硕士学位论文

旨在防伪造的主动式 IC 计量技术研究

SUTDY OF ACTIVE IC METERING FOR ANTI-COUNTERFEIT

钱学森

哈尔滨工业大学

2017 年 12 月

国内图书分类号：TN47　　　　学校代码：10213
国际图书分类号：621.38　　　　密级：公开

工学硕士学位论文

旨在防伪造的主动式 IC 计量技术研究

硕士研究生：钱学森
导　　师：崔爱娇　副教授
申请学位：工学硕士
学　　科：微电子学与固体电子学
所在单位：深圳研究生院
答辩日期：2017 年 12 月
授予学位单位：哈尔滨工业大学

Classified Index: TN47
U.D.C: 621.38

A dissertation submitted in partial fulfillment of the requirements for the professional degree of Master of Engineering

STUDY OF ACTIVE IC METERING FOR ANTI-COUNTERFEIT

Candidate：	Qian Xuesen
Supervisor：	Associate Prof. Cui Aijiao
Academic Degree Applied for：	Master Degree in Engineering
Specialty：	Microelectronics and Solid State Electronics
Affiliation：	Shenzhen Graduate School
Date of Defense：	
Degree-Conferring-Institution：	Harbin Institute of Technology

摘　要

随着半导体制造工艺的发展，如今，人们已经可以将数以亿计的晶体管集成在一块芯片上，集成电路（IC）的设计复杂度也随之迅猛提升。用于芯片制造的资金投入也迅速攀升。在这种情况下，越来越多的公司选择将自己设计的芯片交由代工厂进行生产制造。该模式促进了芯片设计公司和代工厂各司其职，各自做自己最擅长的事。然而，这种不对称的生产模式也导致了很多安全及知识产权的问题。当设计公司将他们的设计提交给代工厂进行生产制造时，设计公司并不能够有效控制芯片生产数量，因为在生产制造过程中，代工厂已获得该芯片的所有制造信息。这种IC设计者与代工厂之间的不对等的关系给设计者带来了诸多不利。为了能够使设计者有效的控制芯片的后端生产，研究者提出了IC计量技术，这项技术能够使得设计者通过主动或被动的措施，避免这种过量生产的问题。根据工作机理，现有的计量技术可以分为被动式IC计量技术与主动式IC计量技术两种。

被动式IC计量技术是指给每一块生产出来的芯片分配一个独特唯一的ID，并将这些ID记录在数据库中。如果测得一块芯片的ID没有在数据库中或者两块芯片有一样的ID，那么就可以认为代工厂过量生产了芯片。但这种技术仅仅能检测到过量生产的芯片，而过量生产的芯片依然能够正常使用。并且，需要花费的大量精力去检测和统计市场上是否有过量生产的芯片。而主动式IC计量技术不仅给每块芯片分配了一个独特的ID，并且给芯片加了一把锁。当将设计描述交给代工厂进行生产后，芯片制造出来之后是锁住的，不能正常工作的。这些制造出来的芯片必须从设计者手中获取相应的独特钥匙，并对芯片进行解锁激活后才能进行后续的测试、封装以及流向市场。从而，即使代工厂多生产了芯片，这些芯片也是不能通过测试以及流向市场的，因为这些多生产的芯片没有设计者提供的独特钥匙。因此，主动式IC计量技术能够更好的保护设计者的知识产权。

通过以上对比，我们知道主动式IC计量技术能够更有效的保护设计者的知识产权。根据主动式IC计量技术的加锁机理的不同，可将主动式IC计量技术分为外在式IC计量技术和内在式计量技术两种。然而，现存的主动式IC计量技术不管在开销上还是安全性上都有一定的不足。在外在式的主动计量机制中，首先，并没有很好的克服ID生成器的稳定性不足的问题。因为目前物理不可克隆函数（PUF）多用于ID的生成，而PUF响应总是随着环境温度以及电压的变化发生变化，而

ID 又与芯片的钥匙相关。如果芯片的 ID 发生变化，将导致原来的钥匙失效。其次，现存外在式的加锁机制多为在组合逻辑电路的非关键路径上插入异或门，然而这种加锁机制可能给电路的时序造成影响。在内在式的主动式计量机制中，目前，主要通过扩展原始设计中的 FSM 实现加锁设计。然而，这种计量机制中，由于解锁时从额外增加的状态回到初始复位状态的入口单一，如果，攻击者识别出这个复位状态并通过入侵式的攻击方法，并旁路掉额外增加的状态，使得电路直接上电到初始复位状态，这将导致该保护方案失效。如何克服主动式 IC 计量技术的不足，这是现今这个课题的研究热点以及难点。在本课题中，我提出了两个新的主动式计量机制，不仅能帮设计公司保护他们的知识产权，并且能有效的克服以上这些主动式 IC 计量技术中的缺点。

本课题首先提出了一个新的外在的主动式 IC 计量机制。在该机制中包含三个部分，锁的机制，钥匙产生机制以及控制部分。在介绍加锁机制前，我们先了解一下扫描链结构，我们知道，为了提高芯片的测试效率，扫描链结构已经广泛应用于芯片设计。扫描链主要是通过把电路中原有的 D 触发器转变成扫描单元并将这些单元连接而形成。扫描单元有一个控制工作模式的 *tc* 端口，当测试控制端 *tc*=0 时，扫描单元工作在测试模式，扫描链传输测试数据；当 *tc*=1 时，扫描单元工作在正常模式，其功能等同于原始设计中的 D 触发器。由此可见，*tc* 端口可以用于控制电路中时序器件的工作模式。基于此，我提出了基于对扫描单元的 *tc* 端口的加锁实现机制。具体来说，在扫描单元的 *tc* 端口和系统的测试控制信号 *TC* 之间，可以插入一个反熔丝结构，该反熔丝受控于输入钥匙和正确钥匙的比对结果。两钥匙一致，反熔丝结构导通，扫描单元的 *tc* 信号可正常受控于系统的 *TC* 信号。否则，扫描单元的 tc 信号处于混乱状态，在正常工作时，不能作为 D 触发器正常工作，整个电路工作异常。该加锁机制在输入钥匙正确的情况下，通过反熔丝结构的引入可以使电路永远处于解锁状态，克服了基于 PUF 的钥匙的可靠性不足的问题。另一方面，该锁结构仅仅与时序器件的工作模式有关，因此，并没有给原始设计的时序造成任何负面影响。

在钥匙机制中，PUF 用于给每块芯片产生独一无二的 ID。基于 PUF 的钥匙，在公钥作用下，钥匙在芯片中通过非对称加密算法进行加密，加密的数据将反馈给设计者。设计者根据其所掌握的私钥对加密数据进行解密生成解锁芯片的钥匙。然后将钥匙传给代工厂对芯片进行解锁。仅当一个正确的钥匙输入芯片时，芯片才能够被解锁并正常工作。该计量机制允许用户多次输入钥匙进行芯片解锁。一旦芯片解锁成功，加锁电路将永久性失效。

在控制单元中包含四个计数器。一个 2bit 的计数器用于判别芯片是处于正常工作模式，还是测试模式。一个 Q-bit 的钥匙计数器用于记录输入钥匙的长度。而

输入的钥匙与 PUF 钥匙将通过一个 2 输入的异或门进行比对。比对结果由另一个 Q-bit 的结果计数器记录。并且该计数器的输出端接一个多输入与门，用于给后面下降沿触发的 D 触发器产生一个解锁信号。如果输入的钥匙正确，下降沿触发的 D 触发器将产生一个解锁信号使电路解锁。该计量机制对原始设计引入的面积开销极低，并且主要是非对称加密算法引入的，且对芯片测试没有影响。而且，该设计方案也能抵御众多典型的入侵式和非入侵式攻击。

本课题还提出了一个改进的内在主动式 IC 计量技术。该方案对一个基于扩展有限状态机（BFSM）计量方案进行了改进。该方案中，原始有限状态机引入了众多伪初始状态。PUF 的响应信息用于从众多伪初始状态中唯一确定一个上电初始状态。FSM 修改之后，这些伪初始状如何跳转到真实初始状态，只有芯片设计者知道。原始设计中单一的真实初始状态是芯片正常工作的唯一入口，这为攻击者旁路掉所有伪初始状态而直接进入真实初始状态提供了可能。为了克服这个安全上的漏洞，本课题提出了一个在原有 FSM 中增加伪真实复位状态的机制来迷惑攻击者。在不知道设计细节的情况下，一个人很难识别真正的复位状态。因此，攻击者不能够旁路掉额外增加的状态以及新增的转移而致使主动式计量机制失效。

在此方案中，我们首先复现了原来的基于 FSM 的内在式计量机制，从所增加的伪初始状态中设计回到真实初始态的路径使得电路能够正常工作。为了提高攻击者识别真实初始状态的难度，我们添加了伪真实复位状态，并进行规则检查，如果符合，开始进行综合。这些伪真实复位状态有真实初始状态的部分性质，但并不是全部。即也有路径从额外增加的伪初始状态进入伪真实复位状态，使得电路工作。而且，这些伪真实复位状态拥有和真实复位状态相同的输出转移。如真实复位状态 s_0 的输出转移为：输入“01”，输出为“1”，并实现 s_0 跳转到 s_1。那么，伪真实复位状态也将会在相同的输入条件下，输出“1”，并跳转到 s_1。而伪真实复位状态和真实复位状态相同的输入转移却不同。通过这种方法，我们提高了设计者识别原始复位状态的难度，并增加了攻击者旁路额外增加伪初始状态的难度。在此方案中，通过增加伪真实复位状态的方法，提高了原有计量机制抗攻击的能力，并且此方案，在原来的基础上仅仅引入了一个低的开销。

关键词：过生产；盗版；外在计量机制；内在计量机制；物理不可克隆函数

ABSTRACT

With the advances in semiconductor process technology, billions of transistors now can be integrated in a single die. The complexity of integrated circuit (IC) design has hence been increased dramatically. This also causes the investment in IC fabrication to increase rapidly. So lots of companies choose to outsource their IC design to other desperate foundries for fabrication. This facilitates the fabless and foundry to do what they do best. However, this also created an asymmetric IC overbuilding problem: as the owner of the design intellectual property (IP), the fabless design companies will not have the control on how many copies of their design will be fabricated by the silicon foundries while the foundry can fabricate chips of any number. In order to have a good control manufacture processing, IC metering is proposed to overcome this kind of problems. Existing IC metering techniques can be classified into passive metering or active metering. Compared to the passive metering, the active metering enables the fabless to protect his own intellectual property (IP) more efficiently and it hence attracts more interest. In this work, some new active metering methods are explored to help the fabless to protect the copyright of their designs.

An improved external active metering method was first proposed. Lock was inserted on the test control (TC) port of some scan flip-flops. Without a correct key, these flip-flops cannot work normally under normal mode. Physical unclonable function (PUF) was adopted to generate a unique key for each fabricated IC. The PUF key is encrypted by public-key cryptographic (PKC) algorithm and the passed to the design house for decryption with his private key. The decrypted key was then passed to the foundry house. Only with the correct key input, can the design be unlocked and work normally. Such locking scheme will not affect the timing of the functional path. Also, this metering method allows multiple input of key friendly. After the first successful activation, the unlocking circuitry will not function any more, which overcomes the weakness of multiple queries of correct key from design house due to the variation of PUF key with environmental change or aging. The metering method just incurs acceptably low area overhead and no compromise of testability. It can resist typical attacks.

This work also proposed an improved internal metering method based on a scheme of boosted finite-state machine (BFSM). The FSM of an original design is boosted with multiple pseudo initial states introduced. PUF response is used to uniquely determine the power-up state from multiple newly introduced states. The FSM was modified such that only designer knows what to input to invoke the design to transit from the power-up state to the original initial state. Solo initial state of the original design was an obvious entrance to the normal chip operation and such metering scheme was vulnerable to the attack based on bypassing all the pseudo initial states. To overcome this weakness, it was proposed to introduce extra original initial states to perplex the attacker. It is difficult for one without the knowledge of design detail to identify which is the true original initial state. Thus, he cannot easily bypass all newly introduced states and their transitions to original initial state to nullify the IC metering scheme. Little overhead is incurred while the resilience of IC metering against the invasive attack is improved.

Keywords: overbuilding, piracy, external metering, internal metering, PUF

ACKNOWLEDGEMENT

First of all, I would like to give my greatest gratitude to my supervisor, Dr. Cui Aijiao. During my study for master's degree, she gave me a lot of teaching, encouragement, help and support, both in study and in life. She encouraged me to put forward my own new ideas and put them into practice in my research work. Once there is some achievement, she supported me to share it with peers. Without the support of the Dr. Cui, it is really hard for me to believe that I could have a chance to participate in a cutting-edge international academic conference and give report. The experiences of participating in academic conferences are not only valuable memories during my school days, but also benefited me in my later working and life. Dr. Cui's positive attitude in life is always encouraging me to look for the sunny side of life and pass the positive energy to everyone around me.

