Design of Security Primitives for Trustworthy Integrated Circuits

by

Yuan CAO

A Thesis Submitted to
The Nanyang Technological Univerisity
in Partial Fulfillment of the Requirements for
the Degree of Doctor of Philosophy
in the School of Electrical and Electronic Engineering

May 2015, Singapore

Authorization

I hereby declare that I am the sole author of the thesis.

I authorize the Nanyang Technological Univerisity to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize the Nanyang Technological Univerisity to reproduce the thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

Student: Yuan CAO

May 12th, 2015

Abstract

The horizontal business model in semiconductor industry has brought economic benefits but relinquished the control that integrated circuit (IC) designer had in chip design and manufacturing, thus making chips expose to greater security threats and vulnerable to various kinds of hardware attacks. As electronic devices becoming increasingly ubiquitous and permeated into our daily lives, critical basic infrastructures and national defense systems, hardware security features that can assure the trustworthiness of an integrated system in a reliable, efficient and inexpensive way are highly desirable. In the dissertation, two embedded hardware security primitives, namely active current sensors and Physical Unclonable Functions (PUFs) are investigated for hardware Trojan (HT) detection, device identification and authentication.

Hardware Trojans are the deliberate and malicious alterations to original IC designs that can jeopardize the design integrity, stealing the confidential information or paralyzing the system connected to the subverted chip upon their activation. In this thesis, a transient power supply current sensor to facilitate the screening of an IC for HT infection is proposed. Based on the power gating scheme, it converts the current activity on local power grid into a timing pulse from which the timing and power related side channel signals can be externally monitored by the existing scan test architecture. Its current comparator threshold can be adjusted for calibration against the quiescent current noise floor to reduce the impacts of process variations. Post-layout statistical simulations of process variations are performed on the ISCAS'85 benchmark circuits to demonstrate the effectiveness of the proposed technique for the detection of delay-invariant and rarely switched

HTs. Compared with the detection error rate of a 4-bit counter based HT reported by an existing HT detection method using the path delay fingerprint, the proposed method shows an order of magnitude improvement in the detection accuracy.

Physical Unclonable Functions are emerging security primitives that are useful in secure key generation, device authentication, and counterfeit detection and prevention. This thesis presents two main contributions in PUF research community: 1) An ultra-low power and small footprint hybrid RO PUF with very high temperature stability is proposed as an ideal candidate for lightweight applications. The classic ring oscillator (RO) based PUF is resilient to noise impacts, but its response is susceptible to temperature variations. Additional components or complex algorithms are usually employed to address this problem at the expense of large area and power consumption overheads. The proposed PUF exploits the negative temperature coefficient property and the low-power subthreshold operation of current starved inverters to mitigate the variations of differential RO frequencies with temperature. The new architecture uses conspicuously simplified circuitries to generate and compare a large number of pairs of RO frequencies, and facilitate logical reconfigurability to thwart machine learning attacks. The proposed 9-stage hybrid RO PUF was fabricated using 65 nm CMOS technology. Its measured challenge-response pairs (CRPs) possess larger entropy per unit area than the classic RO PUF design. The PUF occupies only 250 μm^2 of chip area and consumes only 32.3 μV per CRP at 1.2 V and 230 MHz. The measured average and worst-case reliabilities of its responses are as high as 99.84% and 97.28%, respectively over a wide range of temperature from -40 °C to 120 °C. 2). Another new low-cost CMOS image sensor based PUF is also proposed. It targets a variety of security, privacy and trusted protocols that involve image sensor as a trusted entity. The proposed PUF exploits the intrinsic imperfection during the image sensor manufacturing process to generate a rich set of unique and stable digital signatures. The proposed differential readout algorithm stabilizes the response bits extracted from the random fixed pattern noise (FPN) of selected pixel pairs determined by the applied challenge against supply voltage and temperature variations. The threshold of difference can be tightened to winnow out more unstable

response bits from the huge challenge-response space offered by modern image sensors to enhance the reliability under harsher operating conditions or it can also be loosened to improve its resiliency against masquerade attacks in routine operating environment. Experimentations conducted on a 64×64 image sensor fabricated in 180 nm 3.3 V CMOS technology demonstrated that robust and reliable challenge-response pairs can be generated with a uniqueness of 49.37% and a reliability of 99.10% under temperature variations of $15 \sim 115$ °C and supply voltage variations of $3 \sim 3.6$ V.

Acknowledgements

The research work undertaken in this thesis has been thoroughly enjoyable. That enjoyment is largely a result of the interaction that I have had with my supervisors, the lab-mates, the university and the people who have helped me so far.

It is my honor to work with my supervisor, Prof. Chen Shoushun and my co-supervisor, Prof. Chang Chip-Hong. Prof. Chen is very generous in securing the scholarship from Advantest Cooperation to finance my PhD program. He also helps me greatly in the technical details and supports my chip fabrication. Prof. Chang has taught me a great deal about the research of hardware security by sharing with me the joy of discovery and investigation that is the heart of my research. I owe him a great debt of gratitude for his patience, inspiration and friendship.

I would like to thank Zhang Le, Zhang Li, Sergey, Jeremy, Hanhua, Thian Fatt and Sachin in the Chips family, with whom I spent a lot of happy time both in research and entertainment. I also would like to thank Feng Xiaohua, an excellent Ph.D student, in our lab. With him, I developed a few interesting smartphone based applications. Dr. Ye Wenbin, Lin Jiafu, Wang Yong, Dr Yi Xiang, Dr Zhao Bo, Yu Hang, Zhang Xiangyu and all my other friends in VIRTUS, the IC Design Center of Excellence, also advised me on algorithms, hardware design and analysis, and chip testing. Without them, I doubt that many of my ideas would have come to fruition.

I wish to thank Advantest Cooperation for supporting my study with the research scholarship and traveling grants for attending conferences. I also thank my manager Adrion Yap who is supportive of both my study and work.

Last but definitely not the least, thanks also to my family, especially my wife, who has been extremely understanding and supportive of my study. I feel very lucky to have such a family that shares my enthusiasm for academic pursuit.

Contents

Abstract **i**

Acknowledgements **v**

1 Introduction **1**

1.1 Motivation 1

1.2 Thesis Objective and Contributions 5

1.3 Thesis Organization 7

2 Background **11**

2.1 Hardware Trojan 11

2.1.1 Hardware Trojan Taxonomy 13

2.1.2 Hardware Trojan Detection Methods 15

2.1.3 Summary 21

2.2 Physically Unclonable Function 22

2.2.1 Types of Silicon PUF 22

2.2.2 PUF Applications in Hardware Security 27

2.2.3 PUF Qualities and Metrics 28

2.2.4 Summary 30

3 A Cluster-Based Distributed Active Current Sensing Circuit for Hardware Trojan Detection **31**

3.1 Introduction 31

3.2 Motivating Example 33
3.3 Scan-enabled Active Current Sensor 38
3.3.1 Current Mirror 39
3.3.2 Current Comparator 40
3.3.3 Scan Register 43
3.4 Results and Discussion 45
3.4.1 Experiment Setup 45
3.4.2 Trojan Circuits 46
3.4.3 Detection of Trojan with Low Switching Activity 47
3.4.4 Detection of Trojan with No Delay Impact 51
3.4.5 Scaling the Trojan 54
3.4.6 Sensor Security 55
3.5 Summary 56

4 A Low-power Hybrid Ring Oscillator Physical Unclonable Function with Improved Thermal Stability for Lightweight Applications 59

4.1 Introduction 59
4.2 Classic RO PUF's Temperature-induced Response Stability Problem 61
4.2.1 Temperature Dependence of RO PUF Responses 61
4.2.2 Temperature Coefficient of Regular Inverter 62
4.3 Proposed Temperature Coefficient Compensated Hybrid Inverter based RO PUF 64
4.3.1 Temperature Coefficient of Current Starved Inverter 64
4.3.2 Temperature Coefficient of Hybrid RO 65
4.3.3 Architecture and Operation of Proposed Hybrid RO 69
4.4 Quality and Security Analysis of Proposed Hybrid RO PUF 72
4.4.1 Uniqueness of Proposed Hybrid RO PUF 72
4.4.2 Reliability of the Proposed Hybrid RO PUF 73
4.4.3 Unpredictability of the Proposed Hybrid RO PUF 75
4.4.4 Attack Analysis 77

4.5 Experimental Result 80
4.6 Summary 86

5 CMOS Image Sensor based Physical Unclonable Function for Coherent Sensor-level Authentication 89
5.1 Introduction 89
5.2 Related Works 92
5.3 Circuits and Operations 94
5.3.1 CMOS Image Sensor Fundamentals 94
5.3.2 Proposed Image Sensor based PUF 96
5.3.3 Reliability Enhancement 99
5.4 Experimental Results and Discussions 104
5.4.1 Uniqueness Assessment 105
5.4.2 Reliability Assessment 106
5.4.3 Unpredictability Assessment 108
5.4.4 Implementation Overheads 110
5.4.5 Attack Analyses 111
5.5 Emerging Applications 113
5.5.1 Smart phone authentication and anti-counterfeiting 113
5.5.2 Against Virtual Camera Attack 114
5.5.3 Optimize P_{th} for Different Applications 115
5.6 Summary 115

6 Conclusion 117
6.1 Conclusion 117
6.2 Future Work 119
6.2.1 Temperature and Voltage Invariant Hybrid RO based PUF with Adaptive Self Biasing 119
6.2.2 Cognitive Image Sensor Based PUF 120

List of Publications 123

List of Figures

1.1 Vulnerability of a modern IC in the ASIC design and fabrication flow reported by DARPA [1]. . . . 3

2.1 An example of hardware Trojan [2]. . . . 12
2.2 Detailed taxonomy showing physical, activation, and action characteristics of different types of hardware Trojan [3]. . . . 13
2.3 Path delay measurement architecture using a shadow register [4]. . . 18
2.4 Power-based side-channel analysis [5]. . . . 19
2.5 Example of regional power-based side-channel analysis [6]. . . . 20
2.6 The schematic of arbiter PUF [7]. . . . 24
2.7 Classic ring oscillator PUF architecture. . . . 25
2.8 The basic structure of the SRAM cell [8]. . . . 26
2.9 The logical structure of the latch PUF cell [9]. . . . 27

3.1 Example of a HT (a) with no delay impact, (b) with no switching power impact. . . . 32
3.2 I_{DDT}, input and output waveforms due to a sensitized path in C432. 34
3.3 Supply current waveforms for the sensitized path of Trojan-free and Trojan-infected circuits: (a) the Trojan is inserted in series, (b) the Trojan is inserted in parallel. . . . 35
3.4 Example of the deployment of the proposed HT detector with six virtual-power clusters. . . . 36
3.5 The HT detection flow using the proposed HT-detector. . . . 37

3.6 Schematic of the proposed current sensing to path delay monitoring circuit. 38
3.7 Schematic of Traff's current comparator [10]. 41
3.8 Corner simulation of comparator output pulse width: (a) without calibration, (b) with calibration. The process corner is represented by a two-letter designator, where the first and second letters refer to the NMOS and PMOS corners, respectively. The letters T, F and S denote typical, fast and slow corners, respectively. 42
3.9 Simulation of comparator output pulse width under temperature variations: (a) without calibration, (b) with calibration. 43
3.10 Primary and secondary scan chains for the detection of current comparator output pulse width. 44
3.11 Timing diagram of the sampling of transition delay. 45
3.12 Counter-based Trojan circuit architecture [11]. 46
3.13 Monte Carlo simulation results for the active current duration distributions: (a) before calibration, (b) after calibration. 48
3.14 The delay impacts with different placements of Trojan: (a) Trojan embedded in serial, (b) Trojan embedded in parallel. 52
3.15 Monte Carlo simulation results for the average active current amplitude distributions: (a) before calibration, (b) after calibration. . . 54

4.1 Change in oscillation frequency with temperature for an RO. 62
4.2 Output bits of two different temperature induced frequency distance scenarios of two RO pairs: the output bit (a) flips, (b) is stable. . . 63
4.3 Circuit schematic of (a) a regular inverter, (b) a current starved inverter. 64
4.4 Relative frequency deviations against temperature for three ROs with 9 stages of regular, current starved and hybrid inverters, respectively. 66
4.5 Effect of regular inverter scaling on the frequency deviation of the hybrid RO. 67

4.6 Effect of regular inverter scaling on the frequency deviation of the hybrid RO. 68
4.7 Effect of combined regular and current starved inverter scaling on the frequency deviation of the hybrid RO. 69
4.8 Architecture of the proposed hybrid RO PUF. 71
4.9 Timing diagram of the operations of the proposed hybrid RO PUF. 72
4.10 Frequency distribution of the simulated inter-die HDs. 73
4.11 Frequency distribution of the simulated PUF response reliability with ambient noise. 74
4.12 Corner simulation of oscillation frequencies of hybrid RO against the temperature variation. 75
4.13 The simulated CRP reliability at different temperatures for the classic Suh's [12] and proposed RO PUF. 76
4.14 The number of independent bits that can be produced by the classic Suh's RO PUF [12] and the proposed hybrid RO PUF with the same number of transistors. 77
4.15 Prediction accuracy by SVM for 64-bit arbiter PUF [13] and the proposed 64-bit hybrid RO PUF. 79
4.16 The microphotograph of the proposed hybrid RO PUF chip. 81
4.17 The probe station for the testing of the sample chips. 81
4.18 The distribution of hybrid RO's oscillation frequency of one sample chip. 82
4.19 Inter-die HD distribution measured from the hybrid RO PUF chips. 83
4.20 The measured average reliability of hybrid RO PUF against (a) voltage variations, (b) temperature variations. 83
4.21 The measured power consumption per CRP of the proposed PUF chip at different RO's frequency. 85
4.22 The measured EM radiation from (a) the regular RO, (b) the proposed hybrid RO. 86

5.1 A typical FPN image of a CMOS image sensor [14]. 91

5.2 Typical CMOS image sensor architecture. 95
5.3 The schematic of (a) 3T-APS pixel, (b) 4T-APS pixel. 96
5.4 Architecture of the proposed CMOS image sensor based PUF. 97
5.5 Architecture of CRP generator circuit. 99
5.6 Procedure for CRP generation. 100
5.7 Monte Carlo simulation results of V_{rst} and V_{sig} against the variations of (a) supply voltage, and (b) temperature. 102
5.8 Effects of P_{th} on PUF reliability and the number of CRPs. 103
5.9 Simulation results of BER for different parametric combinations of P_{th} and ε. 104
5.10 The microphotograph of the image sensor used for the validation of the proposed PUF. 105
5.11 The distribution of pixel voltage values of the image (a) without CDS and (b) with CDS under office lighting. 106
5.12 Frequency distribution of (a) the simulated inter-die HDs for 100 PUF instances and (b) the measured inter-die HDs from the five image sensor based PUF chips. 107
5.13 The measured average reliability of hybrid RO PUF against (a) voltage variations, (b) temperature variations. 108
5.14 The measured relationship between P_{th} versus the number of valid pixels and the reliability. 109

6.1 Current starved inverter with external bias V_{ctrl}. 120
6.2 Simulation results of the 9-stage hybrid RO's frequency versus V_{ctrl}. 121
6.3 Simulated results of 9-stage hybrid RO's frequency versus the supply voltage V_{DD}. 122

List of Tables

3.1 Transition delays of detector outputs for the genuine and infected designs . . . 47
3.2 Key parameter variations used in the dynamic timing analysis . . . 51
3.3 Statistics of Fig. 3.13 . . . 51
3.4 Detection error rate with and without PV calibration for serial placement of Trojan in ISCAS'85 benchmarks . . . 52
3.5 Detector outputs for the genuine and infected designs for Trojan with no delay impact . . . 53
3.6 Statistics of Fig. 3.15 . . . 54
3.7 Detection error rate for Trojan with no delay impact in ISCAS'85 benchmarks with and without PV calibration . . . 55
3.8 DERs of the proposed method for different Trojan area overheads. . . 55

4.1 Comparison of the 9-stage regular, current starved and hybrid ROs. 66
4.2 Comparison of power consumption per CRP of the proposed hybrid RO PUF with other temperature invariant RO PUFs. . . . 84
4.3 Comparison of the qualities and costs of the proposed PUF with other PUFs. . . . 86

5.1 NIST test results on the random sequences generated by the proposed image sensor based PUF. . . . 109
5.2 Resources consumed by CRP generator in FPGA implementation. . 110
5.3 Comparison of qualities of our proposed PUF with other PUFs. . . 111

Chapter 1

Introduction

1.1 Motivation

The continued advancement of semiconductor manufacturing technology has revolutionized the world and enabled many unimaginable applications. For example, the smartphones and tablets have now become so prevalently used in online payment, web browser, gaming, personal data assistant and personal healthcare than the routine functions of its predecessor feature phones and personal computers. The all-pervasive influences of electronic devices can be felt in every aspect of our daily life. The propeller behind this ever faster renewal of electronic gadgets is the perpetual increase in device integration density (the number of devices per unit area in an integrated circuit (IC)) projected by the Moore's Law in the "silicon era".

The dramatically increase in the cognitive and organizational complexity of IC design is pushing the semiconductor industries towards a vertical specialization where various stages of IC design are disintegrated, outsourced to external firms and relocated across national boundaries that have the tacit knowledge and expertise. Generally, the design of an IC is facilitated by the following external service and resource providers:

- Electronic design automation (EDA) companies provide the powerful and complicated software tools that aid the design and verification of modern ICs.

- Semiconductor foundries provide the IC designers with the electronic device models and the services to fabricate and manufacture the chips with their facilities so that the designers can benefit from the lower per capital cost of chip manufacturing and focus their research and development effort on the product functions required by the end markets.

- Cell library developers and Intellectual property (IP) core vendors provide the IP blocks, such as the standard and specialized cell libraries, CPU cores, memories and controllers that have been fully tested and optimized to deliver the desired performance. These IP blocks help to reduce the design time, improve the reliability and yield, and meet the short time-to-market window for the development of the complex system-on-chip.

The active participation of the various external agents in the design and manufacturing flow of an IC has made the entire IC supply chain highly susceptible to chip contamination and subversion. Fig. 1.1 shows the potential vulnerability of a modern IC to various forms of security threats in the design and fabrication flow. Examples of these threats in different stages of the IC design flow are:

- Malicious logics (hardware Trojan) insertion [3]: The original design can be modified in the design phase or during the fabrication phase, if the adversary gains the access to it. The hardware Trojans may potentially leak the sensitive data, reduce the IC reliability or cause a system to fail at a critical time. The Trojans generally do not change the original function of the circuit and are very small in size, which can hardly be detected by the functional and parametric tests performed from the view points of the customers or legitimate end users.

- IP theft: The attacker can analyze the design or steal the IP. The stolen IP can be illegally used or copied to mass produce or counterfeit the design. Results of the analysis on the stolen IP can also be used by colluding attackers to aid in future software or hardware-based attacks or attacks on related designs as well.

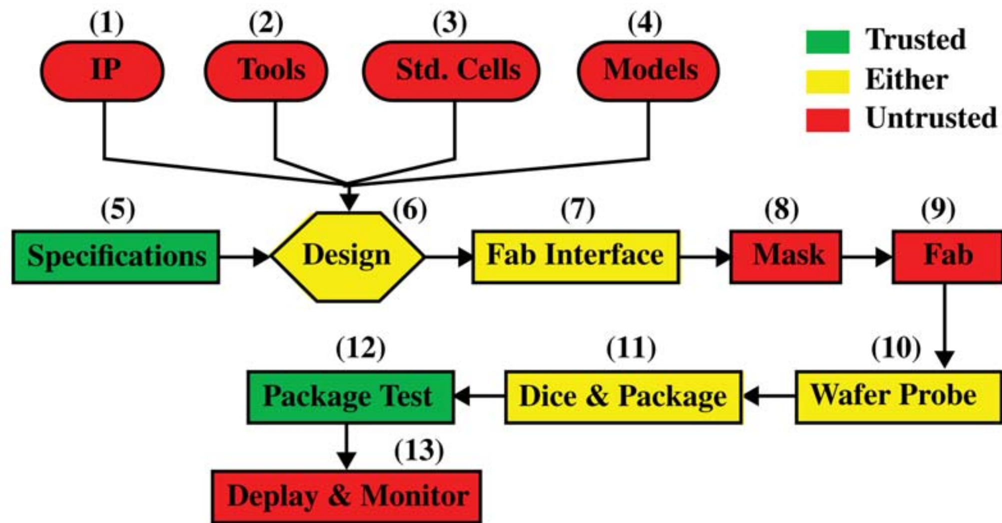

Figure 1.1: *Vulnerability of a modern IC in the ASIC design and fabrication flow reported by DARPA [1].*

- Reverse engineering [12]: High-class adversaries can spend days accessing the chip surface directly and observe the IC layout layer by layer with the help of the modern equipments. These invasive attacks can help the attackers understand the internal features and structures of the design. With this information, the attackers can easily counterfeit the design, and implant malicious hardware Trojan to evade detection or steal the sensitive data stored in the IC.

- Fault injection: The hardware Trojans or the back doors embedded in an IC can be triggered by exposing it to abnormal working conditions (intensive light pulses, radiation, local heating, etc.).

