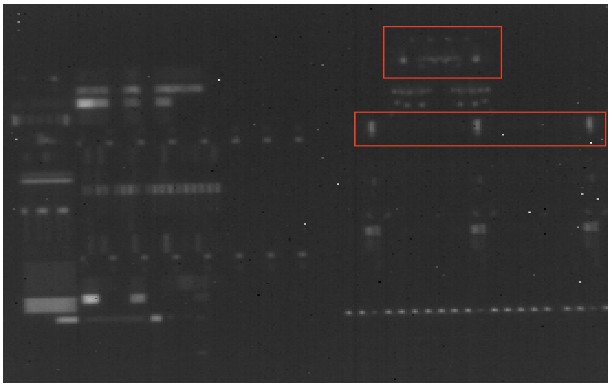


Figure 5.17: Photon emissions from block M and part of block X (subblocks X_{13} to X_{15}) during the execution of the store word instruction, with differences highlighted when compared to the load word instruction.

5.3.2 Exploring Photon Emission of Column/Row Decoder: Writing a Word to Data Memory

This section aims to observe the photon emissions of block M and block X when writing to data memory and to assess the consistency of findings for row and column detectors. The "load word" instruction in the infinite loop of Code 2 was replaced with a "store word" instruction (sw), causing a value of all 1s to be stored in the targeted word in the infinite loop. The photon emissions of the chip with this code were recorded for different target addresses, including words with different columns and rows, to check the consistency of the photon emissions of the targeted words in the blocks X and M for the "store" instructions with the patterns found for the "load" instructions.

Figure 5.17 presents the photon emissions from Block M and a part of Block X (specifically, subblocks X_{13} to X_{15}) for the store word instruction at target address 0x8000002C, captured using a 50x objective lens. A comparison of the photon emissions of different addresses indicates that the patterns for Blocks A and B for the store instruction are similar to those found for the load word instruction in the previous section 5.3.1.

After examining the locations related to subblock X_{13} to X_{15}, it was found that the locations of photon emissions based on their column for the store instruction were the same as those for the load instruction. However, some locations above subblocks X_{13} to X_{15} display photon emissions that were not present during the load word instruction execution. These locations are highlighted in Figure 5.17 and will be further investigated in Section 5.5.2.

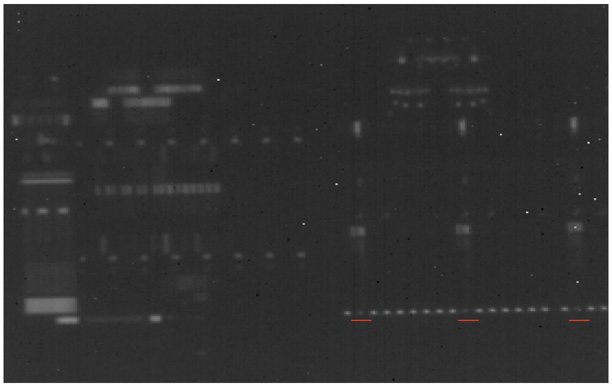


Figure 5.18: Photon emissions from block M and part of block X (subblocks X_{13} to X_{15}) during the execution of the store word instruction, emphasizing the dimmer photon emission locations.

It was observed that in the lit-up row, 32 small pixels displayed dimmer photon emissions. Upon examining the photon emissions of all the targeted words in a fixed row, it was noticed that the location of these dimmer pixels in the lit-up row changed according to the targeted column. Figure 5.18 highlights the dimmer pixels of the lit-up row for address 0x80000030. It is highly likely that these pixels correspond to the photon emissions of the bits for the targeted word, which receive the new value during the store instruction.

5.3.3 Exploring Photon Emission of Column/Row Decoder: Accessing Byte or Half Word

In the next step, the same process will be repeated for other data memory-related instructions that target Byte or half word instead of an entire word, to determine if the patterns are consistent with previous findings. In the first step, the load byte will be replaced in the previous Code 2, and the photon emissions of Block M and part of Block X for different addresses will be recorded with 50x objective lens.

Upon examining the photon emissions of different target bytes, it was observed that the photon emissions of all four bytes in a word were the same in both Block M and Block X. Figure 5.19 shows the photon emissions of Block M and subBlock X_{15} with the lb instruction in address 0x80000009, using 50x objectives.

After analyzing the photon emission patterns for different columns and words, it was found that the pattern of photon emissions for the load byte in Block A and subblocks

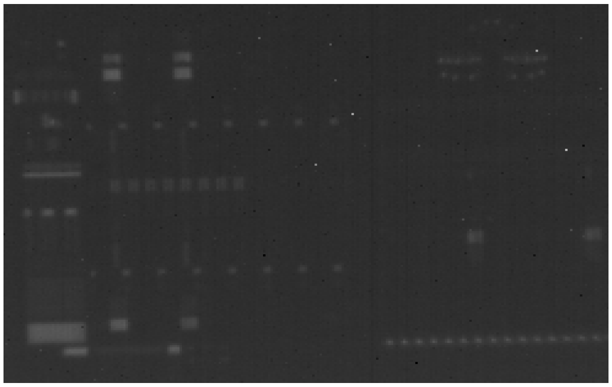


Figure 5.19: Photon emissions from block M and part of block X (subBlock X_{15}) during the execution of the load byte instruction for address 0x80000009.

B_2, and B_3 were similar to the load word and store word patterns. However, subblock B_1 exhibited some differences in the photon emission pattern compared to the previous cases. Despite the load/store word having photon emissions in one location in addition to the pattern of subblock B_1 for the load byte, the overall pattern is still consistent and the pattern exists. The photon emission pattern for subblock B_1 for the load byte is shown in Figure 5.20.

To investigate the photon emissions of Block M and Block X for other instructions, the lb instruction was changed to lbu, lh, and lhu for different addresses, and the photon emissions related to each code were recorded. It was observed that the photon emissions for all of these instructions were similar to those for the lb instruction.

In this section, first a specific address in the data memory was selected, and the contents of that address were loaded into a register in an infinite loop. The photon emission of Block M and part of Block X was then recorded using a 50x objective lens. By comparing the photon emissions of these blocks for many different data memory addresses, patterns in the photon emissions of the blocks were identified. Thus, by recording the photon emission of Block X and Block M for an unknown target word and matching it with the identified patterns, the address of the targeted word could be determined. The same results were obtained for other instructions related to accessing the data memory, such as sw, lb, lh, lhu, and lbu.

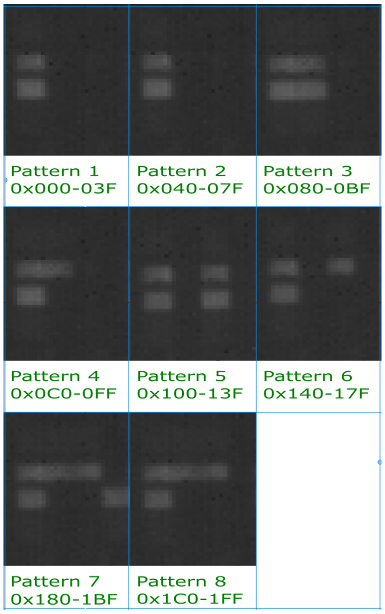


Figure 5.20: Photon emission pattern in subblock B_1 during the execution of the load byte instruction.

5.4 Revealing Targeted Column in Data Memory Using SSIM Technique

Thus far, the address of the targeted word has been identified by observing the photon emission of locations inside block M with a 50x objective lens and comparing it visually with the expected pattern. However, with a smaller objective such as 10x, related locations like Block A are less visible, and the pattern cannot be detected by the eye. In this section, the goal is to explore the feasibility of utilizing image processing metrics, such as SSIM, to discern the address of an unknown targeted word when the photon emission patterns are not readily discernible to the eye. This will be done using recorded photon emissions from locations within Block M, captured with a 10x objective lens. This technique could be particularly useful for chips with higher technology, where the transistor sizes are smaller and the patterns cannot be easily detected by the eye. By exploring this approach, the aim is to enhance the scalability of this side-channel attack and increase its applicability in the field of hardware security.

To achieve this, the steps from section 5.3.1 were repeated, but this time a 10x objective was used. Code 2 with the ”load word” instruction was used, and the target address in each step was changed to have different columns and rows. The corresponding photon emissions were recorded, and 308 images with different addresses were captured.

To test the approach, Block A was selected as it has the potential to reveal the targeted column from four different blocks (A, B, C, D). All images, recorded with varying addresses, were categorized based on their column value. From each set of columns with differing values, one image was randomly selected. The location of Block A in these images was then cropped to create a template for its corresponding column. For each of the remaining recorded images, the area corresponding to Block A was cropped and compared with the 16 column templates using SSIM. The column template that yielded the highest SSIM score with the image was predicted to represent the targeted column's number. The experiment was conducted using a total of 308 photon emission images, each representing distinct column values. Notably, these column values could assume one of 16 different possibilities. The approach was successful in predicting the accessed column with an accuracy rate of 93%. The same approach can be applied to the photon emissions of Block B to reveal the target row. However, the target row can also be detected by the location of the lit-up row. Consequently, it is feasible to identify the address of an unknown target by recording its photon emissions in both Blocks A and B, and by employing the SSIM method in situations where the photon emissions are not readily discernible to the eye.

This and the previous section demonstrate that by monitoring the photon emission of column and row detectors, the accessed memory address can be determined. Identifying the unknown access address in memory is crucial information and can be used to reveal more important details of the cryptographic algorithms executed on the device. For example, in the context of a known plaintext attack, the secret key utilized in an AES algorithm can be uncovered by knowing the data memory access address. By monitoring the accessed memory address during the first round of AES execution, the accessed S-box value can be determined. Based on the AES algorithm, as depicted in Figure 2.1, it can be inferred that knowing the plaintext and the S-box value enables the revelation of the round key for the first iteration. This could potentially lead to the discovery of the AES key.