My family and friends gave me a lot of spiritual support in my school days. When the negative emotion covered me, they forgave my willfulness and accepted my talk. They always take the dark cloud away, and bring the sunshine to me. In the future, I hope to be able to do my best to reward them for their unselfish favors.

Give thanks to all dear teachers who gave me guidance during my school days.

I am so grateful to professors who took valuable time to review my dissertation and gave me useful criticism.

I give my appreciation to each friends in the lab, Luo Yanhui, Wang Jiadong, Huang Xiaonan, Wang Wenxuan, Yang yan, Zhou wei and Chang zhenxing. They provided me plenty advices about my experiments and dissertation.

CONTENTS

Page

List of Tables

Table **Page**

List of Figures

Figure **Page**

Nomenclature

AICM	Active IC Metering
AMD	Advanced Micro Devices
ASIC	Application Specific Integrated Circuit
BFSM	Boosted Finite State Machine
CK	Common Key
CUT	Circuit Under Test
DFT	Design for Testability
ECC	Error Code Correct
EK	Encrypted Key
EPIC	End Piracy in Integrated Circuits
FF	Flip-flop
FIB	Focused Ion Beam
FPGA	Field Programmable Gate Array
FSM	Finite State Machine
IC	Integrated Circuit
ID	Identification
ICID	Integrated Circuit Identification
IK	Input Key
IP	Intellectual Property
LSB	Least Significant Bit
MK	Master Key
MSB	Most Significant Bit
NVM	Nonvolatile Memory
PKC	Public-Key Cryptography
PUF	Physical Unclonable Function
RCK	Random Common Key

RSA	Rivest-Shamir-Adleman
RUB	Random Unique Block
SD	Scan Data
SFF	Scannable Flip-flop
SI	Scan In
SO	Scan Out
SoC	System-on-chip
STG	State Transition Graph
TC	Test Control
TI	Texas Instruments
TRN	True Random Number Generator
UK	Unique Key
VLSI	Very Large Scale Integrated Circuits

CHAPTER 1
INTRODUCTION

1.1 The Problem of IC Overbuilding

With the advances in semiconductor process technology, billions of transistors now can be integrated in a single die and the design complexity of integrated circuit (IC) has increased dramatically. This also causes the investment in IC fabrication to increase rapidly. Most design houses today cannot afford the in-house manufacture and have to outsource the fabrication of their chips. Such horizontal business model facilitates the fabless design houses and the foundries to do what they do the best and focus on design and manufacture, respectively. In this business mode, design houses can not only lower their manufacturing cost but also can enjoy the advanced fabrication process. Even the largest IC companies such as Advanced Micro Devices (AMD) and Texas Instruments (TI) have claimed that they will outsource some of their production to silicon foundries worldwide to low the fabrication cost, especially sub-45-nm fabrication [1].

However, such horizontal business model makes the IC supply chain face some risks of security. For example, a hostile IC design house may reverse engineer the IC from other company (IP venders) in a destructive way [2] to reduce the developing time.

Another more serious problem is IC overbuilding. It is caused by the asymmetric relationship between design houses and foundries: as the owner of the IC design, the fabless companies have no control on how many copies of their design will be fabricated. The silicon foundry can however fabricate a design at any quantity or even insert some malicious design into the original design. However, this is totally transparent to the IC designer.

As shown in Figure 1-1, Alice denotes a fabless design house and Bob denotes a silicon foundry. Alice delivers its design specification in GDS II or OASIS files to Bob and signs a contract with Bob on fabrication of *n* chips. According to the contract, *n* copies should be sent back to Alice by Bob. However, Bob may fabricate *m* extra chips and then ship these overbuilt *m* copies into grey market to gain great profits at very low cost.

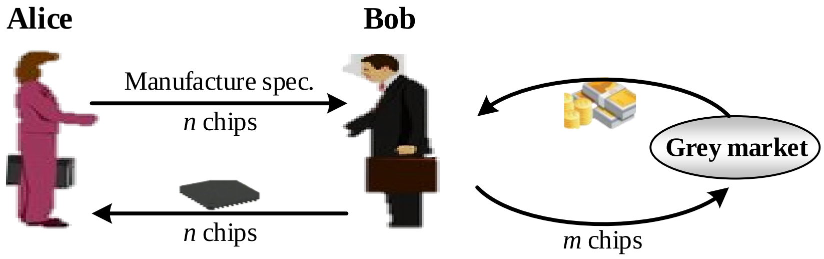

Figure 1-1. Overbuilding problems in supply chain.

This overbuilding problem not only causes great financial loss to the IC owners, but also may cause security risk to a nation. If the overbuilt chips are used in security-sensitive scenarios such as military or defense systems of adversary, a catastrophic damage is unavoidable. Therefore, there is an urgent need to find effective countermeasures to solve the IC overbuilding problem.

1.2 Related Countermeasures

To protect the IC from being overbuilt, the methods based on license and deterring can be exploited to prohibit the illegal copy or distribution. However, these traditional methods cost much time, money of the IC owner and sometimes the third party needs to be involved. Then the detection [3] methods were explored to protect the intellectual property of IC owner. The detection methods propose to insert the authorship information into the IP core or IC during the design phase. When some chips are susceptible to be illegally copied, the chip can be invoked to unload the authorship information for authentication. Different from the methods based on license or deterring, the method based on detection enables the owner of IP or IC to self-protect their own product.

The detection methods can be classified into watermarking method [4] and fingerprinting method [5, 6]. The mainstream watermarking and fingerprinting methods always transform the authorship information into extra constraints, which will be inserted into an optimization process so that the solution to the optimization is limited into a very small set. Then the probability that a design without specific information inserted achieves the same solutions is sufficiently low. And this low probability can then be used as the proof of authorship. However, as a passive way to protect the copyright of the chips, digital watermarking and digital fingerprinting cannot guarantee that every illegally copied chip to be effectively traced or identify how many chips have been theft or illegally distributed. Also, these methods always involved law issues, which will cost much time, money of the owner of the IC.

In 2001, Koushanfa and Qu first proposed the technique of IC metering [7]. The IC metering technique involves a set of complete security protocol, in which, the owner of IC can actively or passively count the number of manufactured IC or control the post-fabrication by remotely disable/enable the working of the ICs. The metering technique can benefit both the business and the military security.

1.3 IC Metering

The existing IC metering techniques can be classified into passive IC metering [7-9] and active IC metering [10]. The passive metering implements the statistics of the number of manufactured chips by assigning a unique ID to each chip. This technique require the IC designer to perform much investigation and statistics on market. Based on whether a chip with an ID recorded in database is detected for multiple times, the IC designer can know whether the IC is overbuilt. However, the passive metering method cannot prohibit the illegally copied chips from being distributed or applied. On the contrary, the active metering technique can not only trace the illegal copies, but also implement the scheme that the fabricated IC without authentication from the IC designer cannot work normally.

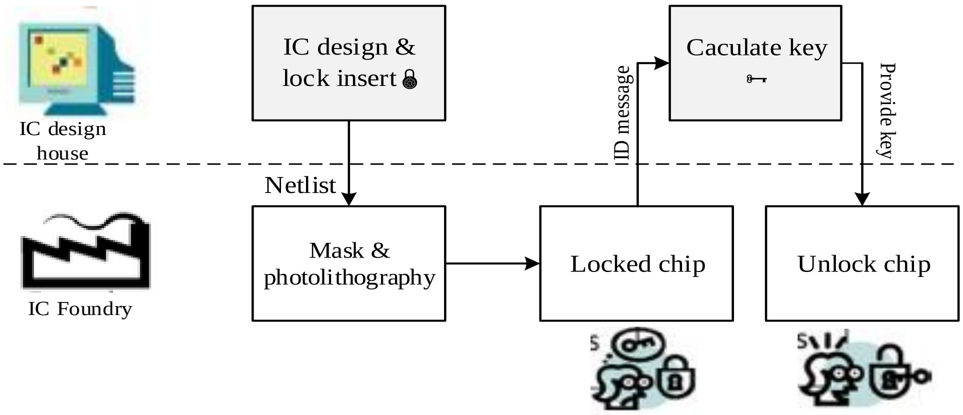

Figure 1-2. Typical active IC metering method.

In a typical active IC metering technique, as shown in Figure 1-2, the designer inserts a lock into the chip during the design phase. Each chip should have a unique and unclonable mark upon fabrication. This can be achieved by using physical unclonable function (PUF) [11-18, 47-49]. PUF can use the unique and unpredictable timing or current characteristics to create an unclonable ID for each chip. Designer can use the ID and the lock structure to create a unique key for each manufactured chip. As only the designer knows the high level design, he can achieve the unique key to unlock each chip. By this way, the designer can effectively count the number of the fabricated chips.

The existing active IC metering can be classified into the internal active metering and the external active metering. In the internal active metering [10], the lock is embedded into the behavioral synthesis design. As in [10], the original finite-state machine (FSM) is boosted. The newly added states and transitions are hidden in the high level design, which can only be known to the designer. In the external active metering [1], the lock can be inserted into the design in netlist form and the lock is controlled by the extra encryption module.

It is noted that all active metering techniques usually rely on PUF to implement the unique key for each chip. However, the reliability of various PUF is not perfect, which means that under different temperature or the voltage or aging factor, the response of PUF cannot keep unchanged. Under such case, the key for unlocking chip cannot maintain, which improves difficulty in using the chip normally for a long turn. Also, the external lock always incurs timing overhead on the original design. In the internal active metering method, the extra pseudo initial states always transmit to a uniform real initial state. This will indicate an obvious vulnerability that an attacker can easily bypass the extra hardware for the lock design.

To protect the copyright of each design, effectively metering methods should be explored.

1.4 Motivations and objectives

Illegal copy and distribution of ICs have caused great economic loss for the IC designer. Also, it may form great threat to the security of a nation. Active IC metering technique enables the control of IC piracy and the protection of IP of the IC designer to be possible. However, most existing metering techniques rely on the PUF to implement the unique key for each chip. The PUF has weakness in reliability and some techniques cause much hardware overhead. Some are even vulnerable to possible attacks. It is an urgent need to study and explore the robust and low-overhead active IC metering technique. This work proposes robust and low-overhead active IC metering methods.

In the first proposed scheme, PUF is proposed to be implemented using the parallel scan design to generate an ID for a chip. Then asymmetric encryption is applied on the ID using the public key. The encrypted information is passed to the designer, who can decrypt the information using private key. The decrypted data (the key unlocking the chip) is passed to the manufacturer to unlock the chip. The lock design is implemented by controlling the working modes of some scan cells. If the key is correct, these flip-flops can work normally. Otherwise, the circuit logic is obfuscated. The key based on PUF enables the scheme of "one chip, one key". Once the chip is unlocked, the locking circuit will never work. This scheme overcomes the weakness in the PUF reliability. The PUF design is implemented by reusing the scan chain in the original design, which reduces the overhead due to PUF. The lock design will never affect the timing of the critical path.

Another scheme is proposed to improve the robustness of an internal IC metering technique [10, 19]. The scheme in [10, 19] proposed to add more pseudo initial states depending on PUF information. These initial states can march to the real initial state by inputting specific input combination. A solo real initial state makes the scheme vulnerable to the attack based on bypassing the extra design. The work proposed to introduce some states similar to the real initial states such that some pseudo states will move to the extra real initial states. This makes it difficult for one without design knowledge to identify the solo real initial states. Thus, he cannot easily bypass the extra design without compromising the function of the original design.

1.5 Organization of the dissertation

The dissertation is divided into five chapters.

In Chapter 1, the motivation of the IC metering and objectives of this work are introduced.

Chapter 2 reviews the existing IC metering techniques, which includes the passive metering and active metering. More discussion is focused on active metering, which can be classified into internal active metering and external active metering.

In Chapter 3, a new external active metering method is introduced. The design structure is elaborated and the performances of the metering method are evaluated.

In Chapter 4, an improved internal active metering method is proposed. It not only inherits the merits of the existing internal metering method, but also improves the robustness against the typical attack based on bypassing the extra design.

The last chapter concludes this dissertation and highlights the potential future work.

CHAPTER 2
LITERATURE REVIEW

IC metering is a set of security protocols that enable the design house to achieve post-fabrication control over their ICs. According to the implementation scheme, the existing IC metering techniques can be classified into passive metering technique and active metering technique. In passive metering, each IC is specifically identified, either by its functionality or by the form of unique identification. If the identification or a detected IC match with the recorded ID in a pre-formed database, this may reveal unregistered ICs or overbuilt ICs. In active metering, each IC is also uniquely identified. Also, parts of the chip's functionality can only be locked/disabled or unlocked/enabled by the designer or the owner of the IP as the knowledge on the high level design is kept confidential to the foundry. A detailed classification of each metering technique is shown in Figure 2-1. As follows, both these metering techniques are reviewed and the advantages and disadvantages of each method are discussed.

