Abstract

Title of Dissertation: ADVANCED ENCRYPTION STANDARD IN COUNTER MODE ELECTROMAGNETIC ANALYSIS USING TEMPLATE ATTACK

Marcial Tienteu, Ph.D., May 2023

Dissertation Chair: Kevin T. Kornegay, Ph.D.
Department of Electrical and Computer Engineering

Embedded devices such as smart cards, cell phones, personal digital assistants (PDAs), and passports rely on cryptosystems to perform secure operations or transactions. Cryptosystems use a wide range of cryptographic algorithms that may be used to protect user information and data. These cryptographic algorithms are divided into symmetric and public key algorithms. Several embedded devices rely on the security of symmetric algorithms, such as Advanced Encryption Standard (AES).

The National Institute of Standards and Technology (NIST) document SP 800-38A recommends modes of operation that may provide confidentiality in conjunction with AES or other cryptographic primitives. The Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) are all included in the special publication 800-38A. AES in Counter mode (AES-CTR) is used extensively in many applications, triggering interest in studying its vulnerabilities and weaknesses. Since most attacks related to CTR mode and its associated appendages, such as AES-CTR, are primarily theoretical, there is still room for practical exploitations. This study evaluates the implementations of AES-CTR using Side-Channel Analysis (SCA).

To carry out the evaluation, the work analyzes the SCA of AES-CTR in a few hardware and software implementations. This study uses two hardware devices: a microcontroller board with an arm Cortex-M4F chip and a System-on-Chip (SoC) CoraZ7 board from Xilinx. The power trace acquisition method was used to collect trace sets on the microcontroller, and the electromagnetic method was used to collect trace sets on both microcontroller and the SoC. The findings of this study present a novel approach that improves points of interest selection for template attacks. The improved point of interest (POI) selection algorithm developed in this work compares the output from multiple points of interest using the same method to get the best samples that yield the correct key hypothesis.

This study's method narrows the point of interest to the exact position of the correct key hypothesis. Two sets of traces are needed to perform POI for the target. The comparison algorithm gives the precise position of the samples that match byte-wise; if there is a mismatch in points of interest, then the difference between the calculated distance from both trace sets helps determine if the sample will yield a correct key hypothesis. Reasonable sample distance for mismatch samples should be within the same clock cycle. After determining the points of interest, one of the two traces is used to create a profile for the family of devices. Then a third trace is set with an unknown key from the same device family and collected for the attack phase. We show that by performing our comparison algorithm, we can successfully recover the entire key from a set of AES-CTR traces.

ADVANCED ENCRYPTION STANDARD IN COUNTER MODE ELECTROMAGNETIC ANALYSIS USING TEMPLATE ATTACK

by

Marcial Tienteu

A Dissertation Submitted in Partial Fulfillment
of the Requirements for the Degree
of Doctor of Philosophy

MORGAN STATE UNIVERSITY

May 2023

ADVANCED ENCRYPTION STANDARD IN COUNTER MODE ELECTROMAGNETIC ANALYSIS USING TEMPLATE ATTACK

by

Marcial Tienteu

has been approved

February 2023

DISSERTATION COMMITTEE APPROVAL:

_____, Chair
Kevin T Kornegay, Ph.D.

_____
Kemi Ladeji-Osias, Ph.D.

_____
Edgar Mateos Santillan, Ph.D.

_____
Thierry Wandji, Ph.D.

DEDICATION

This dissertation is dedicated to my father, Pierre Tientcheu.

Dad, you could have had the happiest day of your life today, but, as you taught me, I trust and praise the Lord in all circumstances.

ACKNOWLEDGEMENTS

The Almighty GOD, who has given me the inner strength, perseverance, and focus to accomplish my goal, who has blessed me with the most amazing family and coworkers, and who has been ever-present in both the most significant struggles and victories of my life, deserves all the praise and glory.

During my undergraduate studies, I was lucky enough to meet my advisor, Dr. Kevin Kornegay. He introduced me to the fascinating world of cryptography and embedded security and later encouraged me to get a Ph.D. in the field. Dr. K, as we refer to you, thank you for all the effort and consideration you put into making the time spent together memorable.

