IP Core Protection and Hardware-Assisted Security for Consumer Electronics

Anirban Sengupta and Saraju P. Mohanty
Chapter 1: Introduction to IP Core Protection and Hardware-Assisted Security of Consumer Electronics

1.1 Consumer Electronics and Security Perspectives

1.2 Hardware-Assisted Security and IP Core Protection

1.3 Intellectual Property (IP) Cores/Hardware
   
   1.3. A Utility of IP Cores in CE Devices
   
   1.3. B Why Security and Protection of Hardware/IP Cores?

   1.3. C Traditional Forms of IP Protection not enough?

1.4 IP Core Protection and Hardware-Assisted Security of CE Hardware -- DSP Core

   1.4. A Security and Protection Methodologies available for IP Core/Hardware

   1.4. B Different IP Core Protection and Hardware-Assisted Security Mechanisms: Advantages and Disadvantages


1.5 Hardware-Assisted Media Protection

1.6 Physical Unclonable Functions

1.7 Organization of the Book

1.8 Conclusion

1.9 Exercises
Chapter 2: Security in Consumer Electronics and Internet of Things (IoT)

2.1 Internet of Things (IoT) - A Broad Overview

2.1.1 IoT - Architecture

2.1.2 IoT - Driving Technology

2.1.3 IoT - Applications

2.1.4 IoT - Challenges

2.2 Security, Privacy, IP Right in IoT and CE Systems - A Big Picture

2.2.1 IoT Security - Attacks and Countermeasures

2.2.2 Trustworthy Consumer Electronic Systems

2.2.3 Hardware-Assisted Security and Protection

2.2.4 Different Aspects of Security and Privacy

2.2.5 Different Aspects of Intellectual Property (IP), Ownership Right, or Copyright Protection

2.3 Memory Security

2.3.1 Memory Security Attacks

2.3.2 Memory Security Solutions

2.4 Radio Frequency Identification (RFID) Security

2.4.1 RFID Security Attacks

2.4.2 RFID Security Solutions

2.5 Near Field Communications (NFC) Security

2.5.1 NFC Security Attacks

2.5.2 NFC Security Solutions

2.6 Smart Transportation Security

2.6.1 Smart Car Security

2.6.2 Unmanned Ariel Vehicle (UAV) Or Drone Security

2.7 Smart Healthcare Security

2.7.1 Smart Healthcare Security Attacks
2.7.2 Smart Healthcare Security Solutions

2.8 Firmware

2.8.1 Firmware Attacks

2.8.2 Firmware Solutions

2.9 Blockchain Technology

2.9.1 Blockchain-Overview

2.9.2 Blockchain-Application

2.9.3 Blockchain as a security framework

2.9.4 Blockchain-issues

2.10 Conclusions

2.11 Exercises

Chapter 3: Trojan Security Aware DSP IP Core and Integrated Circuits

3.1 Introduction

3.2 Types of Hardware Trojan

3.2.1 Trojan Features

3.2.2 Benefit of Trojan Security at Higher Abstraction Level

3.2.3 Threat Model

3.3 Hardware Trojan in a 3PIP Module

3.3.1 An Example of Hardware Trojan

3.3.2 Trojan Detectability in a 3PIPModule at RTL/Lower Levels

3.4 Selected Trojan Security Approaches

3.4.1 Trojan Security Approaches for DSP cores

3.4.2 Trojan Security Approach for Combinational/Sequential Circuits

3.5 Trojan Security Aware DSP IP Core

3.5.1 Definition
3.5.2 Goal
3.5.3 Formulation
3.5.4 Models
3.6 Design Process of Trojan Secured DSP IP Core
   3.6.1 Deriving CDFG of a DSP Core
   3.6.2 Generating DMR of CDFG
   3.6.3 Trojan Secured Scheduling of DMR CDFG
3.7 Analysis on Case Studies/Test Cases
   3.7.1 DSP applications and System Setup for the Case Studies
   3.7.2 Security Analysis
   3.7.3 Design Cost Analysis
   3.7.4 Comparative Perspectives
3.8 Conclusion
3.9 Exercises

-----------------------------------------------------------------------------------------------------------------------------

Chapter 4: IP Core and Integrated Circuit Protection using Robust Watermarking

4.1 Introduction
4.2 Selected Watermarking Approaches
4.3 Design Process of Watermarked IP Core/Hardware
   4.3.1 Problem Formulation
   4.3.2 Design Process of Single-Phase Watermarked IP Core/Hardware
   4.3.3 Design Process of Triple-Phase Watermarked IP Core/Hardware
   4.3.4 Desirable Properties of Watermark
   4.3.5 Possible Cases of Dishonest Claim of IP core/Hardware Ownership and its Resolution
4.4 Analysis on Case Studies
   4.4.1 Security Analysis of Triple-Phase Watermark for DSP IP Cores
4.4.2 Design Cost Analysis of Triple-Phase Watermark for DSP IP Cores

4.5 Conclusion

4.6 Exercises

-------------------------------------------------------------------------------------------------------------------------

Chapter 5: Symmetrical Protection of DSP IP Core/IC Using Fingerprinting and Watermarking

5.1 Introduction
   5.1.1 Background on Watermark and Fingerprint
   5.1.2 Threat Model
   5.1.3 Benefits of Protection at Higher Abstraction

5.2 Fundamentals of IP Core Protection
   5.2.1 Overview on Non-Symmetric IP Core Protection Techniques
   5.2.2 Overview on Symmetric IP Core Protection Techniques

5.3 Symmetrical IP Cores Protection for DSP core
   5.3.1 Problem Formulation
   5.3.2 Symmetrically Protected Design - Area Evaluation Model
   5.3.3 Symmetrically Protected Design - Delay Evaluation Model
   5.3.4 Symmetrically Protected Design - Cost Evaluation Function
   5.3.5 Encoding Rules of Buyer Fingerprint and Seller Watermark for DSP IP cores
   5.3.6 Multi-Variable Signature Embedding Process
   5.3.7 Signature Detection Process
   5.3.8 Desirable Properties of Signature