5.5 Photon Emission Investigation for Variation in Content of Data Word

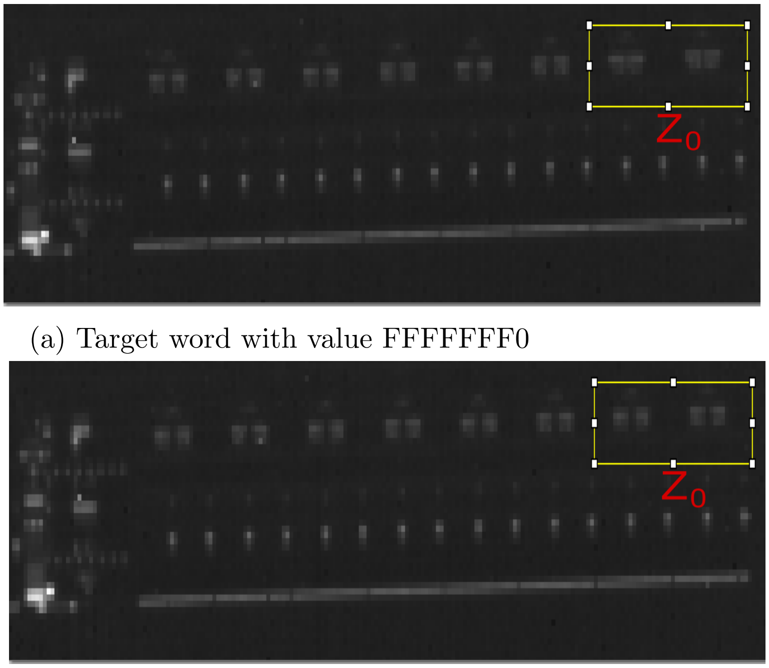
In the previous steps, the focus was on investigating the change in photon emission with variations in the target address while keeping the data in the address fixed. The goal of the next step is to explore how the photon emission changes with variations in the content of the data memory in a fixed address and identify any patterns that may emerge.

To begin, the photon emission was recorded using a 10x objective lens to observe the chip in a larger scope. In the next phase, a 50x objective lens will be used to observe the interested area in greater detail. The photon emission of data memory will be observed for both the read (load word) and write (store) actions to gain further insights into the underlying processes. By analyzing the patterns that emerge from these observations, a better understanding of the behavior of the chip and its performance under different conditions can be gained.

5.5.1 Investigation for Reading from Data Memory

The objective of this experiment was to investigate the relationship between photon emission and the content of a targeted word. To achieve this, Code 2 was modified with slight adjustments, as shown in code 3. The first word in the data memory address (0x80000000) was selected as the fixed address for the experiment. All the words in the first row, except for the first word, were filled with a value of 0xFFFFFFFF. However, the content of the first word was modified each time to have a different value. The first word was continuously loaded into a register using an infinite loop while the photon emission of the data memory was recorded. This process was repeated several times for different contents in the target word to observe any correlations with the photon emission.

Figure 5.21 presents the photon emissions for two specific values: ”FFFFFFFF” and ”FFFFFFF0”. Upon analyzing the variations in photon emissions, changes were observed at certain locations, particularly within block Z and the lit-up row. Block Z is composed of eight smaller subblocks, denoted as Z_0 through Z_7. Subblock Z_0 is highlighted in Figure 5.21. Additionally, it was observed that altering a single digit among the eight digits in the word content resulted in changes in photon emission only in the corresponding Z_i subblocks. For instance, when the word content was altered from ”FFFFFFFF” to ”FFFFFFF0”, the photon emission of the rightmost subblock (highlighted as Z_0 in the figure) changed. Similarly, when the word content was changed from ”FFFFFFFF” to ”FFFFFF0F”, the second subblock from the right (Z_1) exhibited a change in its photon emission. These findings suggest a correlation between alterations in the content of the targeted word and the resulting photon emission. It can be inferred that each subblock Z_i corresponds to a single digit in the hexadecimal notation or the four least significant bits, suggesting a potential relation to the sense amplifier and drivers.



(a) Target word with value FFFFFFF0

(b) Target word with value FFFFFFFF

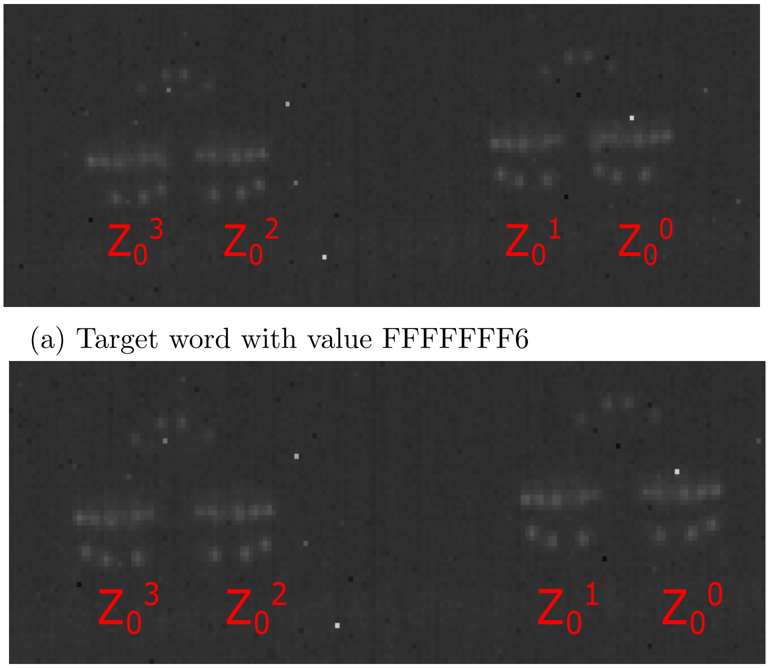
Figure 5.21: Photon emission from the right side of the data memory block during the execution of the 'load word' instruction for a target word, contrasting two different values, captured using a 10x objective lens, with subblock Z_0 highlighted.

```
"li x20,0x80000000\n"     //DATA RAM Pointer initialized with the base
"li x21,0xFFFFFFFF\n"     //Data All 1s
    //store data in one row
"sw x21,0(x20)\n"
"sw x21,4(x20)\n"
"sw x21,8(x20)\n"
"sw x21,12(x20)\n"
"sw x21,16(x20)\n"
"sw x21,20(x20)\n"
"sw x21,24(x20)\n"
"sw x21,28(x20)\n"
"sw x21,32(x20)\n"
"sw x21,36(x20)\n"
"sw x21,40(x20)\n"
"sw x21,44(x20)\n"
"sw x21,48(x20)\n"
"sw x21,52(x20)\n"
"sw x21,56(x20)\n"
"sw x21,60(x20)\n"
"li x21,0x00000000\n"  //store different value for target word
"sw x21,0(x20)\n"
"WHILE_1:\n"       //Infinite loop
"lw x22,0(x20)\n"
"j WHILE_1\n"
```

Listing 5.3: Code number 3 for investigating the photon emission of data memory for different value in target word

To examine the photon emission of block Z in more detail, the emissions from one of the subblocks, Z_i, were analyzed using a 50x objective lens. Specifically, the photon emission from the rightmost subblock (Z_0), which is responsible for the four least significant bits in the target word, was investigated. The content of the targeted word was alternated between "FFFFFFF0" and "FFFFFFFF", and the corresponding photon emissions were recorded. Figure 5.22 depicts the photon emissions from subblock Z_0 for the values "FFFFFFFF" and "FFFFFFF0". As can be observed, subblock Z_0 is composed of four smaller components, labeled Z_0^0 through Z_0^4.

By observing the photon emission changes for different content in the target word, a pattern was recognized. Each smaller component of subblock Z_0 is related to changes in one bit. The component that is located in the rightmost position (Z_0^0) is related to the Least Significant Bit (LSB), and the next component (Z_0^1) is related to the second bit, and so on. Figure 5.23 shows the pattern for a bit having a value of 0 or 1 for Z_0^0 and Z_0^1. It can be observed that when a bit has a value of zero, its corresponding component exhibits



(a) Target word with value FFFFFFF6

(b) Target word with value FFFFFFFF

Figure 5.22: Photon emission from subblock Z_0 during the execution of the load word instruction for a target word, contrasting two different values, captured using a 50x objective. The smaller components are labeled from Z_0^0 through Z_0^4.

a photon emission pattern with its dot closer to the central line. Conversely, for a value of one, the dot is positioned at a farther point. The lines in the figure indicate whether the pattern is closer to the center or the edge, with the zero value illustrated by a red color line, and the one value shown in blue.

Hence, the value inside the targeted word for a read instruction can be determined by examining the photon emission of each subblock Z_i with a 50x objective lens and conducting a thorough analysis of its photon emission patterns.

5.5.2 Investigation for Writing from Data Memory

In the following section, the focus will shift to investigating photon emissions from data memory when different values are stored in a fixed target word. This examination will include an analysis of changes related to content value during the writing process. Con-

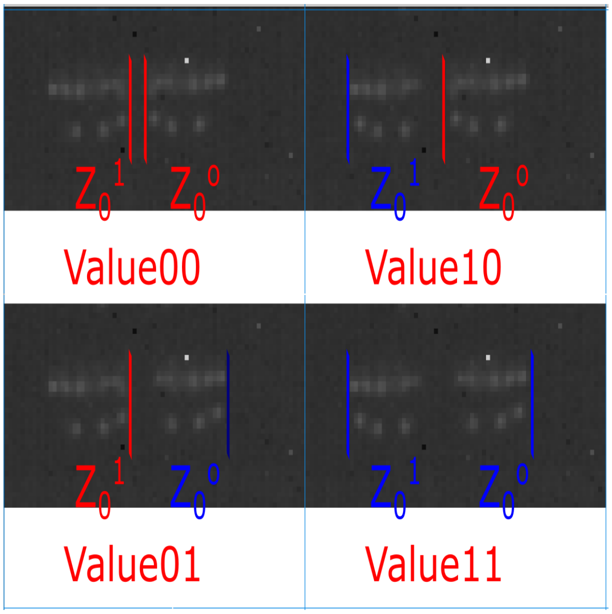


Figure 5.23: Photon emission pattern for Z_0^0 and Z_0^1 showcasing differing values - blue represents the value one, while red illustrates zero.

sequently, Code 3 from the previous section will be modified, changing the load word instruction to a store word instruction. The same process outlined in subsection 5.5.1 will then be repeated. The objective is to check whether there is any correlation between the photon emissions of data memory and the value that is stored. The value stored in data memory will be changed in each step to observe any changes in the photon emissions.