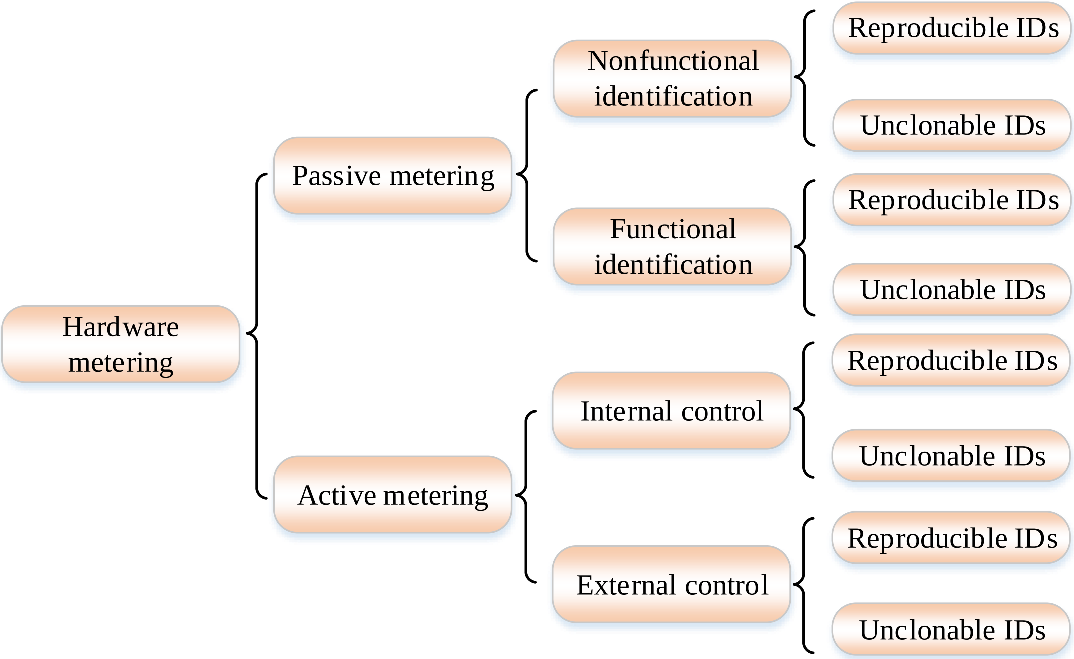

Figure 2-1. The classification of passive metering.

2.1 Passive IC metering

Passive IC metering can be classified into multiple sub kinds, as shown in Figure

2-1. It mainly includes passive nonfunctional metering and passive functional metering method.

2.1.1 Passive nonfunctional metering method

Nonfunctional passive methods have been used many years. It was usually implemented by physically indenting an ID on each chip or just storing the ID in nonvolatile memory. The well-known event is that it has been proclaimed that a unique serial number was contained in the Intel Pentium III processors [20]. However, the IDs generated by the two referred techniques can be easily removed or duplicated by attackers with little. Also, these two methods are not immune to foundries misconduct as it's easy for them to indenting or writing a duplicate ID into the overbuilt chips. So it's a significant idea if we can produce an unclonable ID for each chip.

To overcome the drawback of the above methods, in 2000, an unclonable ID technique which called ICID was firstly introduced by Lofstrom et al. and it was based on the unclonable processing variations [21]. Since the process variations can't be controlled by anyone, chip ID will be different from each other when circuits are fabricated. And some more advanced and acceptable identification and authentication techniques are developed after ICID, including PUF as shows in [22, 23]. As the above methods are implemented independent of the design, it was named passive nonfunctional metering method. For unclonable ID technique, up to now, if a new extra circuit structure is introduced into the original circuit design, it can be classified as extrinsic identification methods, otherwise it is classified into intrinsic one. The first proposed unclonable method [21] and the PUF technique [22, 23] can be classified as extrinsic methods. The technique proposed in [24, 25] can be classified as intrinsic method. The result in [21-25] shows that these two technique indicated that it is possible available for IC designs to create a unique serial number for chips, if external test vectors can be applied to the manufactured chips and the structural tests such as leakage, timing can be performed.

2.1.2 Passive functional metering method

A typical passive IC metering proposed in [7] introduced a scheme that each fabricated chip of the same design should have a unique locked control path which requires a specific control sequence. However, the chips fabricated from the same mask must have the same behaviors of input and output. How can fabricate each chip with a unique control path? The work in [7] and [8] proposed that each chip is designed to have a single data path, which can be controlled by multiple control paths which all satisfy the above requirements. Part of the chip can be programmed. The compiled control path design is integrated into the post-silicon design of each chip. Based on this scheme, the work in [7] and [8] also proposed other design methods as obfuscate the subset of variants assigned to a specific registers. In this scheme, during logic synthesis, redundant equivalent states are created based on a selected set of states. The set of states can then be selected based on the design constraint that concurrent states must be stored in separate variant to reduce the overhead of registers. The copies of each variant will achieve different assignment of states. Any different permutation assigned to each copy is suitable for those equivalent states. As the assignment of states is implemented by graph coloring, the generated redundant states correspond to the vertices added into graph with the edges related to the copied vertices copied to the new vertices. The tool of graph coloring can be used to assign the states in the new graph. The programmable reading logic design for the registers can select proper sequence of the variants for each unique control path.

The passive metering technique detects the pirated chips by monitoring and counting the chips in application. Before detecting a chip, the specific control path sequence is loaded into the programmable part. If a certain sequence is detected in multiple chips, these chips are marked as pirated chips. The success of this scheme relies on that most chips work online and their internal control sequences can be accessed. One way to implement the online access is to check the sum of these states by the operation of exclusive OR or to check the integrity of variants for the states.

The experimental results evaluated by the work in [7], [8] shows that different multiple sequences can be achieved at the minimum overhead. The obvious weakness of the passive metering technique is the introduction of programmable part into the application specific integrated circuit (ASIC). This introduces extra mask design, which indicates much overhead. Also, the scheme requires most chips work online and their internal sequences can be accessed. However, this condition cannot be satisfied all the time. As this way is based on the monitoring of the market and the statistics, much time, money and man power are unavoidable.

2.2 Active IC metering

Comparing with passive ones, active IC metering (AICM) can not only provide an identifier for each manufactured chip, but also can provide an active mechanism to lock/unlock the IC post fabrication by applying the corresponding identifier. According to locks inserting mechanism, it can be classified into internal AICM and external AICM [46].

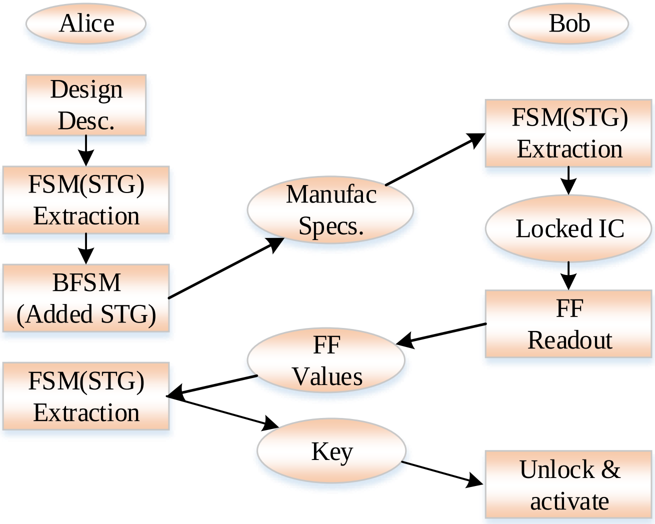

Figure 2-2. Design flow of AICM.

2.2.1 Internal active IC metering and attacks

Alkabani & Koushanfar proposed the first AICM method in 2007 [10]. An improved scheme and a comprehensive description with some new security proofs were presented in [19]. The design flow of this scheme can be shown in Figure 2-2. Firstly, the designer Alice use high level description language (VHDL: Very High Speed Integrated Circuits Hardware Description Language or Verilog HDL: Verilog Hardware Description Language) to describe her designs. Then, the control part of the design, FSM is extracted and the lock will be adding into the FSM design. We call the modified FSM as boosted FSM (BFSM). And then, the processes follow the normal synthesis, mapping, placing and routing. When the design specifications (GDS II files and test vectors for ICs) are sent to foundries for fabrication, the manufactured chips can’t be sent to test as it has been locked. The power-up state value of the BFSM needs to be sent back to design house for a key to unlock the chip. When the key corresponding to each chip is returned to the foundry, the foundry can use it to unlock the chip. Finally, testing and packaging can be performed normally. The locking mechanism is shown in Figure 2-3.

When the chip is powered up, the challenge for PUF, which is fixed in the design or stored in nonvolatile memory invokes the PUF to generate a response. The response is fed in the extra flip-flops (FFs). This response will be used to initialize the BFSM into one of the added states. To make the circuit work normally, the BFSM must transit from the power-up state to the real initial state of FSM. As Figure 2-3 shows, assuming that the power-up state is s_5, it must transit from s_5 to s_0 with the input key (IK): (P_1, P_2, P_3), then the chip can work normally. If the key is improper, then, the state of the BSFM may transit to an unknown added states, which makes the chip locked. As the state transition graph (STG) is only known by the design house and it cannot be extracted from the GDS II files. The design house is the only one who can calculate the IK according to the power-up state. This guarantees the security of the locking mechanism. Correct keys for unlocking the chip may not be unique. The authenticated key can be used as an ownership proof as stated in [19].

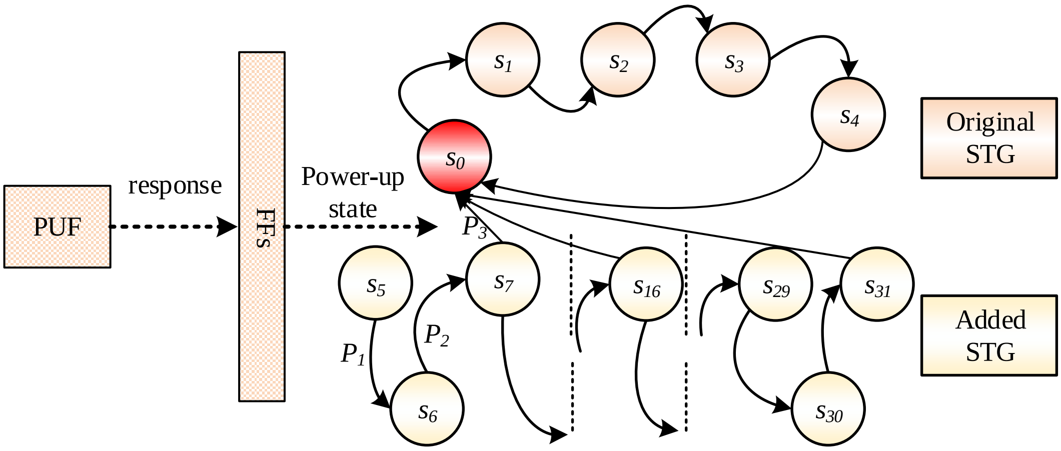

Figure 2-3. The locking mechanism of internal metering design.

In this scheme, the locking was implemented by expanding the original FSM. PUF was adopted to generate random bits, which would place the design in an added nonfunctional state. These states can transit to the functional reset state, however, the input that determines such transition was the designer’s secret. Thus, the locking and unlocking mechanism provide a way for the designer to actively control the number of activated ICs from one mask. It is noted that PUF structure can create many different output responses and all these responses should be considered as nonfunctional states in FSM. Hence, the complexity of FSM was aggravated and consequent overhead may be unexpectedly high. A similar approach which can actively control multiple cores was proposed by Alkabani & Koushanfar in [26]. These schemes can be discussed as follows:

First, the number of the extra adding states should be large enough to guarantee that the power-up state to be one of the added states and the probability that the power-up state is one of functional states is sufficiently low. This is guaranteed by exponentially large number of adding states which are used to obfuscate attackers.

Second, the reliability of PUFs is not perfect. As we all know, PUFs response may be changed as aging issue or temperature, voltage variations. If PUFs response changed, then the previous key may turn invalid to unlock the chip. In [27], Yu & Devadas proposed that error coding correct (ECC) can be used to ensure PUFs response to be correct. But this may result in large area overhead.

Finally, every added state should have a unique transition path to transit from the power up state to the original reset state. As all extra states will definitely reach one original reset state, one may think to bypass all the extra states and extra transitions and directly lead the design to the power-up state. This indicates a weakness in security.

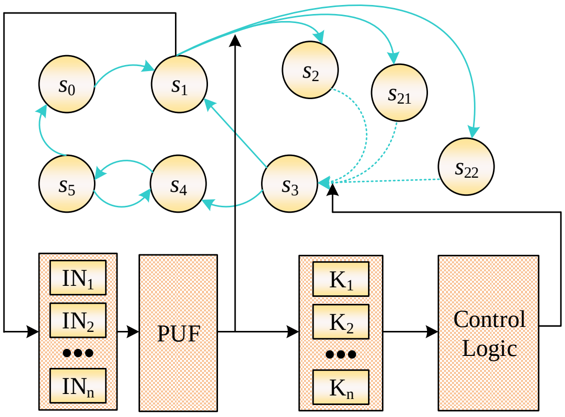

Figure 2-4. FSM with a lock on replicated state (s_2).