5.4 Case Study of Symmetrical IP core Protection
   5.4.1 Demonstration of Fingerprinting Constraints Embedding Process
   5.4.2 Demonstration of Watermarking Constraints Embedding Process

5.5 Analysis of Case Studies for DSP cores
   5.5.1 Analysis of Embedding Cost, Security Metric on DSP Cores symmetrical protection
5.5.2 Comparative Study Between Symmetrical and Non-Symmetrical Technique

5.6 Conclusion

5.7 Exercises

Chapter 6: Computational Forensic Engineering for Resolving Ownership Conflict of DSP IP Core

6.1 Introduction

6.1.1 Overview of Forensic Engineering

6.2 Computational Forensic Engineering Technology

6.3 IP Core Feature Extraction Algorithms

6.3.1 Feature Extraction Rules

6.3.2 IP Core Validation

6.3.3 Important Characteristics of Customized CFE

6.4 Analysis on Case Studies

6.4.1 Results of the Customized CFE Approach

6.5 Conclusion

6.6 Exercises

Chapter 7: Structural Obfuscation of DSP Cores used in CE Devices

7.1 Introduction

7.1.1 Threat Model

7.1.2 Benefits of Providing Security at Higher Design Abstraction Level

7.2 Obfuscation for IP Core Protection – A Broad View

7.2.1 Code Obfuscation Techniques

7.2.2 Logic Obfuscation Techniques

7.2.3 Structural Obfuscation Techniques

7.3 Compiler Transformation Driven Structural Obfuscation
7.3.1 Formulation and Evaluation Models
7.3.2 Multi-Stage High-Level Transformation Techniques
7.4 Low-Cost Structural Obfuscation for DSP IP Core
  7.4.1 Overview on PSO
  7.4.2 Movement of Particle
  7.4.3 Terminating Condition of PSO
7.5 A Case Study for Multi-stage Structural Obfuscation
7.6 Analysis on Case Studies
  7.6.1 Result of Multi-Stage Structural Obfuscation
  7.6.2 Comparative Study and Discussion
7.7 Conclusion
7.8 Exercises

Chapter 8: Functional Obfuscation of DSP Cores used in CE Devices
8.1 Introduction
8.2 Attack Scenarios and Threat Model
  8.2.1 Possible Attack Scenarios
  8.2.2 Threat Model
8.3 Selected Functional Obfuscation Approaches
8.4 Design of Functional Obfuscated DSP Core
  8.4.1 Formulation
  8.4.2 Low-Cost Obfuscation Method for DSP Core
8.5 Security of Functionally Obfuscated DSP Core Design
  8.5.1 Keyspace
  8.5.2 Security Analysis
  8.5.3 Countermeasures Against Attacks
8.6 Optimization Engine for Functional Obfuscation of DSP Cores

8.6.1 Particle Encoding
8.6.2 Particle Fitness
8.6.3 Updating Particle

8.7 Analysis on Case Studies

8.7.1 Security Analysis
8.7.2 Overhead Analysis
8.7.3 Comparative Analysis

8.8 Conclusion

8.9 Exercises

Chapter 9: Obfuscation of JPEG CODEC IP Core for CE Devices

9.1 Introduction

9.2 Overview of JPEG Compression and Decompression

9.2.1 DCT-Based JPEG Image Compression Process
9.2.2 DCT-Based JPEG Image Decompression Process

9.3 Design Process of Structurally Obfuscated JPEG IP Core

9.3.1 Threat Model, Problem Formulation and Optimization Framework
9.3.2 Constructing Non-Obfuscated DFG for JPEG Compression
9.3.3 Generating Structurally Obfuscated JPEG Compression IP Core
9.3.4 Generating Structurally Obfuscated JPEG Decompression IP Core

9.4 Implementation of JPEG CODEC IP Core

9.4.1 Designing Obfuscated JPEG Compression IP Core
9.4.2 Designing Obfuscated JPEG Decompression IP Core
9.4.3 End To End JPEG CODEC through Designed Hardware/IP Core
Chapter 10: Advanced Encryption Standard (AES) and its Hardware Watermarking for Ownership Protection

10.1 Introduction

10.2 Advanced Encryption Standard (AES) Algorithm

10.2.1 Overview of AES

10.2.2 AES Algorithm – Description and Custom Hardware Design

10.3 AES Digital Watermarking

10.3.1 AES Watermark Encoding

10.3.2 Process of embedding watermark in AES

10.3.3 Signature Detection

10.4 Case Study of a Watermarked AES hardware

10.5 Conclusion

10.6 Exercises

Chapter 11: Hardware Approaches for Media and Information Protection and Authentication

11.1 Intellectual Property (IP) Protection - A Broad Overview

11.1.1 Digital Rights Management (DRM)

11.1.2 Copyright Protection of Multimedia - A Brief History

11.1.3 Hardware Versus Media Protection

11.2 General Framework for Copyright Protection

11.2.1 The Encoder

11.2.2 The Decoder
11.2.3 The Comparator

11.3 Types of Digital Watermarks

11.3.1 Spatial Vs Frequency Domain Watermarking

11.3.2 Based on Multimedia Objects

11.3.3 Based on Human Perception

11.3.4 From Applications Point of View

11.3.5 Based on Embedding Techniques

11.3.6 Hardware based Watermarking Systems

11.4 Applications of Digital Watermarks

11.4.1 Copyright Protection

11.4.2 Ownership Assertion

11.4.3 Authentication and Integrity Verification

11.4.4 Fingerprinting

11.4.5 Usage Control

11.4.6 Broadcast Monitoring

11.4.7 Content Labeling

11.4.8 Misappropriation Detection

11.4.9 Anti-counterfeiting

11.4.10 UAV Safety

11.4.11 Medical Signals Authentication

11.5 Desired Characteristics of Watermarks

11.5.1 Perceptibility

11.5.2 Robustness

11.5.3 Tamper-Resistance

11.5.4 Bit-rate

11.5.5 Modifiability, Multiplicity, Cascadability and Orthogonality
11.5.6 Scalability
11.5.7 Unambiguity and Universality
11.5.8 Pixel Alteration and Human Intervention
11.5.9 Reliability
11.5.10 Blindness
11.5.11 Security
11.5.12 Real-Time operation
11.5.13 Cost and Complexity
11.5.14 Energy Consumption
11.5.15 Integrability
11.5.16 Characteristics Specific to a Watermark