Figure 5.24 presents the photon emissions from the upright side of the data memory. This figure was recorded using a 10x objective when the value 0xFF00BC80 was stored in the target address 0x80000080. It was previously observed (in Figure 5.17) that additional photon emissions are present when writing to data memory, which were not observed when reading from the data memory. These photon emissions vary with changes to the stored value and are highlighted as block Y in Figure 5.24. Block Y consists of eight smaller subblocks named from Y_0 to Y_7. Subblock Y_0 is the rightmost subblock and is highlighted in Figure 5.24.

Similar patterns in the photon emission block Z were observed when writing various values to the data memory using a 10x objective, compared to when reading from the data memory. The photon emissions from subblocks Z_i were noted to change when the stored value was altered, with each subblock corresponding to one digit in the hexadecimal

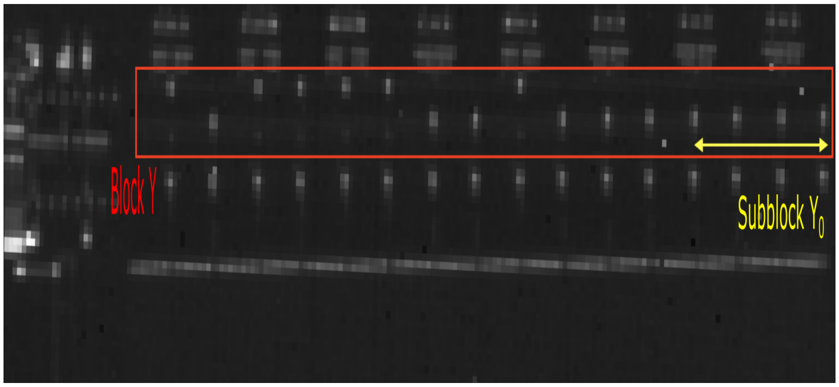


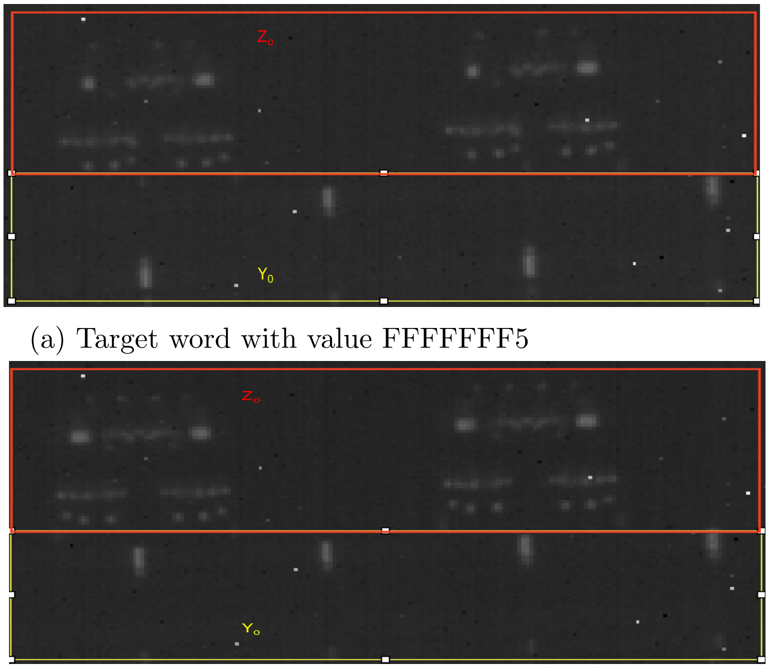
Figure 5.24: Photon emissions from the right side of the data memory block during the execution of the 'store word' instruction, captured with a 10x objective lens. A section of block Y and subblock Y_0 are highlighted.

notation.

To obtain more detail about the photon emissions at these locations, the photon emissions of the rightmost subblocks (subblock (Z_0) and subblock (Y_0)), which correspond to the four least significant bits, will be investigated using a 50x objective. The content stored in the data memory was changed incrementally from 0xFFFFFFF0 to 0xFFFFFFFF in each iteration, and the corresponding photon emissions were recorded. Figure 5.25 displays the photon emissions of the Z_0 and Y_0 blocks captured with the 50x objective lens when the values 0xFFFFFFFF and 0xFFFFFFF5 were written to the data memory.

Similar to Z_0, Y_0 also consists of four smaller components named Y_0^0, Y_0^1, Y_0^2, and Y_0^3, each corresponding to the four least significant bits in the target word. Each component is linked to one bit, with Y_0^0 being the component located on the far-right side and related to the least significant bit in the target word, followed by Y_0^1, and so forth. The pattern in the photon emission of subblock Y_0 indicates that when a stored bit value is zero, the photon emission of its corresponding Y_0^i block is located at a lower position, such as Y_0^1 in Figure 5.25a. Conversely, when the bit has a value of one, the photon emission of its corresponding subblock Y_0^i is situated at a higher position, like Y_0^0 in Figure 5.25a. Figure 5.26 illustrates the pattern when Y_0^0 holds a value of either one or zero. Thus, Y_0 reveals the value that is stored more easily compared to Z_0. Furthermore, the photon emissions of subblock Z_0 were examined across different addresses with varying columns and rows, and the findings were consistent with the previous observations.

The analysis of the photon emissions allowed us to uncover the value inside the target word in data memory for both read and write processes. These results highlight the



(a) Target word with value FFFFFFF5

(b) Target word with value FFFFFFFF

Figure 5.25: Photon emission from subblock Y_0 and Z_0 during the execution of the store word instruction for a target word, contrasting two different values, captured using a 50x objective.

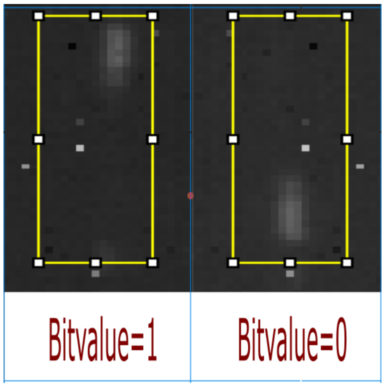


Figure 5.26: Photon emission pattern for Y_0^0 for both zero and one values, illustrating the distinct emission patterns corresponding to these bit values.

potential of utilizing photon emissions as a side-channel attack method for extracting confidential information from a microprocessor.

5.6 Investigating Photon Emissions for the Lit-up Row

In the previous section, the content of the target word accessed in the infinite loop was uncovered. It was observed that the row in which the target word was situated became illuminated. The aim of this section is to investigate whether any information can be derived from the lit-up row, which could potentially disclose details about the other 15 words located in the same row as the target word.

5.6.1 Investigation of Bit Locations in a Row

In the initial step, the objective is to examine the feasibility of identifying the locations of 16 words in a row and their corresponding bits. In previous sections, it was observed that during writing to data memory, 32 locations in the illuminated row exhibited dimmer photon emissions. It was hypothesized that these locations might correspond to the bits in the targeted word.

To test this hypothesis and verify the word locations in a row, a target row was chosen. In each step, a fixed value was stored in one of the words located in the target row, and the resulting photon emission was recorded. This process was repeated for all other words located in the target row. The aim was to observe changes in the photon emission of the lit-up row for all the words located in the target row and to locate the positions of the dimmer photon emissions related to each targeted word.

Observing the photon emissions with a 10x objective, some changes in the photon emission were detected, but the patterns were difficult to discern by eye. To examine the changes in more detail, the photon emissions were recorded with a 50x objective. Figure 5.27 displays the location of dimmer photon emissions for all 16 different words within a portion of the data memory's illuminated row. The image was captured in two steps using a 50x objective. These images were then stitched together to create a single, composite image. The dots with the same color in the figure are related to locations that became dimmer for one target word.

These findings are consistent with the photon emission observations in the X location that were investigated previously. It can be concluded that the dimmer photon emissions

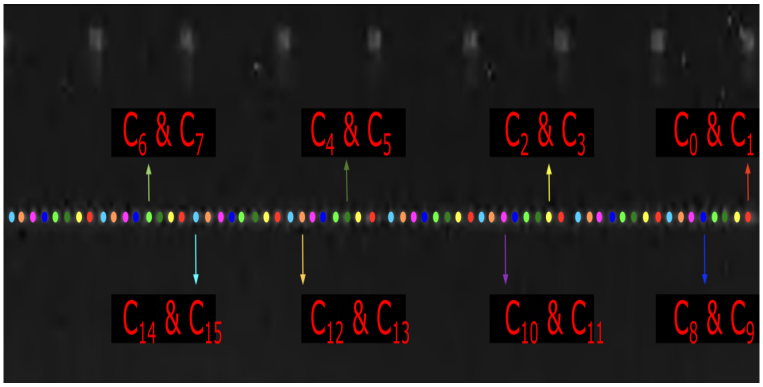


Figure 5.27: Patterns illustrating the locations of words within a section of a row in a data memory block. Dots of the same color correspond to the same words.

correspond to the bits in the targeted word, and the position of these emissions follows a pattern in the lit-up row. Moreover, it is demonstrated that every two consecutive words are located at a very close distance to each other, appearing to be situated in the same place when observed with a 50x objective lens. These results demonstrate that it is possible to locate the 16 words in a row through the analysis of photon emissions.

To confirm the previous findings about the location of words in a row, the photon emissions of a word in a row were recorded with different values stored in it. The objective was to check if the photon emission patterns change for different values and if these changes occur at the expected locations for the target word. For this purpose, Code 3 from the previous section was used. The first word in the first row (TW_{00}) was selected as the target address, and the photon emissions of the row were recorded with a 50x objective while the value zero was repeatedly written to the target word in an infinite loop. This process was repeated for the value "FFFFFFFF" (which sets all bits of the word to one) stored in the target address.