In [10], the design complexity is increased by introducing BFSM. To reducing the adding states, the work in [28] proposed to lock each working IC by replication of a few states of FSM and adding control to the state transitions. As Figure 2-4 shows, s_2 is the initial state and it is replicated two times as s_{21} and s_{22}. s_2 and the two replicated states have the same functionality but with different inputs fed. We assume that the FSM have two input ports and state transitions from s_1 to the next state with following mapping relationship: 01: $s_1 \rightarrow s_2$, 10: $s_1 \rightarrow s_{21}$, 11: $s_1 \rightarrow s_{22}$. When the FSM transits to s_1, the PUF will be activated to create a random response. And part of the response is used to control the transition. It means that the transition will randomly transit to one of the states which correspond to the mapping relationship. The remaining part depends on the IK. Unless a properly key was given, the FSM can't transit to s_3. And the mapping relationship is just known by the design house. So in this way, the overbuilding problem can be prohibited actively by designers.

Though the approach in [28] can actively control the post fabrication process without introduction of many states, this technique will impact the performance of the design. When the chips began to work, as shown in Figure 2-4, the state transits to s_1. To make the FSM work normally, it must provide a driving signal to invoke PUF to generate a response. Finally, the response works as a control signal to make the state transit from s_1 to the next state. This process delays the original chip operation. When delay-based PUF, such as arbiter PUF, or oscillation PUF is used, it may result in more timing delay and greatly impact the performance of the design.

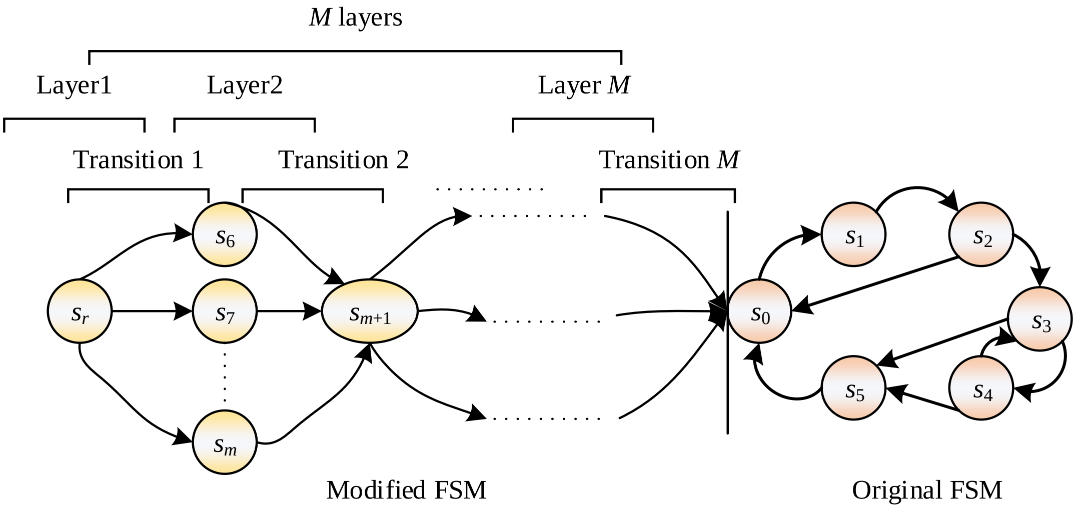

Figure 2-5. The binding FSM structure in [29].

A new approach different from the above two metering structures was proposed by Zhang et al. in [29]. The mechanism of this approach is shown in Figure 2-5. This approach is totally different from that in [10, 19]. The initial power-up state of each chip is fixed at s_r as shown in Figure 2-5. In [29], partial PUF response is used to map the state transition and partial of the response is used to perform the exclusive or operation with the IK, which makes the state transit to the fixed node state. The mapping relationship is just known to the design house. From Figure 2-5, we can see that M layers of states are added into the design to bind the original FSM. The added states are distributed at each layer. Each layer with even number as index contains m states and each layer with odd number as index just contains one states. How the states can transit from odd layers to even layers is determined by the PUFs response. And how the states can transit from even layers to odd layers is jointly determined by PUFs response and the IK. For example, a reliable PUF response is 0100, and the first two bits (01) is used to control s_r to transit to next layers and the last two bits is used to combine with the keys to make state transit to odd layers. The mapping relationship from S_r to next layer is as follows: 11: $s_r \rightarrow s_6$, 01: $s_r \rightarrow s_7$, 10: $s_r \rightarrow s_8$, 00: $s_r \rightarrow s_9$. And the next mapping relationship is: 01: $s_6 \rightarrow s_{or}$, 10: $s_7 \rightarrow s_{\mathrm{or}}$, 11: $s_8 \rightarrow s_{or}$, 00: $s_9 \rightarrow s_{or}$. So we know that the state can transit from s_r to s_7. And to make the state transit to the original reset state s_{or}, we deduce a key IK as ‘10’ which can be exclusive or operated with ‘00’ to obtain ‘10’.

As a whole, internal active hardware metering implements locking mechanism at a high design level and possesses high resilience against attacks based on reverse engineering. However, the overall overhead due to it is also hard to predict or control [4]. Also, these metering methods may be attacked by invasive attacking especially the approach in [19]. And the method proposed in [29] need more PUF response bits than the methods in [10, 19], though this method can resist invasive attacks.

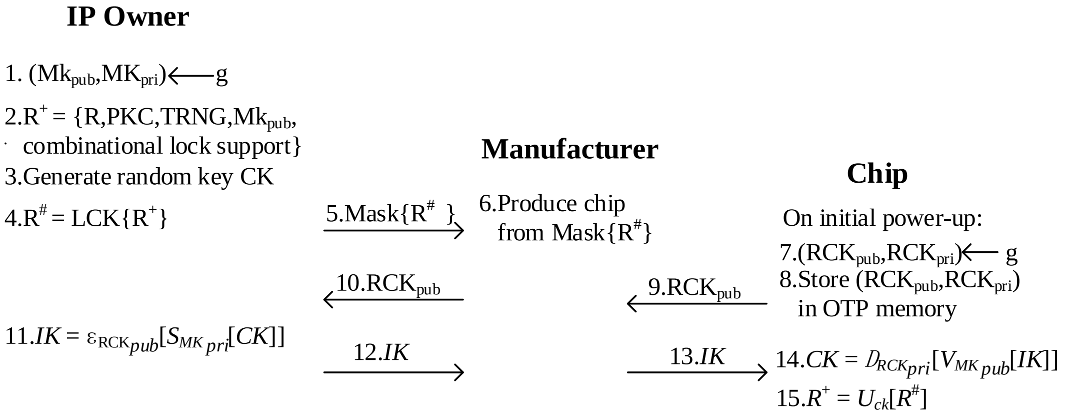
IP Owner
1. $(Mk_{pub}, MK_{pri}) \leftarrow g$
2. $R^+ = \{R, PKC, TRNG, Mk_{pub},$ combinational lock support$\}$
3.Generate random key CK
4. $R^\# = LCK\{R^+\}$
5.Mask{R# }
Manufacturer
6.Produce chip from Mask{R#}
Chip
On initial power-up:
7. $(RCK_{pub}, RCK_{pri}) \leftarrow g$
8.Store (RCK_{pub}, RCK_{pri}) in OTP memory
9. RCK_{pub}
10. RCK_{pub}
11. $IK = \varepsilon_{RCK_{pub}}[S_{MK_{pri}}[CK]]$
12. IK
13. IK
14. $CK = D_{RCK_{pri}}[V_{MK_{pub}}[IK]]$
15. $R^+ = U_{ck}[R^\#]$

Figure 2-6. The protocol of EPIC proposed by Koushanfar.

2.2.2 External active IC metering

External active hardware metering technique adopts asymmetrical cryptographic techniques so that only the chip designer can provide the key to unlock design using his private key. In [1, 30], Roy et al. proposed a technique to end piracy in integrated circuits (EPIC). Since many external metering method origins from this technique, the external active metering based on EPIC is elaborated. The protocol of EPIC can be shown in Figure 2-6. The core idea underlying EPIC is to insert lock in the non-critical combinational paths which can only be unlocked with correct Common Key (CK). The chip authentication involved double public-key cryptography (PKC). IP rights owner holds a pair of Master Keys (MK). When fabricated, each chip generates a pair of private and public keys (RCK) based on the initial power-up states. Then *CK* is encrypted as *IK* with the private key of *MK* and public key of RCK. *IK* is sent securely to fab and entered into chip. Then, it is decrypted using private key of RCK and public key of *MK*. When *CK* is produced correctly, chip is unlocked successfully.

The early version of EPIC [30] is studied by Maes et al., who showed that EPIC is not secure enough and can’t resist some attacks as discussed in [31]. The improved EPIC was proposed in [1] and it can resist many known attacks as analyzed in [30]. However, besides a unit for generation of a pair of public and private keys, two decryption parts need to be inserted in the design, which account for high hardware overhead as the decryption process is significantly more computationally intensive than encryption.

The work in [32] proposed a protection method for bus-based ICs. The designs are locked by scrambling the central bus and such scrambling renders the IC unusable for anyone without correct key. The key shared between the chip and design plant is interfaced with the combinational logic and used for the connection and interface of multiple cores in one chip. Its application is limited in bus-based design. Huang in [33] proposed to implement an authentication scheme in a resource-constrained scenario as it just adopts an encryption part instead of two decryption parts [1, 30] in the protected design. Although the schemes in both [33] and [30] located the lock in uncritical paths, the accumulative delayed timing may affect the critical path delay. The work in [34] proposed to introduce a specific programmable part in chip which is transparent to the fabrication party and can only be activated using a secret key. Obviously, the added process and mask overhead is incurred due to the introduction of programmable components in application specific integrated circuits (ASICs).

2.3 Summary

In this chapter, most existing IC metering methods are reviewed and evaluated. The passive metering methods are found to have a great limitation in application as this method cannot prohibit the overbuilt chips to be applied. The active metering technique provides a better choice for effective control of the post-fabrication. However, both internal and external active metering techniques have some weakness in robustness and design overhead. In the following two chapters, a new external metering method and an improved internal metering method are proposed to overcome these weaknesses.

CHAPTER 3 A NEW ACTIVE IC METERING TECHNIQUE BASED ON LOCKING SCAN CELLS

To prohibit IC overbuilding problem, in this chapter, a new AICM technique based on locking scan cells is proposed. This chapter is organized as follows. First, the preliminary knowledge on PKC and scan chain is introduced. The new proposed technique is then introduced. The analysis and evaluation of the proposed technique is given in the next section. At end, this chapter is summarized.

3.1 The preliminaries

To facilitate the introduction of the proposed scheme, the preliminary knowledge on PKC and scan chain is introduced first.

3.1.1 Asymmetric cryptographic algorithm

In 1976, the concept of asymmetric cryptography was firstly invented by Diffe and Hellman and it can also be called as PKC [35]. In the symmetric cryptography, the encryption process and the decryption process both use the identical keys. So it will very be dangerous if the secret keys are obtained by attackers. The attackers/eavesdroppers can easily achieve the plaintext as the secret key have been obtained by them. But this problem will never happen in the asymmetric cryptography. Even the public key is obtained by the attackers, he cannot decrypt the cipher text easily.

In PKC, a pair of keys is generated by each user independently. One is called public key and the other is called private key. The public key can be obtained by everybody, but the private key will never be delivered to anyone. It is only kept by the owner. Also, the private key cannot be deduced from public key as both the decryption and encryption process depend on the hard-to-reverse one-way function. So the users can exchange messages securely. Suppose *A* denotes a sender and *B* denotes a receiver. *A* can send a message to *B* which have been encrypted by *B*’s public key. And this message can only decrypted by *B* as he/she is the only one who holds the private key.

Among various PKC algorithms, RSA is best known and widely used nowadays. It was proposed by Rivest, Shamir and Adleman in 1977 [36]. Though research have been able to break the RSA when the key size is 768 bits, but it is time consuming and not an efficient way [37]. And up to now, it has not been reported that there are an efficient method to break the RSA when the key size turns to 1024 bits. It is widely applied in many area, such as key distribution and management in large-scale web applications, realizing the digital signature in web, with the key size equal or greater than 1024 bits.

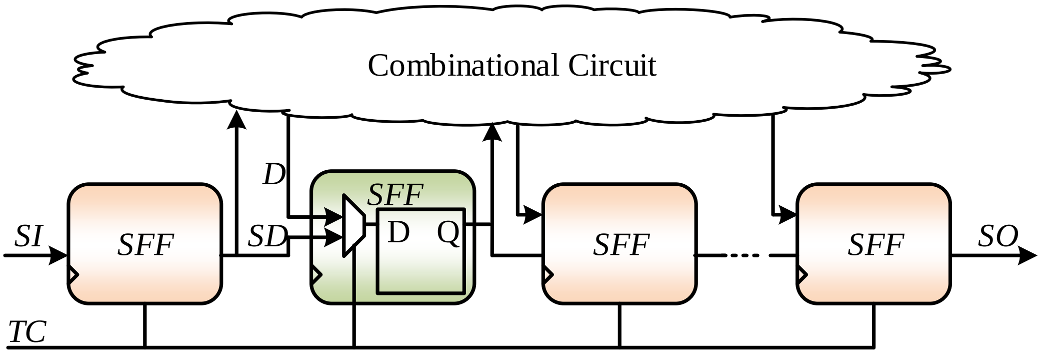

Figure 3-1. Scan design in circuit.