11.6 Technical Challenges for Watermarking
11.6.1 Properties of Visual Signals
11.6.2 Properties of the Human Visual System
11.6.3 How much Watermark Signal to add and Where?
11.6.4 Spread Spectrum Communications

11.7 Hardware Based Approaches For Watermarking
11.7.1 Image Watermarking Hardware Systems
11.7.2 Video Watermarking Hardware Systems
11.7.3 Secure Better Portable Graphics
11.7.4 Trust Cam

11.8 Dynamic Watermarking in Smart Car or UAV

11.9 Medical Signal Authentication

11.10 Side Channel Information Leakage Attacks and Countermeasures
11.10.1 An Encryption Hardware
11.10.2 Side Channel Analysis Attacks
11.10.3 Side Channel Attack Countermeasures

11.11 Attacks on Watermarks and Watermarking Systems

11.11.1 Removal and Interference Attacks

11.11.2 Geometric Attacks

11.11.3 Cryptographic Attacks

11.7.4 Protocol Attacks

11.12 Limitations of Watermarks and Watermarking

11.13 Conclusion

11.14 Exercises

Chapter 12: Physical Unclonable Functions (PUFs)

12.1 Introduction

12.2 Physically Unclonable Function: Principle

12.3 Properties or Characteristics of PUFs

12.3.1 Uniqueness

12.3.2 Reliability (Correctness)

12.3.3 Randomness (Uniformity)

12.3.4 Correlation (Bit Aliasing)

12.3.5 Power Consumption

12.3.6 Speed

12.4 Classification of PUFs

12.4.1 Device Based

12.4.2 Security Based

12.5 Ring Oscillator Based PUFs

12.6 Reconfigurable or Dynamic PUFs

12.7 Static Random Access Memory (SRAM) Based PUF
Chapter 01
Introduction to IP Core Protection and Hardware-Assisted Security of Consumer Electronics

This chapter presents an overview of the book. Some discussions which can serve as introductory materials toward the overall text of the book. It is assumed that the readers have some background on areas like VLSI, embedded systems, hardware design flow before adopting this text.

1.1. Consumer Electronics and Security Perspectives

Consumer Electronics (CE), embracing high-end devices ranging from digital camera, multi-spectral camera, IP TV, smart tablets, night vision camera to smart meter, accompanied by data and communication knowhow makes emerging smart cities and Internet of Things (IoT) a reality. In the world of CE and IoT, security, privacy, and protection of hardware and its information are critically imperative. It is universally acknowledged that for internet-of-things (IoT), security of underneath hardware is pivotal for correct operation. The underlying hardware may have been affected by several threat actors. An adversary may generate secret exist that leaks crucial data such as encryption key employed in secure transmission line, the maker could meddle the design by implanting hardware Trojans, or inserting artifacts with recognized dependability susceptibilities. Current generation designs assimilate IP blocks from manifold vendors; mass-produced and verified by diverse companies worldwide. Accordingly, numerous access points exist for hardware to be attacked. For a trusted hardware design, defense of intellectual property cores is of ultimate significance [(Sengupta & Kundu, 2017), (Sengupta, Mohanty & Rose, 2018)].

A typical consumer electronic system presented in Fig. 1.1 has DSP, embedded processor, memory, system software, and application software. Significantly diverse forms of attacks can happen to this CE system including the following: system security, information security, system privacy, information privacy, network security, firmware security, system trustworthiness, hardware IP rights, information copyrights. The origins of these attacks are different, for example, remote or local. They can be either by software or
References


Chapter 02

Security in Consumer Electronics and Internet of Things (IoT)

In a typical consumer electronics including diverse forms of attacks, following are not the same: System Security, Information Security, Information Privacy, System Trustworthiness, Hardware IP protection, Information Copyright Protection. They hold a different meaning and each serve different purpose. This chapter aims at differentiating each of the terms in the context of Internet of Things (IoT). IoT is a very hot topic of research where different devices, sensors and computers are connected to a network, collect data and process it for different purposes. A network of devices and sensors connected to the cloud can complete many tasks that are without them, very difficult to achieve and complete. But there exists a problem of security and privacy everywhere. With all the different devices connected to the internet, attackers pose a huge threat to the system. When the system is implemented in home, for healthcare or running an entire city, this threat can be much more catastrophic.

This Chapter is organized as follows. Section 1 presents an introduction and broad overview of Internet of Things. Section 2 presents a broad view of security, energy, and cost trade-offs in Consumer Electronic systems. Section 3 presents different security threats and solutions to the memory modules of the system, Section 4 provides different threats and solutions to the RFID modules, Section 5 provide security flaws and how to mitigate them in an NFC module of the system. Section 6 discusses different security flaws in the Smart Vehicles, The Autonomous Cars and The UAVs. Section 7 discuss different ways an attacker can attack a healthcare device and solutions for some of the attacks, Section 8 discusses the threats on firmware of the devices and Section 9 discusses the emerging technology of blockchain, its advantages and issues. The conclusion and future directions are presented in Section 10.

1 Internet of Things (IoT) - A Broad Overview

Communication has evolved in the world at a very fast pace. Many solutions has been proposed for communications, short or long distance. Technological growth also helped this in developing high performance computing devices making it a necessity needing newer inventions. All of them combined gave rise to "Internet of Things" which has become an integral part of every-day-life without realizing it. There are many definitions to IoT depending on the individual’s perspective. In an Internet of Things environment, all of the devices or “THINGS” are connected to a network and exchange data among themselves or send to the cloud [57]. The “3-I’s” in the context of IoT are shown in Figure 1. They are ‘Interconnection’, ‘Intelligence’ and ‘Instrumentation’. These three are the important aspects of an IoT environment, as shown in the figure, the Smart City environment. Interconnection is the communication platform that provides the network for the devices an Internet connection that helps in transmitting the data among themselves or to the cloud services where post processing takes place. Intelligence is the brain of the entire Environment and Instrumentation is various devices and sensors that are present in the environment. There are various devices present in an IoT environment like microcontrolleres, single board computers and sensors. Each of them should have a unique IP address to be considered as a THING for the IoT [55].