The findings revealed that the photon emission patterns change with two different values stored in the target address, and these changes occur at the expected locations for the first word in the row. The step was repeated for all the other 15 words in the row, and the findings were also consistent. These results confirm the previous findings regarding the location of words in a row.

The next goal is to identify the location of all bits related to words in a lit-up row. Based on the distance between the bits of a word and the location of words as shown in Figure 5.27, it can be hypothesized that the same bit number of all words are located close to each other. To test the hypothesis, the position of bits for one word was first

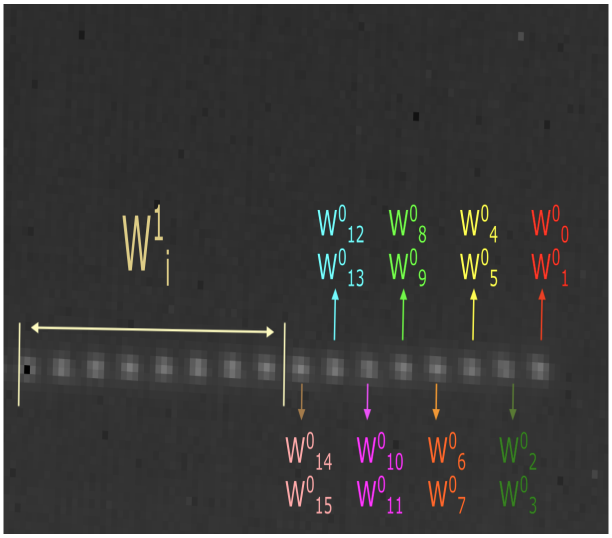


Figure 5.28: Patterns that illustrate the locations of the least significant bits within one row.

investigated. The first word in row one (TW_{00}) was chosen as the target word. Like the previous procedure, the value of the target word was changed in Code 3 in each step, but this time in a way that one bit changed each time from 0 to 1. The photon emission related to the value kept loaded in data memory was recorded and analyzed.

By observing the location of changes in photon emissions and comparing it with the corresponding word value in the target word, it was possible to identify the location of the bits for word 0. It could be seen that the least significant bit of the first word in row(w_0^0) is located on the rightmost side of the data memory, and then the order of the bits goes from the least significant bit to the most significant bit from right to left side.

In the next step, the least significant bits for all the 16 words were investigated. In each step, one of the words was targeted, and its least significant bit was set to zero or one in the Code 3, and the photon emission related to it was recorded. Investigating the photon emission of all least significant bits of words in the row confirmed the hypothesis. Figure 5.28 displays the locations of the least significant bits in the row. The w_i^1 are located next to them. It can be concluded that by analyzing the photon emissions of data memory, it is possible to locate the 16 words in a row and their corresponding bits. This information can be used to extract sensitive information from a microprocessor, making it a potential side-channel attack.

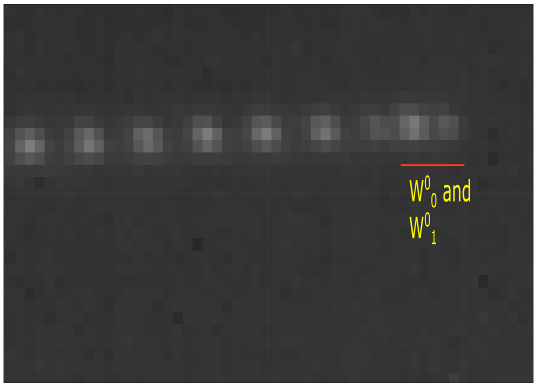


Figure 5.29: Photon emission revealing the locations of the least significant bits when the zero bit of word zero (w_0^0) and word one (w_1^0) both carry the value one, while the rest are zero.

5.6.2 Investigation of Bit content in a Row

After determining the location of bits in a row, the next step involves investigating the photon emissions of a bit with different values of zero and one. The objective is to identify whether a discernible pattern emerges in the photon emissions based on the bit value,

In this experiment, a 50x objective was employed, as it was not feasible to observe changes in the bits of the lit-up row with the eye in a 10x objective. The least significant bits of all the words in one row were targeted consecutively for observation with different values. The photon emissions of every two LSB that are located at the same position were recorded, such as bit zero of word zero (w_0^0) and word one (w_1^0), for all four possible values for these two bits. The photon emissions were recorded while continuously writing the values in an infinite loop.

Observing the photon emissions, it was seen that the photon emission of the targeted two bits varies as their values change. Figure 5.29 shows the photon emission for the location of least significant bits while the bit zero of word zero (w_0^0) and word one (w_1^0) both have one value and the rest have zero value. The location for w_0^0 and w_1^0 is highlighted with a red line. The same process was repeated for some other two-bit locations in the row, and the photon emission was investigated. Due to the small size of bit locations, it is challenging to see the pattern clearly, even with a 50x objective lens. However, the observable pattern is depicted in Figure 5.30. The process was repeated for the reading instruction, and the same pattern of bit values was observed.

Although the patterns of photon emissions corresponding to bit values were sometimes

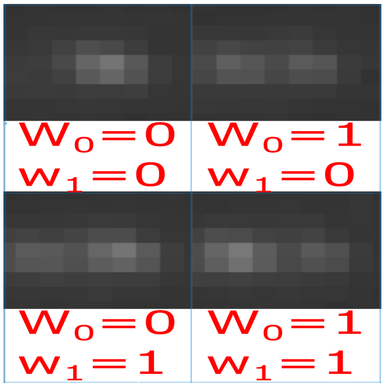


Figure 5.30: Photon emission patterns for different values in two bits located at the same position.

difficult to recognize visually, it was observed that there is a distinct pattern of photon emissions and that the intensity and location of emissions change with the bit value. Therefore, the techniques used in the previous chapter for the PIC chip, such as Pearson correlation, differential attack, or SSIM, can be employed here as well to extract information about the values stored in the row using a 50x or 10x objective lens.

In this section, it was observed that the photon emissions of the lit-up row in the data memory change with the variation of the content, and a pattern for the contents of 2 bits located in the same location was discerned using a 50x objective.

5.7 Summary

This chapter investigates the photon emissions of the data memory block within a RISC-V chip for the first time. Initially, the photon emissions of SRAM words for different word addresses were examined to ascertain the location of each word within the SRAM, paralleling the approach of the previous chapter and [66].

Subsequently, the spatially-resolved switching photon emissions associated with row and column detectors were investigated using a 50x objective. This enabled the precise identification of each target address visually, facilitating the recognition of all accesses to SRAM and the S-box in the AES algorithm. This can be instrumental in revealing the AES key. The row driver's temporal photon emissions were examined in [88] to conduct a simple photon emissions attack aimed at reducing the number of possible keys and discovering the AES key.

To the best of our knowledge, the exact access address of the SRAM, deduced from the photon emissions of row and column detectors when the pattern of photon emissions is not visibly discernible, has not been previously investigated. Consequently, for the first time, the image processing measure SSIM was employed in this research to find the target address, achieving an accuracy of approximately 93%.

Following this, the photon emissions related to sense amplifiers and drivers were examined. This investigation successfully identified photon emission patterns for the values inside the target address, enabling the determination of the value of the target word for both read and write operations, similar to [99]. Lastly, the photon emissions of the SRAM cell in the target row were investigated, and the locations of bits within a row were also discovered, mirroring the approach of the previous chapter and [66]. It was demonstrated that the contents of the row can be revealed using a 50x objective lens, consistent with [32][25].

Figure 5.31 highlights different blocks of data memory whose photon emissions were investigated in this chapter. Block X, discussed in Sections 5.2 and 5.3, and Blocks A and B, analyzed in Section 5.3, are part of this examination. Furthermore, the study of photon emission from Blocks Z and Y, detailed in Section 5.5, is complemented by the analysis of the illuminated row, as covered in Section 5.6.

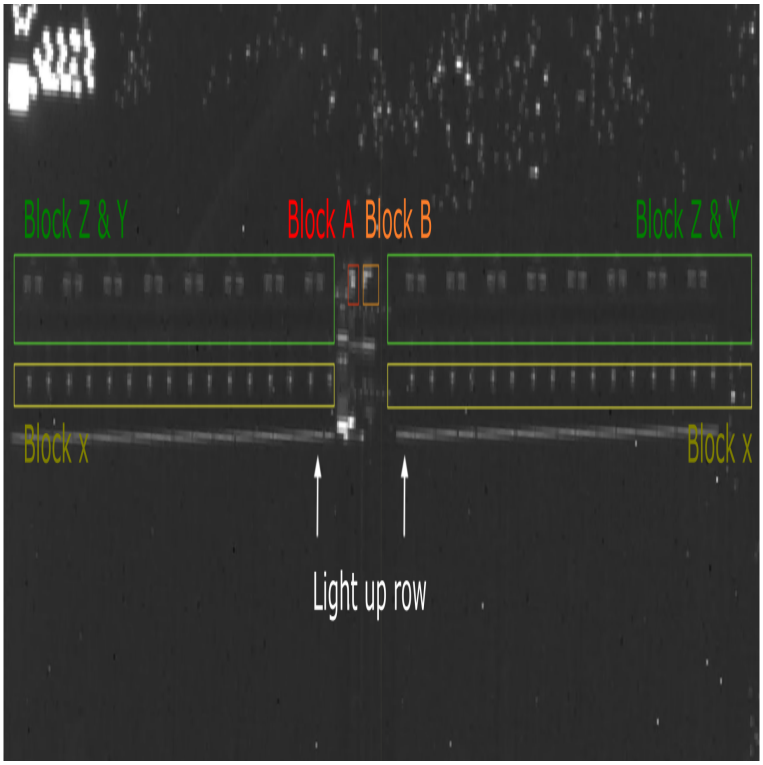


Figure 5.31: Highlighting different blocks of data memory of the RISC-V chip investigated in this chapter.

Chapter 6

Conclusions and Future Work

In this chapter, we discuss the research and the contributions of this work. We then delve into potential countermeasures and the limitations of our study. Lastly, we provide suggestions for future work and the next steps to be taken.

6.1 Discussion and Contributions

In this research, we investigated the photon emissions from SRAM using a low-cost setup and image processing techniques. Our findings demonstrate that critical information can be extracted from SRAM blocks via this side channel, particularly when the emission patterns are not immediately discernible.