3.1.2 Scan chain

With the development of manufacturing process, integrated design has experienced a paradigm shift and enter into the era of system-on-chip (SoC).To guarantee a satisfied yield, manufacture testing is becoming indispensable. To facilitate the test, design for testability (DFT) is adopted widely into chip design. Among existing DFT techniques, full scan chain design is regarded as the best discipline and has been widely applied. Figure 3-1 shows a typical scan chain design. In the scan chain design, all or partial of the flip-flops in a design are modified to scannable flip-flops (SFFs), which contains a multiplexer before each original flip-flop. Then these SFFs will be connected to form one or more scan chains. Scan design provides a high controllability and observability to the circuit under test (CUT). To reduce the test application time, scan-based techniques such as scan tree design and multiple scan design [38, 39] have also been proposed.

In each SFF, as shown in Figure 3-1, a standard flip-flop is combined with a two-to-one multiplexer. A test control (TC) signal is introduced to switch the SFFs between normal mode and test mode. When *TC* = 0, the chip works under test mode with the scan data (SD) selected to the scan chain. And then, the test pattern from scan in (SI) port can be shifted into the scan chain and the output response can be unloaded from the scan out

(SO) port. When *TC* is set to ‘1’, the design works under normal mode. All SFFs will work as the normal flip-flops in the original design.

We can see that if under normal mode, the SFFs cannot be controlled by a high *TC* control signal, these sequential components cannot work normally such that the CUT cannot work normally. If a lock can be inserted on the signal path to the *TC* port of these SFFs, a lock on the normal function can be implemented. This idea will be introduced in the proposed metering scheme to implement the lock scheme.

3.2 The proposed IC metering Technique

The proposed external AICM scheme, as shown in Figure 3-2, includes three parts: a key generation unit, a locking mechanism and a controller. We elaborate the design and implementation of the metering scheme in this section.

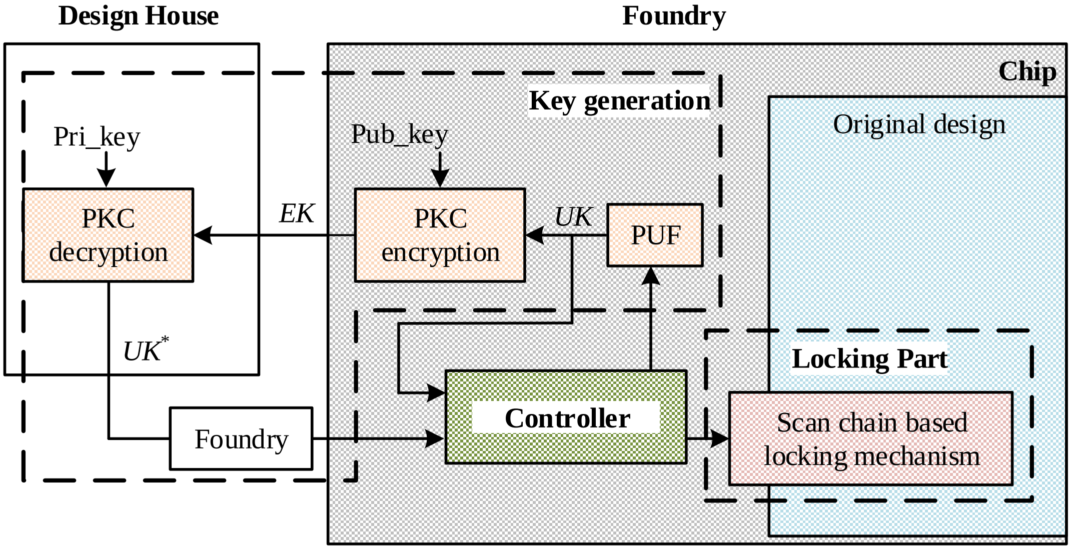

Figure 3-2. The proposed IC metering technique.

3.2.1 Key generation unit

The key generation unit implements the generation of a unique key (*UK*) and the encryption by PKC. To uniquely identify each chip, we require the foundry to create a unique *N*-bit key with PUF [6, 40] or true random number generator (TRN) [41] (see the block marked as PUF in the middle of Figure 3-2). As the generation of the *UK* relies on the physical characteristics (such as fabrication variation) of the IC, the *UK* will be unclonable and unique for each IC. In addition, keys generated this way will be more resilient against attacks than the keys stored in the memory. The *UK* is then encrypted to an encrypted key (*EK*) by the public-key cryptosystems such as Rivest-Shamir-Adleman (RSA) or elliptic curve cryptography [42] with a given public key. Unlike symmetric cryptography, the PKC algorithms do not require a secure channel for the exchange of one secret key between two pairs as only the holder of the private key can decrypt the encrypted message with the public key.

The manufacturer will send the *EK* to the design house, who can decrypt *EK* with the corresponding secret private key. Let *UK** be the decrypted key. The design house then sends *UK** back to the manufacturer, who will compare *UK** and *UK*. If a match is found, the chip will be unlocked. Otherwise, the manufacturer can continue to *IK* for authentication until a pre-determined limit of input times is reached. This will be further elaborated in the controller part.

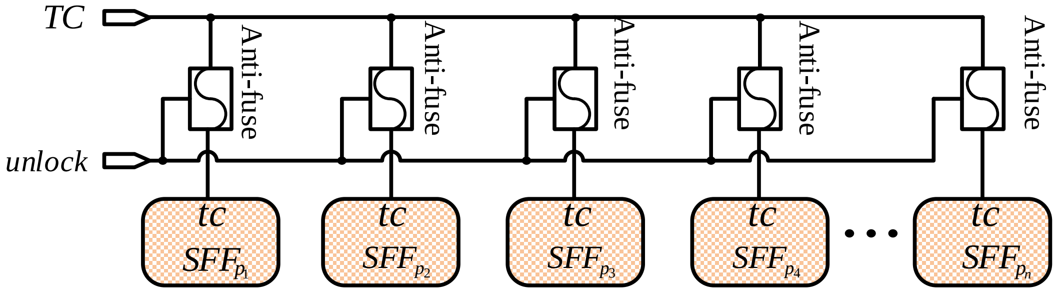

Figure 3-3. The scan chain based locking scheme.

3.2.2 Locking mechanism

We propose to implement the locking scheme by monitoring the sequential components in the design. To facilitate post-fabrication testing, the flip-flops in the original design are usually modified to SFFs and connected to form one or multiple scan chains. Under normal mode, these SFFs act as normal flip-flops. Under test mode, they work as a scan chain and each SFF just fetches the data from the previous SFF and transmits it to the next SFF through the scan chain. The switching between normal mode and test mode is controlled by the signal *TC*. From these observations on the scan chain, we can see that the working status of the sequential components can be controlled by *TC*. The locking scheme is proposed to add a lock on specific SFFs by controlling their *tc* ports.

Suppose that the scan chain S contains L scan cells as $S=\{SFF_i\}_{i=1}^{L}$. Pseudo-random number generator is used to generate *N* random numbers in the range [1 .. *L*] as $P = \{p_i\}_{i=1}^{N}$, ($1 \le p_i \le L$). The SFFs at positions p_i are considered being selected and will be controlled by inserting a fuse to their *tc* ports, as shown in Figure 3-3. A high voltage on signal unlock can blow the anti-fuse (just as those in FPGA) and then *TC* is connected to *tc* ports of these specific SFFs. The unlock signal is determined by the comparison result between the user decrypted key *UK** and the correct key *UK*. If the user key matches with the correct key, the signal 'unlock' is high and all *N* specific SFFs can work normally as their *tc* is controlled by *TC*. When *UK** does not match with *UK*, the SFFs may fetch data in the scan chain instead of that from the functional part and hence the overall design works abnormally.

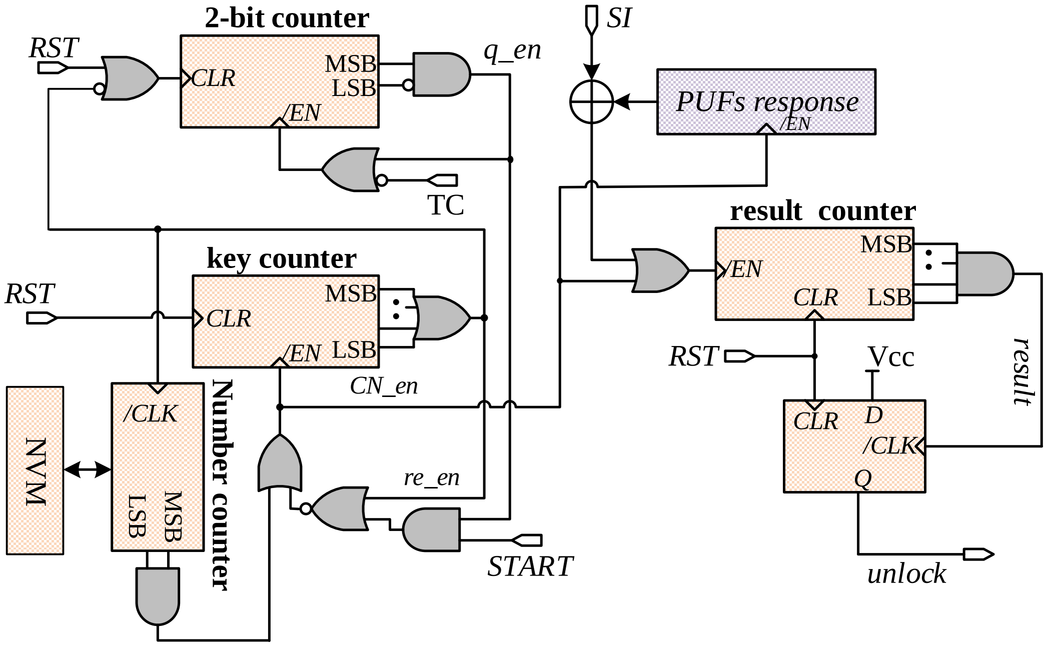

Figure 3-4. The controller of the proposed metering scheme.

3.2.3 Controller

The controller controls the working procedure of key authentication and the locking mechanism. It consists of a 2-bit counter, a number counter for counting times that the foundry enters a key, and two *q*-bit ($q = \log_2 N$) counters known as the key counter and the result counter. We now describe each of these components and then the working flow of the controller.

(1). 2-bit counter

The 2-bit counter is used to identify whether the chip works under normal mode (TC can keep high at least for two clocks). As shown in

Figure 3-4, upon system reset, i.e., RST = ‘1’, the counter will be cleared to zero. As long as the TC input to the controller is low (i.e., the CUT is operating in the test mode), the 2-bit counter will be disabled. When TC turns high (i.e., the CUT is operating in normal mode), the 2-bit counter will be enabled by the low output signal of the OR gate connected to its /EN port and start counting from zero. The counter will count as long as the TC signal remains high for two clock cycles. Counting will be halted by the q_en signal when the output of the counter reaches “10”.

(2). Number counter

The proposed metering scheme allows three times for the foundry to *IK* to activate the design. Upon system reset, the number counter will fetch the content in the nonvolatile memory (NVM), which is initialized as “00”. When an *N*-bit key is input, the number counter starts counting and the updated value on most significant bit (MSB) and least significant bit (LSB) will be written into the nonvolatile memory. After three times, the output of number counter reaches “11” and the input of user key will be disabled forever.

(3). Key counter

This key counter can count $N = 2^q$ numbers to allow the *N*-bit *UK** to be input. Upon system reset, the key counter is cleared to zero with the OR gate connected all the outputs of counter presenting zero. The introduced *START* input signal is used to indicate that the user starts inputting key with *START* = ‘1’. Thus, when *START* = ‘1’, *q_en* = ‘1’ and the number counter does not reach “11”, the enable signal of the key counter, *CN_en* presents low and the counter starts counting. The *START* signal should be set low after one clock. Meanwhile, the registers storing the PUF response are enabled to shift out the bit one by one under the clock. The bit will be compared with the bit of the *IK*. After the first clock is counted, the OR gate after key counter will output high and this enables the */EN* port of counter to be effective. When the counter counts up to *N*, the OR gate outputs zero, which clears the 2-bit counter and results in a high *CN_en*. Also, the negated edge signal at the OR gate output will invoke the number counter to count, which indicates one more trial of *IK*. With a high *CN_en*, both the key counter and result counter will stop counting.