Many thanks to my committee member: Dr. Edgar Mateos Santillan, for all the time and effort put into helping to learn skills in the field of side-channel analysis. I will never forget our many Saturday meetings from 11 a.m. to 12 p.m. (EST). Dr. Kemi Ladeji-Osias, you have supported me since 2012, and all your advice has been a life changing gift. Dr. Thierry Ketchiozo Wandji, you are more than an advisor; you are a good mentor, and I will never forget you telling me that,: "I won't give you fish, but I will teach you how to fish." Thank you to all CREAM, CAP, and ECE faculty: Dr. Yacob Astatke, Dr. Michel Kornegay, Dr. Kofi Nyarko, Dr. Gregory Wilkins, Dr. Paterne Sisinto, Dr. Hailu Kassa, Dr. Wondimu Zegeye, Dr. Onyema Osuagwu, Dr. Kimberly Reaves, Dr. Tsion Yimer, Dr. Otily Tousop, Mr. Andre Lewis, Mr. Vinton Morris, Mr. Albert Sweets, and Asia Mason, among others.

My labmates Edmund Smith, Paige Harvey, Loic Djomo Tchuenkou, and others deserve special thanks for their daily support. I would like to express my gratitude to my coworkers at WMATA, particularly Frederick Stidam, Maurice McCall, Victor Grubb, Zoran Bozic, Daniel Gebremeskel, Yawo Codjia-Dossou, Brent Mortley, and others. I ap-

preciate Miss Denise Magla, my second-grade teacher at the Ecole Publique de la Cite-Sic Bassa Group 3, and Mr. Francois Bakapa Honla, and Mr. Martin Naoussi, my vocational middle and high school lab instructors at Institut Secondaire de Technology (IST), for laying the groundwork for my education.

To my family: My dear mother, Alise Kouenga Tientcheu, you are the most wonderful woman who sacrificed all to raise your five children, myself, Ghislain Yamdjeu, Carine moumeni, Myriam Siemeni, and Franklin Kakmeni. Today, it gives me great pleasure to recognize that I would not have become the man I am without the betting you gave me in my childhood. Maman, je te dit infiniment merci. My lovely wife, Nida Carole Tienteu, thank you for your immeasurable support. Taking care of our three kids (Aaron, Elsie, and Ryan) and managing the house so I can focus on my research have been demanding tasks for you all these years, but we made it by the grace of God. Drs. Lucas Kemeni and Rosine Kemeni, thank you for your countless words of encouragement and motivation. Dr. Simplice Nouala and Eugenie Nouala, thank you for all the support and advice you have given me since my teenage years. Mr. Eric Nana Mfomen, Mr. Magellan Yepmezoue, Mr. Jean Calvin Djieya, and Mr. Simeon Seumga deserve a special thank you because all of you have been central to my success in ways that I cannot put into words. Line Tientcheu, Justine Siekoueyanou, Eric Wande, maman Helene Patipe, Afred, and Sylvie Fondjio, and Reine Florence Williams I thank you for your words of encouragement and support.

To all my friends: Joel Diogo, Eduardo Herrera, Bertrand Larose, Phillibert Nganou, Isidore Patipe, Bernard Coleman, Heric Takougem, Simplice Dimo, Magaret Donfack, Clement Tita, Martine Ggako Yonga and others, I thank you for your words of encouragement and support. To all others who I did not name, I have not forgetting you; instead, I keep you close to my heart.

Contents

List of Figures

List of Tables

List of Acronyms

AES Advanced Encryption Standards
CBC Cipher Block Chainning
CIA Confidentiality, Integrity, and Availability
CCA Chosen Ciphertext Attack
CFM Cipher Feedback Mode
CTR Counter Mode
CPA Correlation Power Analysis
DPA Differential Power Analysis
ECB Electronic Code Book
EM Electro-Magnetic Radiation
FPGA Field Programmable Gate Array
IV Initial Vector
GCM Galois Counter Mode
HW Hamming Weight
HD Hamming Distance
LRA Linear Regression Analysis
MIA Mutual Information Analysis
PCA Principal Component Analysis
SC Short circuit
SCA Side Channel Analysis
SoC System on Chip

Chapter 1

Introduction

1.1 Motivation and Contributions

Networking, communications, and embedded devices are growing trends in the modern world. Associated with them are a rising number of security threats to the confidentiality, integrity, and availability (CIA) of the processed information or data. Information and data security are crucial to maintaining CIA's principles. In the past, information security was mostly used for diplomatic or military intelligence transmissions. The rapid evolution of modern communication technology and devices also creates the need to secure data and information for all users. Cryptography is a predominant solution to provide communications with secrecy, integrity, availability, and authenticity. Communication systems rely on cryptographic algorithms to protect information and data from malicious attacks. Malicious attackers are adversaries with the sole intention of compromising a cryptographic system. It has been a widespread concern in cyberspace to meet the CIA's principles. An adversary can acquire access to a device during the encryption process, which is becoming more common as embedded devices find use in communication, medical tracking, banking, and other daily activities. Physical access to those gadgets suggests that they can be studied and modified.