- Side-channel attack [15]: This attack is based on information gained from the physical implementation of a crypto-system, rather than by brute force or through exploiting theoretical weaknesses in the cryptographic algorithms. The side-channels of a device can be the path delay, power consumption or the electronic magnetic radiation.

The rapid growing complexity of ICs and the reliance on outsourcing of routine

and less value-added functions in the IC value chain have made assuring the IC integrity more difficult than ever. Meanwhile, modern and emerging technologies, such as scanning optical microscopy, light induced voltage alternation and machine learning, are also making it easier to attack an IC after its deployment.

Contrary to the impending end-of-the-road CMOS device scaling predicted by the pessimists many years ago, technology scaling turns out to be a key enabler of hardware cryptography. Security primitives have been built into lightweight applications that would have been unthinkable just a decade ago. In 2005, the Defense Advanced Research Projects Agency (DARPA) initiates the Trust in ICs program [16]. From then on, continuous innovations have been brought into this nascent field. With Internet of Things (IoT) envisaged to become an ultimate driver for the next growth phase of semiconductor industry, Radio frequency identification (RFID) and several other lightweight electronic tagging technologies will avail themselves most in this ubiquitous computing revolution of advance connectivity of devices, systems and services. Unfortunately, the footprint and power budget have severely limited the strength of cryptographic algorithm implementable on an RFID or other intelligent tags, and the secret data stored in these lightweight devices can be easily read or reverse engineered and copied. Critics are concern that the wide spread of IoT will make cyber-attack an increasingly devastating physical (as opposed to virtual) threat. Another reason that makes hardware security an attractive research area is that it is the last line of defence. Software security has been plagued by security issues for many years, and hardware has long been touted as a safe haven for privacy protection. In general, hardware-oriented security has the following two unique advantages over the software-based security:

- Lowest operation level: The operation of the hardware is located in the lowest level. Hardware security primitives can be faster, highly application-specific and more efficient than the software tools. Furthermore, software security measures can do little against some powerful hardware attacks, for example, microprobing.

- Modifiability: The ability to easily modify or update the software is a double-edged sword. On one hand, this can help the programmers fix and patch known software bugs quickly. On the other hand, the same flexibility can also be exploited by the attackers to install viruses or Trojans in the operating system. In contrast, the embedded secure hardware circuits in a chip cannot be easily modified after the IC deployment.

Nevertheless, without adequate protection, any hardware can be as vulnerable as the software. Any successful attacks to a hardware integrated system can cause greater disruptions, leading to heavier economic losses and may even endanger human lives. Given the tight coupling between information and communication technologies and physical systems today, the new security concerns of disastrous hardware attacks are requiring a rethinking and re-examination of the commonly used objectives and methods.

1.2 Thesis Objective and Contributions

The objective of this thesis is to investigate innovative and hardware-efficient solutions to overcome the hardware-based attacks during IC design, manufacturing and post-deployment. Specifically, the following two aspects of hardware security are pursued:

- Hardware Trojan (HT) detection [17]: HTs are among the most challenging attacks to prevent and detect. The malicious logics embedded in the original design are extremely difficult to be detected because of their small size and stealth. The triggering mechanism of HT is generally unknown and its behaviors cannot be modelled or predicated. Exhaustive functional test can have a full coverage but is impractical for the modern design as the test time is exponentially increased with the design's complexity. More importantly, such tests designed from the perspective of the benign end users can hardly succeed in activating the stealthy circuit implanted by the malicious adversary. Besides, the persistence of HT attacks (i.e., the threat is present as long

as the infected IC is in use) makes detection of their presence extremely important. Furthermore, a well-designed HT can also aid many other software or hardware attacks on the design. In this thesis, a transient power supply current sensor has been proposed and developed to monitor and screen an IC for HT infection. Based on the power gating scheme, it converts the current activity on the local power grid into a timing pulse from which the timing and power related side-channel signals can be externally monitored by the existing scan test architecture. Its current comparator threshold can be calibrated against the quiescent current noise floor to reduce the impacts of process variations. The proposed method takes advantage of both timing and power based side-channel signal analyses to increase the success rate of difficult HT detection. The state-of-art HT benchmarks have been used to examine the efficiency of the proposed method.

- Physically Unclonable Functions (PUFs) [18]: PUFs are emerging security primitives that are used in secure key generation, device authentication, and counterfeit detection and prevention. It utilizes the IC manufacturing variations to generate unique, random and unclonable signatures. In contrast to the conventional technology that uses specifically designed and costly security-hardened non-volatile memory to store secret keys and confidential data, the secrets are intrinsically embedded in the structure of a PUF. Any invasive or semi-invasive attacks that can physically disrupt the structure of the PUF will also destroy the secret key. PUF is also investigated in this dissertation as it is an emerging secure solution to deal with the reverse engineering, IP theft, counterfeiting, and other physical attacks. The contributions with respect to PUFs are: 1) an ultra-low power and small footprint hybrid RO PUF with very high temperature stability is proposed. The negative temperature coefficient property of the low-power subthreshold operation of current starved inverters is exploited to mitigate the variations of differential RO frequencies with temperature. The current starved inverter stages in the RO working in the subthreshold region also bring down the

entire power consumption of the PUF. This new PUF architecture uses conspicuously simplified circuitries to generate and compare a large number of pairs of RO frequencies, and facilitates logical reconfigurability to thwart machine learning attacks. Its low power and interleaving structure also make it highly resilient to side-channel attacks based on electro-magnetic signal measurements. Its amenability to lightweight applications has been demonstrated by measurement results of the proposed PUF chip fabricated in 65 nm CMOS technology. 2) A new low-cost CMOS image sensor based PUF targeting for tightly integrated security protection with the image sensor itself is also proposed. The proposed PUF exploits the fixed pattern noises of the image sensor to generate the unique and reliable digital signatures. With the proposed differential readout algorithm for the fixed pattern noises of selected pixel pairs, the effects of global power supply and temperature variations are suppressed. The user defined threshold provides a trade-off between the reliability and the number of valid CRPs, which increases its versatility for different security applications. The experiments on a pre-fabricated 64×64 image sensor in 180 nm 3.3 V CMOS technology show that robust and reliable challenge-response pairs can be generated with a uniqueness of 49.37% and a reliability of 99.10% under temperature variations of 15∼115 °C and supply voltage variations of 3∼3.6 V. New applications against smartphone counterfeiting and virtual camera attacks that are made feasible with this proposed PUF are also identified.

1.3 Thesis Organization

The thesis is organized into six chapters. The first chapter introduces the research motivation, objective and the major contributions.

The background on hardware Trojans and PUFs are detailed in Chapter 2. This chapter firstly describes the basic components for a hardware Trojan. Based on the physical, activation, and action characteristics of the hardware Trojans, a comprehensive taxonomy is introduced. The taxonomy facilitates the researchers

to enable a systematic study of Trojans and their detection method. Then the state-of-the-art Trojan detection methods are reviewed. Both advantages and limitations of these methods are introduced and compared. Next, the existing silicon-based PUFs are discussed in details. The figures of merit and the typical applications for these PUF are illustrated.

Chapter 3 presents a novel cluster-based distributed active current sensing circuit for hardware Trojan detection. This chapter firstly illustrates a transient active current phenomenon that lead to the design of a current sensing circuit to facilitate the Trojan detection at-speed. The design of the basic components, namely the current mirror, the current comparator and the AC scan registers, of the HT sensor are explained. Experiments are conducted by inserting the difficult-to-detect hardware Trojans into ISCAS'85 benchmark circuits to demonstrate its feasibility and high HT detection rate. The corner simulations and Monte Carlo simulations are also performed to show its tolerance against process variations. The security of the sensor itself and the implementation overhead are discussed at the end of this chapter.

In Chapter 4, a low-power hybrid RO PUF with improved thermal stability and small footprint is presented. The chapter begins with a discussion of the temperature-induced response stability problem of RO PUF. The temperature characteristics of three different types of RO: the regular inverter RO, the current starved inverter RO and the hybrid inverter RO are analysed both in theory and by simulation. Next, the architecture of the proposed PUF and its operation, as well as the timing diagram are detailed. The figures of merit, which are uniqueness, reliability, unpredictability, power and area of the PUF are accessed through the measurement of five prototype chips fabricated in 65 nm CMOS technology. In addition, the resilience against machine learning attack due to its augmented feature of reconfigurable challenges is explained. An electro-magnetic (EM) radiation measurement is performed to prove that its low-power dissipation and interleaving structure increase the resiliency to the EM-based side-channel attacks. Finally, its security performances and VLSI implementation efficiency are also compared with other silicon-based PUFs.

Chapter 5 highlights the threats associated with the use of CMOS image sensors in security surveillance and biometric authentications, and shows that these threats can be eliminated by embedding the dedicated security functions into the image sensors. A new image sensor based PUF is then proposed to provide a secure and low-cost solution for the sensor-level device identification and authentication, as well as secure key generation. This intrinsic PUF is extracted from the fixed pattern noise (FPN) of the most popular CMOS image sensors (e.g. 3T-APS sensor and 4T-APS sensor). After introducing the root source of the FPN in a CMOS image sensor, the differential readout method is then proposed to remove the common mode noise due to the global power supply and temperature variations. The circuit for the challenge-response pair generator and its algorithm are explained. The proposed PUF is validated on a pre-fabricated 3T-APS image sensor using 180nm CMOS process. Its figures of merit as a PUF are evaluated with the measurement results of five sensors and its randomness is tested by the NIST suite. At the end of this chapter, emerging applications against smartphone counterfeiting and virtual camera attacks are suggested and discussed.

Finally, Chapter 6 concludes the thesis by summarizing the results achieved in the research. Promising applications for the proposed hardware security primitives are discussed. Some ideas that are worthy of further investigation are also presented.

Chapter 2

Background

In this chapter, some background and challenges pertaining to the research in hardware Trojans (HTs) and physically unclonable functions (PUF) are introduced.

2.1 Hardware Trojan

With the globalization of the semiconductor industry, the risk of inserting malicious logics by the adversaries into the original design is on the rise [3]. The malicious logics inserted into the integrated circuits and systems have been broadly referred to as hardware Trojan. They can do harm to the whole electrical system in various aspects:

- The modifications may be designed to leak the confidential information to the adversaries for illegal usage.
- The modifications may be designed to cause a system to fail or exhaust resources such as the computation capability, power consumption or bandwidth at a critical time while operating in the normal conditions.
- The modification may be designed to inject stuck-at, bridging or other faults that can reduce the reliability of the system.

There are many different implementations of hardware Trojans. However, they typically consist of two major components [3]:

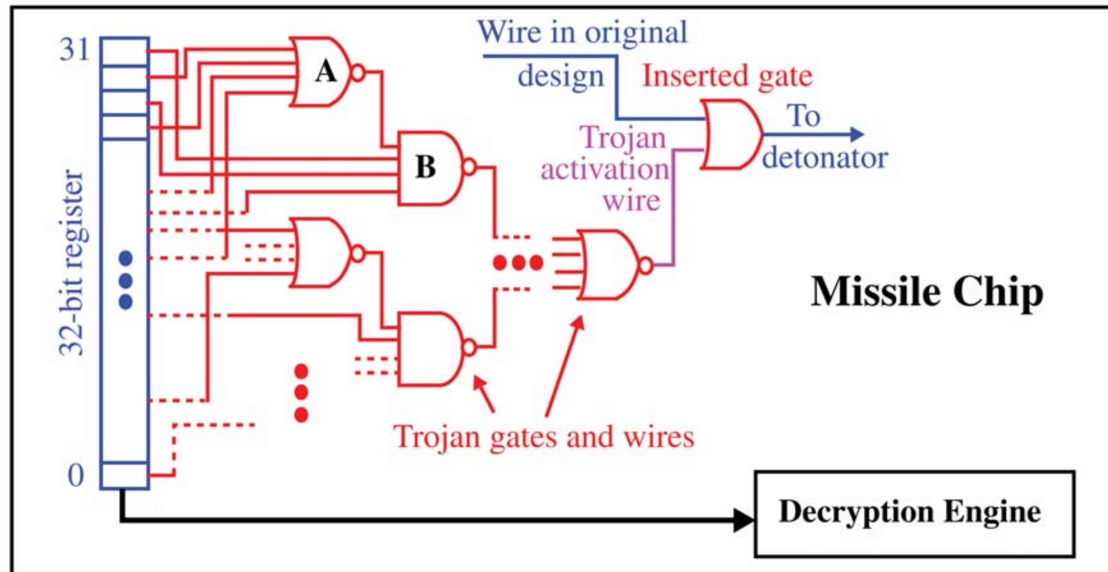

Figure 2.1: *An example of hardware Trojan [2].*

- Triggering mechanism: The trigger waits for a special event or unusual condition to activate special functions. The special events can be rare external input patterns or internal logic states. Before the Trojan is triggered, the Trojan-infected IC behaves normally as intended (excluding the trigger's activity).

- Payload: After the Trojan is triggered, the payload is responsible for the malicious tasks of the Trojan. It is the action that a Trojan executes that unleashes the threat it has been carrying in its load.

Fig. 2.1 illustrates an example of the hardware Trojan which is embedded into the missile control system [2]. In this example, it is assumed that the missile control chip receives encrypted commands from an RF channel and stores the value in the 32-bit register for subsequent decryption. The adversary may transmit "code" that causes activation such that the missile detonates before reaching its target. The "code" in this example is the triggering mechanism, while the activation that detonates the missile is the payload. Many other payload implementations are possible, e.g., pass-gate version, which is better than others in terms of minimizing the anomalies of the power supply.

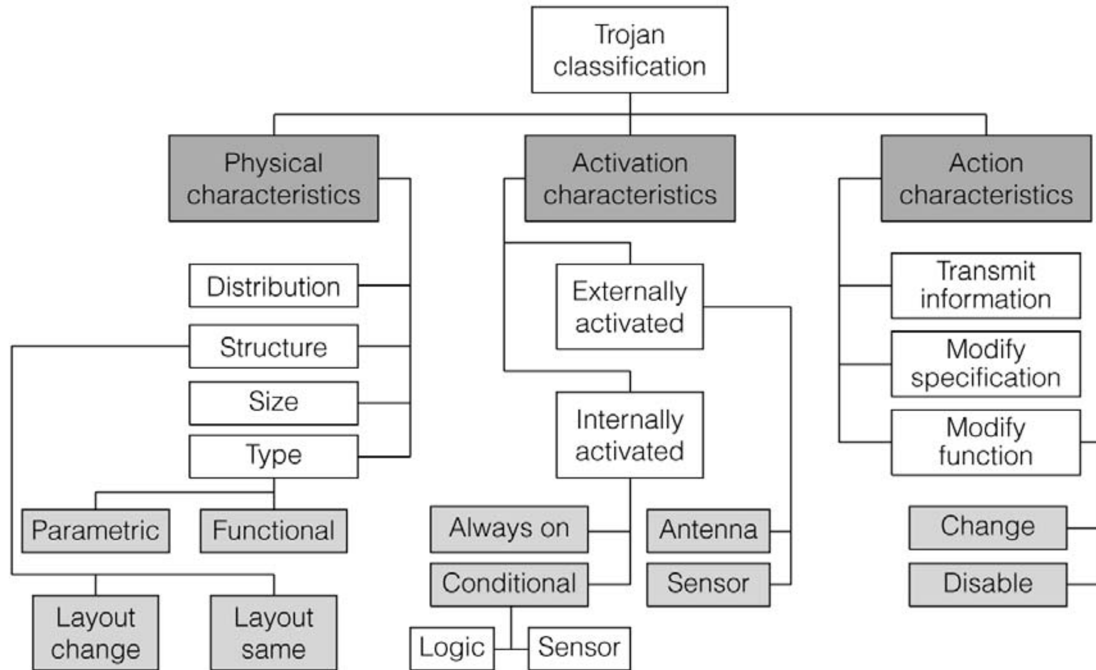

Figure 2.2: *Detailed taxonomy showing physical, activation, and action characteristics of different types of hardware Trojan [3].*

2.1.1 Hardware Trojan Taxonomy

It is important to systematically classify the hardware Trojans, because: 1) It facilitates the development of the Trojan mitigation, detection and protection techniques for each category of the hardware Trojans. 2) The Trojan benchmarks can be produced for Trojans belonging to different classes. They can provide metrics to evaluate the effectiveness of different methods in Trojan detection. There are many types of taxonomy that can be found in the literature. One comprehensive example of the taxonomy is shown in Fig. 2.2 [3]. It helps the researchers examine their methods against different Trojans. Although the Trojans are different in the structure, function and placement, Fig. 2.2 divides the Trojans into three categories based on their physical, activation, and action characteristics.

- The category of *physical characteristics* identifies the types of Trojan with different physical manifestations. The *distribution* category describes the location for the Trojan to be inserted. The location can be a single component or spread across the whole chip. Specifically, Trojans can be distributed

in the processor, I/O ports, power grid, clock tree or memory block. The category *structure* describes the physical layout that may be changed to be able to embed the Trojan. For example, the routing and placement of cells can be altered to provide enough area for the Trojan. The category *size* accounts for the number of cells for a design that has been added or deleted. In the *type* category, the *functional* type refers to Trojans that are physically realized through the addition or removal of original functionality, while *parametric* refers to Trojans that are implanted through modifications of physical characteristics, such as path delay, power, bandwidth, etc.

- The Trojans can be categorized by their *activation mechanism*, either *external* or *internal*. The *external* triggering mechanism requires the external signals to activate the malicious logics in the Trojan module. It can be an antenna or other sensory circuits that interact with the target IC. The *internal* trigger needs a special event that occurs inside the device. It can be designed to be always on or remain dormant until a specific condition is met. The condition can be electromagnetic interference, humidity, altitude, atmospheric pressure, etc. Typically, a counter in the design can trigger a Trojan at a pre-determined value. This is more commonly known as a time-bomb.
- The Trojans can also be characterized by their undesirable *action effects*. The severity of their impacts on the infected system can range from subtle disturbances to catastrophic system failures. It can *transmit the sensitive data* to the attacker for the illegal purpose. For instance, the Trojan may leak the encryption key through the RS-232 port. Besides, the *modify-specification* class describes Trojans that change IC's parametric, such as path delay or power consumption by modifying the wire and transistor geometries. Finally, Trojan can *modify the functionality* of the original design and cause subtle errors that may be difficult to be detected.

Specially, more sophisticated Trojans can be the hybrids of these three. This taxonomy shows the essential characteristics of Trojans and is helpful for defining and evaluating the capabilities of various HT detection strategies.

2.1.2 Hardware Trojan Detection Methods

As the Trojans can be serious threats to all systems and sectors that are dependent on electronic devices, prevention and detection of hardware Trojans have drawn a significant interest not only in academia, but also in governmental agencies and industry. Many HT detection techniques have been reported [4, 6, 17, 19–33] in recent years. These different techniques are explained and compared with respect to their capabilities and limitations in this section.

2.1.2.1 Physical Inspection

Physical inspection is a destructive method to reveal the feature and layout of the circuitry. The engineer repeatedly scans the surface of the chip while grinding each layer using scanning electron microscope (SEM) or scanning optical microscope (SOM). Then, the layout image is reconstructed and analyzed to identify transistors or gates and routing wires. A bottom-up reverse-engineering approach is utilized. These techniques may be the most effective way to check the integrity and genuineness of an individual IC, while its complexity, time-consuming, high costs and destructive nature limit its scope. In fact, this destructive HT detection method is often used to find out the "golden chip" [3] or the Trojan-free reference. It may not need too many attempts to find the Trojan-free sample as Trojan-free chips are usually the large majority. Moreover, as every unsuccessful reverse-engineering attempt to obtain a golden chip means the discovery of a subverted or dubious chip, the effort is not completely fruitless. Therefore, it is suitable for the physical inspection technique to test a small sample of fabricated chips so that key parametric measurements from a set of golden chips can be pre-acquired and used for process calibration and comparison of side-channel parameters with the rest of the ICs.

2.1.2.2 Functional Test

This detection method stimulates the input ports of a chip and monitors the outputs to detect manufacturing faults. If the logic values of the outputs do not match

the genuine pattern, then a defect or a Trojan could be found. Unfortunately, the functional test cannot be used to reliably detect the Trojans, because Trojans are often triggered under a rare condition. Besides, it is possible for the triggered Trojan to have no impact on the functional outputs, such as the Trojan that leaks the sensitive information through the current signatures. Furthermore, it is extremely challenging and time consuming to exhaustively generate test vectors for triggering a Trojan and observing its output effects. This is especially true for the sequential Trojans or so-called "time-bombs", which are triggered only on the occurrence of a sequence of rare events.

2.1.2.3 Built-In-Self-Test

Built-in-self-test (BIST) is the test that additional functionality is embedded in the design to assist the verification of the original functionality. BIST can be implemented with additional circuitry module to monitor signals, input stimulus, and/or assist in detection of defects. These methods are mainly targeted to detect the manufacturing failures, but could possibly be used to detect the unintended (malicious) alternations on the chip. The same problem of the functionality exists in the BIST: the intelligent attackers can embed the Trojan without affecting the original functionality to evade the BIST. Additionally, BIST functionality can perform at-speed (high- speed) verification beyond the capability of normal design for testability scan chains or other low-speed designs with embedded test functions. Most modern chips will fuse or disable (through hardware configuration) the ability for chip to perform BIST outside of a manufacturing or testing environment, because BIST facilities themselves could be used in a subversive attack on the chip.