An IoT can be defined as Any TIME connection, Any THING connection and Any PLACE Connection as shown in Figure 2 [35]. IoT can be anywhere. Some of the IoT devices can be deployed in places where they are not monitored continuously. Their duty will be monitoring a parameter and transmitting the data over the air [111]. In such cases, it should be continuously connected to the internet which needs “Any PLACE Connection”, “Any TIME Connection” and “Any THING Connection”. With the technological advancements, various devices and board are attaining communication capabilities which can help in implementing an IoT environment at a very low cost.
References


Chapter 03

Trojan Security Aware DSP IP Core and Integrated Circuits

This chapter discusses different security approaches to design digital signal processing (DSP) cores that have detection capability against functional type Hardware Trojan in a global supply chain. In the current design and fabrication supply chain, design houses, circuits and system core vendors, and manufacturing houses are globally scattered. It is quite possible that Trojan can be inserted in this design and manufacturing supply chain by anyone involved at any phase. Such Trojans can give backdoors to hackers and affect the operation of the system that uses such as infected hardware. In a worst case, in critical applications such as aircrafts, medical devices etc can be completely stopped from functioning causing catastrophic consequences. The chapter is organized as follows: Section 2 discusses different features and threat model of hardware Trojan; Section 3 explains how a Trojan could be inserted in a 3PIP core and why it is difficult to detect; Section 4 discusses different hardware Trojan security approaches that are available in the literature with emphasis on DSP cores; Section 5 presents definition, goal and design evaluation models for Trojan security aware DSP IP core; Section 6 discusses design process of Trojan secured DSP IP core; Section 7 presents analysis and comparison of different Trojan security approach for DSP IP core; finally we conclude this chapter in Section 8.

3.1. Introduction

Use of heterogeneous System-on-Chip (SoC) architecture in modern Consumer Electronics (CE) devices such as smartphones, gaming consoles, tablets, digital cameras, etc. have become a common practice in the semiconductor industry. The in-house SoC designer or the system integrator mostly imports Intellectual Property (IP) cores from third party IP vendors to minimize the design
References


S. Bhunia et al. (2013), ‘Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution,’ in *IEEE Design & Test*, vol. 30 (3), pp. 6-17.


Chapter 04

IP Core and Integrated Circuit Protection using Robust Watermarking

This chapter discusses robust watermarking approaches for the ownership protection of hardware cores (aka IP cores). Watermarking ensures some additional attributes inserted in the hardware core such a way that it can be used to verify ownership of the hardware core when required. Robust watermarking approaches have been discussed as these are resilient to various attacks that happen in global supply chain for various reasons. The remaining chapter is structured as follows: Section 2 provides an overview on selected hardware/IP core watermarking approaches; Section 3 discusses design process of watermarked IP core; Section 4 analyses the hardware watermarking approaches on case studies/test cases; finally, Section 5 draws the conclusion.

4.1. Introduction

A watermark is a secret mark implanted into an entity such as official documents, currency notes, postal stamps, audio/video files etc. to protect ownership right of an owner. Usually, a watermark embedded into an entity is expected to preserve its quality and functionality. However, for the domains in which watermarking is applied such as audio/video, documents etc., slight degradation of the quality is usually noticed. Given the advantages of a watermark, it may be considered an extremely useful tool for protecting hardware (e.g. DSP core) ownership as well. However, the prime difference from watermarking in other domains is zero tolerance towards modification of quality/functionality of the hardware design. This makes hardware watermarking challenging but extremely useful for protecting legal rights of an intellectual property (IP) vendor/owner. It is widely acknowledged that complex consumer electronics system design relies heavily on DSP IP cores realized as system-on-chip (SoC). Thus hardware watermarking plays an integral role in IP core protection of CE devices (Mohanty et al., 2017; Voyatzis et al., 1999; Cox et al., 2006; Roy et al., 2013; Sengupta, 2017).

In the modern era of consumer electronics (CE), use of DSP intellectual property cores in global supply chains become an inexorable part of complex SoC design process. IP cores not only speedup the design productivity massively but also decreases the design period immensely. Importing these IP cores from third-party IP vendors by the system integrator or SoC designer has become a common industry practise. Previously, IP vendors have mainly focused on IP performance and IP functionality but have neglected IP security. As evidence it can be observed that in a typical IP design flow, measurement of performance and functionality is only included in the IP specification. However, prevailing usage of IP cores in SoC design process increases the
References


Chapter 05
Symmetrical Protection of DSP IP Core and Integrated Circuits using Fingerprinting and Watermarking

This chapter discusses the use of watermarking and fingerprinting for symmetrical protection of DSP IP cores and integrated circuits. Symmetrical IP core protection is a mechanism in which both seller and buyers of an IP can have signature for double-proof of ownership and whereas significantly reducing false ownership claims. The chapter is structured as follows: Section 2 discusses the fundamentals of IP core protection with emphasis on symmetrical IP core protection techniques for DSP cores; Section 3 discusses the low-cost DSP core IP core protection; Section 4 explained that methodology with a motivational example. Section 5 discusses the results of that approach. The conclusion of this chapter is provided in Section 6.