Every day, a large number of cybercrimes are committed all over the world. These crimes are put into groups based on how they are attacked and what kind of business or industry they happen in. Some industries are more likely to be attacked than others. Between March 2021 and March 2022, IBM Security conducted studies in 550 companies that had

experienced data breaches [22]. The affected organizations were located across 17 different countries and 17 sectors. IBM's report classifies the data breach into three categories: the cost of cybercrime, the sector of activity, and attack vectors. In the last 12 years, the United States has registered the highest financial loss from cyber crimes, as shown in Figure 1.1.

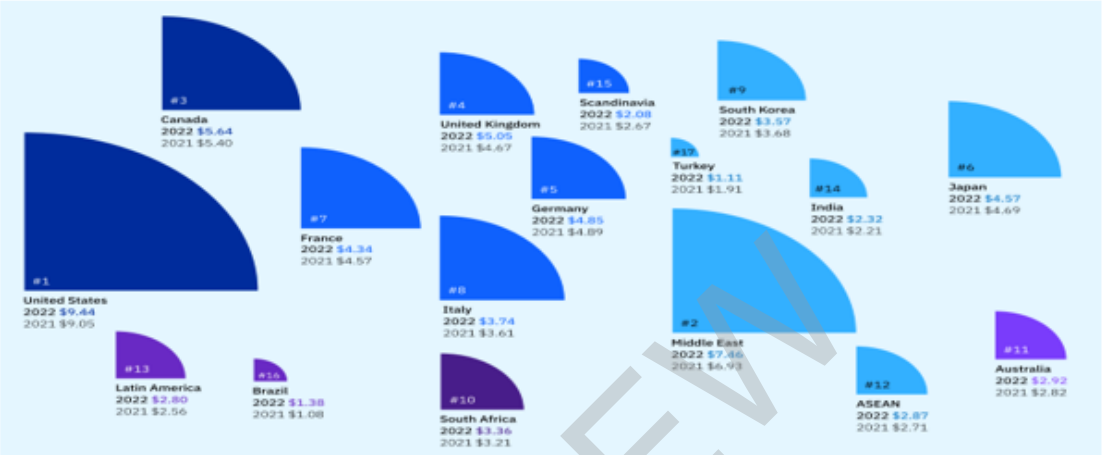

Figure 1.1: Average cost of a data breach by country or region [22]

The healthcare industry is at the top of the list of industries that have suffered significant losses as a result of data breaches. The average overall cost of a healthcare breach climbed from USD 9.23 million in 2021 to USD 10.10 million in 2022, a 9.4% rise [22]. Figure 1.2 presents the cost of data breaches per industry or sector of activity.