Generally, the photons emitted are associated with the operational points of transistors and can be directly observed. This makes the photon emission side channel uniquely suited to investigating changes in an embedded device with high spatial resolution, down to the level of individual registers, gates, or even transistors. Such granularity allows for the analysis of data value changes at the bit level. This contrasts sharply with other side channels. For instance, the power consumption side channel measures changes in the power of an entire embedded device. Electromagnetic (EM) side channel analysis, on the other hand, studies emanations at a more limited spatial resolution, encompassing several blocks, due to its inherent characteristics [99]. Consequently, the photon emission side channel holds promise for being more insightful than other side channels, such as power consumption or electromagnetic emanation. Its potential lies in its capacity to offer in-depth insights into the internal operations of an embedded device, right down to the changes in individual transistors.

However, it's important to note that the photon emissions side channel represents a semi-invasive attack, unless the chip's backside is exposed or accessible. To observe these photon emissions, the device's package must be removed from the backside, granting access to the substrate. This means there's a heightened level of preparation required for the chip compared to non-invasive side channels, such as those relying on power measurements. That said, advancements in modern technology have simplified this process. With the advent of flip chip packaging, accessing the backside and, consequently, the photon emissions has become more straightforward without any sample preparation procedure [7][84].

The photon emission observed can typically be related to either switching transistors or the leakage current in an idle state, known as quiescent photon emission. Photon emissions emitted during each switching event are extremely faint. Hence, to delve into the photon emissions associated with specific executed instructions, these instructions need to be reiterated numerous times. This characteristic might not be feasible in real-world scenarios. However, for quiescent photon emission, it's possible to 'freeze' the device during a specific cycle of interest and record the emission [32]. This feature allows capturing an image and data regarding the states in each area of interest at the desired clock frequency without the need for repetition. As such, examining quiescent photon emission proves both valuable and more practical. This method offers the unique advantage of limitless access to various chip parts for potential adversaries. Consequently, countermeasures designed for other side channels, such as content masking or encryption, may not be as effective against this side channel as they are against others [49]. This elevates the potential of this side channel, making it more powerful and attractive for future applications in hardware security. Adversaries can feasibly record the photon emission across all points of interest, checking the key transfer between different blocks via registers and SRAM and ultimately revealing crucial data or encryption keys. An illustrative example of this, a successful correlation attack aiming to recover an AES key, has been detailed in this dissertation, in chapter 4.

Discovering the symmetric key of a cryptographic system through photon emission has many potential applications. For instance, in many embedded IoT devices, devices from the same manufacturer often share identical keys. Uncovering the key used in one device leads to a security breach, revealing the keys associated with all similar devices from the same manufacturer. Furthermore, should an attacker manage to uncover a key related to firmware or bitstream encryption of a chip through the photon emissions side channel, they could decrypt the firmware/bitstream to clone or tamper with the Intellectual Property [50][83]. Another area of application concerns smartcards. By analyzing photon emissions and subsequently revealing the key and vital information stored on the card, such as access credentials within passwords or patient data on health cards, the stakes are raised significantly.

Moreover, investigating photon emissions can help identify the location of different functional blocks, which can be used to identify and reverse-engineer the chip. This information can be employed to pinpoint vulnerable locations, which can then be targeted for more powerful fault injection attacks. In such attacks, the vulnerable locations found through photon emission microscopy can be used instead of brute force attacks that scan the entire chip to find a location for attack. This approach leads to more powerful attacks in a shorter time frame. For example, in the RISC-V chip used for investigating photon emissions, it was observed that the locations with strong photon emission leakages, even at the nominal voltage of 1.8 V, were also the locations where the EM fault injections were successful [31]. This demonstrates the potential of combining photon emission analysis with other hardware attack techniques for a more efficient and targeted approach to compromising embedded devices.

Conversely, the adoption of Public-Key Cryptography (PKC) or asymmetric encryption offers a unique private key for every device. Consequently, even if the private key of one device is compromised, other IoT devices would remain secure. Employing PKC generally increases the security of IoT devices, though this often comes at the cost of the slower execution speed inherent to asymmetric encryption algorithms. Nonetheless, photon emissions have demonstrated their potential in deciphering the private key of individual devices by observing operational sequences and deploying simple photon emission attacks [22]. Additionally, photon emissions can enhance the efficacy of Laser Fault Attacks (LFA), which also extract the private key of devices utilizing PKC [5]. Thus, photon emissions emerge as critical and potent side channels that warrant further exploration.

6.2 Contributions

Much of the research on photon emission relies on costly equipment, such as million-dollar PHEMOS setups or ASAP machines for chip de-packaging [29][36][115]. This limits such investigations to well-funded laboratories. In this study, a low-cost setup of around 40K similar to [32] was employed to make the research more accessible. Information about the photon emissions recorded using this cost-effective setup and its signal-to-noise ratio (SNR) was obtained, demonstrating the feasibility and effectiveness of a more budget-conscious approach to photon emission research.

In this study, we highlighted the usefulness and effectiveness of image processing combined with side channel attacks. We were able to extract important information from

SRAM blocks, even when visual inspection was not possible, using the PIC16F687 microcontroller and the FE310-G00 chip. Our work shows that using image processing on photon emission side channels can be a powerful tool for checking the security of embedded devices. This is especially true when visual inspection does not reveal any information. As technology gets smaller and more advanced, understanding the security of these devices is even more important. Moreover, the investigation into quiescent photon emissions was more limited than that of switching photon emissions, making it essential to further explore them. Overall, a detailed, step-by-step methodology was performed on two different chips, and the process of revealing information about the SRAM of these chips was described.

In summary, the primary contributions of this dissertation, also discussed in our forthcoming work [30], are as follows:

- Utilizing a low-cost setup for investigating photon emissions and preparing samples, similar to [32], diverges from many research methodologies that rely on expensive equipment [115][36].
- Unlike most of the research in this field [36][51] [88], this study also investigates the quiescent photon emissions of SRAM, as [32][25] did.
- Differential or correlation attacks have previously been conducted on the temporal switching photon emissions of the driving inverters of SRAM, not the SRAM cells themselves [51]. In contrast, this dissertation directed the attack at the SRAM cells themselves, similar to the approach in [32]. Furthermore, the photon emissions recorded were quiescent and time-integrated ones. For the first time, these techniques were successfully used to launch an attack on AES.
- A methodology is introduced in this work which employs more image processing techniques than previous research [102] to accurately align the recorded photon emissions.
- For the first time, image processing measures such as the SSIM have been used to reveal SRAM cell contents in cases where patterns are not easily detected by the eye. In contrast, past research relied on methods such as visual inspection [99] or image differences [111] which detect changes in photon emission from previously known values.
- This research marks the first investigation into the photon emission of the RISC-V chip. It involved detecting photon emission patterns for different elements and subsequently launching successful attacks.

- The access address of the SRAM was revealed by detecting the pattern for the column and row detectors. The SSIM method was successfully used for low zoom objectives to detect the target access address. Furthermore, it was demonstrated that the AES secret key could be uncovered on this RISC-V chip by identifying the accessed S-box element.
- The pattern likely associated with the sense amplifier in a RISC-V chip was identified. This led to the successful determination of the accessed SRAM word's value.
- The photon emission pattern for the SRAM cells of the target row in the RISC-V chip was detected, revealing the memory map and bit locations of data memory with the aid of photon emissions. Additionally, the photon emissions of SRAM cell values for different bits were examined, and the patterns for various bit values were uncovered. As a result, it was determined that attacks like correlation or bit revealing with the help of SSIM, which were previously used with PIC microcontrollers, could also be successful in the context of this RISC-V chip.

6.3 Limitations

Photon emission microscopy, while offering powerful insights into electronic device behaviour, is not without its limitations. The research setup employed in this study was subject to various limitations. Notably, the microscope lacked a secure clamping or fixing mechanism, which complicated alignment procedures. The absence of a motorized mechanism necessitated manual handling in all three dimensions, thus impacting the precision of observations. Utilizing an automated, closed-loop microscope could mitigate jitter and misalignment issues and expedite the process. Moreover, the lack of integrated lighting in the microscope made it more challenging to locate various structures and maintain optimal focus. The microscope in use, while capable of efficient infrared light transportation, was a simple light microscope. This nature potentially decreased the signal-to-noise ratio due to photon absorption and restricted the detection of photons at shorter distances due to resolution constraints inherent to its objectives. While employing a more advanced microscope could enhance image quality, it would also increase setup costs.

The camera deployed in this research also encountered several limitations. Its restricted resolution imposed constraints on the precision of the device detection and the accuracy of photon emission capture. Moreover, the camera's detector had sensitivity limitations within the wavelengths of interest. Despite its satisfactory sensitivity, the chosen InGaAs camera suffered from high dark current noise, which adversely affected the image quality and restricted the integration time. A longer integration time, while beneficial in increasing the number of received photon emissions, could potentially lead to camera saturation. A more comprehensive discussion on the limitations of the setup is available in Section 3.2.

The limited knowledge regarding the layout of the DUT, which is typically not provided by the manufacturer, presented a significant challenge. This lack of comprehensive information lengthened the time necessary to identify the sensitive areas within the chip. Moreover, image alignment presented a significant challenge throughout this research. Despite strides made to address this issue, more precise alignment could significantly enhance the effectiveness of the attacks in future investigations.

Increasing the power supply to the DUT for the purpose of observing photon emissions could potentially cause the device to malfunction, thereby complicating the attack process. Moreover, certain chips equipped with robust power management and internal regulators may not display an increase in the intensity of photon emissions simply by amplifying the external power supply.

As modern technology advances, transistors continue to shrink in size. This scaling down presents challenges, particularly when it comes to the limited optical resolution for observing photon emissions. Optical resolution is essentially the ability of an optical system to distinguish between two objects that are close together. When the distance between two points in a gate, each having a unique emission signature, becomes smaller than the optical resolution, it becomes harder to differentiate them [50].