5.1. Introduction

The designs of integrated circuits have evolved into greater sophistication than ever before with the revolution of implementation and application technology in Consumer Electronics (CE) industry. The usage of digital signal processing (DSP) Intellectual Property (IP) cores [1] generated using architectural synthesis not only maintains a proper balance between time-to-market pressure and design productivity but additionally help in design cost reduction. HLS [2, 4] is an automated design process that transforms an algorithmic/behavioral description of a digital circuit or IP into its corresponding Register Transfer Level (RTL) digital hardware through numerous sub-processes like scheduling, hardware and register allocation and binding. In the process of manufacturing an IP core two entities are involved viz. seller and buyer. An IP seller also known as IP vendor is the creator of an IP, whereas an IP buyer also known as IP user is the purchaser of an IP. However, to maintain a viable application of IP cores in composite SoC-based designs, protection of both the entities against threats is extremely crucial. Let us now discuss on the protection aspect of IP buyer and IP seller: In a IP core, an IP buyer may claim buyer privilege as a buyer so that the same IP copy should not be usable/accessible to his competitors in the market. This is possible when customized specifications of an IP core are obtained by an IP seller from an IP buyer, thus creating an exclusive one-to-one mapping between both parties. Embedding a unique buyer’s signature (known as buyer fingerprint) into an IP core design facilitates detection of unlawfully redistributed/resold duplicates of an IP core by a deceitful seller [3]. Likewise, an IP seller must protect his design from piracy and false claim of ownership before selling it to an IP buyer. Embedding a unique seller’s signature (known as seller watermark) into an IP core design protects an IP core from ownership abuse [5-11] [35-38].
References


Chapter 06
Computational Forensic Engineering for Resolving Ownership Conflict of DSP IP Core

The previous few chapters focused on watermarking and fingerprinting for ownership protection. This chapter will focus on another technique called forensic engineering for ownership protection. Forensic engineering extracts features of IP cores and matches to statistically suggest the original ownership. This section discusses various steps involved in forensic engineering of a hard IP core as well as presents specific details with case study examples.

6.1. Introduction

The rapid proliferation of electronic/system-on-chip (SoC) industry along with fierce competition has demanded ways to remain competent. To beat the competition, companies seek to reduce time-to-market and design cost. These goals can be easily met through utilisation of reusable IP core(s) [4],[9]. This is because reusable IP core(s) minimise design time by reducing man-hours required to reproduce an IP. Therefore, reusable IP core has become a mandatory component of generic SoC/IC design flow. Moreover, a design process at higher level of design abstraction such as High Level Synthesis (HLS) is always crucial for complex SoCs such as DSP-multimedia cores [29],[30]. This is because higher level of design abstraction reduces design complexity and identifies optimal (low cost) design architecture based on several orthogonal design objectives. Therefore, reusable IP core(s) such as DSP-multimedia core generated through HLS is an essential component for consumer electronics devices. However, an IP core is vulnerable to various threats such as IP piracy, Trojan insertion, IP overbuilding, false claim of ownership, etc [31], [32], [40]. An estimate based on report presented in [1] shows that electronics industry loose roughly minimum 1.5 trillion USD annually due to piracy and counterfeiting [2]. Therefore, it becomes mandatory to devise methodologies that can safeguard an IP core from these aforementioned threats. There are several IP protection mechanisms to overcome these threats, as shown in Fig.6.1.

Another technique that targets protection of IP core(s) is hardware obfuscation. Obfuscation targets protection against IP piracy and Trojan insertion [32]. Hardware obfuscation aims to obfuscate a design through either structural obfuscation [5],[38] or functional obfuscation [6]. The primary aim is to increase effort of an attacker to identify correct functionality of an IP [32], thus making it hard for an attacker to secretly insert Trojan that can go undetectable during testing phase of an IC design. Further, this also makes it difficult to re-sell or utilise an IP core because its correct functionality is unknown to an adversary. Obfuscation does not aim to provide protection against ownership conflict (since it does not insert a unique ID or signature). However, functional
References


Chapter 07

Structural Obfuscation of DSP Cores used in CE Devices

In the previous few chapters, watermarking, fingerprinting, and forensic engineering have been discussed for resolving various ownership related problems. This chapter discusses structural obfuscation approaches to thwart IP piracy and reverse engineering. This approach when effective can save billions of dollars of revenue losses to CE and semiconductor industry. Specifically, a multi-level transformation based structural obfuscation process has been presented for DSP IP cores as hardware hardening technique. The chapter is structures as follows: Section 7.2 highlights the fundamentals of obfuscation with stress on structural obfuscation; Section 7.3 discusses different compiler transformation driven structural obfuscation methodology. Section 7.4 discusses low-cost structurally obfuscated design exploring technique. Section 7.5 demonstrates a multi-stage structural obfuscation technique through a motivational example. Section 7.6 presents the results of a case study.

7.1. Introduction

Today’s Consumer Electronic (CE) devices, ranging from modern smart phone, smart TV, home appliance, set-top box, tablet, digicam to recent smart speaker, are designed using System-on-Chip (SoC) platforms (Thavalengal and Corcoran, 2016; Mohanty, 2015; Kim et al., 2015). These SoCs comprises of various system modules such as memory (SRAM, Flash), A-to-D converter, custom processor or co-processor, Digital Signal Processor (DSP) kernels, A/V codecs, wireless modems, etc. Among these modules, DSP kernels in the form of Intellectual Property (IP) cores are primarily responsible for data/power intensive computation at high speed, minimal silicon area and low power in a SoC (Li et al., 2015). Thus, DSP IP cores are the heart of every SoC based CE devices. For example, ConnX D2 DSP IP core used in telecom infrastructure of voice over internet protocol (VoIP) and wireless mobile device (ConnX, 2009). In a cellular telephone system, it is used in speech encoding/decoding process. Low-end

![Diagram](image-url)

Fig. 7.1. A thematic representation of secured DSP IP core for CE devices that is resilient from adversary.
References


ExtremeTech, iphone 5 A6 SoC reverse engineered, reveals rare hand-made custom CPU, and tri-core GPU (2012).


Chapter 08

Functional Obfuscation of DSP Cores used in CE Devices

The previous chapter detailed many approaches for structural obfuscation but we now move forward to another class of obfuscation called ‘functional obfuscation’. Use of either of the techniques is the choice of design engineers. This chapter presents several methods to thwart IP piracy and RE attacks through functional obfuscation. More specifically, we will discuss IP functional locking blocks (ILBs) based logic obfuscation for DSP cores used in CE devices as hardware hardening technique (Sengupta et al., 2018). Moreover, a Particle Swarm Optimization (PSO) based Design Space Exploration (DSE) is performed to generate a low-overhead functionally obfuscated design solution for DSP cores (Sengupta and Sedaghat, 2011; Sengupta and Sedaghat, 2013). The rest of the chapter is organized as follows: Section 8.2 discusses different attack scenarios and threat model. Section 8.3 explains selected functional obfuscation techniques that are available in the literature. Section 8.4 discusses design process of functional obfuscation for DSP IP cores used in CE devices. Section 8.5 presents security analysis of functional obfuscation methodology for DSP IP core design. Section 8.6 discusses PSO-based optimization for functionally obfuscated design. Section 8.7 presents analysis on case studies/test cases.