2.1.2.4 Side-channel Signal Analysis

Even though it is impossible to model all possible Trojan placements, structures, functions, sizes, etc., and the Trojan may not affect the circuit's functionality, their presence can still alter the IC's speed, power consumption characteristics or reliability. This makes it possible to diagnose a chip for potential Trojan infection

by side-channel analysis albeit many challenges [4, 6, 17, 20–24, 26, 28–32]. Side-channels are signals of an IC in operation that can be probed externally to detect any anomalies in the internal behavior of a circuit. One important advantage of side-channel analysis over the other HT detection methods is the Trojans can be detected without being fully triggered [19]. Hence, test pattern generation for side-channel analysis is expected to be less challenging. Examples of popular side-channel analysis methods include time-based analysis [4, 20–23] and power-based analysis [6, 17, 24, 26, 28, 29].

2.1.2.4.1 Time-based Side-channel Analysis Time-based side-channel analysis can succeed in hardware Trojan detection if the additional delay due to the Trojan is distinguishable from the delay difference caused by process variations. One such method [4] adds a "shadow register" to latch the data of the destination register of a path. The shadow register clock has the same frequency as the main clock, but with adjustable phase shift to measure the path delay. This method uses a sweeping-clock-delay measurement technology to measure selected register-to-register path delays. The basic architecture of the time-based side-channel analysis using the shadow register is shown in Fig. 2.3. The source register and the destination register are triggered by the main system clock (Clk 1). Clk 1 can run at the normal working frequency. The shadow register latches the same input of the destination register by the shadow clock (Clk 2) which runs at the same speed as Clk 1 with a controllable phase shift. The results latched in the destination register and the shadow register are compared by the following comparator. The unequal result indicates that the path has a high probability of hardware Trojan existence. The "shadow register" technology employs an on-chip temperature sensor to reduce the effect of the temperature variation that could greatly affect the path delay. This sensor consists of an inverter ring oscillator whose output frequency is temperature dependent and a counter to measure the frequency. S-ince the oscillator is located within the main circuitry, the effective temperature of the chip can be obtained from its frequency response. The equivalent path delay signature can then be calculated from the temperature-delay relationship of the

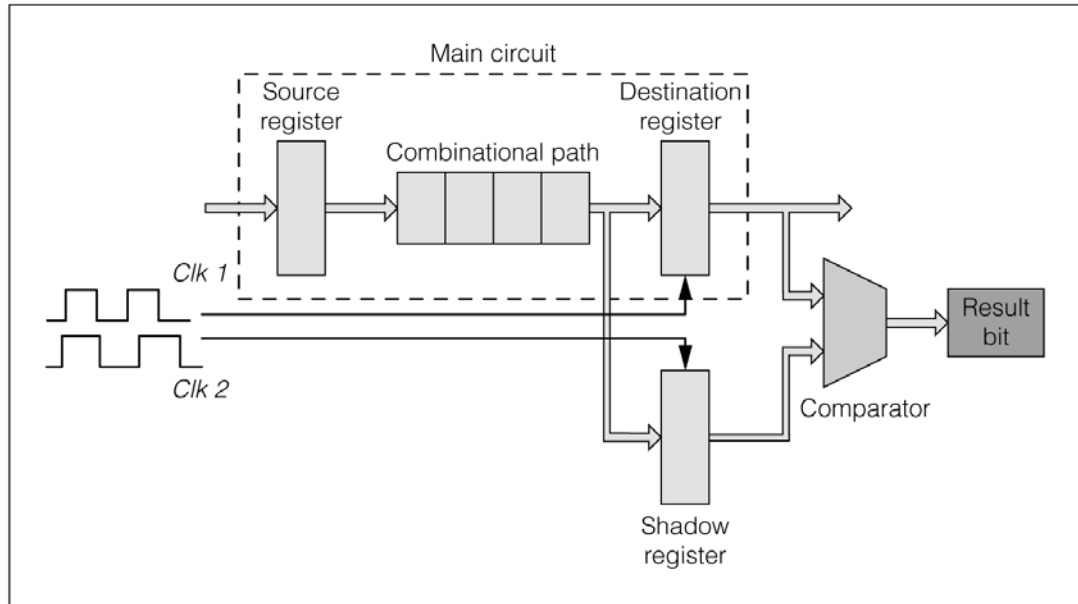

Figure 2.3: *Path delay measurement architecture using a shadow register [4].*

path based on the sensed operating temperature [4].

The main problems of the "shadow register" analysis are: it suffers from a high area overhead due to the extra register and comparator required for every path to be monitored, which is not practical for modern VLSI design. The dedicated "shadow clock" also complicates the clock distribution networks and clock skews may become a critical timing problem. Furthermore, Trojans inserted in the internal nodes for the design without primary inputs or outputs cannot be detected by this approach.

2.1.2.4.2 Power-based Side-channel Analysis Power-based side-channel analysis provides the visibility of the chip's internal switching activities. In [5], random input patterns are applied to obtain a power signature for comparison with that of the Trojan-free chip. Fig. 2.4 shows an example of the power-based side-channel analysis. This method assumes is the existence of a "golden chip/die" which can be trusted as the reference. This reference can be found by physical inspection (reverse-engineering). However, the cost of the reverse-engineering is very expensive. It is impractical to use the reverse-engineering to detect the Tro-

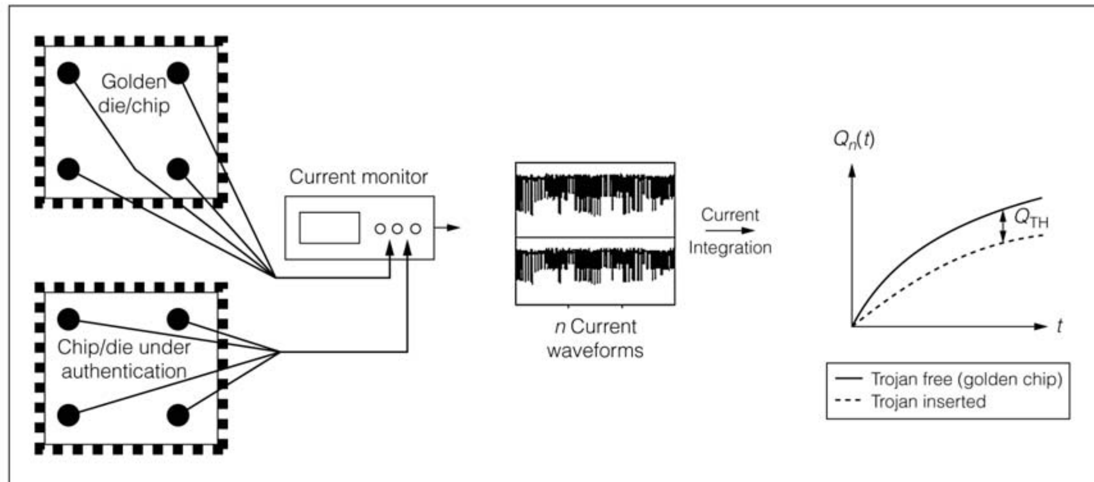

Figure 2.4: *Power-based side-channel analysis [5].*

jans in all the dies. After the same random patterns are applied for the reference and the IC under authentication (IUA), the power consumption of the circuits is measured by integrating the transient current. In Fig. 2.4, the integrated power consumption for the Trojan-free circuit is the bold line, while the dash line is for the IUA. The measured power consumption data for the IUA may consist of several parts: power consumption of the circuit after applying the inputs as those applied to all Trojan-free ICs; measurement noise, which can be removed by multi-measurements; process variations, which are random and cannot be removed; and Trojan contributions to the measured power consumption. If the IUA's power consumption signature exhibits a difference that considerably exceeds the one introduced by the process variations, it is highly probable to be Trojan-infected.

The major problem of this method is its sensitivity to random noise induced by the process and temperature variations. If the Trojan is comparable in size with the circuit, its impact on the circuit-transient current will be significant and could be measured easily. Otherwise, if the Trojan has a small size, its power consumption will be masked by the process and temperature variations. In addition, it has a stringent requirement on the test pattern: the random patterns have to (partially) trigger the Trojans multiple times in order to consume enough power to distinguish the Trojan activity from the process variations.

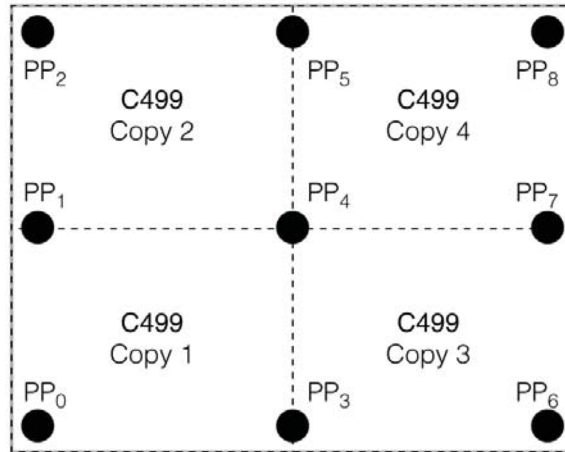

Figure 2.5: *Example of regional power-based side-channel analysis [6].*

Advanced power-based analysis method has been proposed to reduce the effect of process variations [6]. It partitions the entire chip into several regions to magnify the Trojan-to-circuit activity. A region is a portion of the whole layout that receives the major power from the surrounding power ports. Fig. 2.5 shows an example of region-based power analysis. In this example, the original design employs nine power ports. The transient current integration methodology to detect the Trojan is performed through each power port individually. Trojan detection capability can be enhanced through the local power measurements. However, its drawback is that each region has to have its own power ports for the power signature analysis. The area overhead makes it improper for large circuit partitioning. In addition, the regional analysis alone is not enough to tackle the adverse effects of process variations on detection resolution. Thus, calibration technology is necessary [24]. The calibration is performed on each power port and for each chip separately. It measures the power response of an impulse. The response of each power port X is normalized by the sum of the currents drawn from power ports in the same row as X. The calibration matrix comprises the normalized values of power ports. After each test pattern is applied, the response is calibrated using the calibration matrix.

2.1.2.4.3 Gate Level Characterization (GLC) GLC [34] approach provides another solution to cope with the increasing impact of process variations. It constructs linear extrapolation between the gate-level properties and non-destructively measured side-channel signals (e.g., timing, static power, etc.) to formulate a system of linear equations. The process variation is considered as a scaling factor for each nominal gate value in the linear equation system. The nominal gate value is obtained from the simulation model. The scaling factors for each gate in the equation array are the variables to be solved. Linear programming and singular-value decomposition are employed to solve the linear equation array. The existence of HT will cause the anomalies of the gate scaling factors in the solution. This HT detection method is promising as it does not rely on any physical golden sample. However, it does not perform well for larger chips with more gates, higher accumulated measurement noise, and more sophisticated process variation models [35].

2.1.3 Summary

In this section, characteristics of hardware Trojans have been analyzed. The taxonomy of hardware Trojans is introduced, which classifies Trojans based on their physical characteristics, activation mechanism and attack effects. An overview of existing Trojan detection techniques for the post-silicon trust validation is presented. The major challenges with respect to each Trojan detection method are explained. Among the modern hardware Trojan detection methods, the side-channel signal analysis methods are most popular due to its un-destructive nature and the advantage of requiring the test patterns to only partially trigger the Trojans. It is also noted that any existing Trojan detection technique might not be able to provide a full coverage of Trojan detectability. A possible way is to combine various Trojan detection approaches with complementary capabilities. In fact, the proposed Trojan detection technique presented in the following Chapter 3 is a combination of the power and timing based side-channel analysis. Furthermore, it is also possible to monitor the IC's behavior during operation to improve the level

of assurance [31]. For example, a Trojan that leaks information from a crypto-chip might consume large spikes in power during a relatively idle period. Hence, a run-time framework of monitoring the power can be used to detect such kind of Trojan.

2.2 Physically Unclonable Function

In response to the counterfeiting and tampering attacks discussed in Chapter 1, PUF has been proven to be a promising aid to the countermeasures against many of these attacks. It is essentially an extension of biometrics towards physical objects. The idea to use the intrinsic random physical features to identify objects can be dated back to the nineteenth century [36]. The formalization of this idea on silicon devices began only in the twenty-first century, known as physical one way function [37], physical random function [38] and now as physical unclonable function [39]. PUF extracts the unique signatures from the unpredictable and uncontrollable process variations during IC manufacturing. Unlike the way to store the sensitive data in a specific memory, PUF keeps the confidential information within its structure. Any invasive or semi-invasive attacks will inevitably destroy the chip's physical structure. Therefore, the sensitive information that the attacker obtained is invalid without the interrogation with its physical device. This section reviews the literatures on the types, quality assessment and typical applications of PUFs.

2.2.1 Types of Silicon PUF

Over the last couple of years, many new types of PUFs have been successfully proposed for the security applications due to the promising properties of physical unclonability, tamper evidence and small hardware overhead. This review focuses on the most popular silicon based PUFs, as they are easy to be integrated with the standard CMOS process. Generally, there are two primary applications of PUFs: authentication and secure key generation. Based on the two applications, the PUFs are broadly categorized as "strong PUFs" and "weak PUFs". Strong

PUFs can be targeted for authentication, while weak PUFs are more suitable for the key generation.

Before the discussion of the categories and operations of the PUFs, the terminologies for PUF are introduced. The inputs and outputs of PUF circuits are typically referred to as the challenges and responses, respectively. An applied challenge and its measured response are named as a challenge-response pair (CRP). In this dissertation, all the PUF response bits are referred to as the PUF signature. In fact, the fundamental difference between the weak and strong PUFs lies in the relationship between their challenges and responses [40].

2.2.1.1 Strong PUF

Strong PUFs are disordered physical systems with a complex challenge-response behavior characterized by a large challenge-response space. It is impossible to physically clone a strong PUF whose CRPs behave exactly the same as the original one. Besides, it is impossible to measure or determine all the CRPs for a strong PUF within a limited time. Typical examples for the strong PUFs are: the arbiter PUF [7] and the ring oscillator (RO) PUF [12].

2.2.1.1.1 Arbiter PUF In the arbiter PUF, a race condition is established in a symmetric circuit. Fig. 2.6 shows the implementation of the basic arbiter PUF. It consists of a sequence of switches, each controlled by one bit of the challenge. A rising edge is split into the two multiplexors at the very beginning of the input. The different input challenges select different paths. Although the two selected paths are laid out in an identical fashion, the manufacturing variations in the gate delay of each stage will result in one edge arriving at the latch faster than the other. The two inputs of the latch acting as the arbiter are the upper and lower paths. Therefore, the response is determined by the challenge bits.

It is noted that the metastability of the arbiter makes the PUF highly sensitive to the environmental noises. In addition, the digital delay in the basic arbiter PUF is additive. In other words, the delay of each chain of switch blocks is the sum of the delay of the separate delay stages. This makes the arbiter PUF vulnerable

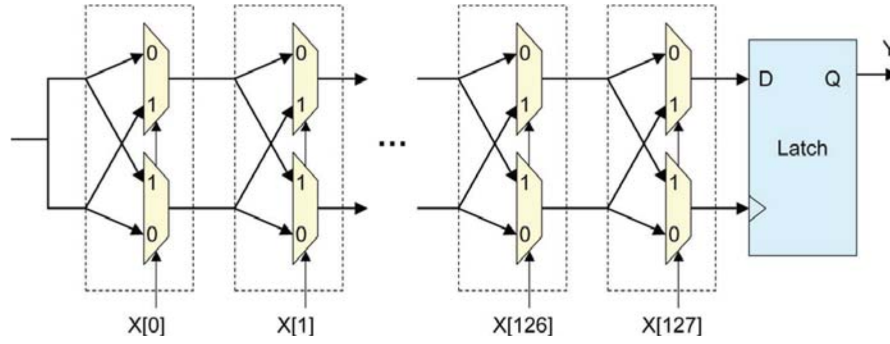

Figure 2.6: *The schematic of arbiter PUF [7].*

to the model-building attacks. With a number of observed CRPs, one can build a mathematical model that predicts the response to a future challenge with a high accuracy [41]. There are a few of modified architectures proposed to focus on defeating model-building, by introducing nonlinearity in the delays and by restricting the I/Os to the PUF [41].

2.2.1.1.2 Ring Oscillator PUF (RO-PUF) The classic RO PUF architecture [12] is made of 2 N-to-1 multiplexors, 2 counters, 1 comparator and N identical ROs, as shown in Fig. 2.7. Each RO contains an odd number of inverters in a feedback loop. Due to the inter- and intra-chip process variations and environmental variability, the delay of the inverter chain in each RO differs, which results in a deviation of oscillation frequencies between any two ROs. A $2log_2N$-bit challenge is fed to the data select lines of the two multiplexors to select a pair of ROs. The output frequencies of the selected ROs are then used to clock two identical counters. The counter outputs are connected to a comparator. The comparator output, which is the response bit of the PUF, is either 0 or 1 depending on which oscillator has reached the same pre-loaded count value earlier. Therefore, the greater the difference between the oscillation frequencies of any RO pair, the more reliable is the output response bit of the PUF.

RO PUFs are more robust to layout differences among ROs, e.g., routing of the output to the counters. Moreover, the difference in RO output frequencies can be amplified by allowing them to oscillate for a longer time. However, its relatively

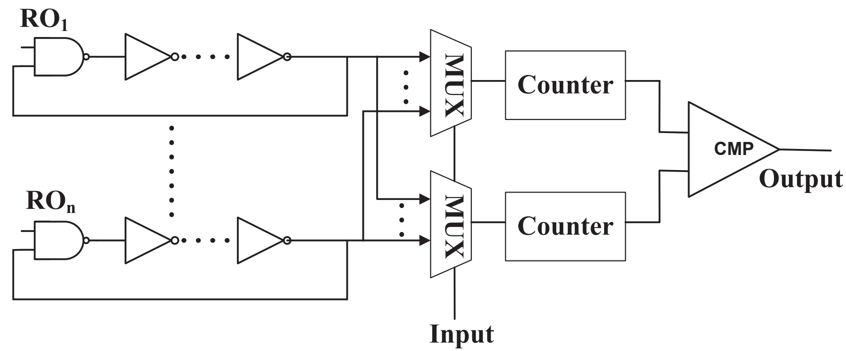

Figure 2.7: *Classic ring oscillator PUF architecture.*

high cost in hardware area and power consumption limits its applications in the mobile devices and lightweight applications, e.g., RFID.

2.2.1.2 Weak PUF

In contrast to the strong PUFs, the weak PUFs may have very few CRPs. Weak PUFs can essentially be regarded as a special form of memory, but they are more resilient to the invasive attacks than the non-volatile memory like EEPROM. The most typical weak PUFs are the memory-based PUFs: SRAM PUF [8], latch PUF [9] and butterfly PUF [42].

2.2.1.2.1 SRAM PUF SRAM is a popular weak PUF structure that exploits the positive feedback loop in a SRAM cell [8]. The SRAM cell structure is shown in Fig. 2.8. It has two stable states: either '1' or '0'. The positive feedback in the cell forces it into one of these two states. Once it enters either state, it prevents the cell from transiting out of this state accidentally.

Structurally, the two cross-coupled inverters are symmetrical in Fig. 2.8. It should be in the meta-stable state during the power-up phase. However, in the real implementation, the devices in the cross-coupled inverters are mismatched due to the manufacturing process variations. One feedback loop is slightly stronger than the other. The mismatches will be amplified by the positive feedback of the cross-coupled inverters and will eventually generate either a logic '1' or a logic '0'. Assuming random device variations, each SRAM cell will also generate either logic

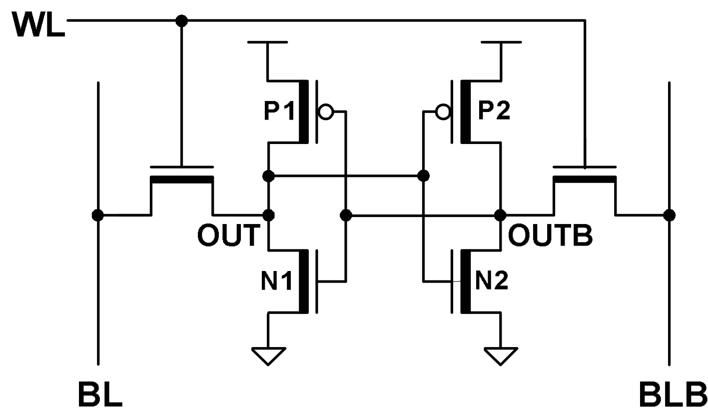

Figure 2.8: *The basic structure of the SRAM cell [8].*

'1' or logic '0' randomly with an equal probability of 50%. This makes the binary output string read out from an SRAM array unique, random and non-traceable.

However, random noises, e.g., thermal noise and shot noise, can also trigger the positive feedback loop when it is in the meta-stable state, which makes the responses of an SRAM PUF unstable. It is noted that the final state depends on the difference between two feedback loops. The measurement is taken differentially so that the effects of common mode noise such as die temperature, power supply fluctuations, and common mode process variations will be reduced.