A potential solution is the use of a Solid Immersion Lens (SIL), which can enhance optical resolution, making it viable for probing even in 10 nm technology nodes [16]. On the flip side, it's noteworthy that SRAM blocks don't scale down at the same rate as the technology node [50][7]. The transistors in SRAM cells tend to be significantly larger than the chip's minimum transistor sizes, primarily because of the need to reduce leakage current. Additionally, in our context, what's crucial is the distance between two transistors impacting photon emissions, not the actual size of the transistor. These factors suggest that while optical resolution might be a challenge, it's less of an issue for our specific application with current technologies [50][7]. However, this is an area that will require more scrutiny as technology continues to evolve.

6.4 Countermeasures

Given the strength of photon emissions, it's crucial for technology manufacturers and system architects to recognize this potential threat and develop effective countermeasures. Countermeasures against the exploitation of photon emissions fall broadly into two categories: making the observation of photon emissions from the device's backside more difficult, and modifying the circuit design to mask the locations of interest and their changes.

The silicon substrate lacks safeguards against photon examination. Consequently, this unprotected silicon can be readily exploited by attackers seeking access to on-chip resources [84]. One straightforward approach to making the observation from the backside more challenging is to add an opaque layer to the chip's backside, rendering photon emissions undetectable. However, this layer can be removed using specialized equipment, limiting its effectiveness [82]. More advanced countermeasures might involve integrating active mechanisms on the chip's backside. These mechanisms could be designed to detect any tampering attempts, immediately triggering alerts if malicious activity is detected [8][60]. However, as of now, there isn't an active backside coating solution ready for large-scale production [50][84].

At the circuit level, one countermeasure involves the integration of dummy active gates placed close to significant or sensitive gates [50][84]. The aim is to mask the authentic photon emissions by producing a ”noise” of emissions, complicating the attacker's task of differentiating between genuine and decoy signals. However, the use of dummy gates presents its challenges. Firstly, the dummy gate must be positioned extremely close to the targeted gate, within an area smaller than the optical resolution limit. Such positioning ensures that from an external perspective, the emitted photon signatures of the two are indistinguishable. Achieving designs at these minute spatial scales can be technically demanding, especially considering the challenges surrounding optical resolution mentioned earlier. Secondly, it's not enough to merely install a dummy gate. The values within these gates must be dynamic, changing randomly. This variability prevents attackers from discerning any consistent patterns through differential analyses. Implementing this randomness necessitates supplementary circuitry to govern the dummy gates' values. The introduction of this additional circuitry not only complicates the design but also results in heightened costs, increased power demands, and potential design headroom issues. For many embedded and IoT devices, which often operate with tight power restrictions due to their applications, finding the right balance between security, cost, and power efficiency is an ongoing challenge.

As previously mentioned, the ongoing scaling in modern technology presents challenges due to optical resolution limitations. However, this same limitation can serve as a natural countermeasure against specific threats. Designing smaller SRAMs with reduced leakage current, while challenging, can be a beneficial approach to bolster security measures. Such designs, albeit technically demanding, offer greater resistance to photon-based side-channel attacks, adding another layer of defense in the rapidly evolving domain of hardware security.

6.5 Future Work

Despite these limitations, the research opened more avenues for future exploration. For example, the revealed photon emission patterns for SRAM cells in RISC-V chips could make RISC-V chips susceptible to the same attacks as PIC chips. Future studies could investigate these attacks further. The current study of the RISC-V chip concentrated on the continuous reading of photon emissions from the SRAM. However, there is room for further investigation. Specifically, examining the quiescent photon emissions, similar to the work done with the PIC chip, can be the next step. This could extend our understanding of potential vulnerabilities.

Future research could look into techniques to overcome the limitation on circuits with better power management units, such as bypassing power management to capture photon emissions, which would widen the range of potential security vulnerabilities and countermeasures that can be investigated.

In light of the challenges posed by technology scaling, reaching the limits of optical resolution emerges as a significant concern for the future. As detailed in the dissertation, image processing techniques have proven instrumental in unveiling information from chips with advanced technology nodes, especially when photon emission patterns aren't discernible to the eye. Given this, a pivotal area for future research lies in the deeper exploration of image processing within the context of photon emission microscopy. There's a pressing need to understand its full potential and ascertain how it can be harnessed more effectively to extract valuable information. Furthermore, the integration of machine learning techniques into photon emission microscopy warrants exploration, drawing inspiration from recent studies in power and electromagnetic side channels [11][52]. The potential application of machine learning could involve capturing vast amounts of photon emissions from chips under varied conditions, training predictive models, and subsequently automating the process of revealing values stored in critical areas, such as SRAM cells.

Overall, addressing these limitations and expanding the research scope as suggested could further illuminate the security vulnerabilities in microchips and contribute significantly to the development of countermeasures against potential threats.

References

[1] Asap-1 – ultra tec. http://www.ultratecusa.com/asap-1. Accessed on 1/3/2023.

[2] The automatic microscope. https://www.microscopyu.com/applications/live-cell-imaging/the-automatic-microscope. Accessed: 202-04-01.

[3] Fiji:, 2023. Accessed: May 16, 2023.

[4] Dakshi Agrawal, Bruce Archambeault, Josyula R Rao, and Pankaj Rohatgi. The em side—channel (s). In *International workshop on cryptographic hardware and embedded systems*, pages 29–45. Springer, 2002.

[5] Karim Amin. *Dynamic Laser Fault Injection Aided by Quiescent Photon Emissions in Embedded Microcontrollers: Apparatus, Methodology and Attacks*. PhD thesis, University of Waterloo, 2020.

[6] Karim Amin, Catherine Gebotys, Mustafa Faraj, and Haohao Liao. Analysis of dynamic laser injection and quiescent photon emissions on an embedded processor. *Journal of Hardware and Systems Security*, 4:55–67, 2020.

[7] Elham Amini, Kai Bartels, Christian Boit, Marius Eggert, Norbert Herfurth, Tuba Kiyan, Thilo Krachenfels, Jean-Pierre Seifert, and Shahin Tajik. Special session: Physical attacks through the chip backside: Threats, challenges, and opportunities. In *2021 IEEE 39th VLSI Test Symposium (VTS)*, pages 1–12. IEEE, 2021.

[8] Elham Amini, Norbert Herfurth, Anne Beyreuther, Jean-Pierre Seifert, and Christian Boit. Generation and tracking of optical signals inside the ic to improve device security and failure analysis. In *2019 IEEE 26th International Symposium on Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–6. IEEE, 2019.

[9] G Apostolidis, D Balobas, and N Konofaos. Design and simulation of 6t sram cell architectures in 32nm technology. *Journal of Engineering Science and Technology Review*, 9(5):145–149, 2016.

[10] SE Aw, HS Tan, and CK Ong. Optical absorption measurements of band-gap shrinkage in moderately and heavily doped silicon. *Journal of Physics: Condensed Matter*, 3(42):8213, 1991.

[11] Ryad Benadjila, Emmanuel Prouff, Rémi Strullu, Eleonora Cagli, and Cécile Dumas. Deep learning for side-channel analysis and introduction to ascad database. *Journal of Cryptographic Engineering*, 10(2):163–188, 2020.

[12] Anne Beyreuther, Norbert Herfurth, Elham Amini, Tomonori Nakamura, Ingrid De Wolf, and Christian Boit. Photon emission as a characterization tool for bipolar parasitics in finfet technology. *Microelectronics Reliability*, 88:273–276, 2018.

[13] Bhphotovideo. Optical anomalies and lens corrections explained. *Available: https://www.bhphotovideo.com/explora/amp/photography/tips-and-solutions/optical-anomalies-and-lens-corrections-explained [Accessed: Mar- 2020].*

[14] Liton Kumar Biswas, Leonidas Lavdas, M Tanjidur Rahman, Mark Tehranipoor, and Navid Asadizanjani. On backside probing techniques and their emerging security threats. *IEEE Design & Test*, 39(6):172–179, 2022.

[15] Johannes Blömer and Jean-Pierre Seifert. Fault based cryptanalysis of the advanced encryption standard (aes). In *International Conference on Financial Cryptography*, pages 162–181. Springer, 2003.

[16] Christian Boit, Anne Beyreuther, and Norbert Herfurth. Photon emission in silicon based integrated circuits. *Microelectronics Failure Analysis Desk Reference,*, pages 180–195, 2019.

[17] Christian Boit et al. Fundamentals of photon emission (pem) in silicon-electroluminescence for analysis of electronic circuit and device functionality. *Microelectronics failure analysis: Desk reference*, 356:368, 2004.

[18] Christian Boit, Tuba Kiyan, Thilo Krachenfels, and Jean-Pierre Seifert. Logic state imaging from fa techniques for special applications to one of the most powerful hardware security side-channel threats. In *2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–7. IEEE, 2020.

[19] Anthony Boscaro, Sabir Jacquir, Samuel Chef, Kevin Sanchez, Philippe Perdu, and Stéphane Binczak. Automatic localization of signal sources in photon emission images for integrated circuit analysis. *Signal, Image and Video Processing*, 12:775–782, 2018.

[20] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In *Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings 6*, pages 16–29. Springer, 2004.

[21] Carbide 3D. Nomad - the nomad 883 pro, 2023. Accessed: Mar- 2020.

[22] Elad Carmon, Jean-Pierre Seifert, and Avishai Wool. Photonic side channel attacks against rsa. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 74–78. IEEE, 2017.

[23] Samuel Chef, Chung Tah Chua, Jing Yun Tay, Yu Wen Siah, Shivam Bhasin, J Breier, and Chee Lip Gan. Descrambling of embedded sram using a laser probe. In *2018 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–6. IEEE, 2018.

[24] AG Chynoweth and KG McKay. Photon emission from avalanche breakdown in silicon. *Physical Review*, 102(2):369, 1956.

[25] Jacob Couch, Nicole Whewell, Andrew Monica, and Stergios Papadakis. Direct read of idle block ram from fpgas utilizing photon emission microscopy. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 41–48. IEEE, 2018.

[26] Joan Daemen and Vincent Rijmen. A specification for rijndael, the aes algorithm. *NIST (National Institute of Standards and Technology)*, 2001.

[27] Joan Daemen and Vincent Rijmen. *The design of Rijndael*, volume 2. Springer, 2002.