8.1. Introduction

In the current Integrated Circuit (IC) supply chain model, multiple parties are involved to handle the increasing design complexity and cost. To avoid establishing and maintaining charge of a foundry with advanced fabrication facility, fabless semiconductor companies export their designed IC (such as DSP cores) to another company having fabrication facility. Additionally, sometimes system integrator while designing a System on chip (SoC), imports DSP Intellectual Property (IP) cores from third part IP (3PIP) vendors to meet the time-to-market requirement (Castillo et al., 2007). Thus, in this globalized business model for DSP cores, different countries and companies have different IP regulation policies and models. Therefore, in this scenario chip designing process is susceptible to many serious security threats, such as IP piracy, IP overbuilding, IP counterfeiting, reverse engineering, insertion of hardware Trojan, etc. (Sengupta and Kundu, 2017; Sengupta et al., 2018b; Wong et al., 2004; Alkabani et al., 2007). This necessitates improvement in the chip designing process to thwart these threats.

IP piracy is a process of illegal usage or selling of IP cores. An untrusted foundry, present in the design flow of an IP core can steal a design, illegally clone it and then resell it to other entity. Thus, it can bypass a substantial amount of research and development process, workforce, money and time invested by an original IP designer. Moreover, he/she can claim the ownership of
the PSO approach for generating low cost obfuscated netlist for DSP cores. In can also be noted that for very large size DSP IP cores such as JPEG IDCT and MESA (around 50K plus gates), the exploration time is not too large. Therefore, the optimization framework used in (Sengupta et al., 2018) does not suffer from scalability issue.

8.8. Conclusion

This chapter presents a low-cost, functional obfuscation mechanism for DSP IP core. This mechanism inserts reconfigured ILBs to lock a netlist of DSP IP core. Moreover, it integrates AES block to prevent SAT attack as a proactive countermeasure. Moreover, it was observed that (Sengupta et al., 2018) yielded power reduction, design cost reduction and SoO enhancement over other similar approaches. The research on functional obfuscation is still an open area and more research needs to be conducted for protection of other hardware circuits such as combinational/sequential circuit benchmarks against SAT attacks. There are new attacks such as approximate SAT and signal probability skew that are being launched to nullify the effect of Anti-SAT blocks used in conjunction with combinational/sequential circuit benchmarks. There is significant scope of work in the future, in this direction.
8.9. Exercises

1. What is functional obfuscation?

2. What is the difference between structural obfuscation and functional obfuscation in the context of DSP cores?

3. What are the Disadvantages of functional obfuscation?

4. What is Threat model of functional obfuscation?

5. How/ where is locking performed?

6. What are the properties of ILBs?

7. Why functional obfuscation is vulnerable to SAT attack for combinational/ sequential circuits?

8. Why functional obfuscation is not vulnerable to SAT attack for DSP core?

9. What is CNF?

10. How to find CNF for basic gates?

11. How to determine DIP?

12. How does AES protect against removal attacks of ILBs?

13. How is AES customized during insertion with obfuscation design?

14. How is AES removal attack prevented?

15. Design an obfuscated FFT (n=8).

16. What are the possible alternatives of AES for functional obfuscation?

17. What is key sensitization attack?

18. Design an ILB with AND, NAND, NOT, XOR, XNOR gates.

19. What is the difference between pairwise security and multi-pairwise security?

20. What is the role of random variable ‘μ’ in functional obfuscation?

21. What is run of key gates? How is it a drawback in the context of obfuscation?

22. Design a lightweight AES that uses less than 1 % FPGA resources.

23. How do you determine the design cost of an functionally obfuscated DSP design.
References


Altera Quartus, Available: [https://dl.altera.com/13.0sp1](https://dl.altera.com/13.0sp1), last accessed on 2018.

Joint Picture Export Group (JPEG) is the most commonly used image compression standard in the world. One can’t comprehend a consumer electronic system that doesn’t process a JPEG. Without JPEG there is no smart phone photography, no social media. So, authors feel strongly that this important multimedia core ‘JPEG’ needs to give well deserving credit in terms of securing it when security/protection of ‘DSP core’ has been a major focus of all the discussions in this book so far. The chapter is organized as follows: Section 9.2 provides an overview of DCT-based JPEG compression and decompression process. Section 9.3 explains design process of generating structurally obfuscated JPEG CODEC IP core; Section 9.4 provides a detailed insight on implementation process of obfuscated JPEG codec IP core in a CAD synthesis tool. Section 9.5 provides implementation and analysis of JPEG CODEC IP core as well as compressed images through the devised JPEG CODEC IP core.

9.1 Introduction

Currently most of the modern Consumer Electronics (CE) device comprises of a dedicated lens or camera to capture and/or display digital images, such as smartphone, tablets, scanner, laptop, smartwatch etc (Thavalengal and Corcoran, 2016; Kim et al., 2015; Corcoran and Andrae, 2014; Tang et al., 2016). Due to the enhancement of camera lenses, recording components and displaying components, current digital imaging systems are capable of capturing and displaying high-resolution images (Corcoran et al., 2001; Andorko et al., 2011). As high-resolution images contain too much detailed information, therefore, they are large in size. Storing or transmitting these large size images is a critical issue for storage space and transmission bandwidth respectively. Reducing the size of an image while storing and/or transferring it, is one of the popular and commercially successful techniques to address this crisis. Joint Photographic Experts Group (JPEG) standard formed in 1992 proposed Discrete Cosine Transformation (DCT) based image compression. Image compressions are of two types: (i) lossy and (ii) lossless. In lossy image compression, less important information of an image is discarded permanently (Mohanty 2003; Mohanty 1999). Camera (Corcoran et al., 2001; Andorko et al., 2011) in a smartphone, tablets, laptop, smartwatch etc. uses lossy image compression (Hnesh et al., 2016). In lossless image compression, no loss of information occurs. Camera in medical imaging (Bilgin et al., 1998), satellite imaging, forensic imaging etc. uses lossless image compression (Li et al., 2017; Scarmana et al., 2015).