2.2.1.2.2 Latch PUF Not all the ICs have an SRAM array and it is not easy to directly reset the SRAM after powering up for some designs. Therefore, the application of the SRAM PUFs is restricted. Latch PUF [9] was proposed to overcome the limitation of SRAM PUF. The logical structure of a latch PUF cell is shown in Fig. 2.9. The latch PUF is also a weak PUF. Instead of cross-coupling two inverters in an SRAM cell, two NOR gates are cross-coupled. Similar to the SRAM PUF, by asserting a reset signal, this latch becomes unstable and then converges to a stable state again depending on the internal mismatch between the electronic components.

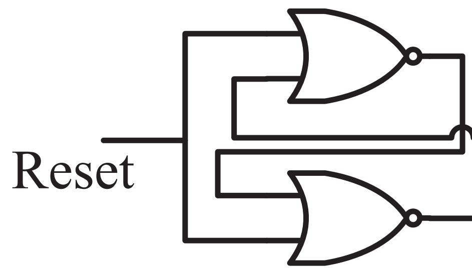

Figure 2.9: *The logical structure of the latch PUF cell [9].*

2.2.2 PUF Applications in Hardware Security

Silicon PUFs are generally designed for two applications in hardware security: device authentication and identification, and key generation for encryption units.

2.2.2.1 Authentication and Identification

PUF can be used to authenticate individual ICs without using expensive cryptographic modules. This type of authentication is very useful for resource constrained RFIDs where cryptographic operations are too costly in terms of silicon area and power consumption.

The authentication with PUF employs a challenge-response protocol. After manufacturing a device, the user of the PUF needs to record the challenge-response pairs (CRPs) of its PUF in an enrollment phase. These CRPs are stored in a secure database. When the identification or the authentication is queried, the challenges chosen from the enrollment phase are applied to the same PUF. Since each PUF provides a unique response and the response can only be measured if one has the physical device, the authentication is considered successful when the response matches (or close enough to) the previously recorded one. To avoid replay (eavesdropping) attacks, the used challenges should not be applied again. Hence, it is extremely useful to have a (strong) PUF that can support a large number of CRPs. This authentication and identification procedure can also be used by IC vendors to prevent counterfeiting attacks [43].

2.2.2.2 Key Generation

The security of a cryptographic system relies not on the secrecy of its algorithm but the secrecy of its encryption and decryption keys. Traditionally, the keys are stored in non-volatile memory of a device which are susceptible to invasive attacks [12]. However, if a PUF's response to a unique challenge (or some derivative of its response) is used as an encryption key, then the key is physically embedded in the device structure rather than stored in memory. Any invasive or semi-invasive attack will inevitably destroy the physical structure. Therefore, the original data will no longer be the same after the attacks. It is also noted that the response of a given PUF cannot be used directly as a key in cryptographic algorithms, because its responses are likely to be different in each evaluation even for the same challenge, and the raw response may not be truly random. These limitations can be overcome by incorporating additional post-processing modules, such as the error correction coder (ECC) or the fuzzy extractor. There are two steps in the error correction process: initialization and re-generation. In the initialization step, an error syndrome is computed when the challenge is applied. This syndrome is used later during re-generation to correct any bit errors that might have occurred in the PUF response. The corrected PUF response is then taken through a hash function to generate the random secret key.

The attractive security applications for PUFs have also drawn the attention in industry by Verayo [44] and Intrinsic ID [45]. Verayo provides the PUF product as an IP to be licensed for RFID, ASIC and FPGA applications. Intrinsic ID offers secure key storage solutions to protect semiconductor products from cloning and reverse-engineering.

2.2.3 PUF Qualities and Metrics

There are three most important properties to evaluate the quality of a PUF [12] design, which are uniqueness, reliability and unpredictability. They are briefly explained as follows.

2.2.3.1 Uniqueness

Uniqueness measures how different are the CRPs produced by one PUF from the others. Uniqueness can be estimated by the average inter-die Hamming Distance (HD) of the responses produced by different PUFs. Let R_u and R_v be the n-bit responses of two different chips, u and v, to the same input challenge C. The uniqueness U for m chips is expressed as [46]:

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \times 100\% \tag{2.1}$$

To maximally discriminating the different CRPs generated by a PUF, its uniqueness should ideally be 50%. In order to make the PUF designs close to the ideal value, the post-processing is needed for the response bitstream.

2.2.3.2 Reliability

The reliability measures how reproducible or stable are the CRPs of a PUF under varying operating conditions. The dynamic operating conditions can be arisen from the variations in temperature, supply voltage and ambient noise. The reliability of a PUF can be measured by its bit error rate (BER), which can be characterized by comparing the responses taken at different time with a reference response to the same challenge. Let R_i be an n-bit response to an input challenge C produced by the PUF of a chip i under a nominal operating condition. The same set of challenges are then applied k times to the same PUF under varying environmental conditions to obtain the responses $R_{i,j}$ for $j = 1, 2, \cdots, k$. The reliability S for chip i can be computed by [46]:

$$S = 1 - BER = 1 - \frac{1}{k} \sum_{j=1}^{k} \frac{HD(R_i, R_{i,j})}{n} \times 100\% \tag{2.2}$$

An ideal PUF should have 100% reliability, which means that its CRPs can be infinitely regenerated without any errors. The reliability is possible to be improved by the ECC [47]

2.2.3.3 Unpredictability

Since PUFs can be used to store secrets and cryptographic keys, PUF responses should be unpredictable/random with a number of known CRPs in order to ensure that the confidential data remains safe. Several measures of unpredictability have been utilized in the literature. As high prediction accuracies greater than 90% can be achieved through machining learning attacks on linear PUFs such as Arbiter PUFs, one ad-hoc measure of unpredictability is by determining how well machine learning attacks can be used to model PUF CRPs [48]. More widely used formal metric of unpredictability such as the entropy [12] measures the randomness in the signatures. The entropy of a discrete random variable X with probabilities $Pr[X = x] = p_x$ is defined as [12]:

$$H(X) = -\sum_{x \in X} p_x \log p_x \tag{2.3}$$

2.2.4 Summary

PUF is a function that uses physical structure of the device to produce a response to a challenge, which is easy to evaluate but hard to tamper with, physically prone or mathematically model. In this section, typical silicon PUFs and their figures of merit have been introduced. The categories of the PUFs determined by the typical applications are discussed: Strong PUFs can be used for authentication, while weak PUFs can be employed for secret key generation. The PUF as a secure primitive is attractive because of its low cost and high resiliency.

Chapter 3

A Cluster-Based Distributed Active Current Sensing Circuit for Hardware Trojan Detection

3.1 Introduction

In the diverse global economy, outsourcing of production tasks is a common way to lower a product's cost. However, the risk for the chips to be subverted with hardware Trojans has increased dramatically due to this geographical dispersion of chip design flow. Hardware Trojans may cause unwanted effects that are detrimental to the electronic systems that host the subverted chips. Many Trojan detection techniques have been reported [4, 6, 17, 19–33] not only in academia, but also in governmental agencies and industry, which have been discussed in 2.1.2. Among these methods, side-channel analysis is advantageous because the Trojans can be detected without being fully triggered [19]. However, each side channel analysis has its own limitations. For example, the attacker may design a Trojan that can be inserted in a manner that results in no difference in external delay measurements to evade the delay-based side-channel analysis [30]. Fig. 3.1(a) illustrates such an example. Since the Trojan logics are embedded along the path in parallel, it is unlikely that the delay-based side-channel analysis will pick up any anomaly in timing path from the primary input PI_1 or PI_2 to the primary output PO.

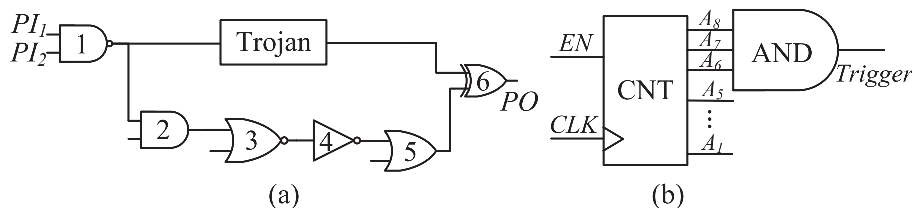

Figure 3.1: *Example of a HT (a) with no delay impact, (b) with no switching power impact.*

Meanwhile, for the power based side-channel analysis, it is also possible to embed a Trojan that is activated only on a very rare condition [30], which results in no observable difference in the power signatures. The example in Fig. 3.1(b) shows an AND gate whose inputs are fed from the most significant bits of a counter. The Trojan can be triggered only after the counter has run for a much longer time than any standard test time. In [31], a power-gated Trojan has been demonstrated to be able to bypass the power-based side-channel signal analysis. However, to realize the triggering mechanism, the inputs of the Trojan are connected to some existing logic nodes of the original design. The Trojan gate connections that increase the capacitive load on those nodes [32], together with the multiplexer inserted into an existing timing path to control the Trojan activation, increase the path delay even if the Trojan remains dormant. Therefore, it is possible to detect such Trojan by the delay-based side-channel analysis instead of power-based side-channel analysis.

This chapter presents an active current sensing circuit to extract a signature that encapsulates both the timing and amplitude of switching activity from the transient power supply current (I_{DDT}) to provide a reliable HT detection solution. The proposed sensor utilizes the industrial power gating scheme, which is one of the most effective techniques in low power circuit design [49–52]. It employs sleep transistors to disconnect logic clusters from the power supply or ground to reduce the power consumption. The dynamic IR-drop across the sleep transistors in the active mode of operation can be sensed to detect path delay elongation by Trojan through region-based excitation of a number of paths per endpoint, including unobservable internal paths, such as paths without primary inputs, primary outputs or scan latches. Based on the experimentation [53], Trojan infected circuit can

cause errant timing behaviors that are often shown up in logic as power supply droop, which can be picked up by monitoring the supply current. On the other hand, if the Trojan logics are inserted into a path in parallel (Fig. 3.1(a)), the timing signature alone will not be able to distinguish the difference of Trojan-free and Trojan-infected paths. But the abnormality of the I_{DDT} amplitude due to the Trojan will be detected by the sensor. The proposed design includes a simple tunable threshold current comparator that can be calibrated to maximally discriminate between transient current and background noise and a multiplexer-based scan register to enable its transition-delay to be detected at the scan output vectors by the AC scan test with a pulse width modulated clock. This on-chip Trojan detection solution enables a more efficient screening of a large number of dubious chips by eliminating the post-processing requirements from characterization-based methods [54].

The rest of the chapter is organized as follows. Section 3.2 presents an example to illustrate the viability of the principle of detection behind the proposed method. In Section 3.3, the design and operations of the proposed sensor for HT detection are elaborated. Simulation results are presented and discussed in Section 3.4. Finally, the summary is given in Section 3.5.

3.2 Motivating Example

I_{DDT} conveys the unitary profile of switching activity and timing information of the sensitized paths of a chip. Fig. 3.2 shows the I_{DDT}, input and output voltage waveforms when an arbitrarily selected data path of ISCAS'85 benchmark circuit C432 is activated. C432 is a 27-channel interrupt controller which has 36 inputs and 7 outputs. It contains 160 gates. The propagation delay for this data path is 1.836ns based on the 50%-to-50% full swing voltage delay definition. The commencement and termination of the active switching current is clearly discernible from the quiescent current. The duration 1.1836ns is the same as the propagation delay of the sensitized path. This timing signature of a subcircuit is found to be susceptible to subtle functional and topological modifications. Fig.

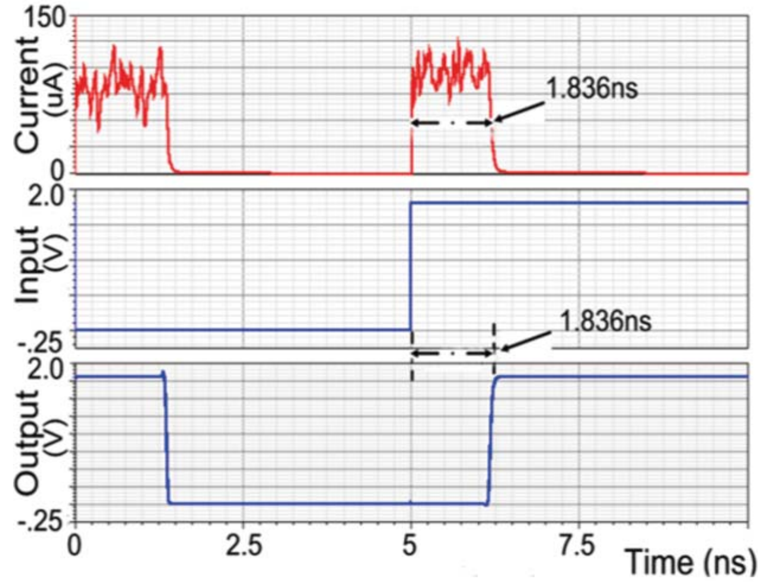

Figure 3.2: *I_{DDT}, input and output waveforms due to a sensitized path in C432.*

3.3 demonstrates the transient current differences between a Trojan-free path and a Trojan-infected path of C432. The Trojan inserted into this path consists of 7 logic gates, which contributes approximately 4% of additional logic to this original design. In Fig. 3.3(a), the Trojan inserted in series with the infected path induces current spikes that can evoke momentarily supply voltage droop and increase the path delay. Thus, the Trojan-infected path is distinguishable from the Trojan-free path with an elongated active current duration due to its extraneous switching. On the other hand, the Trojan inserted in parallel (Fig. 3.1(a)) does not show distinguishable timing difference from the original design. However, the peak current is larger as shown in Fig. 3.3(b). While the Trojan path is shorter than the original path, its presence increases the loading and hence switching activities when the original path is sensitized. As a result, the amplitude of the switching current increases, although the switching duration remains the same.

The above observation leads to the thought of the implantation of small current sensors into a circuit to aid a more accurate and faster post-silicon Trojan detection and diagnosis. Its justification is analogous to the deployment of on-chip thermal sensors to aid thermal management when chip reliability and catastrophic failure due to thermal runaway is of great concern. A current detector based on the coarse-

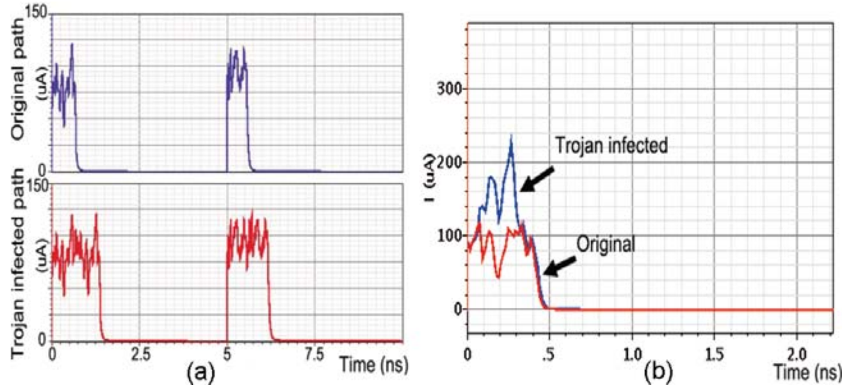

Figure 3.3: *Supply current waveforms for the sensitized path of Trojan-free and Trojan-infected circuits: (a) the Trojan is inserted in series, (b) the Trojan is inserted in parallel.*

grained power gating technology is proposed to be implanted into the circuit. During the design phase, the original circuit is divided into regions. A current sensing circuit to be described in the next section is embedded into each region to monitor the transient current from the power strap or trunk of the power grid as depicted in Fig. 3.4. In coarse-grained region segmentation, the logic circuits of the same functional module are placed close to each other in the same power cluster and a sleep transistor is used to cut off the power to each cluster. The devices are powered by the virtual power supply VV_{DD} in its local power mesh. During the Trojan detection phase, only one cluster is powered on at a time by turning off the other sleep transistors to amplify the Trojan-to-circuit effect and reduce the test power. Since no transition will occur in the power-down clusters, no effort is needed to develop specific test patterns to trigger only part of the circuit but a small design effort is needed to divide the circuit into power grids and split the scan chain. Many power gating architectures and algorithms [49–52] can be considered. The scan partitioning technique [50] with very low DFT overhead in terms of die-area, circuit performance and power is used for the proposed design. The switching time of the sleep transistors for all the clusters is controlled by a decoder. The characteristic signatures of the switching current envelope from each virtual power supply are extracted by its embedded detector and scanned out through the scan chain. By amortizing the circuit switching activities into clusters,

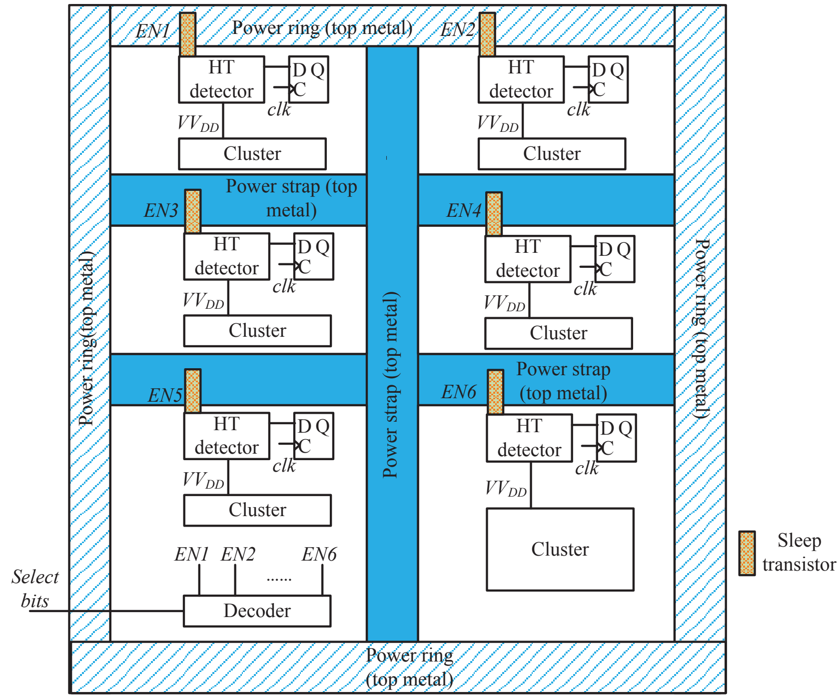

Figure 3.4: *Example of the deployment of the proposed HT detector with six virtual-power clusters.*

extraneous activities that transcend regular circuit activities and process variations are more likely to be detected by the cluster-based current sensors in those regions where the Trojan resided. In this sense, the number of regions provides a trade-off between the resolution of the detectable Trojan and the hardware overhead.

The flow of the Trojan detection is shown in Fig. 3.5. Random test patterns are applied through the functional-test scan chain to locally activate the paths in the target region while the remaining regions are kept inactive by turning off their sleep transistors. The signature extracted from the regional current detector is compared with that of the Trojan-free chip (golden sample) for the same test patterns. If the difference of any region exceeds a threshold determined by the process variations, it signifies a probable existence of a Trojan in that region. If none of the regions exhibits an above threshold difference, the chip is most probably Trojan free based on the detectable HT resolution. The Trojan-free signatures can be extracted from a golden sample before its genuineness is confirmed by reverse engineering [55]. It may not need many attempts since only one golden chip is needed. Also, every

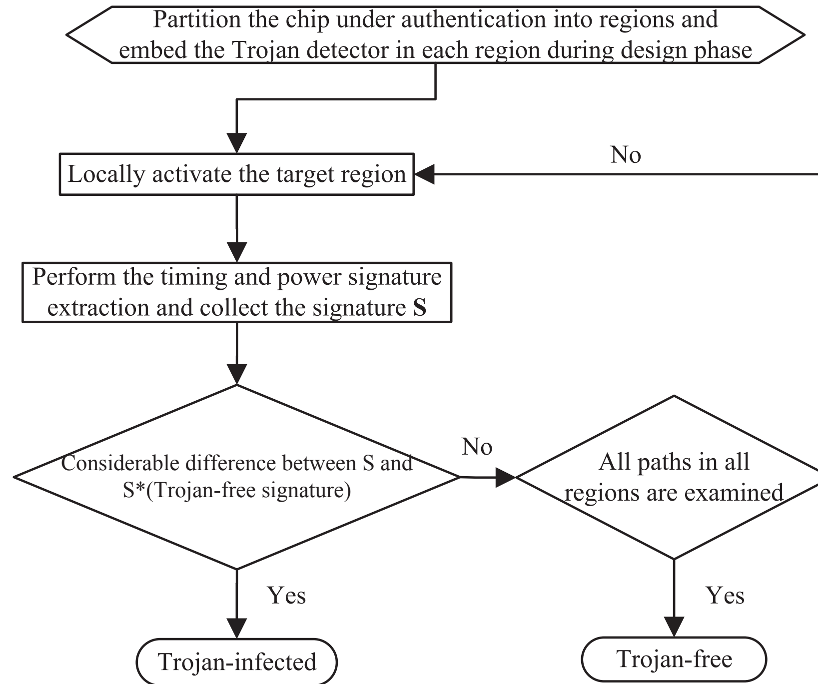

Figure 3.5: *The HT detection flow using the proposed HT-detector.*

unsuccessful attempt in this process is not completely fruitless as it means the discovery of a subverted or dubious chip. Presently, only a rare few emerging methods [21, 29, 54] are able to detect HT without the golden model but they are not without limitations. Typical prices for avoiding the golden model include the requirements of expensive computations, sophisticated process variation models and a large number of measurements to ensure accuracy for large chip with more gates [35].