(4). Result counter

The result counter is used to count the number of matched bit pairs between the

PUF key and user key. *N* matched bit pairs will indicate that the user key *UK** passes the authentication. When *CN_en* = ‘0’, key counter starts counting the number of input bits while the result counter is also enabled to count the matched bit pairs. If one PUF bit matches with its counterpart in the *IK*, the XOR gate outputs zero and the result counter is enabled to count one. Otherwise, the result counter maintains its counting result. When the result counter counts up to (*N*-1), the output of the AND gate connected all the outputs of the result counter, result turns high and it will turn low if one more clock (i.e., totally *N* numbers are counted) is counted. This negated edge will invoke the DFF to output a high signal, unlock. This high unlock signal will blow the fuses (as shown in Figure 3-3) and enable all the *tc* ports to be controlled by *TC*. Then all the specific SFFs can work normally. Otherwise, if one or more bit mismatch occurs, the result counter cannot reach *N*. No effective unlock signal can open the ‘lock’ on each specific SFF.

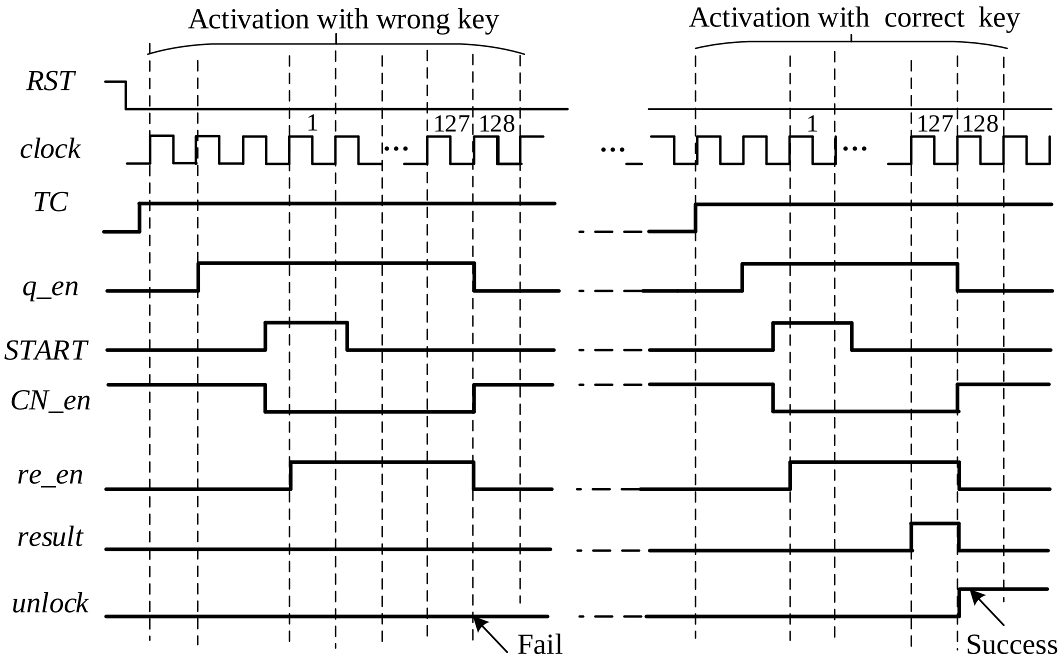

Figure 3-5. The timing diagram of the activation process based on the proposed metering method.

3.2.4 Working procedure

The timing diagram of the proposed metering scheme is shown in Figure 3-5 in the example of *q* = ‘7’. Upon power-up reset, the content in NVM is read into the number counter and all other counters are cleared. To activate the chip, the *TC* input is set high to switch the CUT into normal mode. After two clocks, the *q_en* signal turns from ‘0’ to ‘1’. To start the activation, the foundry sets the signal *START* = ‘1’ for one clock while beginning to input the key from SI. The signal *CN_en* turns high and the key counter counts up from zero. After the first clock, the signal *re_en* turns high and enables the key counter to continue counting. The result counter will count up if the bit from SI and that from PUF matches. After *N* clocks, the *re_en* turns low. The negated edge will invoke the number counter to count and the updated value will be written into the NVM. The 2-bit counter is cleared and *q_en* turns low. The signal *CN_en* turns from ‘0’ to ‘1’ and both the key counter and the result counter are halted. If the result counter has counted *N* times, i.e., the *N*-bit user key matches with the PUF key, the result signal will generate a negated signal to enable the *unclock* signal to present high. The chip will be activated as the effective unlock signal can enable the specific SFFs to work normally. Otherwise, the chip will not be activated and the foundry needs to re-input his key for authentication by setting the *START* signal for two more times.

3.3 Analysis and evaluation

As a design for security, the proposed metering technique is evaluated in terms of overhead, possible compromise of testability and security against possible attacks.

3.3.1 Analysis of testability

After the original design is synthesized, the scan chain is inserted and test patterns are then generated. As an extra design part, the proposed metering design is inserted to the original design with scan chain to form the final design. During activation, if the user key is correct, the unlocked design is equivalent to the original design. The original chip can be tested with the original test patterns without sacrificing its testability. Hence, the testability of the original design is not affected at all.

If some faults occurred in the extra circuitry introduced by the metering design, they cannot be detected by the original scan design. One possible solution is to create a specific scan chain for the extra design. Before activation, the extra design for security should be tested with this specific scan chain. If no faults is detected, the foundry can start chip activation process. It should be noted that the scan cells in the specific scan chain should not be used for those introduced in the locking scheme.

3.3.2 Analysis of security

We analyze some possible attacks against the proposed metering method to show its security. In the referred attack scenarios, we suppose Alice is the chip owner and Bob is the foundry who would like to pirate or overbuild Alice's design.

(5). Nonintrusive attacks

Bob may conceive to predict the PUF key directly without intruding Alice's design. As PUF key relies on the variation during manufacturing, it is hard for Bob to gesture the PUF key of a chip. Even Bob obtains a key for a chip by legal means, it cannot be used for other similar chips due to the unclonability of PUF. Bob may use exhaustive trial to find the correct key. However, for a 128-bit PUF key, the probability for Bob to figure out the correct key coincidently in the admitted 3 times for trial is 8.82E-39.

Bob may also think to deduce the private key based on the public key to decrypt the correct key. The strength of a public key cryptography system relies on the degree of difficulty (computational impracticality) for a properly generated private key to be determined from its corresponding public key. Brute-forcing the private key is impractical for Bob due to the unreasonable computational effort [33]. Bob may also try to deduce the private key by analyzing the decrypted result of some chosen ciphertexts. Obviously, Alice has no responsibility to answer Bob's request. Bob may think to perform side-channel attacks by analyzing power, temperature and timing information. However, the decryption using private key is off-loaded to Alice and Bob hence has no way to spy the necessary information for side-channel attack.

(6). Intrusive attacks

Bob may think to intrude the Alice's design on mask to bypass the overall design for security. This is a great threat to Alice's ownership. All existing external active metering techniques face such problems. Bob may think to find where the fuses are placed and then blow them or connect the *TC* signal to *tc* ports of those specific SFFs directly using Focused Ion Beam (FIB) to rewire the design. To resist such attacks, the security related wires can be buried under metal layers which contain interconnections vital to the normal function of the IC or these wires are well obfuscated with other wires in functional part so that it is hard to discern them or the cost for a correct detection is dramatically high.

It is also possible for Bob to reverse engineer the design by peeling off the metal layers to bypass the objective secure design. However, this will result in re-fabrication of new IC, which indicates extremely high cost of money and time. Also, the success for such reverse engineer is extremely hard when the process technology is sub-45nm or even smaller.

3.3.3 Analysis of overhead

After the first-time activation, the unlocked design is equivalent to original functional design. The extra design for security does not affect the functional paths part or delay path timing. Hence, the timing performance of the design is not compromised. Most existing metering methods implement the locking scheme in the combinational uncritical paths. However, the accumulative result of delay on each path is not considered or evaluated. Also, after the successful activation, the chip can be normally used without any more operation before working. The aging and unreliability due to PUF will not affect the application of the chip any more. However, after activation, the scheme in [33] requires the stored key to be compared with the correct each time the chip is powered up or reset. The scheme in [10] also requires the user to *IK* for normal use. These not only delayed chip for start of normal operation, but also when the PUF key varies due to the environmental factors or aging, the user needs to bother the IC owner to regenerate the key for activation.

The area overhead due to the metering design mainly contain that of PUF, RSA encryption, controller and lock on scan chain. The PUF [6] can be implemented by using the SRAM in original design. The applied 1024-bits RSA from opencores [43] is synthesized using the Synopsys Design Compiler with the technology library of TSMC 0.18μm. Its area equals to 7295 2 input NAND gates. All other part in the secure design accounts for 931 2 input NAND gates. If this proposed secure design is applied on the pipelined AES with 128-bit key [44], the overall area of the secure design just equals to 3.87% of the AES design (its area equals to 212280 2 input NAND gates). The area overhead is acceptable for a reasonably large design. In a resource-constrained scenario, ECC can be selected as the PKC because it is more computationally efficient than the others by using a shorter key and similar area to offer a similar level of security [42].

3.4 Summary

Chip overbuilding has become a real concern for the fabless IC design houses as the illegally overbuilt chips will bring financial loss to the design house and can cause damage to the chip users. IC metering has been proposed as a promising solution to this problem. We propose a new external active metering technique where PUF is used to generate a unique key for each IC during fabrication. The PUF key is encrypted by PKC algorithm and then passed to the design house who can decrypt with the associated private key. Only when the foundry gives correct decrypted key back to the design, can the design be unlocked and work normally. A new locking scheme is implemented by controlling the working mode of some selective scan cells in the scan chain. Unlike traditional approaches in locking the combinational paths, the proposed locking scheme will not affect the timing of the functional path. In addition, this metering method allows multiple input of key. After the first successful activation, the unlocking circuitry will be disabled to overcome the weakness of multiple queries of correct key from design house due to the variation of PUF key with environmental change or aging. This proposed metering method incurs low area overhead and does not compromise the testability of the design while remaining resilient against typical attacks.

CHAPTER 4
AN IMPROVED ACTIVE IC METERING METHOD AGAINST INVASIVE ATTACKS

In this chapter, an improved FSM-based AICM method is proposed. PUF response will uniquely determine the power-up state from multiple newly introduced states. IC designer modifies the FSM such that designer can determine what to input to invoke the design to transit from the power-up state to the original initial state. Differently, multiple pseudo original initial states are introduced to perplex the attacker such that it is difficult for him to identify which is the true original initial state. Thus, he cannot easily bypass all newly introduced states and their transitions to original initial state to nullify the IC metering scheme. Little overhead is incurred while the resilience of IC metering against the invasive attack is improved.

4.1 Internal active IC metering in [10]

The concept of AICM is firstly proposed by Koushanfar in 2007 [10]. In this design, two key parts are contained, a random unique block (RUB) and a BFSM. The RUB part is used to generate a unique identification for each chip, in this way, it will make chips different with each other. And also, the unique signature sequences is used to initialize the BFSM to make the chip locked when chip is firstly powered-up. And BFSM part represents an FSM, which is obtained by boosting the original FSM by adding many nonfunctional states and every added state has a unique path returning to the original reset state S_0. After it returns to the original reset state, the FSM will work normally. The added states are used to obfuscate the original designs. In this AICM scheme, the FSM is first extracted followed by many new states added into the original FSM. The synthesis, routing and mapping process can then be performed normally. After this process, the GDS II files are sent to the foundry for fabrication. The fabricated chips are locked and testing process cannot be performed upon power-up. The power-up state should be feedback to the design house to query for the corresponding keys to unlock the design. The design house is the only entity who knows the mapping relationship between states. Only when a proper key is given, can the chip be tested and work normally. As shown in Figure 4-1, all the extra states will be guided to the original initial state s_0. In an invasive attack, the state s_0 may be identified and then the design is modified to enter the state s_0 when powered up with all the extra states and transitions related with the added states bypassed. In this way, the metering scheme is nullified while the original function is maintained. It can be seen that a uniform state s_0 which acts as the only entrance to the normal functional design results in the vulnerability of the proposed scheme against the invasive attack. As follows, an improved metering method is proposed to overcome this weakness.

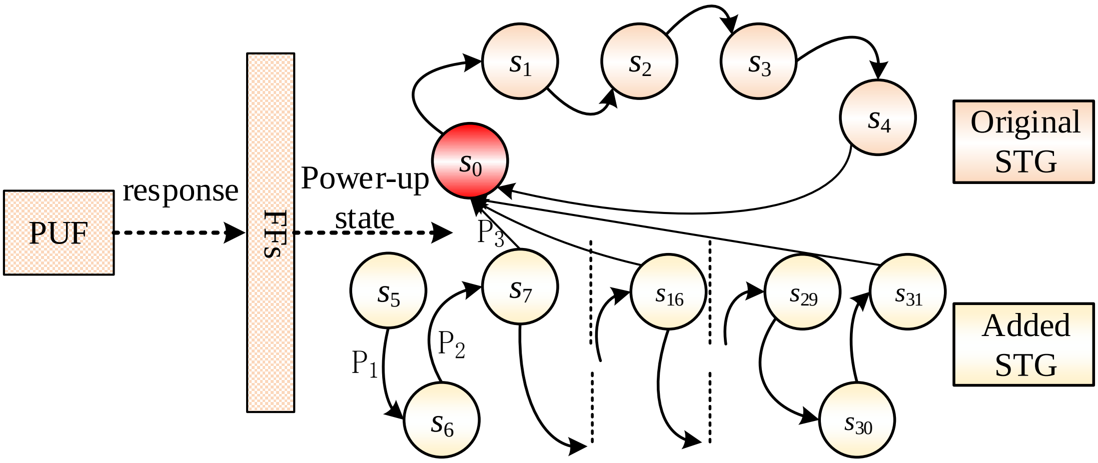

Figure 4-1. The mechanism of internal AICM in [10].