DCT-based JPEG image compression is lossy by nature (Obukhov et al., 2008). DCT segregates an image into multiple sub-parts or blocks based on the visual quality of the image and then convert each block to the frequency domain from spatial domain. It discards small high-frequency components; therefore, DCT-based JPEG image compression method is lossy.
References


Chapter 10
Advanced Encryption Standard (AES) and its Hardware Watermarking for Ownership Protection

In this era of consumer electronics cybersecurity is one of key challenges. Any security, privacy, or protection methods that is deployed relies on cryptography. Advance Encryption Standard (AES) is one of heavily used cryptography algorithms for its advantages. This chapter is dedicated to the process of AES and its hardware design in the form of IP core. Several hardware security techniques rely on AES IP core as an important block. Additionally, since this is such an important core its self protection against forgery/piracy is also crucial. This chapter also discusses AES IP core protection using watermarking.

10.1 Introduction

Cryptography is widely used in everyday life, ranging from established applications such as wireless local area network, procuring items with a credit or debit card, installing a software update, smart cards, banking application, voice of internet protocol (VOIP) to emergent domains such as electronic health system, Internet of Things (IoT) security, smart city security and hardware security [(Paar & Pelzl), (Tehranipoor & Bhunia 2018), (Sengupta 2017), (Sengupta 2015), (Sengupta, Bhaduria & Mohanty 2017), (Sengupta & Bhaduria 2016), (Sengupta & Sedaghat 2011), (Mishra, Bhunia and Tehranipoor 2017), (Sengupta & Sedaghat 2013), (Sengupta & Roy 2017), (Sengupta, Roy, Mohanty & Corcoran 2017)]. Cryptography comprises of cryptographic algorithms which are symmetrical by nature. There is tremendous usage of symmetric ciphers, especially for encryption of data and integrity check of messages. Further, cryptographic protocol deals with the application of cryptographic algorithms. An example of cryptographic protocol is Transport Layer Security (TLS) scheme, widely employed in browser Advanced Encryption Standard (AES) is a very popular symmetric cipher used today. The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data recognized by the U.S. National Institute of Standards and Technology (NIST) (). In the context of AES (Rijndael family), three members were designated by NIST, each with a block size of 128 bits, but dissimilar key lengths: 128, 192 and 256 bits. It is a mandatory standard in several industry/commercial systems and US government applications such as Wi-Fi encryption standard IEEE 802.11i, TLS, VOIP [(Paar & Pelzl, 2009)].

In this chapter, we focus on the following aspects (a) AES algorithm – description of each step and its flow diagram (b) corresponding hardware mapping of AES block cipher – overview of how each step can be mapped to a specific hardware sub-block (c) key scheduler – description of each step (d) corresponding hardware mapping of key scheduler used in AES (e)
References


Chapter 11

Hardware Approaches for Media and Information Protection and Authentication

Technology scaling has allowed us to design high performance devices with a low power consumption. The advent of Internet of Things has increased the versatility of data collection and there are many different ways of collecting and transferring data over the internet. The data that is being collected is also in different forms, text, images, videos and audio. When they are shared, for a legit use, attackers can break the security and use them for illegible purposes or claim ownership to sell them commercially. This has been the trend lately where many counterfeit products are appearing in the market. This section discusses the digital watermarking, different schemes of digital watermarking and how a media object can be secured using a watermark. They are also not completely resistant to attacks and measures need to be taken to secure the content that is being watermarked. The chapter also presents different issues with the watermark implementations, attacks and countermeasures to those attacks on watermarking. Section 1 presents a broad overview of the intellectual property (IP) protection. Section 2 discusses the generic overview and components of any watermark system. Section 3 summarizes the various types of watermarks. Various applications of watermarking are discussed in Section 4. Desired characteristics of watermarks are presented in Section 5. Sections 6 discusses the technical challenges of the watermarking. Hardware based watermarking systems available in the current literature are discussed in Section 7. Section 8 discusses about watermarking in smart vehicles. Section 9 discusses about medical signal authentication. Section 10 highlights side channel information leakage and its countermeasures. Section 11 outlines various forms of attacks on watermarks and watermarking systems. Section 12 presents the difficulties involved in making use of them in practice.

1 Intellectual Property (IP) Protection - A Broad Overview

With the advent of new technology, new devices are being introduced into the world and high performance applications are being designed. With better systems coming out every-day, there is also a problem that they are used for various malicious applications like counterfeiting. This is a major problem in hardware and also media. Many people now-a-days are producing content and sharing it with the world [68, 47]. But the content that they own is being illegally used by many commercially without paying royalties to the owner and in some cases, misusing the content. This raises many problems pertaining to the Intellectual Property Rights and their protection. Fig. 1 gives a broad overview on the area of counterfeiting. An image can be produced by the owner and watermarked but an attacker can attack the watermark, tamper or remove it from the image and claim ownership. This creates many issues on the copyrights and ownership Rights.

1.1 Digital Rights Management (DRM)

Fig. 2 shows the different media and the threat levels that they are vulnerable to attacks. A cinema will have a high privacy where-as a broadcast content will have low security. This has become a major issue lately where the content of the owner is being reproduced without paying a royalties ot he owner.