For this HT-detection scheme to work, a dedicated and compact current sensor is required. When the sleep transistor connected to the virtual supply of a target region is turned on, it measures the duration and amplitude of transient current drawn from the virtual supply to a group of timing paths in the target region activated by the input pattern. The design of this current sensor is the focus of this chapter.

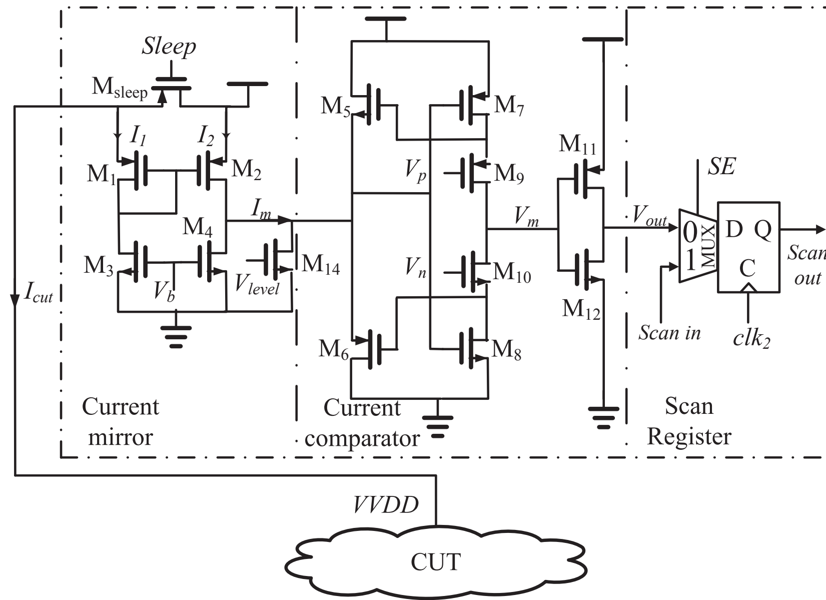

Figure 3.6: *Schematic of the proposed current sensing to path delay monitoring circuit.*

3.3 Scan-enabled Active Current Sensor

The schematic of the proposed active current sensor is shown in Fig. 3.6, where the cluster under test (CUT) refers to the cluster of circuits whose switching current is being monitored by the current sensor. Its principle of operation as a Trojan detector is explained as follows. The dynamic IR-drop across the on-resistance R_{on} of the sleep transistor M_{sleep} can be sensed to provide the visibility of the active current for the CUT. The dynamic current is mirrored to a current comparator to produce two voltage transitions that mark the path delay. The comparator output is latched into a scannable flip-flop. The latched output is propagated to an external output pin by daisy chaining the scan flip-flops of all detectors. The delay transition of the comparator output from each detector can be determined from the corresponding scanned output by varying the phase shift between the system clock and the sampling clock of the scan chain in the detectors. In what follows, the design and operation of each subcircuit will be elaborated.

3.3.1 Current Mirror

The current mirror utilizes the current monitor [56] originally developed for the I_{DDQ}/I_{DDT} testing. When the sleep transistor M_{sleep} is turned on initially, the gate voltage V_{level} for M_{14} is 0. When there is no current drawn by the CUT, i.e., $I_{cut} = 0$, the gate-source voltages of the transistor pair $(M_1 - M_2)$ are equal. A voltage drop is induced in the on-resistance R_{on} of M_{sleep} when the current I_{cut} drawn by the active CUT passes through R_{on}. This voltage drop causes a difference in the gate-source voltages of transistor pair $(M_1 - M_2)$ and produces the mirrored current $I_m = I_2 - I_1$, where I_1 and I_2 are the drain current of M_1 and M_2 respectively. I_m is given by [56]:

$$I_m \approx R_{on}(2\mu_p C_{ox}\frac{W}{L}{I_1}^3)^{\frac{1}{2}}(1 + \frac{I_{cut}}{I_1}) \tag{3.1}$$

where μ_p, C_{ox} and W/L are the hole mobility, oxide capacitance and channel aspect ratio of M_1, respectively. The level shift transistor M_{14} is used to add a negative current offset to I_m. When its gate voltage V_{level} increases, the output current for the current mirror becomes:

$$I'_m = I_m - I_{14} \tag{3.2}$$

where I_{14} is the drain current of M_{14}. V_{level} can be tuned to detect the peak current duration.

An important consideration is the sizing for the sleep transistor M_{sleep}. To reduce the area and power (leakage power and dynamic power) overheads caused by the addition of sleep transistors, smaller sleep transistor is preferred. A smaller sleep transistor with greater resistance will also improve the detector sensitivity. On the other hand, a greater on-resistance of the sleep transistor can result in a larger voltage drop across it and lower the VV_{DD} supply to the CUT. The sleep transistor is sized to meet the performance requirements of the CUT. As the maximum instantaneous current of a cluster of gates is much smaller than the summation of the peak currents of individual gates within the cluster, the

size of a sleep transistor supporting a cluster of gates is much smaller than the combined area of sleep transistors connected to individual gates. To reduce the area overhead, a reasonably-sized sleep transistor is assigned to each cluster of mutually exclusive switching gates [57] under the peak current constraint of the sleep transistor.

The on-resistance R_{on} for an NMOS transistor is given by:

$$R_{on} = \frac{1}{(\mu_n C_{OX} \frac{W}{L})(V_{GS} - V_t)} \tag{3.3}$$

where V_t is the threshold voltage of the transistor.

To limit the supply voltage droop to less than 5%, $(I_{cut}+I_1)R_{on} < 0.05V_{dd}$. R_{on} is empirically determined to be around 200Ω based on GF 65nm CMOS technology with a supply voltage of 1.2V.

3.3.2 Current Comparator

The current comparator compares the mirrored current against the quiescent current threshold to produce a high output voltage level during the period of activity and a low voltage level when all sensitized path transitions have settled. The current comparator circuit in Fig. 3.6 is modified from the Traff's current comparator [10]. The original Traff's comparator is shown in Fig. 3.7. The transistor pair $(M_5 - M_6)$ of Traff's current comparator operates in the subthreshold region at the start of each comparison before the feedback loop takes effect, which results in a long settling time. This problem is overcome in the proposed design by introducing two transistors, M_9 and M_{10}, in Fig. 3.6. This pair of transistors is biased in the linear region, which increases the gate voltages of M_7 and M_8 to prevent M_5 and M_6 from entering the subthreshold region. The response time is improved at the expense of a reduced output voltage swing. Therefore, an inverting stage is needed in Fig. 3.6 to restore its rail-to-rail output. These two transistors also act as two voltage-controlled linear resistors. The charging and discharging currents of the comparator load capacitor can be adjusted by their gate voltages to subtly alter the slew rate and hence the width of V_{out}. This is equivalent to adding a

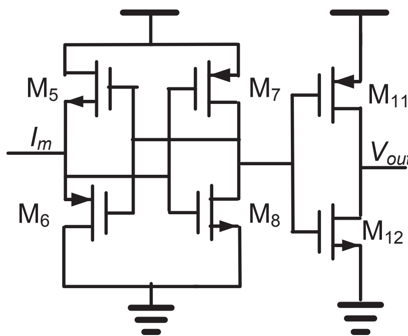

Figure 3.7: *Schematic of Traff's current comparator [10].*

small offset to the comparator threshold to compensate for the minute difference in quiescent currents of different chips due to the process variations.

V_{out} can be calibrated to mitigate the effect of process variation. A "reference pattern" that excites only a small number of paths of the region from the set of stimuli is applied when the power to the region is enabled. The pulse width of the voltage V_{out} is adjusted by V_p and V_n to be the same as that of the "reference chip" under the same test pattern. As only one sleep transistor of a cluster will be activated at any time, only two external pins need to be reserved for the calibration of the V_p and V_n voltages for all CUT detectors. After V_p and V_n have been calibrated, the pulse widths of the voltage V_{out} for other test patterns are then measured. As the Trojan does not affect all the paths of the CUT, the "reference pattern" selected for the calibration of V_p and V_n may or may not trigger the Trojan. If the Trojan logic is not excited by the "reference pattern" during this calibration, the transition delay of V_{out} of the Trojan-infected CUT will be exacerbated and become notably longer than that of the Trojan-free CUT when the Trojan-infected subcircuits are sensitized by other test patterns. If the "reference pattern" activates the Trojan-infected subcircuits, then the extended delay transition of V_{out} due to the excited Trojan under the "reference pattern" will be eliminated by the calibration but a negative offset will also be introduced into the subsequent measurements when the Trojan's infected subcircuits are not activated by the test patterns. In either case, the probability that a Trojan-infected CUT exhibiting disparate pulse width of V_{out} from the Trojan-free CUT under the same

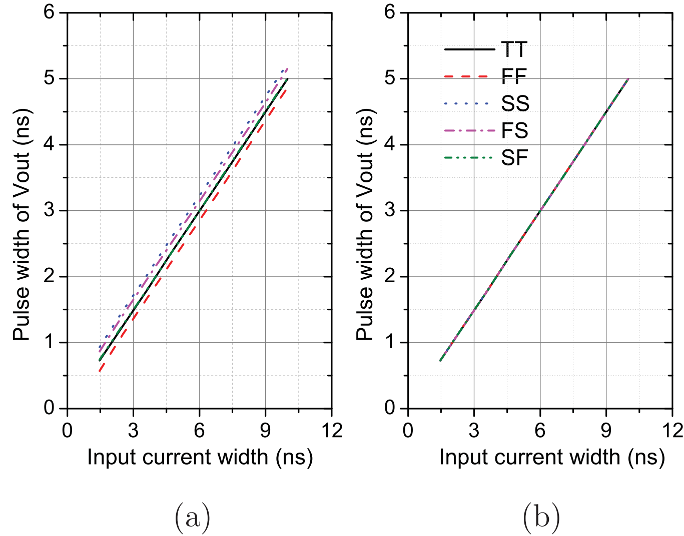

Figure 3.8: *Corner simulation of comparator output pulse width: (a) without calibration, (b) with calibration. The process corner is represented by a two-letter designator, where the first and second letters refer to the NMOS and PMOS corners, respectively. The letters T, F and S denote typical, fast and slow corners, respectively.*

set of test patterns will increase after the calibration.

The proposed current comparator is implemented in GF 65nm, 1.2 V CMOS technology and the circuit is simulated by Cadence Spectre simulator. The input current I_m to the comparator is emulated by a 20μA current source. The pulse width of I_m is varied in step of 100ps. Fig. 3.8 (a) shows that the comparator output pulse width varies linearly with the input current pulse width for the fast (F), slow (S) and typical (T) corners of the process technology. The process variations introduce an offset into the linear transfer characteristic of the comparator. By adjusting the gate voltages V_p and V_n of the current comparator, this offset can be eliminated as shown in Fig. 3.8(b).

Fig. 3.9 shows the simulation results for a path delay measured by the proposed sensor for temperature ranges from 0°C to 100°C. The change in temperature can introduce a DC offset to the measured path delay as shown in Fig. 3.9(a), which can also be compensated by calibration as shown in Fig. 3.9(b).

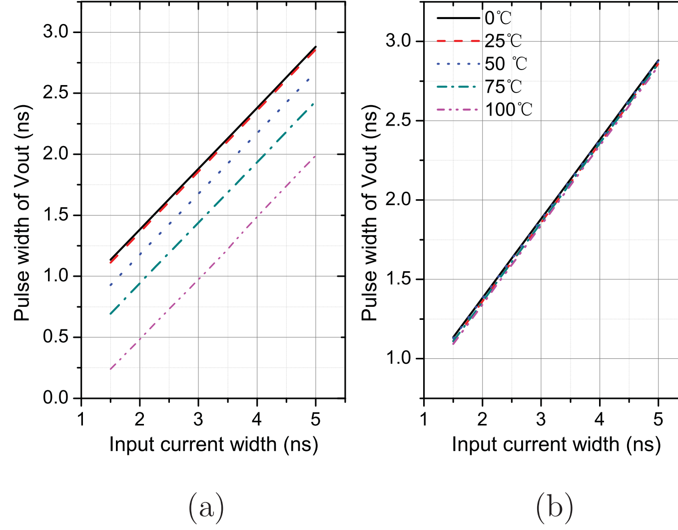

Figure 3.9: *Simulation of comparator output pulse width under temperature variations: (a) without calibration, (b) with calibration.*

3.3.3 Scan Register

The current comparator output V_{out} is fed to a standard multiplexer-based scan FF. The scan FFs of all HT detectors are daisy chained to form a secondary scan chain to propagate the transition of V_{out} to an external scan output pin. The pulse width of V_{out} can be determined by the transition delay test [58] through the functional scan chain SC_1 and the secondary scan chain SC_2 as shown in Fig. 3.10, where n is the number of CUTs. The timing diagram for the transition delay test is shown in Fig. 3.11, where S_i and D_i are the input and output vectors of the i-th CUT. After turning on the sleep transistor of the i-th CUT, the scan-enable signal (SE_1) of the functional scan chain is asserted to shift the test pattern S_i into the input registers of the i-th CUT through SC_1 while the scan-enable signal (SE_2) of SC_2 is disabled. The input data S_i in SC_1 is launched into the i-th CUT at the rising edge of clk_1 when SE_1 is de-asserted. The current detector of the i-th CUT senses the commencement of circuit activities and produces a low-to-high transition on its V_{out}. The logic level V_i of V_{out} in the i-th CUT after a time delay t from the launching clock is captured into the scan FF of SC_2 at the last rising edge of clk_2 before SE_2 is asserted. clk_2, which is gated by $SE_1 \odot SE_2$ ($\odot$ denotes

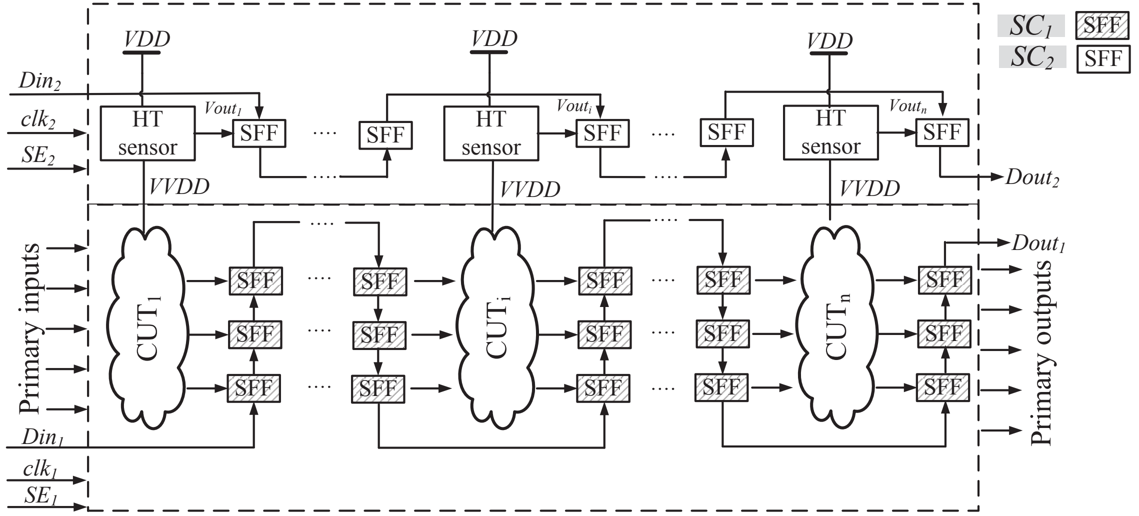

Figure 3.10: *Primary and secondary scan chains for the detection of current comparator output pulse width.*

XNOR), has a phase shift from clk_1. By asserting SE_2, V_i can be scanned out to an observable scan-output pin. The process is repeated by launching the same input data with different capturing time (by changing the assertion time of SE_2 and the phase shift between clk_1 and clk_2) after SE_1 is deasserted until a high-to-low transition is detected at V_i from the scan output of SC_2. To capture the transition of V_{out}, the delay t is initially set to be slightly less than the pulse width of V_{out} of the Trojan-free CUT detector to capture the logic '1' of V_{out} and then the phase shift between clk_1 and clk_2 is incremented in timing steps of $\delta/2$ until the logic '0' of V_{out} is captured, where δ is the minimum discriminable delay exacerbation to signify the existence of Trojan. Idle cycles can be inserted between the last scan-in data and the de-assertion of SE_1 to allow the CUT to recover from the supply voltage droop and heat dissipation due to the input data scanning operation. clk_1 signal is disabled and the primary inputs are held constant during the idle cycles.

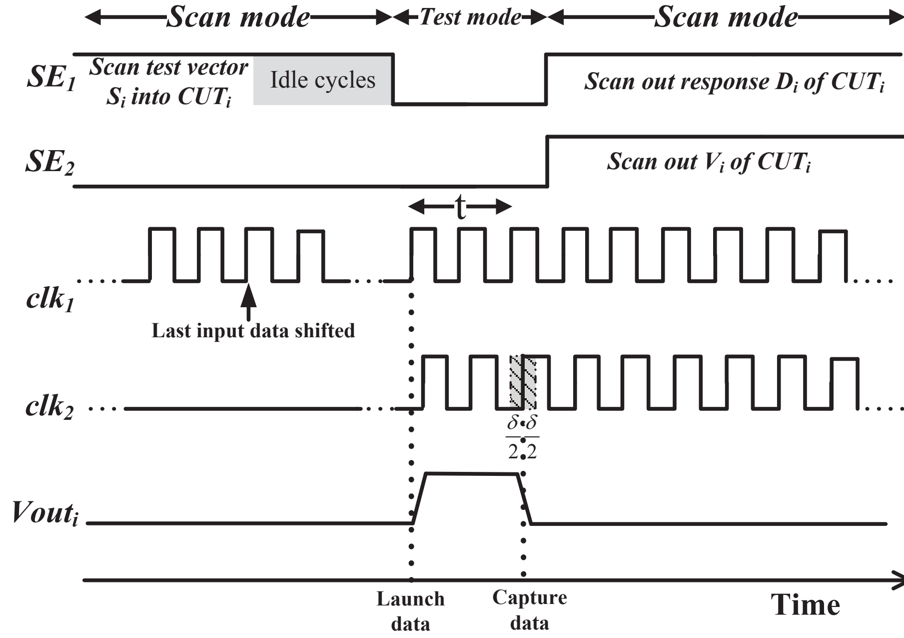

Figure 3.11: Timing diagram of the sampling of transition delay.

3.4 Results and Discussion

3.4.1 Experiment Setup

Four virtual power clusters are considered in the simulation. The proposed detector is added into the CUT of each cluster. The CUT is a circuit from the ISCAS'85 benchmark suite [59]. Synopsys Design Compiler is used to map the benchmark circuits to the GF 65nm standard cell library. The Trojan circuit is inserted into the synthesized Verilog netlists. This is the more likely scenario when the hacker has no access to the RTL code, which is generally not provided to the foundry. Both netlists with and without Trojan are converted to the physical layout by Cadence SOC Encounter and stored in the industry standard GDS-II file. The simulation is carried out in the Cadence Spectre environment with the model file of parasitics and process variations provided by the foundry. Dynamic timing analysis without parameter variations and with parameter variations [60] are then performed on the Trojan-free and Trojan-infected circuits.

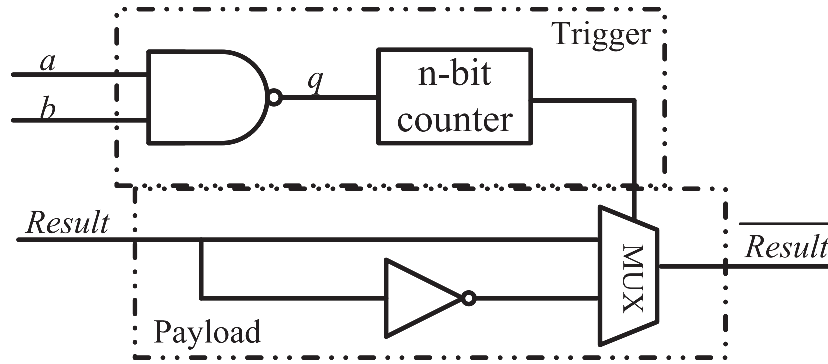

Figure 3.12: *Counter-based Trojan circuit architecture [11].*

3.4.2 Trojan Circuits

The Trojan to be inserted into an arbitrarily selected CUT of the four clusters is designed using an n-bit counter and an NAND gate as shown in Fig. 3.12 [11]. The n-bit counter is clocked by the NAND gate output, which has its inputs a and b connected to the internal signals of the CUT. When the count exceeds a predefined number N, it triggers the Trojan and alters the *Result* of the payload to $\overline{Result}$. The gate count of the one-gate payload and triggering mechanism of the Trojan used in this experiment is equivalent to 52 two-input NAND gates. N is set to a large value, e.g., 1000000, to reduce the chance for it to be detected by functional test. Two types of Trojan placements [30] are considered for each analysis. The first placement method replaces any output port of the CUT by the output $\overline{Result}$ of the Trojan circuit by connecting the input *Result* of the Trojan's payload to the original output of the CUT. This Trojan introduces a very small delay of an inverter and a MUX delay for the inserted path. It exhibits very little additional switching activity during normal operation as it can be activated only by a rare set of input vectors. For the second placement method, the same counter-based Trojan (Fig. 3.12) is embedded into a path in parallel as in Fig. 3.1(a) such that the delay of the Trojan payload is buried within the much longer delay of other reconvergent paths of the CUT. In the following experiments, the former Trojan placement with very low switching activity is first analyzed before the Trojan with no delay impact is analyzed in Section 3.4.4.

