Course guide
2301215 - ASIC - Asic Design Techniques for High Secure Systems

Last modified: 19/04/2024

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 710 - EEL - Department of Electronic Engineering.

Degree: MASTER'S DEGREE IN SEMICONDUCTOR ENGINEERING AND MICROELECTRONIC DESIGN (Syllabus 2024). (Optional subject).

Academic year: 2024 **ECTS Credits:** 4.0 **Languages:** English

LECTURER

Coordinating lecturer: Consultar aquí / See here: https://telecos.upc.edu/ca/curs-actual/coordinadors-i-professorat

Others: Consultar aquí / See here: https://telecos.upc.edu/ca/curs-actual/coordinadors-i-professorat

TEACHING METHODOLOGY

The total number of hours of this elective course is 30, distributed as follows:

â□□Lectures: 18 hours
â□□Laboratories: 12 hours
â□□Final presentation: 1 hour

LEARNING OBJECTIVES OF THE SUBJECT

1.Discuss the security vulnerabilities present in standard Integrated Circuits (ICs).
2.Acquire knowledge on the procedures for analyzing and evaluating security weaknesses.
3.Understand specialized techniques to mitigate side-channel leaks in functional designs and testing infrastructure.
4.Explore auxiliary detectors that aid in minimizing the impact of side-channel attacks.
5.Gain insight into advanced attack techniques currently utilized, particularly within microprocessors.

STUDY LOAD

Type	Hours	Percentage
Self study	70,0	70.00
Hours small group	12,0	12.00
Hours large group	18,0	18.00

Total learning time: 100 h

CONTENTS

Block 1. Historical review and modern cryptography background

Description:
1. Historical context.
In this initial chapter, we will delve into the foundational concepts of Security and Trust, offering a historical perspective that elucidates their evolution within the realm of information technology across various abstraction levels. The discussion will delve into the root of trust and its historical connection to Integrated Technology.
2. Introduction to modern cryptography techniques.
In this second chapter, prevalent techniques and security primitives employed in cryptography will be discussed, highlighting their ultimate implementation at the core of Integrated Circuits (ICs).

Full-or-part-time: 4h
Theory classes: 4h

Block 2. Threats and weaknesses existing in hardware implementations

Description:
3. Vulnerabilities in hardware implementations of Integrated Circuits.
In this chapter, a comprehensive overview of the diverse vulnerabilities inherent in security product ICs is delineated. These vulnerabilities permeate various stages, spanning from the design phase through the production chain, final distribution, and deployment in the field. Following production, the expansive realm of counterfeiting emerges, encompassing a spectrum of methodologies such as reverse engineering techniques. Moreover, an array of techniques is explored, aiming to surreptitiously extract internal secrets by subjecting the ICs to abnormal operational conditions and meticulously scanning for intrinsic emissions, commonly referred to as side-channels.
4. Techniques for reverse engineering: invasive, semi-invasive and non-invasive.
Upon deployment in the field, security breaches affecting ICs are executed through reverse engineering techniques. These endeavor aims to expose internal information at various levels, ranging from the comprehensive recovery of the entire design to the identification of key information in more targeted approaches. The choice of reverse engineering technique - whether invasive, semi-invasive, or non-invasive - depends on the resources at the adversary’s disposal and the countermeasures implemented within the chip. This chapter delves into the intricate details of these aspects, providing a nuanced exploration of the methodologies employed.
5. Side-channel and fault attacks.
Adversaries possessing constrained technical resources leverage side-channel emissions and fault attacks, two cost-effective methodologies that can be augmented with high-performance equipment to enhance their efficiency. ICs produce a diverse array of lateral emissions during operation, thereby compromising the fundamental black box principle of any security system. This chapter elucidates practical use cases wherein the methodology is systematically detailed. To enhance the success of more active attacks, fault attacks are employed. This involves intentionally operating the IC beyond specifications and monitoring its abnormal behavior to identify potential security breaches.