[28] DeepSkyStacker. Deepskystacker.free.fr [online]. *Available: http://deepskystacker .free.fr /english/index.html. [Accessed: Mar- 2020].*

[29] Jerome Di-Battista, Jean-Christophe Courrege, Bruno Rouzeyre, Lionel Torres, and Philippe Perdu. When failure analysis meets side-channel attacks. In *Cryptographic Hardware and Embedded Systems, CHES 2010: 12th International Workshop, Santa Barbara, USA, August 17-20, 2010. Proceedings 12*, pages 188–202. Springer, 2010.

[30] Bahareh. Ebrahimi Sadrabadi and Catherine H. Gebotys. Exploring security of embedded sram in pic and risc-v chips: Insights from image processing of low-cost photon emission microscopy. In *Proceedings of the 2023 IEEE International Conference on PHYSICAL ASSURANCE and INSPECTION of ELECTRONICS (PAINE)*, Huntsville, USA, 2023. in press.

[31] Mahmoud A Elmohr, Haohao Liao, and Catherine H Gebotys. Em fault injection on arm and risc-v. In *2020 21st International Symposium on Quality Electronic Design (ISQED)*, pages 206–212. IEEE, 2020.

[32] Mustafa Faraj and Catherine Gebotys. Quiescent photonics side channel analysis: Low cost sram readout attack. *Cryptography and Communications*, 13(3):363–376, 2021.

[33] Julie Ferrigno and M Hlaváč. When aes blinks: introducing optical side channel. *IET Information Security*, 2(3):94–98, 2008.

[34] Rafael C Gonzales and Paul Wintz. *Digital image processing*. Addison-Wesley Longman Publishing Co., Inc., 1987.

[35] Hamamatsu Photonics. http://www.hamamatsu.com/. Accessed: 2023-04-11.

[36] Clemens Helfmeier, Christian Boit, Dmitry Nedospasov, and Jean-Pierre Seifert. Cloning physically unclonable functions. In *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 1–6. IEEE, 2013.

[37] Michael Hutter and Jörn-Marc Schmidt. The temperature side channel and heating fault attacks. In *International Conference on Smart Card Research and Advanced Applications*, pages 219–235. Springer, 2013.

[38] JA Kash and JC Tsang. Dynamic internal testing of cmos circuits using hot luminescence. *IEEE Electron Device Letters*, 18(7):330–332, 1997.

[39] Jeffrey Alan Kash and James Chen-Hsiang Tsang. Noninvasive optical method for measuring internal switching and other dynamic parameters of cmos circuits, August 17 1999. US Patent 5,940,545.

[40] Ulrike Kindereit. Fundamentals and future applications of laser voltage probing. In *2014 IEEE International Reliability Physics Symposium*, pages 3F–1. IEEE, 2014.

[41] Ulrike Kindereit, Gary Woods, Jing Tian, Uwe Kerst, Rainer Leihkauf, and Christian Boit. Quantitative investigation of laser beam modulation in electrically active devices as used in laser voltage probing. *IEEE Transactions on Device and Materials Reliability*, 7(1):19–30, 2007.

[42] Tuba Kiyan, Heiko Lohrke, and Christian Boit. Comparative assessment of optical techniques for semi-invasive sram data read-out on an msp430 microcontroller. In *ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis*, page 266. ASM International, 2018.

[43] Hamamatsu Photonics K.K. cataloguephemos-1000 emission microscope. *Available https://www.hamamatsu.com/us/en/product/type/C11222-16/index.html [Accessed: Mar- 2020].*

[44] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19*, pages 388–397. Springer, 1999.

[45] Paul Kocher, Joshua Jaffe, Benjamin Jun, et al. Introduction to differential power analysis and related attacks. 1998.

[46] Paul Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi. Introduction to differential power analysis. *Journal of Cryptographic Engineering*, 1(1):5–27, 2011.

[47] Paul C Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Annual International Cryptology Conference*, pages 104–113. Springer, 1996.

[48] Jochen Kölzer, Ch Boit, A Dallmann, G Deboy, J Otto, and D Weinmann. Quantitative emission microscopy. *Journal of Applied Physics*, 71(11):R23–R41, 1992.

[49] Thilo Krachenfels, Fatemeh Ganji, Amir Moradi, Shahin Tajik, and Jean-Pierre Seifert. Real-world snapshots vs. theory: Questioning the t-probing security model. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1955–1971. IEEE, 2021.

[50] Thilo Krachenfels, Tuba Kiyan, Shahin Tajik, and Jean-Pierre Seifert. Automatic extraction of secrets from the transistor jungle using laser-assisted side-channel attacks. In *30th USENIX security symposium (USENIX security 21)*, pages 627–644, 2021.

[51] Juliane Krämer, Dmitry Nedospasov, Alexander Schlösser, and Jean-Pierre Seifert. Differential photonic emission analysis. In *Constructive Side-Channel Analysis and Secure Design: 4th International Workshop, COSADE 2013, Paris, France, March 6-8, 2013, Revised Selected Papers 4*, pages 1–16. Springer, 2013.

[52] Takaya Kubota, Kota Yoshida, Mitsuru Shiozaki, and Takeshi Fujino. Deep learning side-channel attack against hardware implementations of aes. *Microprocessors and Microsystems*, 87:103383, 2021.

[53] Leonidas Lavdas, M Tanjidur Rahman, Mark Tehranipoor, and Navid Asadizanjani. On optical attacks making logic obfuscation fragile. In *2020 IEEE International Test Conference in Asia (ITC-Asia)*, pages 71–76. IEEE, 2020.

[54] Haohao Liao and Catherine Gebotys. Methodology for em fault injection: Charge-based fault model. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 256–259. IEEE, 2019.

[55] Heiko Lohrke, Shahin Tajik, Christian Boit, and Jean-Pierre Seifert. No place to hide: Contactless probing of secret data on fpgas. In *Cryptographic Hardware and Embedded Systems–CHES 2016: 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings 18*, pages 147–167. Springer, 2016.

[56] Feifan Lv, Yinqiang Zheng, Bohan Zhang, and Feng Lu. Turn a silicon camera into an ingaas camera. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 5987–5995, 2019.

[57] Ken Mai. Side channel attacks and countermeasures. In *Introduction to hardware security and trust*, pages 175–194. Springer, 2011.

[58] Stefan Mangard. A simple power-analysis (spa) attack on implementations of the aes key expansion. In *Information Security and Cryptology—ICISC 2002: 5th International Conference Seoul, Korea, November 28–29, 2002 Revised Papers 5*, pages 343–358. Springer, 2003.

[59] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks: Revealing the secrets of smart cards*, volume 31. Springer Science & Business Media, 2008.

[60] Salvador Manich Bou, Daniel Arumi Delgado, Rosa Rodríguez Montañés, Jordi Mujal Colell, and David Hernández García. Backside polishing detector: a new protection against backside attacks. In *DCIS'15-XXX Conference on Design of Circuits and Integrated Systems*, 2015.

[61] Microchip Technology Inc. *PICmicro Family Reference Manual.* Microchip Technology Inc., 2001. Accessed: April-2023.

[62] Microchip Technology Inc. Pic16f687 data sheet. Technical report, Microchip Technology Inc., 2007. Accessed: April-2023.

[63] Microchip Technology Inc. *PICkitTM 3 In-Circuit Debugger/Programmer User's Guide*, 2009. Accessed: April-2023.

[64] Microchip Technology Inc. Mplab® xc8 c compiler user's guide. User's Guide DS50002737D, Microchip Technology Inc., 2020.

[65] Microchip Technology Inc. Mplab x integrated development environment (ide). https://www.microchip.com/en-us/tools-resources/develop/mplab-x-ide, 2021. Accessed: April-2023.

[66] Dmitry Nedospasov, Jean-Pierre Seifert, Alexander Schlösser, and Susanna Orlic. Functional integrated circuit analysis. In *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*, pages 102–107. IEEE, 2012.

[67] Roger Newman. Visible light from a silicon p- n junction. *Physical review*, 100(2):700, 1955.

[68] Yin S Ng, Ted Lundquist, Dmitry Skvortsov, Joy Liao, Steven Kasapi, and Howard Marks. Laser voltage imaging: A new perspective of laser voltage probing. In *ISTFA*, pages 5–13, 2010.

[69] Baohua Niu, Grace Mei Ee Khoo, Yuan-Chuan Steven Chen, Fernando Chapman, Dan Bockelman, and Tom Tong. Laser logic state imaging (llsi). In *ISTFA 2014*, pages 65–72. ASM International, 2014.

[70] OLYMPUS. catalogue of system microscope x53m/bxfm. *Available:https://www.scribd.com/document/341196844/BX53M-BXFM-EN-0116-pdf [Accessed: Mar-2020].*

[71] Olympus Corporation. Olympus life science, 2023. Accessed: 2023-04-1.

[72] Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners.* Springer Science & Business Media, 2009.

[73] Jacques I Pankove. *Optical processes in semiconductors.* Courier Corporation, 1975.

[74] Jacob CH Phang, DSH Chan, SL Tan, WB Len, KH Yim, LS Koh, CM Chua, and LJ Balk. A review of near infrared photon emission microscopy and spectroscopy. In *Proceedings of the 12th International Symposium on the Physical and Failure Analysis of Integrated Circuits, 2005. IPFA 2005.*, pages 275–281. IEEE, 2005.

[75] Stas Polonsky, M Bhushan, A Gattiker, A Weger, and Peilin Song. Photon emission microscopy of inter/intra chip device performance variations. *Microelectronics reliability*, 45(9-11):1471–1475, 2005.

[76] Stas Polonsky and Alan Weger. Off-state luminescence in metal-oxide-semiconductor field-effect transistors and its use as on-chip voltage probe. *Applied physics letters*, 85(12):2390–2392, 2004.

[77] Stas Polonsky, Alan Weger, and Moyra McManus. Picosecond imaging circuit analysis of leakage currents in cmos circuits. In *ISTFA 2002*, pages 387–390. ASM International, 2002.