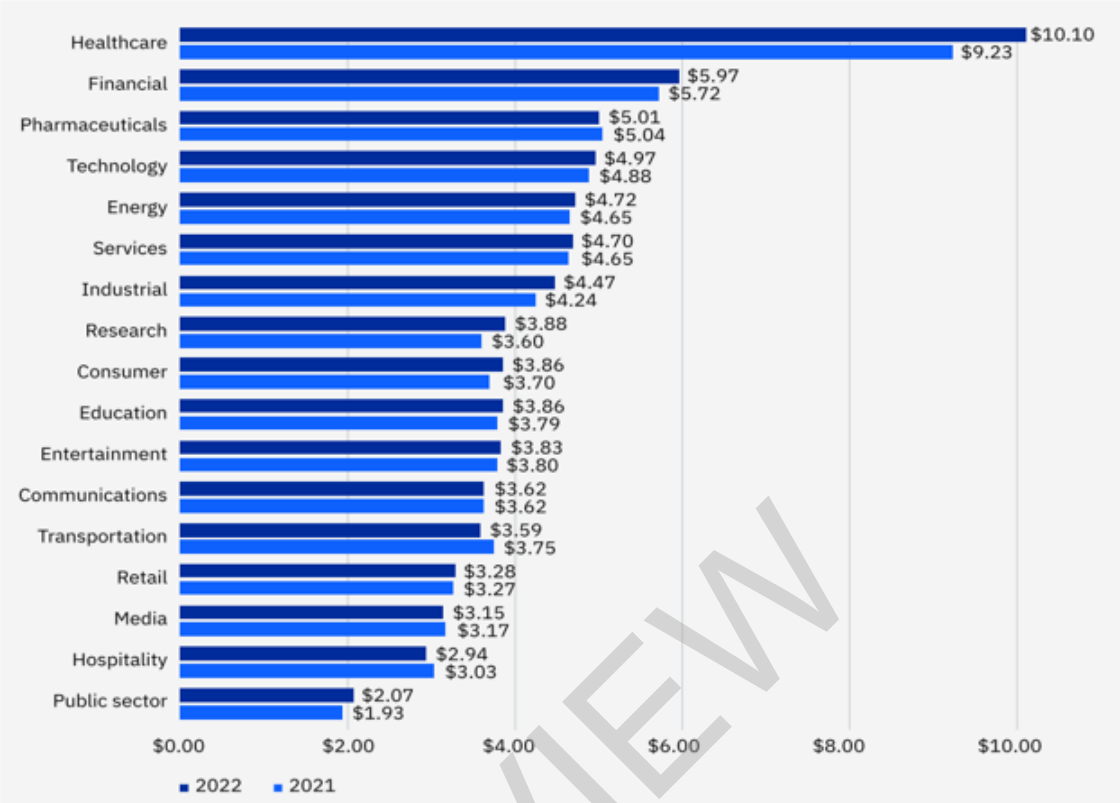

Figure 1.2: Average cost of a data breach by industry [22]

Among all factors that describe the cost of cybercrime, the physical attack vector is the one that is most noteworthy, since the work presented in this thesis is in relation to physical attacks. According to the abovementioned IBM report, the cost of a physical security attack was $3.96 million in 2022. Figure 1.3 shows the average cost of data breaches as per attack vector.

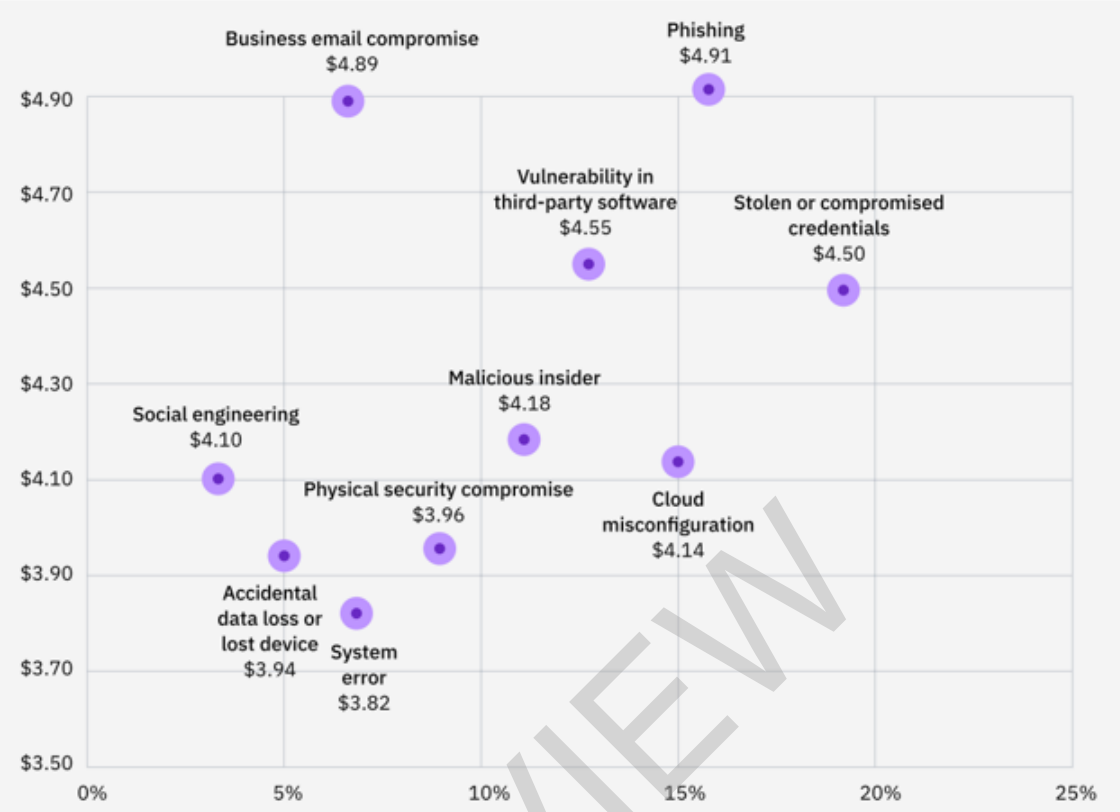

Figure 1.3: Average cost and frequency of data breaches by initial attack vector [22]

Several mitigation proposals for these attacks have focused on protecting the hardware or software. Our interest is in the hardware part of the communication system, primarily encapsulated in the physical security attack vectors mentioned in the IBM report. Since cryptography is the solution to counter or reduce attacks on communication systems and devices, this work investigates an encryption mode associated with a symmetric cipher block that provides confidentiality for communication systems and related devices.