Full-or-part-time: 5h
Theory classes: 5h

Block 3. Strategies to strengthen security primitives at hardware level

Description:
6. Silicon masking and anti-counterfeiting measures.
Outsourced fabrication centers have increased the potential for various types of fraud during the production process. Legitimate owners have responded by implementing anti-fraud techniques that involve masking different parts of the design. This chapter delves into the elucidation of several such masking techniques employed to safeguard against fraudulent activities.
7. Silent gates, logic masking and special logic implementations.
Strengthening the black box means to make the IC operating as much quiet as possible. This means that the lateral emissions to be uncorrelated with the data that is being processed. When this is not completely possible logic masking comes to the rescue in which noise through randomized data is incorporated with the aim to deceive the adversary. Different type of logic implementations exist exploiting these capabilities.
8. Securing test infrastructure.
Test infrastructure is an indispensable component of every IC, specially in digital systems. During the design chain phase, the integration of the test infrastructure is typically automated and constitutes one of several steps in the design process. However, automated procedures often overlook security threats, turning the test infrastructure into a potential backdoor exploited by adversaries seeking to compromise security. Over the past decade, a surge in resources and solutions has emerged to enhance the security of test infrastructures. This chapter sheds light on some of these techniques.
9. Primitives for security.
ICs stand as the foundation of trust in the security domain. Security primitives represent specialized implementations of security functions engineered to be tamper-proof from their very foundation. This chapter introduces two distinct types of security primitives: Physical Unclonable Functions (PUF) and True Random Number Generators (TRNG). Leveraging the inherent physical properties of silicon, these primitives obscure their secrets, rendering them exceptionally resilient and virtually impervious to compromise.

Full-or-part-time: 6h
Theory classes: 6h

Block 4. Advanced research topics in IC design for security

Description:
10. Security implementations for edge devices.
Cloud-based computation is becoming increasingly ubiquitous. Nevertheless, with the escalating concentration of power in computation centers, there is a concurrent acceleration of computation at the edges of the cloud. Edge devices, being the terminal points, are more susceptible to security breaches, primarily due to their constrained resources. This chapter comprehensively addresses various aspects of edge computing concerning security, including key generation, as well as strategies for achieving low power and low-cost security in hardware implementations for these edge devices within IoT applications.
11. Advanced attack techniques in large systems.
Security is an inherent consideration across all facets of automated systems, ranging from the silicon to the algorithmic level. This chapter provides a comprehensive overview, offering a global perspective that spans these diverse layers and addresses pivotal issues, including Trojans, architectural factors impacting side-channels, general malware concerns, and the latest and most perilous threats, such as Spectre and Meltdown.

Full-or-part-time: 2h
Theory classes: 2h

Laboratory 1

Description:
Introduction to designing and implementing an SBOX.

Full-or-part-time: 2h
Laboratory classes: 2h

Laboratory 2

Description:
Dual-rail logic library. Implementation and the library and redesign of the SBOX.

Full-or-part-time: 2h
Laboratory classes: 2h

Laboratory 3

Description:
Wave Precharge Dynamic Logic. Improvement of the dual-rail logic library with this precharge technique. Improvement of the SBOX and analysis of the power consumption and detection of data leakage.

Full-or-part-time: 2h
Laboratory classes: 2h

Laboratory 4

Description:
Project presentation: objectives, evaluation criteria, and work team organization.

Full-or-part-time: 2h
Laboratory classes: 2h

Laboratory 5

Description:
Supervised work session on project.

Full-or-part-time: 2h
Laboratory classes: 2h

Laboratory 6

Description:
Supervised work session on project.

Full-or-part-time: 2h
Laboratory classes: 2h

Final presentation

Description:
Final presentation of the project

Full-or-part-time: 1h
Theory classes: 1h

GRADING SYSTEM

In the evaluation process, three activities are taken into account when grading the students:

â□□Gde (20%): This includes class tests and assignments, which are both conducted in class and assigned as homework.
â□□Grp (40%): Refers to the project presentation, where student groups showcase the attainment of the set objectives.
â□□Gap (40%): Represents the final examination.

The final grade, denoted as Gadhsy, is calculated using the formula: Gadhsy = 0.2 Gde + 0.4 Grp + 0.4 Gap

BIBLIOGRAPHY

Basic:

- Bhunia, Swarup; Tehranipoor, Mark M. Hardware security : a hands-on learning approach [on line]. Cambridge: Elsevier, 2019 [Consultation: 18/03/2024]. Available on: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=5754491. ISBN 9780128124772.
- Goubin,Louis; Matsui, Mitsuru. Cryptographic Hardware and Embedded Systems [on line]. 1. [Berlin ; New York]: Springer-Verlag Heidelberg, [2006] [Consultation: 18/03/2024]. Available on: https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/11894063. ISBN 1611-3349.
- Tehranipoor, Mark; Guin, Ujjwal; Forte, Domenic. Counterfeit integrated circuits [on line]. Cham: Springer, 2015 [Consultation: 18/03/2024]. Available on: https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/978-3-319-11824-6. ISBN 9783319118246.
- Thomas, Donald E.; Moorby, Philip R. The Verilog hardware description language [on line]. 5th ed. New York: Kluwer, 2002 [Consultation: 18/03/2024]. Available on: https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/b116662. ISBN 9780306476662.