[78] J-J Quisquater. Eddy current for magnetic analysis with active sensor. *Proceedings of Esmart, 2002*, pages 185–194, 2002.

[79] Jean-Jacques Quisquater and David Samyde. Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In *International Conference on Research in Smart Cards*, pages 200–210. Springer, 2001.

[80] Jan M Rabaey, Anantha P Chandrakasan, and Borivoje Nikolić. *Digital integrated circuits: a design perspective*, volume 7. Pearson Education Upper Saddle River, NJ, 2003.

[81] M Rahman and N Asadizanjani. Failure analysis for hardware assurance and security. *Electronic Device Failure Analysis (EDFA)*, August 2019.

[82] M Tanjidur Rahman, Qihang Shi, Shahin Tajik, Haoting Shen, Damon L Woodard, Mark Tehranipoor, and Navid Asadizanjani. Physical inspection & attacks: New frontier in hardware security. In *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*, pages 93–102. IEEE, 2018.

[83] M Tanjidur Rahman, Shahin Tajik, M Sazadur Rahman, Mark Tehranipoor, and Navid Asadizanjani. The key is left under the mat: On the inappropriate security assumption of logic locking schemes. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 262–272. IEEE, 2020.

[84] Mir Tanjidur Rahman and Navid Asadizanjani. Backside security assessment of modern socs. In *2019 20th International Workshop on Microprocessor/SoC Test, Security and Verification (MTV)*, pages 18–24. IEEE, 2019.

[85] Chester Rebeiro, Debdeep Mukhopadhyay, and Sarani Bhattacharya. An introduction to timing attacks. In *Timing channels in cryptography*, pages 1–11. Springer, 2015.

[86] Patrick Schaumont and Zhimin Chen. Side-channel attacks and countermeasures for embedded microcontrollers. In *Introduction to hardware security and trust*, pages 263–282. Springer, 2011.

[87] Werner Schindler. A timing attack against rsa with the chinese remainder theorem. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 109–124. Springer, 2000.

[88] Alexander Schlösser, Dmitry Nedospasov, Juliane Krämer, Susanna Orlic, and Jean-Pierre Seifert. Simple photonic emission analysis of aes. *Journal of Cryptographic Engineering*, 3:3–15, 2013.

[89] PE Schmid. Optical absorption in heavily doped silicon. *Physical Review B*, 23(10):5531, 1981.

[90] Jörn-Marc Schmidt and Christoph Herbst. A practical fault attack on square and multiply. In *2008 5th Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 53–58. IEEE, 2008.

[91] SEGGER Microcontroller. J-link base. https://www.segger.com/products/debug-probes/j-link/models/j-link-base/, 2021. Accessed: April-2023.

[92] Luca Selmi. Silicon luminescence techniques for the characterization of hot-carrier and degradation phenomena in mos devices. *Microelectronic Engineering*, 28(1-4):249–256, 1995.

[93] Semitracks. Light emission, 2020. Accessed: Mar-2020.

[94] Andrea Bahgat Shehata, Alan J Weger, Franco Stellari, Peilin Song, Hervé Deslandes, Ted Lundquist, and Euan Ramsay. Time-integrated photon emission as a function of temperature in 32 nm cmos. In *2015 IEEE International Reliability Physics Symposium*, pages 2B–4. IEEE, 2015.

[95] SiFive. Freedom e sdk documentation. https://sifive.github.io/freedom-e-sdk-docs/index.html, 2021. Accessed: April-2023.

[96] SiFive Inc. Sifive fe310-g002 manual. Technical report, 2018.

[97] SiFive Inc. *SiFive FE310-G002 Manual*, v19p05 edition, 2019.

[98] SiFive Inc. *SiFive HiFive1 Rev B Getting Started Guide*, 2019.

[99] Sergei Skorobogatov. Using optical emission analysis for estimating contribution to power analysis. In *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 111–119. IEEE, 2009.

[100] Sergei Skorobogatov. Physical attacks and tamper resistance. In *Introduction to Hardware Security and Trust*, pages 143–173. Springer, 2011.

[101] Sergei P Skorobogatov and Ross J Anderson. Optical fault induction attacks. In *International workshop on cryptographic hardware and embedded systems*, pages 2–12. Springer, 2002.

[102] Michael T Snella. *Drift correction for scanning-electron microscopy.* PhD thesis, Massachusetts Institute of Technology, 2010.

[103] Peilin Song and Franco Stellari. Tester-based optical and electrical diagnostic system and techniques. In *2012 IEEE 30th VLSI Test Symposium (VTS)*, pages 209–214. IEEE, 2012.

[104] Peilin Song, Franco Stellari, Dirk Pfeiffer, Jim Culp, Al Weger, Alyssa Bonnoit, Bob Wisnieff, and Marc Taubenblatt. Marvel—malicious alteration recognition and verification by emission of light. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, pages 117–121. IEEE, 2011.

[105] Zhigang Song and Laura Safran. Lvi and lvp applications in in-line scan chain failure analysis. *Electronic Device Failure Analysis*, 18(4):4–14, 2016.

[106] Raphael Spreitzer, Veelasha Moonsamy, Thomas Korak, and Stefan Mangard. Systematic classification of side-channel attacks: a case study for mobile devices. *IEEE Communications Surveys & Tutorials*, 20(1):465–488, 2017.

[107] François-Xavier Standaert. Introduction to side-channel attacks. *Secure integrated circuits and systems*, pages 27–42, 2010.

[108] F Stellari, F Zappa, S Cova, and L Vendrame. Tools for non-invasive optical characterization of cmos circuits. In *International Electron Devices Meeting 1999. Technical Digest (Cat. No. 99CH36318)*, pages 487–490. IEEE, 1999.

[109] Franco Stellari, Leonidas E Ocola, Ernest Y Wu, Takashi Ando, and Peilin Song. Photon emission microscopy of amorphous hfo2 reram cells. In *2022 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–5. IEEE, 2022.

[110] Franco Stellari, Peilin Song, James C Tsang, Moyra K McManus, and Mark B Ketchen. Testing and diagnostics of cmos circuits using light emission from off-state leakage current. *IEEE transactions on electron devices*, 51(9):1455–1462, 2004.

[111] Franco Stellari, Peilin Song, Manuel Villalobos, and John Sylvestri. Revealing sram memory content using spontaneous photon emission. In *2016 IEEE 34th VLSI Test Symposium (VTS)*, pages 1–6. IEEE, 2016.

[112] Franco Stellari, Peilin Song, Alan J Weger, and Tian Xia. Broken scan chain diagnostics based on time-integrated and time-dependent emission measurements. In *ISTFA 2004*, pages 52–57. ASM International, 2004.

[113] Franco Stellari, ALBERTO Tosi, FRANCO Zappa, SERGIO Cova, et al. Cmos circuit analysis with luminescence measurements and simulations. In *Proc. ESSDERC*, pages 24–26, 2002.

[114] Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert, and Christian Boit. On the power of optical contactless probing: Attacking bitstream encryption of fpgas. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1661–1674, 2017.

[115] Shahin Tajik, Dmitry Nedospasov, Clemens Helfmeier, Jean-Pierre Seifert, and Christian Boit. Emission analysis of hardware implementations. In *2014 17th Euromicro Conference on Digital System Design*, pages 528–534. IEEE, 2014.

[116] James C Tsang, Jeffrey A Kash, and David P Vallett. Picosecond imaging circuit analysis. *IBM Journal of Research and Development*, 44(4):583–603, 2000.

[117] JC Tsang and JA Kash. Picosecond hot electron light emission from submicron complementary metal–oxide–semiconductor circuits. *Applied Physics Letters*, 70(7):889–891, 1997.

[118] Ultratec. *A process for thinning and polishing silicon using the Ultratec ASAP-I IPS.* Ultratec report pdf.

[119] I Vagt and C Boit. Low power and fault isolation: Spectral aspects of photon emission. In *2018 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–5. IEEE, 2018.

[120] D Vallett. Picosecond imaging circuit analysis, pica. *Proc. Microelectronics Failure Analysis Desk Reference*, pages 292–300, 2004.

[121] S Villa, ANDREA LEONARDO Lacaita, and A Pacelli. Photon emission from hot electrons in silicon. *Physical Review B*, 52(15):10993, 1995.

[122] Zhou Wang, Alan C Bovik, Hamid R Sheikh, and Eero P Simoncelli. Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, 13(4):600–612, 2004.

[123] John Wawrzynek, Jonathan Bachrach, Krste Asanovic, John Lazzaro, and Rimas Avizienis. Cs250 vlsi systems design lecture 9: Memory. *Available from: http://www-inst.eecs.berkeley.edu/ cs250/fa12/lectures/lec09.pdf [Accessed: Mar- 2020].*

[124] R Wegerhoff, O Weidlich, and M Kassens. Basics of light microscopy and imaging. *Imaging & Microscopy*, pages 1–56, 2007.

[125] Neil Weste and David Harris. *CMOS VLSI design: a circuits and systems perspective.* Addison-Wesley Publishing Company, 2010.

[126] Xenics. *User Manual: Xeva FPA Cameras.* Xenics, 2013. ENG-2013-UMN002-R005.

[127] Xenics. Xeva-320 series - short-wave infrared imagers, 2023. Accessed: Mar- 2020.

[128] Xenics nv. *Xeneth v2.6 User Manual.* Leuven, Belgium, 2016.

[129] Wai Mun Yee, Mario Paniccia, Travis Eiles, and Valluri Rao. Laser voltage probe (lvp): A novel optical probing technology for flip-chip packaged microprocessors. In *Proceedings of the 1999 7th International Symposium on the Physical and Failure Analysis of Integrated Circuits (Cat. No. 99TH8394)*, pages 15–20. IEEE, 1999.

[130] Boyou Zhou, Ronen Adato, Mahmoud Zangeneh, Tianyu Yang, Aydan Uyar, Bennett Goldberg, Selim Unlu, and Ajay Joshi. Detecting hardware trojans using backside optical imaging of embedded watermarks. In *Proceedings of the 52nd Annual Design Automation Conference*, pages 1–6, 2015.

[131] YongBin Zhou and DengGuo Feng. Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing. *Cryptology ePrint Archive*, 2005.