In 2001, National Institute of Standards and Technology (NIST) released SP 800-38A, a special publication with an encryption mode that can be used with any approved block cipher algorithm. Document SP 800-38A talks about the Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) modes [13]. CTR was suggested by Diffie and Hellman in 1979 [10]. Out of the five symmetric encryption modes described in SP 800-38A, CTR is the one that is used most often today to provide confidentiality. CTR is widely implemented in numerous applications, such as IPSec, Wifi, and Zigbee. CTR's hardware and software implementation presents vast benefits over the other modes [30]. CTR is the core implementation of the widely used authentication modes such as CCM and GCM. Since CTR mode is the foundation of many authentication modes, this study looks at its vulnerability to a side-channel attack on hardware and software implementations of AES 128-bit encryption.

Classic cryptanalysis has demonstrated the mathematical security of CTR mode, which government authorities have validated and standardized. However, the side channel vulnerabilities of CTR mode combined with AES 128 have not yet been extensively examined, especially in hardware implementation.

Fewer researchers have analyzed the implementation of AES 128-bit in counter mode. Josh Jaffe proposed a first-order DPA attack against AES in counter mode, in which the initial counter and key values are unknown [25]. The Josh Jaffe attack method is the only practical side-channel attack on the AES-128 CTR. Leurent et al. [29] studied the missing difference problem and its impact on the security of the CTR mode. O'Flynn et al. [46] published an SCA attack against the wireless protocol IEEE 802.15.4, which supports using AES-CCM to encrypt and authenticate messages. These attacks were either theoretical or carried out against CTR's software implementation. Unlike the work performed by [25, 29, 46], this thesis presents the first electromagnetic template attack on AES-CTR with a novel method that improves points of interest selection. A CPA attack on hardware and software implementation of the AES-CTR mode of operation is also studied, along with a new method to enhance the template attack utilizing points of interest.

1.2 Research Hypothesis

The purpose of this work is to test the resiliency of AES in CTR mode against SCA. We start by proving that AES-CTR software implementation is less resilient to SCA attacks than hardware implementation. Next, the advantages of EM SCA over the power Analysis SCA when attacking the hardware implementation of AES in CTR mode are demonstrated. Lastly, we prove that template attacks can be effective against AES in CTR mode.

Several SCA researchers have focused on the different modes of encryption associated with the AES algorithm, but just a few were done on AES in CTR mode. Even though some attacks were proposed on CTR mode, all those works were software implementations[25, 29, 46]. This leaves a gap in the literature on SCA attacks on Hardware implementation of CTR mode. Based on the existing SCA attack technique (e.g., SPA, CPA, Template, etc...), this research presents a concrete attack on AES128-CTR hardware and software implementation that contributes to answering the questions listed below.

1: Is Hardware implemented AES in CTR vulnerable to SCA?

2: Which leakage SCA source between electromagnetic and power is suitable for launching an attack against AES-CTR?

3: Can the AES in counter mode encryption key be recovered using a template-based attack?

1.3 Thesis structure

Chapter 2 begins with the background of symmetric key cryptography and the mode of operations. Next, all related side-channel analysis work on AES-CTR is presented. Chapter 3 explains the target setup on a development FPGA board and explores some processing techniques. Then, the different CPA attacks performed and the corresponding results are shown. Chapter 4 presents a comparative SCA analysis of AES-128 bits in CTR software and hardware implementation and an analysis of EM SCA and power SCA. Chapter 5 presents an electromagnetic template attack with a new method for enhancing the selection of the point of interest. Chapter 6 summarizes the work and gives direction for future work.

Chapter 2

Literature Review

2.1 Introduction

This chapter provides an overview of the cryptography algorithm topics related to this research. Specifically, it focuses on symmetric key encryption, block ciphers, and mode of operation. The end of this chapter states the advantage of the CTR mode over the rest of the modes of operation.

2.2 Definition of cryptography

In general, cryptography is defined as the science of secret writing with the goal of scrambling the meaning of a message. With the proliferation of cryptographic algorithms, researchers seek more sophisticated techniques to create new algorithms to encrypt users' data. Cryptography has been primarily of interest to the military and diplomatic communities for many years. Private industries and individual businesses are highly involved in cryptography, rendering the sector more competitive today. The cryptography field is classified into three main categories: symmetric, asymmetric, and protocols [39].