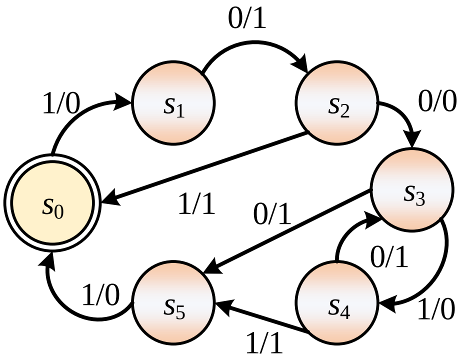

Figure 4-2. An example of STG with 6 states.

4.2 The Proposed Internal Metering Scheme

4.2.1 Building the BFSM

An FSM can usually be described in the language of Verilog HDL or VHDL and represented by state transition graph (STG). Normally, FSM can be defined by a tuple as

$F = (\Sigma, \Delta, S, s_0, \delta, \lambda)$ In this tuple, $\Sigma \neq 0$ and $\Delta \neq 0$ represent the finite set of inputs and outputs respectively. S represents the set of states in the FSM and s_0 denotes the reset state in the FSM. $\delta(s, i)$ and $\lambda(s, i)$ represent the input and output function of the transition, respectively, where s denotes the current state and i denotes the input for the transitions. An FSM can usually represented by an STG. Throughout this work, FSM and STG are used interchangeable. A simple STG can be shown in Figure 4-2. This STG contains 6 states. State s_0 represents the reset state. The string on each edge denotes the input and output for each transition.

Suppose the states of the original FSM before modification are denoted by the set S. Then the FSM has $|S|$ states. Thus, the original FSM can be implemented using $K = log_2|S|$ flip-flops. To implement the locking scheme, the FSM can be modified into a boosted finite state machine (BFSM). To achieve a BFSM with $|B|+|S|$ states, $K_B = log_2\{|B|+|S|\}$ flip-flops are needed. Additional edges between these added states are also introduced into the BFSM so as to guarantee the reachability among these extra states. As the number of possible states bares an exponential relation with that of the FFs, a few FFs which can cause tolerable overhead are capable of generating exponentially many more states than $|S|$.

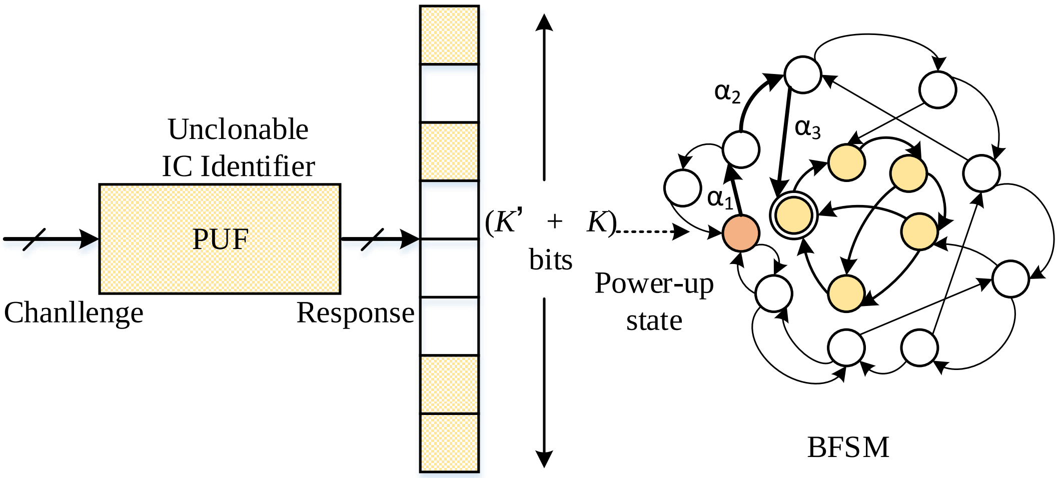

Figure 4-3. The PUF response is fed to the FFs to initial the BFSM.

As shown in Figure 4-3, upon the power up, the initial values of the FFs, i.e., power-up state, is determined by the unique response from the PUF design on each chip. Here, the PUF design proposed in [45] is adopted. It shows to have a good uniqueness greater than 49% and a good randomness and reliability. Initially, to achieve an n-bit PUF response, an n-bit alternate sequence of “0101…” should be loaded into the scan design for PUF. Then, one more clock is needed to generate PUF response, which will be used to determine the power-up state. The value K_B can be set by the designer such that the probability of selecting a state in the original FSM is extremely low while that of selecting a state in the added states is sufficiently high. It can be seen that unless the design is in one of the original states, the design works in nonfunctional mode. Thus, the random FFs states determined by the PUF response would lead the design into a nonfunctional state. A design user should provide appropriate inputs to the BFSM so that it can transit from the nonfunctional initial state to the real reset state of the original FSM, as shown by s_0 in the Figure 4-3.

The IC designer has full access to the STG of the BFSM. It is easy for him to determine or find the set of inputs for traversing from the initial power-up state to the reset state. He just needs to clarify a path on the STG graph and the use the input values corresponding to the path transition according to the STG description so that the states can transit to the reset state. However, there is only one input combination out of the exponentially many possibilities for the input of each edge transition. It is hence extremely hard for one without the knowledge of the BFSM to find the exact input that cause the reachability to the original reset state.

4.2.2 Adding pseudo reset states

To improve the robustness of the above internal metering method against the possible invasive attack. Some pseudo reset states are proposed to be introduced in the original FSM just similar to the original initial state. These pseudo reset states should assemble the functional states but different from the true original reset state while the functionality of the original FSM should be maintained.

In this improved method, we build the BFSM by adding a large number of nonfunctional states to be bound with the original FSM firstly. As shown in Figure 4-4, the added states are shown in the left of the Figure 4-4. These added states are connected together and each of them has a path to reach the original reset state s_0. To make the figure concise, only one arrow is connected from the added states to s_0 and this arrow indicates that each state in it has a pass to s_0.The right part of the Figure 4-4 illustrates the original FSM, which contains six states as s_0 to s_5.

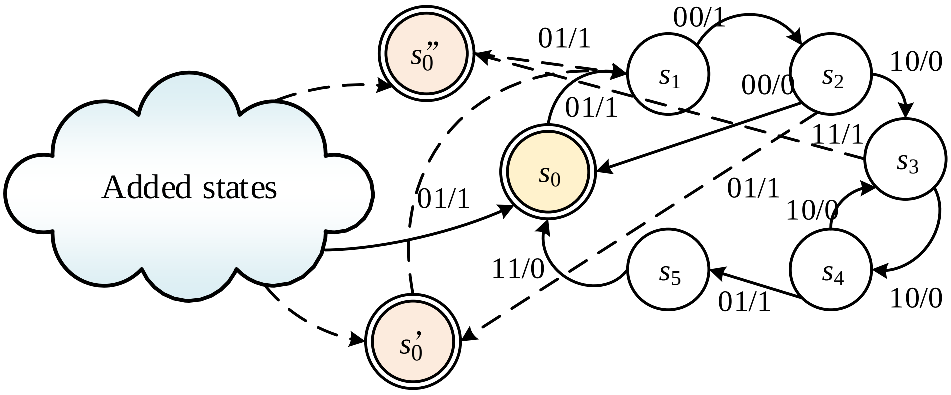

Figure 4-4. The proposed improve method of internal metering method.

Based on the BFSM in Figure 4-4, some new states are added as pseudo reset states (PRS) of s_0' and s_0''. To maintain the original design functionality while making the original initial state well hidden, these PRS should satisfy the following criteria.

(1) Some states out of the set of added states should have paths transmitting to these PRS. Otherwise, these PRS will never be reached under normal function mode. The original initial state s_0 cannot be well hidden among PRS.

(2) As a source state of a transition in FSM, each PRS state should have the similar transitions as the state s_0. Thus, when any powered up state transmits to one PRS, PRS can work as the s_0 to reach to other functional states under a specific input to begin normal operation.

(3) As a sink state of a transition in FSM, each PRS state should have all transitions different from s_0. This will make s_0 different from PRS. During normal operations, the transitions to PRS have no real function.

Thus, for one without the knowledge of the FSM design, it is difficult to distinguish the true initial state from the PRS. As shows in Figure 4-4, similar to s_0, s_0' and s_0'' both have the unique output transition to state s_1 under the input “01”. Also, there are some states out of the added states that can reach s_0' and s_0''. State s_2 can transit to state s_0 under the input “00” and state s_5 can also transit to state s_0 under input “11”. However, state s_0' can only be reached from state s_2 under input “01” and state s_0'' can only be reached from s_3 under input “11”.

As for the number of PRS, if it is too large, the complexity of the FSM is increased dramatically. If it is too small, the initial state s_0 cannot be well hidden. The exact number of PRS can be determined by experiment. In a reasonable range, all possible number of PRS is tried and the one which results in minimum overhead is selected.

Table 4-1. Evaluation of overhead on area.

Circuit	Original design			[10]	Prop.	
	In	Out	Area	Area	Area	Δ(%)
s27	4	1	54	5428	5490	1.14
s208	11	2	155	7463	7443	-0.27
s298	3	6	1039	8914	8803	-1.25
s820	18	19	300	11317	11447	1.15
s832	18	19	308	11447	11447	0.00
s1494	8	19	486	10367	10398	0.31
s420	19	2	156	7980	8030	0.63
s1488	8	19	476	10367	10334	-0.32
s386	7	7	133	8426	8573	1.74
s510	19	7	262	9682	9754	0.74
Average	-	-	-	-	-	0.39

4.3 Experiment evaluation and analysis

The proposed metering method is applied on 10 sequential circuit benchmarks from the LGSyth91. The FSM of these sequential benchmarks are represented in kiss2 format. Both the original scheme in [19] and the proposed scheme are implemented in Python programming language. The original designs are processed by the method in [19] with 2^{10} pseudo initial states added into the original design. The proposed method is also applied on these original designs with 2^{10} pseudo initial states and two pseudo original states added into the modified design, respectively. Then the obtained FSM in kiss2 format is translated into VHDL format. Then the Design Compiler under Synopsys Company and the technology library of TSMC 0.18μm are used to synthesize both the FSM designs. The experimental results, the overhead in terms of area, time delay and power, are presented in Table 4-1, Table 4-2 and Table 4-3, respectively. Next, a detail analysis of these three tables are presented.

Table 4-2. Evaluation of overhead on delay.

Circuit	Original	[10]	Prop.	
	Delay	Delay	Delay	Δ(%)
s27	37.97	35.46	35.46	0
s208	37.26	35.59	35.68	0.25
s298	35.56	32.86	33.57	2.16
s820	37.29	34.95	34.91	-0.11
s832	37.42	34.92	34.55	-1.06
s1494	36.79	33.72	33.31	-1.22
s420	37.31	35.84	35.82	-0.06
s1488	36.73	33.56	33.59	0.09
s386	37.26	34.18	34.2	0.06
s510	36.27	35.06	35.08	0.06
Average	-	-	-	0.02

The overhead on area, delay and power caused by the proposed method are shown and compared with that of the method in [19] respectively in Table 4-1, Table 4-2 and Table 4-3. In Table 4-1, the columns of ‘in’ and ‘out’ just denote the numbers of input and outputs of each FSM. The columns of area present the area of the original FSM, BFSM in [10] and the FSM generated by the proposed method. The area is represented by the number of normal 2 input NAND gates. The percentage overhead of the proposed method to that in [10] is shown in last column of Table 4-1. It is found that area overhead of all design is smaller than 2% and the average area overhead in these 10 test benchmarks is just 0.39%. We can also see that, the designs modified by the proposed method even incurs lower area overhead than that in [10]. It can be explained as that logic synthesis itself is an NP-hard problem. The introduction of more states may result in a design with smaller area.

The evaluation of the delay performance is shown in Table 4-2. The delay of the critical path of each design is shown and the percentage overhead of the delay of the FSM generated by the proposed design to that by work in [10] is shown in last column. The average delay overhead of those 10 designs is just 0.02%, which indicates that the proposed method just incurs negligibly low overhead of delay.

Table 4-3. Overhead analysis in terms of power.