Table 3.1: *Transition delays of detector outputs for the genuine and infected designs*

No.	Clock period (ns)	Phase Shift (ps)	Scan outputs of detectors	
			Genuine	Infected
1	5	350	1111	1111
2	5	400	1111	1111
3	5	450	0000	**1**000
4	5	500	0000	**1**000
5	5	550	0000	0000

3.4.3 Detection of Trojan with Low Switching Activity

Before a randomly sampled manufactured die is reverse engineered to ascertain its genuineness, it is first exercised with random test vectors. The phase shift of clk_2 with respect to the system clock clk_1 is successively increased to capture the logic value of V_{out} in the i-th CUT. Every phase shift when the detector captures the falling edge of V_{out} for each input test vector is recorded. These become the signatures of the golden model once a chip is identified as genuine. The design under test is then exercised with the same set of the test vectors starting with the corresponding phase shifts of clk_2 recorded from the Trojan-free model. The clock shift is gradually adjusted to find the falling edge of V_{out} of the design under test. Table 3.1 lists the four-bit streams corresponding to the logic states of V_{out} latched into the detector scan registers of the four clusters with different phase shifts of clk_2 for the Trojan-free and Trojan-infected benchmark circuit C2670. The period of clk_1 is set to be $5ns$. With the modern clock generator and phase lock loop (PLL), the phase shift of clk_2 is increased at a time step of $\delta/2 = 1\% \times 5ns = 50ps$. This time step determines the smallest Trojan detectable. Given that clock skew as low as $1ps$ in $180nm$ fabrication technology has been reported [61], single-gate Trojan can be detected in principle provided that such precision of phase shift can be generated at reasonable cost and the Trojan-to-circuit induced activity is higher than the background noise. As will be demonstrated in later experiment, the Trojan-to-circuit activity can be increased by reducing the cluster size and the background noise can be reduced by calibration.

By varying the phase shift of clk_2 from $350ps$ to $550ps$, the high-to-low transition of V_{out} is detected in all but the first cluster when the phase of clk_2 is stepped

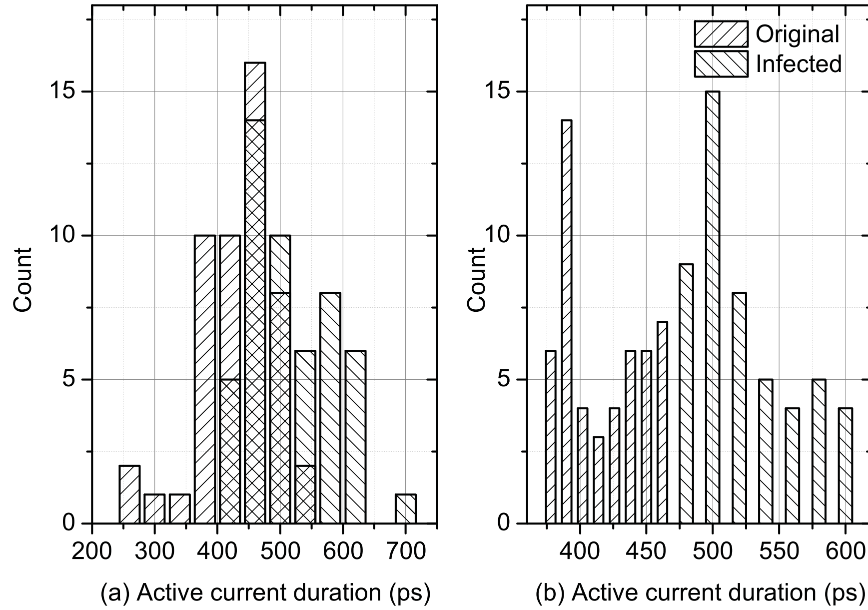

Figure 3.13: *Monte Carlo simulation results for the active current duration distributions: (a) before calibration, (b) after calibration.*

from 400ps to 450ps. The falling transition of V_{out} of the first cluster is detected when the phase shift is increased from 500ps to 550ps. The CUT of the first cluster is indeed the only CUT among the four clusters that is embedded with a Trojan. The Trojan extended the active current duration by about 100ps, which can be captured using a phase shift resolution of 50ps. By increasing the step size $\delta/2$ of the phase shift to 150ps, the falling transitions of V_{out} from all four clusters occurred at the same phase shift of clk_2, which means that the Trojan-infected and Trojan-free CUTs are indistinguishable. The resolution of the phase shift to successfully detect this Trojan may have to be further increased as the extra duration of the switching activity induced by the Trojan may be masked by the manufacturing process variations (PVs). PVs cause important physical and electronic parameters, such as the device length and width, and its threshold and saturation voltages to deviate from the nominal specifications [62].

Monte Carlo simulation method [13] can be adopted to introduce randomly sampled device parameter variations from a normal distribution. Each iteration of the Monte Carlo simulation represents a unique set of variations applied to a de-

sign. Table 3.2 shows the key parameter variations of GF 65nm CMOS technology used in the simulation. This information is provided by the foundry to represent the ranges of parameter values of the physical design due to the manufacturing PVs. To demonstrate the effectiveness of the proposed calibration method, the post-layout statistical Monte Carlo simulation of 100 random process variation tests (50 tests each on Trojan-free and Trojan-infected designs) is performed to measure the actual active current duration of C2670 and compare against that of the golden model. At each iteration, a set of test vectors from the previous experiment are used. The distributions of the active current duration of the Trojan-free and Trojan-infected CUTs before the comparator is calibrated by V_p and V_n (see Section 3.3.2) are shown in Fig. 3.13(a). The difference between the mean values of the two distributions is 87ps, which is slightly lower than the value of $\delta = 100ps$ derived from the dynamic timing analysis without considering process variations. However, the standard deviations of both distributions exceeded $\delta/2$. The overlaps between the two histograms are tests that show no difference in the pulse widths of V_{out} between the Trojan-free and Trojan-infected CUTs due to the masking effect of PVs. Fig. 3.13(b) shows the distributions of the pulse width of V_{out} of the Trojan-free and Trojan-infected CUTs after the comparator threshold calibration proposed in Section 3.3.2). The difference between the means of the two distributions has increased to 99ps and the standard deviations have been lowered to below $\delta/2$ after calibration. In fact, the two distributions do not overlapped unlike Fig. 3.13(a). For ease of comparison, the statistics of the distributions of Fig. 3.13(a) before calibration and Fig. 3.13(b) after calibration are summarized in Table 3.3. The delay difference between the Trojan-free and Trojan-infected circuits due to the process variations has been magnified after calibration, which increases the Trojan detection rate. The detection error rate (DER) can be estimated from the histograms of V_{out} pulse width as follows:

$$DER = \frac{F}{N} \tag{3.4}$$

where F is the number of matching V_{out} pulse widths between the Trojan-free

and Trojan-infected histograms and N is the total number of tests. The DER includes the false negatives (accepting a Trojan-infected design as Trojan-free) and the false positives (rejecting a genuine design as Trojan-infected). To estimate the false positive and false negative rates from the histogram, the mean value between the lowest and the highest active current durations of the overlapped areas of the histograms is determined as threshold. Those tests in the overlapped areas that fall below the threshold are false positives and those above are false negatives. From Fig. 3.13, the DER is 30% (17 false positives and 13 false negatives) before calibration and 0% after calibration. It should be noted that the DER estimated from the histogram assumes that phase shift of clk_2 has infinitesimal resolution. In practice, the active current duration, i.e., the pulse width of V_{out}, is detected from the scan output of SC_2 by the transition delay test with a finite phase shift resolution of clk_2. Table 3.4 shows the DER of the proposed method with and without the PV calibration for different ISCAS'85 benchmark circuits by embedding an 8-bit counter based Trojan in serial into a randomly selected timing path of a cluster. The Trojan and detector overheads are expressed as a percentage of their respective gate count over the gate count of the original design excluding the routing overheads. As the proposed method requires only one scan register per cluster as opposed to one shallow register per path of [4] used in the delay-based HT detection methods [22, 23], the routing complexity of clock and scan enable signals is significantly lower. A post-layout statistical Monte Carlo simulation with a total of 100 runs of device variations were carried out on the Trojan-free and Trojan infected designs (50 runs each) for each benchmark circuit. The DER obtained based on the histogram of the actual pulse width of V_{out} and that detected by the transition delay test with $\delta/2 = 50ps$ are compared. Most circuits have zero DER for the PV-calibrated Trojan detector. The maximum DER is only 4% for C5315 and C6288 with the PV-calibration. The DER obtained by the transition delay test with $\delta/2 = 50ps$ is at most 1% worse than the DER estimated from the histograms with infinitesimal clock phase resolution for both the PV-uncalibrated and PV-calibrated detection.

Table 3.2: *Key parameter variations used in the dynamic timing analysis*

Parameter	Unit	NMOS	PMOS
Channel length chip mean variation L	nm	± 5	± 5
Channel width chip mean variation W	nm	± 13	± 13
Long channel chip mean Vt	mV	± 43	± 45
Vtsat	mV	± 93	$+90 \sim -87$

Table 3.3: *Statistics of Fig. 3.13*

	Before PV calibration		After PV calibration	
	Original	Infected	Original	Infected
Average delay (ps)	430	517	421	520
Standard deviation (ps)	60	69	29	37
Max deviation (ps)	164	190	50	77

3.4.4 Detection of Trojan with No Delay Impact

Trojan with rare switching impact has been demonstrated to be relative well detected by the transition delay test with the proposed current detector. Nevertheless, Trojan with no delay impact [30] may not be detected as successfully by the delay-based side-channel signal analysis. This can be easily demonstrated by the static timing analysis. Fig. 3.14 shows the static timing analysis results for the Trojan-free design and the Trojan-infected design with the 8-bit counter-based Trojan embedded in serial and in parallel. The extra delay for the Trojan embedded in serial can be detected by the delay-based side-channel analysis as shown in Fig. 3.14(a), but there is no observable delay difference from the primary inputs to the primary outputs when the Trojan is embedded in parallel, as shown in Fig. 3.14(b). The proposed current detector provides a means to indirectly compare the amplitude of the switching current profile of a CUT against that of the Trojan-free CUT under the same excitation to detect such a Trojan. This is achieved by adjusting not only the phase shift of clk_2 but also the gate voltage V_{level} of M_{14}. Table 3.5 shows parts of the simulation result. Initially, V_{level} is set to be $0mV$. The phase shift of clk_2 is gradually increased until the falling edge of V_{out} is detected. No difference between the pulse width of V_{out} extracted from the Trojan-free chip and the Trojan-infected design at the same V_{level} is observed at the scan registers in SC_2. When V_{level} is increased to $600mV$, a rising transition

Table 3.4: *Detection error rate with and without PV calibration for serial placement of Trojan in ISCAS'85 benchmarks*

Benchmark	Gates count	Trojan area overhead (%)	Detector area overhead (%)	Estimated DER from histograms (%)				DER with $\delta/2 = 50ps$ (%)			
				Uncalibrated		Calibrated		Uncalibrated		Calibrated	
				False negatives	False positives	False negatives	False positives	False negatives	False positives	False negatives	False positives
C432	160	8.1	2.3	10	10	0	0	10	10	0	0
C499	202	6.4	1.9	9	13	0	0	10	13	0	0
C880	383	3.4	0.98	14	12	0	0	14	12	0	0
C2670	1193	1.1	0.31	13	17	0	0	13	18	0	0
C3540	1669	0.78	0.23	15	16	0	1	15	17	0	1
C5315	2406	0.54	0.16	18	16	2	2	19	16	2	2
C6288	2406	0.54	0.16	20	16	2	1	20	17	2	2

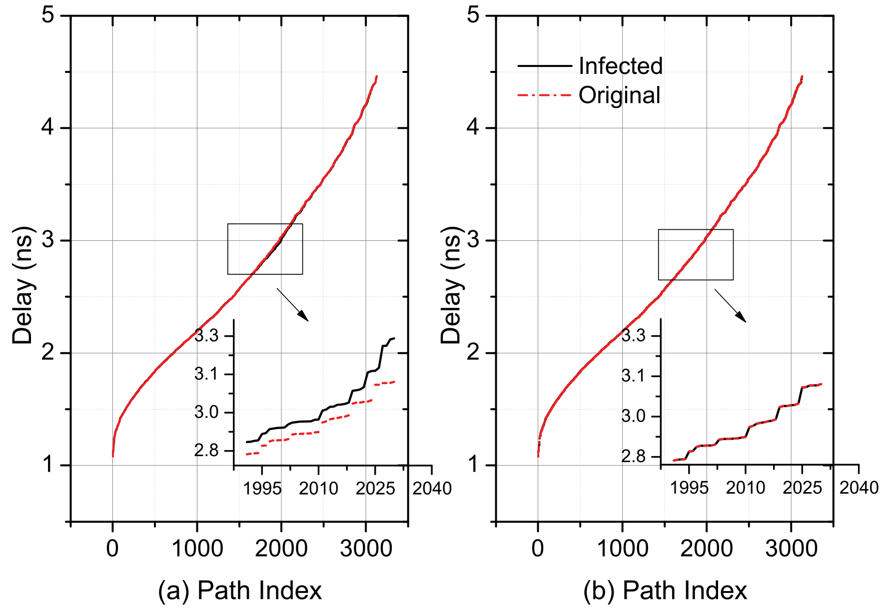

Figure 3.14: *The delay impacts with different placements of Trojan: (a) Trojan embedded in serial, (b) Trojan embedded in parallel.*

at the phase shift of $450ps$ and a falling transition at the phase shift of $550ps$ are detected for the active cluster (Cluster 1 in this case) of the Trojan-infected circuit, whereas no transition is detected for the active cluster from the signature of the genuine design. This narrow pulse width of V_{out} is due to the additional current drawn by the Trojan. V_{level} is increased until V_{out} of the active cluster scanned out of SC_2 is '0' on the first phase shift of clk_2. If no transition in V_{level} is detected upon completion of the phase shift test at this V_{level}, the circuit is declared to be Trojan-free.

The effect of PV has a smaller influence on the amplitude difference introduced by the Trojan. Fig. 3.15 shows the 100 runs of Monte Carlo simulation results

Table 3.5: *Detector outputs for the genuine and infected designs for Trojan with no delay impact*

No.	**Clock period (ns)**	**Phase Shift (ps)**	**Scan outputs of detectors**			
			$V_{level} = 0mV$		$V_{level} = 600mV$	
			Genuine	**Infected**	**Genuine**	**Infected**
5	5	350	1111	1111	0111	0111
6	5	400	1111	1111	0111	0111
7	5	450	1111	1111	0111	**1**111
8	5	500	1111	1111	0111	**1**111
9	5	550	1111	1111	0111	0111
10	5	600	1111	1111	0111	0111
11	5	650	0111	0111	0111	0111

for the average active current amplitude distributions of V_{out} obtained from the Trojan-free and Trojan-infected C2670. Table 3.6 shows the statistics of the histograms in Fig. 3.15. Calibration of the current comparator described in Section 3.3.2 does not lead to appreciable changes in the average current amplitude for both circuits. However, it helps to improve the detection sensitivity by lowering the standard deviation of the average active current amplitude of the Trojan-infected circuit. The standard deviation of the active current for Trojan-infected circuit has been reduced by about 22.5% by calibration, which is more substantial than the 14.7% reduction of standard deviation for the Trojan-free circuit. Before calibration, the DER estimated from the histograms is 3% with 1 false positive and 2 false negatives. It reduces to 0% after calibration. Table 3.7 shows the DER of the proposed method with and without the PV calibration for different ISCAS'85 benchmark circuits by embedding an 8-bit counter based Trojan in parallel into a cluster. The DER estimation from the active current pulse amplitude of V_{out} produces perfect zero DER for all except C6288, which has only one false positive detection. The DER for each benchmark circuit was also obtained by the transition delay test with the same post-layout statistic Monte Carlo simulation of device variations on the Trojan-free and Trojan infected designs. The DER results for the uncalibrated current detector with finite phase shift resolution of clk_2 are the same as those estimated from the histogram. The finite resolution of the clock phase shift leads to only a slightly higher DER than that estimated from the histogram for the calibrated current detector. After the PV calibration, all Trojan-infected

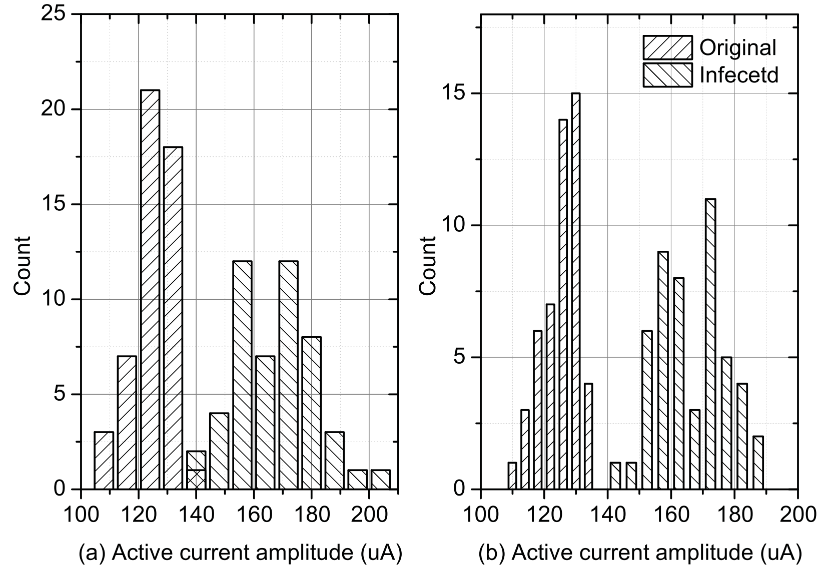

Figure 3.15: *Monte Carlo simulation results for the average active current amplitude distributions: (a) before calibration, (b) after calibration.*

Table 3.6: *Statistics of Fig. 3.15*

	Before calibration		After calibration	
	Original	Infected	Original	Infected
Average current amplitude (μA)	125	167	126	168
Standard deviation (μA)	6.8	13.8	5.8	10.7
Max deviation (μA)	20.4	29.9	14.1	23.6

CUTs have been successfully detected except for C5315 which has a false positive and a false negative. Because the switching current amplitude contributed by this type of Trojan outweighs the PV, the rate of success for its detection is higher than the serially embedded Trojan even without the PV calibration.

It is observed that the false negatives/positives in Table 3.4 and Table 3.7 grow with the size of the cluster due to the increase in circuit activity. For large and complex design, more clusters are needed to maintain the detection accuracy.

3.4.5 Scaling the Trojan

To evaluate the Trojan detection sensitivity of the proposed method, the size of the Trojan is scaled down by reducing the counter length. The Trojan circuits of different counter lengths are randomly inserted into the CUT (C2670) during

Table 3.7: *Detection error rate for Trojan with no delay impact in ISCAS'85 benchmarks with and without PV calibration*

Benchmark	Gates count	Trojan area overhead (%)	Detector area overhead (%)	DER from histograms (%)				DER with $\delta/2 = 50ps$ (%)			
				Uncalibrated		Calibrated		Uncalibrated		Calibrated	
				False negatives	False positives	False negatives	False positives	False negatives	False positives	False negatives	False positives
C432	160	8.1	2.3	0	0	0	0	0	0	0	0
C499	202	6.4	1.9	0	0	0	0	0	0	0	0
C880	383	3.4	0.98	0	0	0	0	0	0	0	0
C2670	1193	1.1	0.31	2	1	0	0	2	1	0	0
C3540	1669	0.78	0.23	1	1	0	0	1	1	0	0
C5315	2406	0.54	0.16	3	4	0	0	3	4	0	1
C6288	2406	0.54	0.16	3	3	0	1	3	3	1	1

Table 3.8: *DERs of the proposed method for different Trojan area overheads.*

Counter length	8-bit	4-bit	2-bit	1-bit
Trojan area overhead	1.09%	0.58%	0.34%	0.21%
DER (un-calibrated)	15%	16%	16%	20%
DER (calibrated)	0%	1%	2%	2%

the 100 runs of Monte Carlo simulation. The results in Table 3.8 show that the DERs obtained by the transition delay test with $\delta/2 = 50ps$ for the uncalibrated and PV-calibrated current detectors. The DER increases slightly as the Trojan size is scaled down. With the proposed PV calibration technique, the Trojan detection sensitivity has been improved significantly, especially when the parametric variation due to the Trojan is small and comparable to the process variations. Compared with the DER of 64% for the detection of a 4-bit counter based Trojan embedded in the one-round DES circuit with a Trojan area overhead of 0.76% in SMIC 0.13μm CMOS technology reported by the delay-based side-channel analysis of [20], the proposed method has a much greater accuracy. Similar 4-bit counter based Trojan with a Trojan area overhead of 0.58% can be detected by the proposed method with a DER of as low as 1% despite simulated in a 65nm technology node with higher variations.