In such cases, the owner will have copyrights violated and misses out on the royalties that are entitled legally. When a content media like a digital video disc (DVD) or BluRay is produced with a video content, it is considered to be secure with the watermarks embedded in it. But there are also many attacks that are available that can remove or tamper the watermark on the content. Fig. 3 shows the different types of multimedia that are available on the internet. Many of the audio services provide audio to the user at a monthly cost. But tampering with the audio that is broadcast over the internet is not difficult with the technological advancements that are
References


Chapter 12

Physical Unclonable Functions (PUFs)

It has been the practice to store information under lock and key for safeguarding it. Even today, we use cryptographic primitives to store information securely under lock and key, encryption and decryption. For the process of cryptography, keys are necessary for any operation. But these keys should be stored in the memory so that they can be used whenever necessary. When a key is stored in the memory, it can be stolen by the adversary using various methods. So storing it in a non-volatile memory is not an option in this age of security threats. Physical Unclonable Functions are the promising security primitives that are used for generating the keys instead of storing them in the memory. These modules use the naturally occurring manufacturing variations in the fabrication process for generating the keys for cryptographic purposes. This chapter discusses different types of PUFs. Section 1 gives a brief introduction of Physical Unclonable Functions (PUF). Section 2 discusses working principles of Physical Unclonable Functions (PUF). Section 3 discusses different characteristics of a PUF design. Section 4 presents different classifications of PUFs. Various designs of PUF based on ring oscillators is presented in Section 5, based on multiplexers and reconfigurability are presented in Section 6. Static Random Access Memory (SRAM) based PUFs are presented in Section 7, Memristor-based PUFs are presented in Section 8 and Diode based PUFs are presented in Section 9. There are also Non-Silicon based PUF designs like Carbon PUFs are presented in Section 10. Microprocessors can also be used for implementing the PUF designs which are presented in Section 11. Magnetic material based PUFs are presented in Section 12 and the Field Programmable Gate Array (FPGA) implementations of PUF and security measures for FPGA are presented in Section 13. Some case study applications are presented in Section 14. Further the issues and challenges that are faced during the design of PUF modules are presented in Section 15. The conclusions and future directions are presented in Section 16.

1 Introduction

The first transistor was invented in 1948. With the introduction of the transistor, vacuum tubes occupying huge space disappeared and led to the invention of the Integrated Circuit (IC) in 1958 [30]. Along came the Moore’s Law which states that the number of transistors on an Integrated Circuit will double every two years. This came true until recently and the number of transistors on a single chip has exponentially increased since its first introduction. With the introduction of the new 10nm technology, each square millimeter of the IC can be packed with 100 million transistors [13]. With technology improving at such a drastic pace, it has penetrated into almost every sphere of human life. Day-to-day activities such as communications, business, financial transactions and so on depend on technology. Digital footprint of human being has become an inevitable parameter and unavoidable [18]. Internet of Things (IoT) has become an integral part of our lives. In an IoT environment, every device is connected to the network and will have a unique Internet Protocol (IP) address [56]. Smart Cities, Smart Grid, Smart Healthcare and so on are various forms of IoT.

With so many devices connected to each other, there are security concerns that are raised. The data that is being collected by various applications, sensors and other devices should be stored securely. There are many attacks reported recently where security needs to be given the highest importance [8, 9]. To secure the data that is being generated, cryptography is being used. It has been around for a very long time. Cryptography is the process of concealing a message or information by converting it into unreadable text and only the end user will be able to extract the original information from the text. It was found that Egyptians used such techniques in the year 1900 B.C. [2]. Various algorithms are available currently for encryption and decryption which can transfer the data securely. National Bureau of Standards proposed data encryption standard (DES) algorithm which lasted for 20 years. Then came advanced encryption standard (AES) algorithm which is very popular now but there have been reports of AES being successfully broken [49]. $7.5 Billion is estimated to be lost by the US semiconductor industry because of IC counterfeiting [61]. Besides all of this, in the case of many devices, sensors or applications, the device itself will not be monitored all the time. It will be in a remote
References

1. http://www.eecs.mit.edu/news-events/media/mit-spinoff-verayo-developed-srini-devadas-gains-increased-
15. Ganta, D., Nazhandali, L.: Study of IC Aging on Ring Oscillator Physical Unclonable Functions. 15th International Symposi-
17. Gassend, B., Clarke, D., Dijk, M.V., Devada, S.: Controlled Physical random Functions. 18th Annual Computer Security
IP Core Protection and Hardware-Assisted Security for Consumer Electronics

*IP Core Protection and Hardware-Assisted Security for Consumer Electronics* presents established and novel solutions for security and protection problems related to IP cores (especially those based on DSP/multimedia applications) in consumer electronics. The topic is important to researchers in various areas of specialization, encompassing overlapping topics such as EDA-CAD, hardware design security, VLSI design, IP core protection, optimization using evolutionary computing, system-on-chip design and application specific processor/hardware accelerator design.

The book begins by introducing the concepts of security, privacy and IP protection in information systems. Later chapters focus specifically on hardware-assisted IP security in consumer electronics, with coverage including essential topics such as hardware Trojan security, robust watermarking, fingerprinting, structural and functional obfuscation, encryption, IoT security, forensic engineering based protection, JPEG obfuscation design, hardware assisted media protection, PUF and side-channel attack resistance.

**About the Authors**

*Anirban Sengupta* is an Associate Professor in Computer Science and Engineering at Indian Institute of Technology (IIT) Indore. He is the author of 172 peer-reviewed publications. He is a recipient of honors such as IEEE Distinguished Lecturer by CESoc in 2017, IEEE Computer Society TC- VLSI Editor Award in 2017 and IEEE Computer Society TC- VLSI Best Paper Award in iNIS 2017. He holds around 12 Editorial positions. He is the Editor-in-Chief of IEEE VCAL (IEEE CS- TCVLSI) and General Chair of 37th IEEE International Conference on Consumer Electronics 2019, Las Vegas.

*Saraju P. Mohanty* is a tenured full Professor at the University of North Texas (UNT). He has authored 280 research articles, 3 books, and invented 4 US patents. He has received various awards and honors, including the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, IEEE Distinguished Lecturer by the Consumer Electronics Society (CESoc) in 2017, and the PROSE Award for best Textbook in Physical Sciences & Mathematics in 2016. He is the Editor-in-Chief of the IEEE Consumer Electronics Magazine (CEM). He has received 4 best paper awards and has delivered multiple keynotes.