Circuit	Original	[10]	Prop.	
	Power	Power	Power	Δ(%)
s27	2.82	24.6	27.78	13.04
s208	3.82	64.0	68.80	7.46
s298	8.33	56.2	56.68	0.93
s820	7.21	125.0	128.65	2.95
s832	7.28	124.4	130.10	4.62
s1494	14.22	93.1	102.74	10.35
s420	3.47	86.9	90.30	3.87
s1488	14.14	96.3	98.84	2.61
s386	3.87	72.7	76.59	5.37
s510	2.9372	104.7	107.13	2.30
Average	-	-	-	5.35

The evaluation of the power performance is shown in Table 4-3. The power of each design is shown and the percentage overhead of the power of the FSM generated by the proposed design to that by work in [10] is shown in last column. The average power overhead of those 10 designs is 5.35%. An industrial design usually has a reasonably large area and power consumption. Such power overhead will become more and more negligible as the design complexity increases.

Above all, compared to the method in [10], the proposed design just incurs low overhead while its resilience against the possible invasive attack is greatly increased.

4.4 Summary

In this chapter, an improved internal metering method to avoid invasive attacks is proposed. Some pseudo original initial states are introduced to impede the attacker to identify the true original initial state. Thus, he cannot easily bypass all newly introduced states and their transitions to original initial state to nullify the IC metering scheme. Compared to the original internal metering method, little overhead is incurred while the resilience of IC metering against the invasive attack improved.

CONCLUSION

IC overbuilding and piracy problems have caused great economic loss for the design house. Also, the security of a nation is threatened when pirated chip is held by the enemy. IC metering techniques have been explored to solve these problems. The passive metering technique can only assign a unique ID to each chip, however, it cannot protect the overbuilt chips from being applied. Active metering can protect the chips more efficiently by inserting a lock into each fabricated chip. As the unique key to unlock each chip can only be provided by the designer, the fabless company can guarantee that each fabricated chip can be detected. However, existing active metering techniques have weakness in security and overhead. To overcome these weaknesses, this work proposed two active metering techniques.

A new external active metering method is first proposed. In this method, the PKC system is used to encrypt the PUF key so that the PUF-based key is confidential to the foundries. The design house is the only one who can activate the manufactured chips as the encrypted information can only be decrypted by the designer with the private key. In this way, design house can actively control the number of fabricated copies. The anti-fuse technology is used to implement the lock on the TC ports of some scan cells. Anti-fuse can only be blown when a correct key is provided to enable these SFFs to work normally under normal working mode. This lock scheme never introduces any overhead on timing. Also, when a correct key activates the chip for the first time, the lock scheme is ineffective any more. This can overcome the weakness of PUF in reliability. The scheme also friendly enables the key to be input for multiple times.

Another improved internal metering method is proposed. To overcome the weakness in security of the internal metering method based on BFSM, some pseudo reset states are introduced to make it difficult for attackers to distinguish the original reset state. Compared to the original metering method, little overhead in area, power and delay were introduced. The security is improved and the invasive attack by bypassing the extra states and transitions can be well resisted.

In future work, the PUF information is explored to be well hidden in the original design so that only the designer can retrieve. In this way, the PKC module for encryption of the PUF-based key can be removed from the external metering scheme to minimize the overhead due to metering. Also, the unlocking status should not be easily identified. A more secure lock scheme is to be studied to make the metering technique more secure against possible attacks.

REFERENCES

1 Roy J A, Koushanfar F, Markov I L. Ending Piracy of Integrated Circuits [J]. Computer, 2010, 43(10): 30-38.

2 Torrance R, James D. The State-of-the-Art in IC Reverse Engineering [J]. Cryptographic Hardware and Embedded Systems - CHES, 2009, 5747: 363-381.

3 VSI Alliance. Intellectual Property Protection: Schemes, Alternatives and Discussion [EB/OL]. [2017-11-25]. http://www.doc88.com/p-9893608484833.html

4 Cui A, Qu G, Zhang Y. Ultra-Low Overhead Dynamic Watermarking on Scan Design for Hard IP Protection [J]. IEEE Transactions on Information Forensics & Security, 2017, 10(11): 2298-2313.

5 Morley R E, Richter E J, Engel G L. Method and apparatus for authenticating a magnetic fingerprint signal using an adaptive analog to digital converter: US, US7210627[P]. 2007.

6 Fu K. DRV-Fingerprinting: using data retention voltage of SRAM cells for chip identification [C]// Proceedings of International Conference on Radio Frequency Identification: Security and Privacy Issues, Piscataway: IEEE, 2012: 165-179.

7 Koushanfar F, Qu G, Potkonjak M. Intellectual Property Metering [C]// Proceedings of International Workshop on Information Hiding, Piscataway: IEEE, 2001: 81-95.

8 Koushanfar F, Qu G. Hardware metering [C]// Proceedings of the 38th annual Design Automation Conference, Piscataway: IEEE, 2001: 490-493.

9 Wei, Sheng, Nahapetian, et al. Robust passive hardware metering [C]// Proceedings of IEEE International Conference on Computer-Aided Design, Piscataway: IEEE, 2011: 802-809.

10 Alkabani Y M, Koushanfar F. Active hardware metering for intellectual property protection and security [C]// Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, New York: ACM, 2007： 291-306.

11 Bolotnyy L, Robins G. Physically Unclonable Function-Based Security and Privacy in RFID Systems [C]// Proceedings of IEEE International Conference on Pervasive Computing and Communications, Piscataway: IEEE, 2007: 211-220.

12 Kumar S S, Guajardo J, Maes R, et al. Extended abstract: The butterfly PUF

protecting IP on every FPGA [C]// Proceedings of IEEE Hardware-Oriented Security and Trust, Piscataway: IEEE, 2008: 67-70.

13 Kursawe K, Sadeghi A R, Schellekens D, et al. Reconfigurable Physical Unclonable Functions - Enabling technology for tamper-resistant storage [C]// Proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust, Piscataway: IEEE, 2009: 22-29.

14 Pappu R, Recht B, Taylor J, et al. Physical One-Way Functions [J]. Science, 2002, 297(5589): 2026-2030.

15 Suh G E, Devadas S. Physical unclonable functions for device authentication and secret key generation [C]// Proceedings of IEEE Design Automation Conference, 2007. DAC '07. ACM/IEEE, Piscataway: IEEE, 2007: 9-14.

16 Gassend, Blaise, Clarke, et al. Silicon physical random functions [C]// Proceedings of the 9th ACM conference on Computer and communications security, New York: ACM, 2002: 148-160.

17 Guajardo J, Kumar S S, Schrijen G J, et al. Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection [C]// Proceedings of International Conference on Field Programmable Logic and Applications, Piscataway: IEEE, 2007: 189-195.

18 Majzoobi M, Koushanfar F. Time-Bounded Authentication of FPGAs [J]. IEEE Transactions on Information Forensics & Security, 2011, 6(3): 1123-1135.

19 Koushanfar F. Provably Secure Active IC Metering Techniques for Piracy Avoidance and Digital Rights Management [J]. IEEE Transactions on Information Forensics & Security, 2012, 7(1): 51-63.

20 Ward B. A detail History of the Processor [EB/OL]. [2017-11-25]. https://www.pcmech.com/article/a-cpu-history/4.

21 Lofstrom K, Daasch W R, Taylor D. IC identification circuit using device mismatch [C]// Proceedings of Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International, Piscataway: IEEE, 2002: 372-373.

22 Clarke D, Gassend B, Dijk M V, et al. Authentication of integrated circuits: US, US 7840803 B2[P]. 2010.

23 Gassend, Blaise, Clarke, et al. Silicon physical random functions [C]// Proceedings

of ACM Conference on Computer and Communications Security, CCS 2002, Piscataway: IEEE, 2002: 148-160.

24 Alkabani Y, Koushanfar F, Potkonjak M, et al. Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach [C]// Proceedings of Information Hiding, Piscataway: IEEE, 2008: 102-117.

25 Potkonjak M, Nahapetian A, Nelson M, et al. Hardware Trojan horse detection using gate-level characterization [C]// Proceedings of Design Automation Conference, Piscataway: IEEE, 2009: 688-693.

26 Alkabani Y, Koushanfar F. Active control and digital rights management of integrated circuit IP cores [C]// Proceedings of International Conference on Compilers, Architectures and Synthesis for Embedded Systems, Piscataway: IEEE, 2008: 227-234.

27 Yu M D, Devadas S. Secure and Robust Error Correction for Physical Unclonable Functions [J]. IEEE Design & Test of Computers, 2010, 27(1): 48-65.

28 Alkabani Y, Koushanfar F, Potkonjak M. Remote activation of ICs for piracy prevention and digital right management [C]// Proceedings of IEEE/ACM International Conference on Computer-Aided Design, Piscataway: IEEE, 2007: 674-677.

29 Zhang J, Lin Y, Lyu Y, et al. A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-Per-Device Licensing [J]. IEEE Transactions on Information Forensics & Security, 2017, 10(6): 1137-1150.

30 Roy J A, Koushanfar F, Markov I L. EPIC: ending piracy of integrated circuits [C]// Proceedings of Design, Automation and Test in Europe, Piscataway: IEEE, 2008: 1069-1074.

31 Maes R, Schellekens D, Tuyls P, et al. Analysis and design of active IC metering schemes [C]// Proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust, Piscataway: IEEE, 2009: 74-81.

32 Roy J A, Koushanfar F, Markov I L. Protecting bus-based hardware IP by secret sharing [C]// Proceedings of Design Automation Conference, 2008. DAC 2008. ACM/IEEE, Piscataway: IEEE, 2008: 846-851.

33 Huang J, Lach J. IC activation and user authentication for security-sensitive systems

[C]// Proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust, Piscataway: IEEE, 2008: 76-80.

34 Baumgarten A, Tyagi A, Zambreno J. Preventing IC Piracy Using Reconfigurable Logic Barriers [J]. IEEE Design & Test of Computers, 2010, 27(1): 66-75.

35 Ferguson N, Schneier B. Practical Cryptography [M].Wiley, 2003: 70-80.

36 Rivest R, Shamir A, Adleman L M. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 26(2): 96-99.

37 Contreras G K, Rahman M T, Tehranipoor M. Secure Split-Test for preventing IC piracy by untrusted foundry and assembly [C]// Proceedings of IEEE International Symposium on Defect and Fault Tolerance in Vlsi and Nanotechnology Systems, Piscataway: IEEE, 2013: 196-203.

38 Chen L, Cui A, Chang C H. Design of Optimal Scan Tree Based on Compact Test Patterns for Test Time Reduction [J]. IEEE Transactions on Computers, 2015, 64(12): 3417-3429.

39 Yu T, Cui A, Li M, et al. A new decompressor with ordered parallel scan design for reduction of test data and test time[C]// Proceedings of IEEE International Symposium on Circuits and Systems, Piscataway: IEEE, 2015: 641-644.

40 Xu X, Rahmati A, Holcomb D E, et al. Reliable Physical Unclonable Functions Using Data Retention Voltage of SRAM Cells[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34(6): 903-914.

41 Tokunaga C, Blaauw D, Mudge T. True Random Number Generator With a Metastability-Based Quality Control [J]. IEEE Journal of Solid-State Circuits, 2008, 43(1): 78-85.

42 Bafandehkar M, Yasin S M, Mahmod R, et al. Comparison of ECC and RSA Algorithm in Resource Constrained Devices [C]// Proceedings of International Conference on It Convergence and Security, Piscataway: IEEE, 2013: 1-3.

43 Basicrsa. RSA: Overview [EB/OL]. [2017-04-20]. http://opencores.org/project, basicrsa.

44 Aes_pipe. *AES: Overview* [EB/OL]. [2014-10-09]. Available: http://opencores.org/project, tiny_aes.

45 Wang W, Cui A, Qu G, et al. A low-overhead PUF based on parallel scan design[C]//

Proceedings of 23rd Asia and South Pacific Design Automation Conference (ASP-DAC), Piscataway: IEEE, 2018 (Accepted).

46 Koushanfar F. Hardware Metering: A Survey [M]. Springer New York, 2012： 103-122.

47 Yu M D, Devadas S. Secure and Robust Error Correction for Physical Unclonable Functions [J]. IEEE Design & Test of Computers, 2010, 27(1): 48-65.

48 Majzoobi M, Koushanfar F, Potkonjak M. Techniques for Design and Implementation of Secure Reconfigurable PUFs [J]. ACM Transactions on Reconfigurable Technology and Systems, 2009, 2(1): 1-33.

49 Beckmann N, Potkonjak M. Hardware-Based Public-Key Cryptography with Public Physically Unclonable Functions[C]// Proceedings of Information Hiding, International Workshop, Ih 2009, Darmstadt, Germany, June 8-10, 2009, Revised Selected Papers, Piscataway: IEEE, 2009: 206-220.

攻读硕士学位期间发表的论文及其它成果

（一） 发表的学术论文

[1]. Cui A, Qian X, Qu G, et al. A new active IC metering technique based on locking scan cells [C]// Proceeding of the IEEE Asian Test Symposium (ATS), 2017, accepted. EI. CCF-C 类会议