3.4.6 Sensor Security

The proposed detector forms an integral part of the power grid, which makes its removal or tampering much easier to be detected than the Trojan itself from the deteriorated circuit performance and structural test results. As the power grid is extremely sensitive to any small change in current, the sensing resistance R_{on} can be placed as close as possible to the power supply node so that the Trojan

cannot be strategically placed to evade detection. Since the Trojan draws the same amount of current regardless of its location, the additional current flows at the power supply node will always be sensed by R_{on}. If the attacker has access to the reference pattern of a cluster, he may implant a Trojan in that cluster and resize the calibration transistors M_9 and M_{10} of Fig. 3.6 to mask the positive delay offset of the Trojan. However, this negative delay offset created by the attacker will be added to the remaining paths in the same cluster. When other random patterns activate these paths, a discernible "negative" deviation of the signatures from those of the golden chip will be detected, which indicates that its calibration circuit has been tampered. Another possible attack is to sensitize the paths under all possible excitations including the reference patterns and then replace the scan registers of the scan chain by a non-volatile memory. However, the memory required to store the responses to these excitations is extremely large. Its area and power consumption are conspicuous and can be easily detected by basic side-channel analysis.

3.5 Summary

This chapter suggests a new possibility of detecting the presence of hardware Trojan in an IC through sensing its local active current based on the power gating technology. A novel on-chip active current sensing circuit that comprises a current mirror, a current comparator with adjustable threshold and a multiplexor-based scan register is proposed to detect the commencement and ceasing of switching current on local power grid when timing paths around the region are sensitized. The active current duration captured by the detector can be easily decoded from the scan output by a structural test methodology. In contrary to many other delay-based side-channel analysis, this method can detect the Trojan with no delay impact by analyzing the deviation in current amplitudes. The detector is built with a calibrator to adjust the current comparator threshold against process variations. Its improved Trojan detection sensitivity has been demonstrated by the post layout Monte Carlo simulation. As the proposed sensor enables at-speed test

without affecting the normal circuit timing and functionality, it can be incorporated into the real-time trust evaluation framework [31] to monitor the active current timing and duration in the field. When an HT is activated during normal circuit operation, the measured characteristics of the power trace will change dramatically to alert for anomalies. Such in situ monitoring is particularly useful for detecting sophisticated Trojans that have escaped the pre-deployment test.

Chapter 4

A Low-power Hybrid Ring Oscillator Physical Unclonable Function with Improved Thermal Stability for Lightweight Applications

4.1 Introduction

The Internet of Things (IoT) is envisaged to become an ultimate driver for the next growth phase of semiconductor industry. Radio frequency identification (RFID) and several other lightweight electronic tagging technologies will avail themselves most in this ubiquitous computing revolution of advance connectivity of devices, systems and services. Unfortunately, the footprint and power budget have severely limited the strength of cryptographic algorithm implementable on a RFID or other intelligent tags, and the secret data stored in these lightweight devices can be easily read or reverse engineered and copied [63]. Critics are concern that the wide spread of IoT will make cyber attack an increasingly devastating physical (as opposed to virtual) threat. In this light, physical unclonable function (PUF) comes in handy as a new secure and low-cost primitive for integrated circuit (IC) authentication and counterfeit prevention [63, 64].

Among the silicon based PUFs introduced in Section 2.2, Chapter 2, RO PUF

is superior to others [65] in the following aspects: 1) The RO can be implemented as a hard macro and instantiated as many times as needed in the top-level design, making all the ROs identical in terms of placement and routing. The output frequencies are also independent of the delay introduced by the routing of the RO outputs to the counter. 2) The difference in RO frequencies can be amplified by allowing them to "ring" for a longer time at the expense of power and area consumption.

Albeit the above advantages of RO PUF, the reliability of its responses is still highly susceptible to temperature variations [66]. Many researchers have attempted to address the thermal induced response instability problem of RO PUF. In [67], a temperature-aware cooperative RO PUF is proposed. Bit generation rules are defined to convert the unreliable bits. In [12], this problem is addressed by selecting only those pairs of oscillators of sufficiently large frequency distances to desensitize their variations with temperature. Methods to correct the noisy bits by using fuzzy extractors have also been proposed [15]. However, these approaches improve the reliability of the PUF at the cost of its hardware area, power consumption and complexity of operation. In [68], multi-level supply voltages are used to ensure the stability of PUF responses at varying operating temperature. The drawback is the requirement of additional power management circuits for voltage monitoring and sequencing.

This chapter presents a novel design of RO PUF that has much lower power and area consumption than the conventional implementations, yet possesses enhanced reliability and high entropy. To counteract the effect of thermal induced deviations in a randomly chosen pair of ROs, each RO consists of a "nearly"[1] balanced number of positive temperature coefficient current starved inverter stages and negative temperature coefficient regular inverter stages to prevent the flipping of response bit. The current starved inverter stages operate in the subthreshold region which reduce the overall power consumption significantly. Each RO in the randomly selected pairs are constructed from one of the two inverters in each inverter stage to exponentially increase the number of RO frequencies that can be generated for a

[1] The term "nearly" is used because the number of inverter stages needs to be odd.

given area. In addition, a bidirectional counter is proposed to replace two counters, two n-bit multiplexors and a comparator in the classic RO PUF represented by [12]. Such RO PUF architecture also makes logical reconfigurability of CRPs affordable by merely including a linear feedback shifter register (LFSR) counter. The challenge is used as a seed of LFSR to randomly select pairs of RO frequencies to compare for the response bit generation. The prototype chip of the proposed hybrid RO PUF is fabricated in GF 65nm CMOS technology.

The rest of the chapter is organized as follows. Section 4.2 discusses the temperature-induced response stability problem of the classic RO PUF. In Section 4.3, the design and operations of the proposed hybrid RO PUF are elaborated. The quality and security of the proposed PUF are analyzed and discussed in Section 4.4. The experimental results of the prototype IC are presented and compared with existing PUFs in Section 4.5. Finally, the summary is given in Section 4.6.

4.2 Classic RO PUF's Temperature-induced Response Stability Problem

4.2.1 Temperature Dependence of RO PUF Responses

Despite the more robust layout and increased entropy extraction per RO pair, the dynamic variation of the oscillation frequency of RO loop with temperature is still a major concern for the response bit stability of RO PUF presented in Section 2.2.1.1.2, Chapter 2. Fig. 4.1 shows the temperature dependence of RO frequency. The output frequency of the oscillator is inversely proportional to the temperature. Fig. 4.2 shows a scenario that the frequency distance (i.e., the difference in the oscillation frequencies between a pair of ROs) may affect the response bit of the PUF [12]. In Fig. 4.2(a), the crossover point in the frequency versus temperature curves of the pair of ROs can reverse the relation between their frequencies and generate an error bit as the temperature varies from t_1 to t_2. Fig. 4.2(b) shows the scenario that the temperature dependent changes in the oscillation frequencies of the two ROs is small enough to avoid the output of the PUF from flipping.

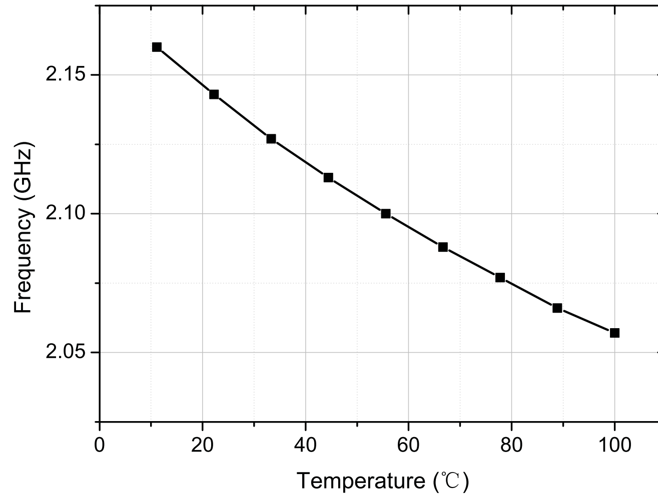

Figure 4.1: *Change in oscillation frequency with temperature for an RO.*

4.2.2 Temperature Coefficient of Regular Inverter

The oscillation frequency of the RO is directly determined by the delay of its inverter stage. The delay t_d of an inverter can be expressed as:

$$t_d = \frac{C_0 V_{dd}}{i_D} \tag{4.1}$$

where C_0 is the total load capacitance, V_{dd} is the power supply voltage and i_D is the average charging current.

In the regular two-transistor inverter circuit, the output capacitance is charged (discharged) by the maximum drain current I_D of the pull-up (pull-down) transistor initially, which decreases during the transition. Disregarding the leakage and short-circuit current, the average current $i_D = \eta I_D$, where the fraction η is fixed for a given inverter. The maximum current I_D is given by:

$$I_D = \frac{W C_{OX}}{2L} \mu (V_{GS} - V_t)^2 \tag{4.2}$$

where I_D, W, L, V_{GS}, C_{OX}, V_t and μ are the saturation current, effective channel width, effective channel length, gate-to-source voltage, gate capacitance, threshold voltage and charge carrier mobility, respectively. The parameters, V_t and μ, are

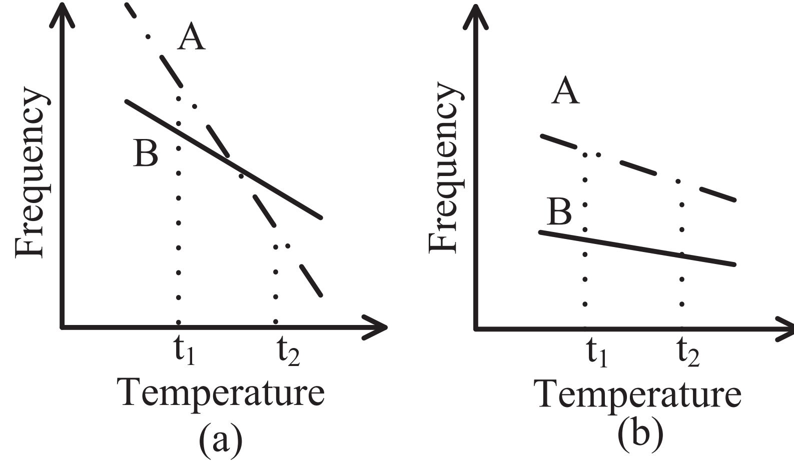

Figure 4.2: *Output bits of two different temperature induced frequency distance scenarios of two RO pairs: the output bit (a) flips, (b) is stable.*

temperature dependent. From (4.2), the temperature coefficient of the switching current (TCC) [69] can be derived as:

$$\begin{aligned} TCC &= \frac{1}{I_D}\frac{dI_D}{dT} \\ &= \frac{1}{\mu}\frac{d\mu}{dT} - \frac{2}{V_{GS} - V_t}\frac{dV_t}{dT} \end{aligned} \tag{4.3}$$

The temperature dependent parameters, V_t and μ, are expressed as [66]:

$$V_t(T) = V_t(T_0) - \sigma(T - T_0) \tag{4.4}$$

$$\mu(T) = \mu(T_0)(\frac{T}{T_0})^{\kappa} \tag{4.5}$$

where T_0 is the reference temperature. The empirical parameters, κ and σ, are respectively the mobility temperature exponent in the range of $1.2 \sim 2$ and the threshold voltage temperature coefficient in the range of $0.5mV/K \sim 3mV/K$.

The threshold voltage $V_t(T)$ decreases with increasing temperature. This results in an increasing drain saturation current as temperature increases. On the contrary, the mobility of the charge carriers decreases with increasing tempera-

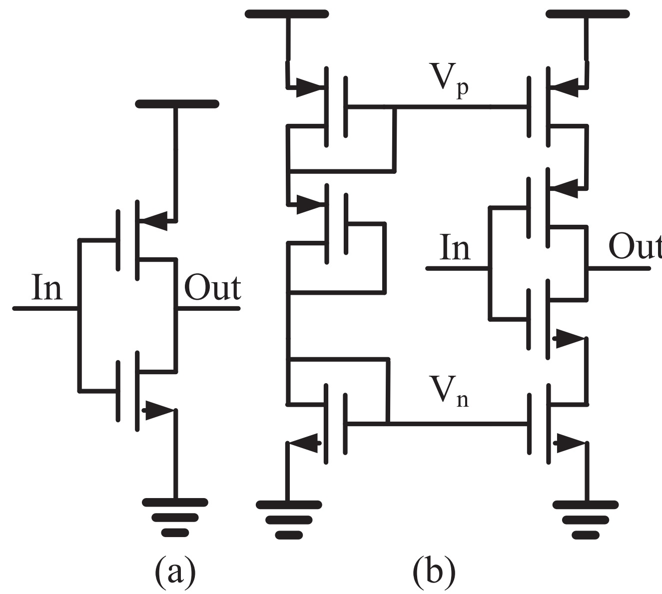

Figure 4.3: *Circuit schematic of (a) a regular inverter, (b) a current starved inverter.*

ture, which in turn reduces the drain saturation current. The reduction in carrier mobility is more prominent than the reduction in threshold voltage in the super-threshold operation region. Consequently, the delay of a regular inverter gate exhibits an overall positive temperature dependence relation.

4.3 Proposed Temperature Coefficient Compensated Hybrid Inverter based RO PUF

To counteract the positive temperature dependence of regular inverters, a hybrid RO PUF constructed with positive temperature coefficient regular inverter stages and negative temperature coefficient current starved inverter stages is proposed here.

4.3.1 Temperature Coefficient of Current Starved Inverter

As opposed to the regular inverter circuit shown in Fig. 4.3(a), the MOSFET transistors of the current starved inverter circuit shown in Fig. 4.3(b) can be

made to operate in the sub-threshold region by adjusting the bias voltages V_p and V_n. The maximum drain current can be expressed as [70]:

$$I_{D,sub} = \mu C_{OX}\frac{W}{L}(\frac{\kappa_B T}{q})^2(n-1)e^{\frac{q(V_{GS}-V_t)}{n\kappa_B T}}(1-e^{-\frac{qV_D}{\kappa_B T}}) \tag{4.6}$$

$$n = \frac{1+(C_S+C_{it})}{C_{OX}} \tag{4.7}$$

where κ_B is a temperature independent coefficient. C_S, C_{it} and C_{ox} are the capacitance associated with the semiconductor, fast surface states and gate oxide, respectively. The temperature coefficient of the switching current TCC_{sub} can be formulated as [69]:

$$\begin{aligned} TCC_{sub} &= \frac{1}{I_{D,sub}}\frac{dI_{D,sub}}{dT} \\ &= \frac{1}{u}\frac{d\mu}{dT} + \frac{2}{T} - \frac{q}{n\kappa_B T}(\frac{dV_t}{dT} + \frac{V_{GS}-V_t}{T}) \end{aligned} \tag{4.8}$$

Since the decrease of the threshold voltage dominates the decrease of charge carrier mobility with increasing temperature in the subthreshold region, the value of TCC_{sub} is negative [69]. As a result, the delay of a current starved inverter stage decreases with increasing temperature.

4.3.2 Temperature Coefficient of Hybrid RO

Based on the above analysis, the positive temperature coefficient effect of the current starved inverters can be used to compensate for the negative temperature coefficient effect of the regular inverters of the classic RO-PUF. The simulation results of the relative frequency deviations (taking the frequency at $27°C$ as the reference frequency) with temperature for the three different types (i.e., regular, current starved and hybrid) of 9-stage RO in GF 65nm CMOS technology are shown in Fig. 4.4. The hybrid RO is made up of 5 regular inverters and 4 current starved inverters. The results show that the frequency of hybrid RO is least

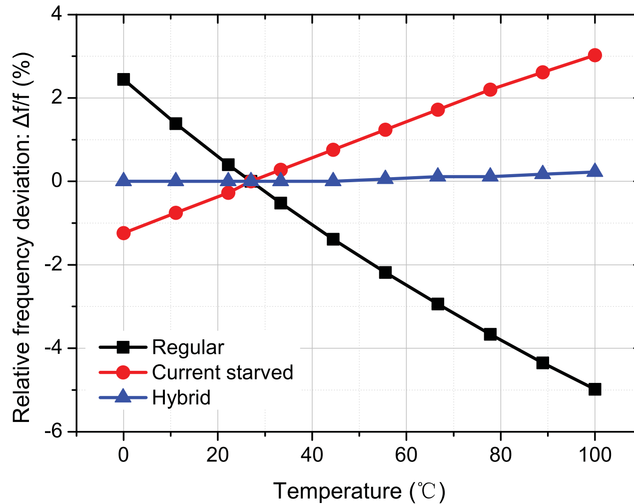

Figure 4.4: *Relative frequency deviations against temperature for three ROs with 9 stages of regular, current starved and hybrid inverters, respectively.*

Table 4.1: *Comparison of the 9-stage regular, current starved and hybrid ROs.*

Type of RO	Regular	Current starved	Hybrid
Power (μW)	58.07	20.75	23.93
Transistor number	20	36	28
Temperature sensitivity kHz/°C	−3160	620	40

susceptible to temperature variations. The characteristics of these three types of 9-stage ROs are summarized in Table 4.1. The temperature sensitivity is defined as the output frequency deviation per degree Celsius. The results show that the hybrid RO has a much lower power consumption and temperature sensitivity than the regular RO. The area occupied by the 8 additional bias transistors is negligible as their diffusion regions can be shared in the layout.

Specifically, the sizing of the regular inverters and current starved inverters can affect the stability under temperature variations. To show the effect of gate sizing on each type of inverter, if the width W of only the regular inverters of the hybrid RO is scaled by a factor α, which is equivalent to multiplying their currents i by α in (4.3) and (4.6). The simulated RO frequency temperature sensitivity (FTS) in 65nm CMOS technology is shown in Fig. 4.5. The slope of the frequency deviation of the hybrid RO is more negative as α increases, making its frequency-temperature

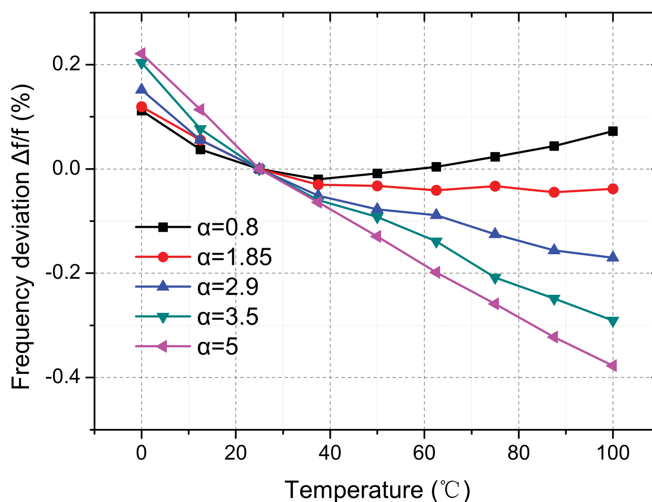

Figure 4.5: *Effect of regular inverter scaling on the frequency deviation of the hybrid RO.*

characteristic inclines towards a RO built solely from regular inverters.

If only the widths of the current starved inverters are scaled, the simulation results in Fig. 4.6 show that the frequency deviation slope becomes more positive as α increases, making its frequency-temperature characteristic inclines towards a RO built solely from current starved inverters.

Only when both the regular and current starved inverters are scaled at the same time can the frequency deviation be tuned to a negligibly small value over a broad range of temperature. This effect is shown in Fig. 4.7.

The principle underpinning the sizing strategy is briefly explained below. The gate length L is fixed at the minimum feature size of the process technology (i.e., 65nm in the design) and the gate width W is sized to make the hybrid RO less sensitive to the temperature variations. For a hybrid RO with $m+1$ regular inverter stages (the two-input NAND gate with an enable input is regarded as a regular inverter) and m current starved inverter stages, the total delay is given by:

$$t_{RO} = (m+1)\, t_r + mt_c \tag{4.9}$$

where t_r and t_c are the delays of regular inverter and current starved inverter,

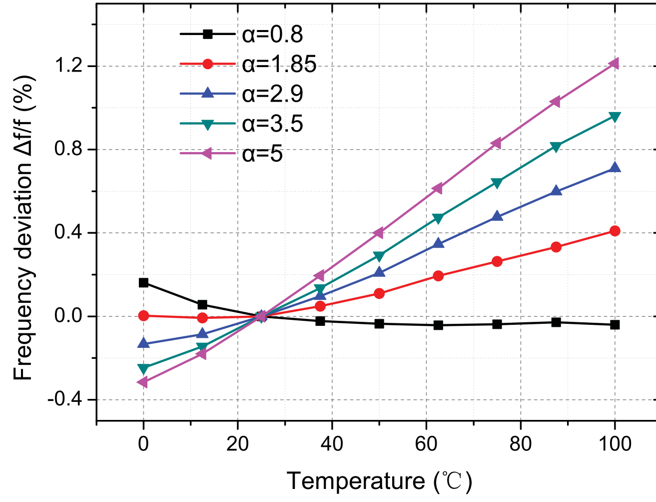

Figure 4.6: *Effect of regular inverter scaling on the frequency deviation of the hybrid RO.*

respectively.

