

# Preface

The increasing production costs of electronic devices and changes in the design methods of integrated circuits has led to emerging threats in the microelectronics industry such as counterfeiting, illegal copying, reverse engineering and theft. The designing process of a microelectronic Very Large Scale Integration (VLSI) circuit evolved, in last decades, towards a continuously growing « design-reuse » method trend. It is structured today with standard functional blocks vendors (around 50 companies worldwide) delivering « Intellectual Property » blocks, i.e. « IPs ». Those companies face a strong counterfeiting as many other industrial domains, with a strong impact on their business model without any technical solutions to exactly count the dissemination of their models in terms of physical unit devices. Since more than a decade, IP protection has become a critical issue for the micro-electronic industry. Electronic devices are increasingly becoming the target of counterfeiting, cloning, illegal copy, theft and malicious hardware insertion (such as hardware Trojans). All these threats cost a lot of money and time to the legal industry. For example in 2014, electronic items counterfeiting was estimated to account for about 7% of the semiconductor market, which represents a loss of around US\$ 22 billion in 2014 for the lawful semiconductor industry. Moreover, these threats' impacts are huge employment loss and customer dissatisfaction. However, unlike for software in computer science, protection of hardware IP is not fully included in electrical engineering curriculum. Most of the VLSI designers are not aware about the threats and the means of protection. This book aims to fill the gap by highlighting promising works that attempt to meet the IP protection challenge.

The electronic industry needs solutions to fight against theft, illegal cloning and reverse engineering of intellectual properties. More precisely, designers need salutary hardware, i.e. embedded hardware systems, hardly detectable/difficult to circumvent, inserted in an integrated circuit or a virtual component, used to provide intellectual property information (e.g. watermarking or hardware licensing) and/or to remotely activate the circuit or IP after being manufactured and during its use. When discussing about IP protection, the Digital Right Management (DRM) concept is certainly an important issue for the IP market. The Digital Rights Management (DRM) principle is generally well known for the exchange of files

(music, video, etc.), or software management. Specialized solutions concerning professional software are behind a business called “Software License Management”. The concept of DRM can be transposed to the IP world, which is a really new concept on this area.

We hope that the readers of this book will learn how an IP can be threatened and to increase the security of the IP by using several different means (hardware obfuscation/camouflaging, watermarking, fingerprinting (PUF), functional locking, remote activation, hardware Trojan detection, protection against hardware Trojan, use of secure element, digital right management, ultralightweight cryptography, etc.). This book will not be like a cookbook as each IP needs specific protection scheme; but it will be like a reference book for design space exploration of security means of IP protection.

Saint-Étienne, France  
Montpellier, France

Lilian Bossuet  
Lionel Torres



<http://www.springer.com/978-3-319-50378-3>

Foundations of Hardware IP Protection

Bossuet, L.; Torres, L. (Eds.)

2017, VII, 240 p. 125 illus., 48 illus. in color., Hardcover

ISBN: 978-3-319-50378-3