The oscillation frequency is given by:

$$f = \frac{1}{2t_{RO}} = \frac{1}{2\left[(m+1)\,t_r + mt_c\right]} \tag{4.10}$$

The hybrid RO's frequency temperature sensitivity (FTS) can be derived by

$$FTS = \frac{\partial f}{\partial T} = \frac{\partial\left(\frac{1}{2t_{RO}}\right)}{\partial T} = -\frac{1}{2t_{RO}^2}\frac{\partial t_{RO}}{\partial T} \tag{4.11}$$

Substitute (4.9) into (4.11):

$$FTS = -\frac{1}{2t_{RO}^2}\left[(m+1)\frac{\partial t_r}{\partial T} + m\frac{\partial t_c}{\partial T}\right] \tag{4.12}$$

From Equation (4.1), FTS can be derived as:

$$FTS = \frac{1}{2((m+1)\,t_r + mt_c)^2}\left[\frac{1}{t_r^2}(m+1)\,C_r V_{dd}\frac{\partial i_r}{\partial T} + \frac{1}{i_c^2} m C_c V_{dd}\frac{\partial i_c}{\partial T}\right] \tag{4.13}$$

where C_r and C_c denote the load capacitances of regular inverter and current starved inverter, respectively.

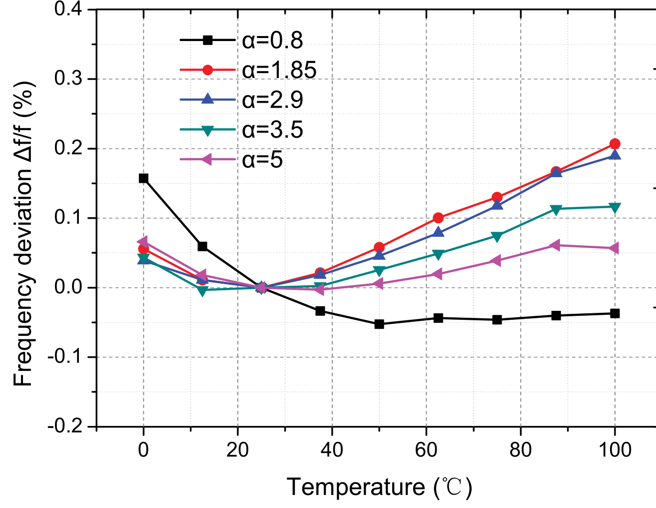

Figure 4.7: *Effect of combined regular and current starved inverter scaling on the frequency deviation of the hybrid RO.*

In general, the load capacitance for each stage can be divided into two parts: the internal capacitance C_{int} and the external capacitance C_{ext}. C_{int} is proportional to the gate width W. For the proposed design, C_{ext} is dominated by the input capacitance of the transmission gate (MUX) and can be treated as a constant. Typically, C_{int} is much smaller than C_{ext} and can be ignored for simplicity.

Let $a = (m+1)C_r V_{dd}$ and $b = mC_c V_{dd}$. By substituting TCC and TCC_{sub} in (4.2) and (4.6) into (4.13), FTS can be rewritten as:

$$FTS = \frac{1}{2}\left(\frac{ai_c^2 i_r \cdot TCC + bi_r^2 i_c \cdot TCC_{sub}}{a^2 i_c^2 + 2abi_r i_c + b^2 i_r^2}\right) \tag{4.14}$$

Based on the analysis in Sections 4.2 and 4.3 above, TCC is positive and TCC_{sub} is negative. As all other parameters in (4.14) are positive, it is possible to optimize the widths of the two types of inverters to make $FTS \approx 0$.

4.3.3 Architecture and Operation of Proposed Hybrid RO

The architecture of the proposed $(n+1)$-stage (n is even) hybrid RO PUF consists of n LFSR counter, one bidirectional counter, a two-input NAND gate, $\frac{n}{2}$ regular

inverter stages and $\frac{n}{2}$ current starved inverter stages. Fig. 4.8 shows the CMOS circuit implementation of a 9-stage (i.e., $n = 8$) hybrid RO PUF. The NAND gate is equivalent to a regular inverter when EN is asserted. Together with 4 regular inverter stages and 4 current starved inverter stages, they make up a 9-stage RO. Two multiplexors are placed in each inverter stage: one at the gate outputs, the other at the gate inputs. The multiplexors are realized with transmission gates to reduce their delay and transistor count. It is difficult to model the temperature dependency of the multiplexors as the transistors can operate in several regions [71]. What is more feasible is to increase their transistors' width to make their contribution to the timing variation of the RO negligible relative to the inverters. In each stage, these two multiplexors share the same select signal. The select signal is one of the 8 bits of the challenge signal C. This select signal picks up either the upper or the lower inverter output of each stage. All the 8 bits of the challenge are connected to the outputs of the 8-bit LFSR counter. From this schematic, 2^8 different possible combinations of inverter path for the RO can be selected. The bidirectional counter reads the two successive ROs' frequency outputs. These two values are then subtracted by alternating the counting direction. The frequency difference for the two ROs is stored in the counter.

Each response bit of this PUF is generated by the comparison of two selected ROs' frequencies. Fig. 4.9 shows the timing diagram of the operation of the proposed PUF. First, the LFSR counter is initialized with the 8-bit challenge C_A through $Serial_In$ port by asserting the $Mode$ signal. The enable line EN of the PUF is set to low initially to disable the RO. After a small delay for the 8-bit challenge C_A from the LFSR counter to be stable, EN is pulled high and the bidirectional counter is reset by the rising edge of Rst. The selected RO_A starts to "ring" and its output is connected to the $Clock$ of the bidirectional counter. The bidirectional counter is configured as an up counter by setting $Up/\overline{down}$ signal high. The counter value after a specific time t, which is determined by the frequency f_A of RO_A, is registered. The method for determining the optimum measurement time t is reported in [72]. Then, EN is set to low. The bidirectional counter is then configured as a down counter by setting $Up/\overline{down}$ signal

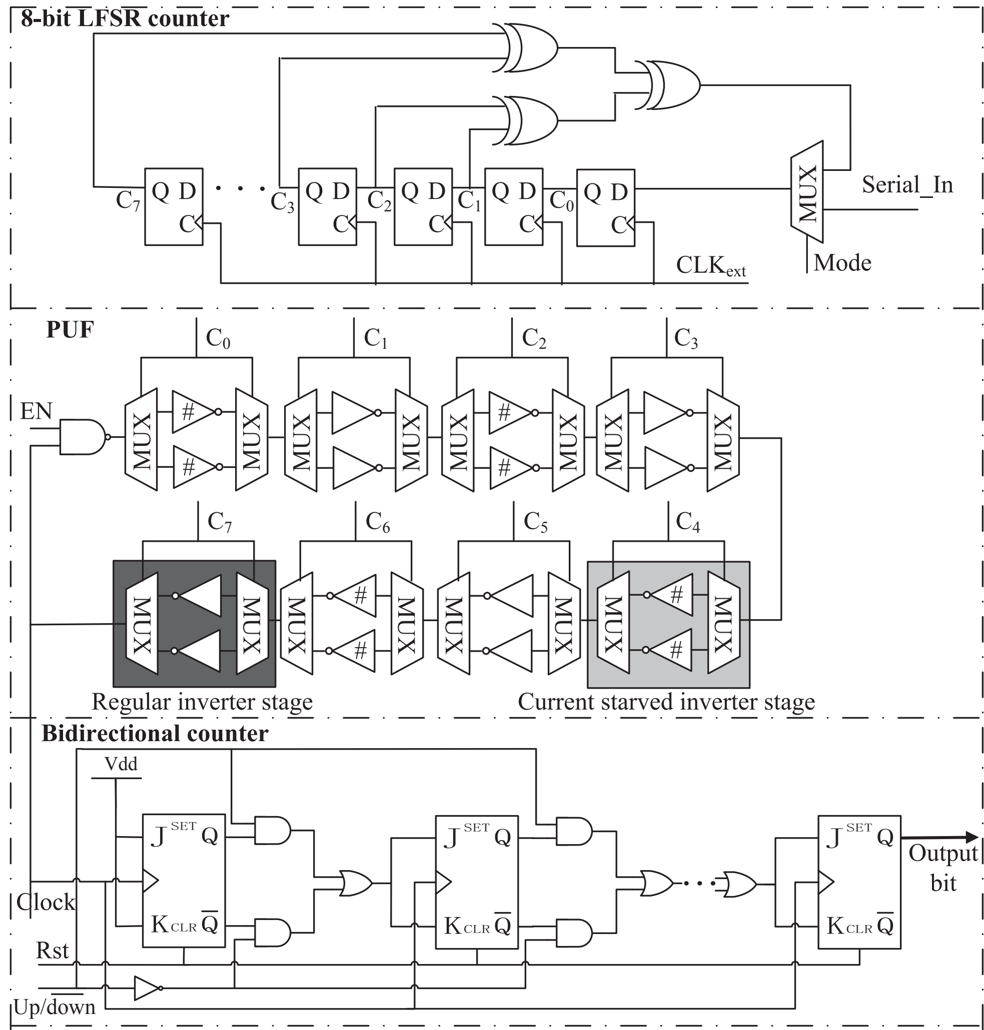

Figure 4.8: *Architecture of the proposed hybrid RO PUF.*

low. Next, a shadow challenge C_B is generated from the LFSR counter after N_{clk} ($N_{clk} < 2^8$) clock cycles. With a well-chosen feedback function, the LFSR counter will produce a pseudo random sequence with a very long cycle and $C_B \neq C_A$. After C_B is stable, EN is set to high. With the same counting time t, the value stored in the counter is directly proportional to the frequency difference of the two selected ROs, i.e., $\Delta f = f_A - f_B$. The most significant bit (MSB) of the counter is the output bit of the PUF. The length of the bidirectional counter has to be large enough to discriminate the two successive RO's frequencies. The same input challenge can generate a different response with a different N_{clk}. This structure can be regarded as a logically reconfigurable PUF [73]. It allows the CRP behav-

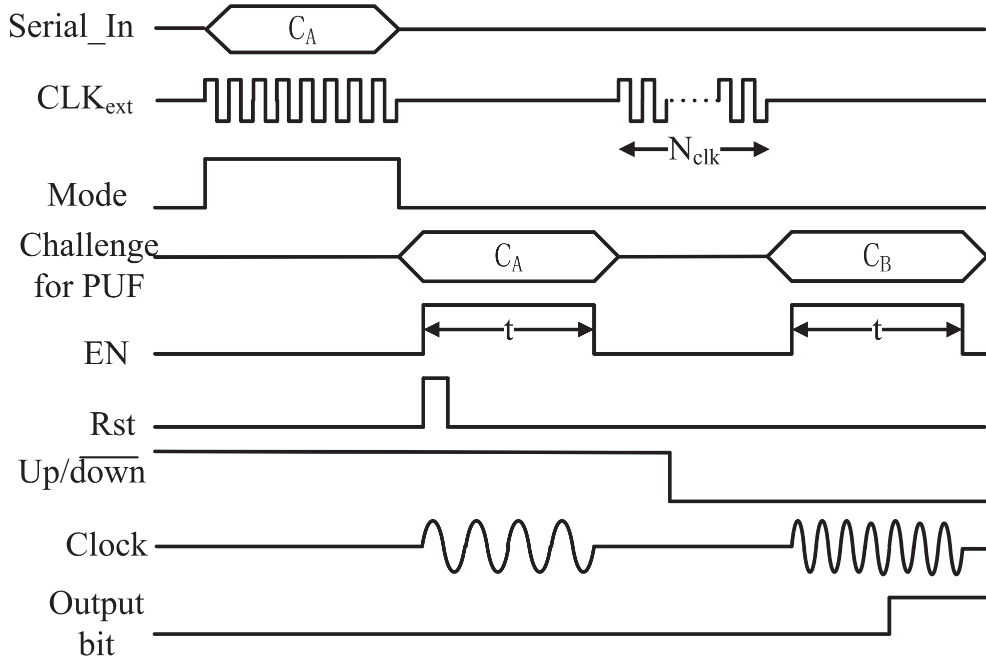

Figure 4.9: *Timing diagram of the operations of the proposed hybrid RO PUF.*

ior to be changed by changing N_{clk} without physically replacing or modifying the underlying PUF. Such logical reconfigurability makes the PUF more resilient to the machine learning attack, which will be discussed in the next section.

4.4 Quality and Security Analysis of Proposed Hybrid RO PUF

The uniqueness, reliability, unpredictability and resilience against modeling and side-channel attacks, which are important figures of merit of PUF, are analyzed in this section.

4.4.1 Uniqueness of Proposed Hybrid RO PUF

To validate the uniqueness of the CRPs, the transistor-level simulations of inter-die variations are carried out by Cadence Virtuoso Spectre using the process design kit (PDK) of GF 65nm 1.2V CMOS technology. Monte Carlo simulation method [13] is adopted to introduce randomly sampled device parameter variations from a

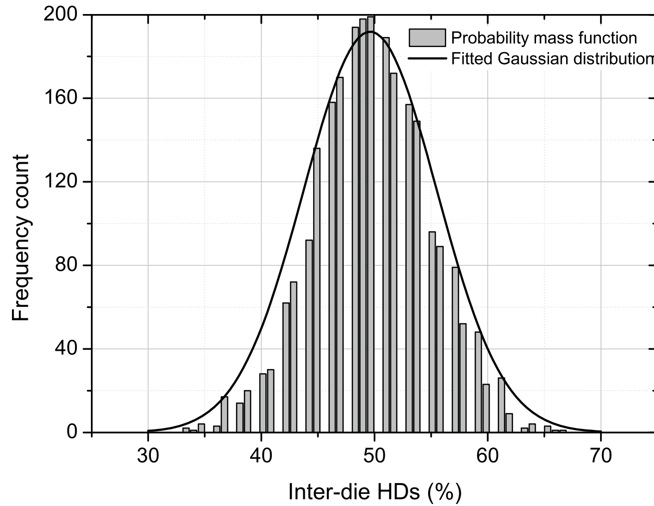

Figure 4.10: *Frequency distribution of the simulated inter-die HDs.*

normal distribution. To simulate a number of CRPs in each iteration of the Monte Carlo simulation, a unique set of variations is applied to a PUF instance in each iteration. The PDK provided by the foundry contains the variation profile of key parameters in the GF 65nm CMOS technology which can well represent the ranges of parameter values of the physical design due to the manufacturing process variations. The simulation results of the proposed 9-stage hybrid RO PUF are then collected and processed by the MATLAB scripts. An 11-bit bidirectional counter is employed to differentiate the pair of RO's frequencies. The nominal working frequency of the 9-stage PUF is $200MHz$. The counting time for each RO is $4\mu s$.

Based on the CRPs collected from 50 PUF instances, with 120 CRPs generated for each instance, the frequency distribution of the inter-die HDs is obtained in Fig. 4.10. The uniqueness of these 50 instances is calculated to be 49.62%. The best fit Gaussian curve to the histogram diagram plotted in Fig. 4.10 has a mean of $\mu = 49.62\%$ and a standard deviation of $\sigma = 5.86\%$.

4.4.2 Reliability of the Proposed Hybrid RO PUF

The reliability against the ambient noise is calculated from 8000 CRPs generated from 50 PUF instances simulated with 10 different sets of random transient noises

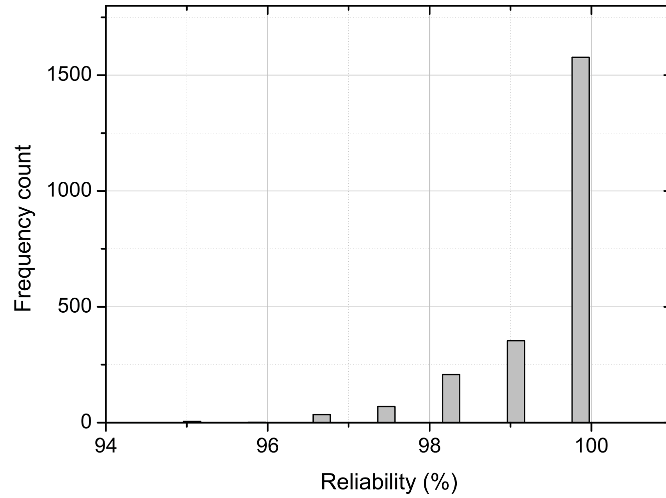

Figure 4.11: *Frequency distribution of the simulated PUF response reliability with ambient noise.*

by activating the transient noise option of Spectre simulator. The Spectre transient noise parameters used in the simulation are: $f_{max} = 10GHz$, $f_{min} = 1kHz$ and $scale = 1$. Fig. 4.11 shows the frequency distribution of response reliability in the presence of ambient noise. The reliability ranges from 93.33% to 100%, with an average reliability of 99.57% over all the instances.

To evaluate the proposed PUF response reliability against temperature variations, the output frequencies of the hybrid RO at different temperatures are simulated for the fast (F), slow (S) and typical (T) corners of the GF 65nm CMOS process technology. The frequencies of the hybrid RO are plotted against the operating temperature in Fig. 4.12. The results show that the output frequency of the hybrid RO has low temperature sensitivity in each corner. The largest frequency deviation among the five corners is 4.22% at FS corner. The inverters are sized to desensitize its temperature variations at TT corner so that the sensitivity of the RO frequency at this corner approaches zero, i.e., it is completely insensitive to the temperature. This sizing appears to have impacted the temperature coefficient of the oscillator more when the NMOS is at the fast corner, and the temperature coefficient of the oscillator is dominated by the regular inverter stage when the

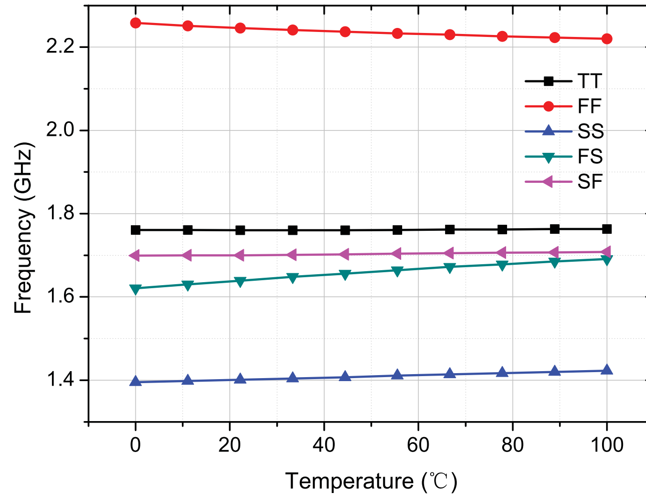

Figure 4.12: *Corner simulation of oscillation frequencies of hybrid RO against the temperature variation.*

PMOS is fast and by the current starved inverter stage when the PMOS is slow.

50 PUF instances at 12 different temperatures from $0°C$ to $100°C$ are also simulated. The 1000 CRPs generated at $27°C$ are used as the reference to calculate the reliability of the proposed hybrid RO PUF against temperature variations. The reliabilities computed from the CRPs of all instances of the proposed hybrid RO PUF and the classic Suh's RO PUF [12] at different temperatures are shown in Fig. 4.13. The average reliability of all simulations at different temperatures is found to be 99.14% for the proposed hybrid RO PUF and 98.24% for the Suh's RO PUF. The CRPs of the proposed hybrid RO PUF are more reliable due to its more stable oscillation frequency against temperature variations.

4.4.3 Unpredictability of the Proposed Hybrid RO PUF

The unpredictability measures how difficult the attacker can predict the CRPs of a PUF. The CRPs of a good PUF are assumed to be unpredictable by any adversaries from a subset of CRPs in their possession. This requires the correlation between any two CRPs generated from the PUF to be acceptably small. For example, in the classic RO PUF design, if RO_1 is faster than RO_2 (which

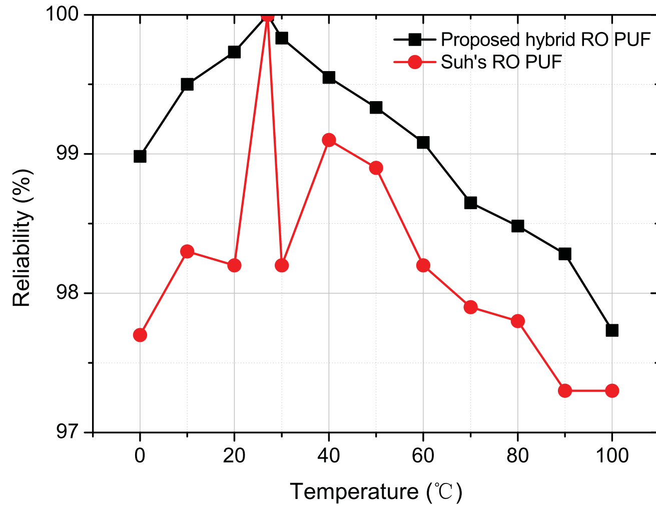

Figure 4.13: *The simulated CRP reliability at different temperatures for the classic Suh's [12] and proposed RO PUF.*

produces a response bit of 1) and RO_2 is faster than RO_3, the PUF output bit obtained by the comparison of RO_1 and RO_3 can be predicted with certainty to be 1. The unpredictability of a PUF can be estimated by the entropy of its CRPs. The entropy of a discrete random variable X with probabilities $Pr[X = x] = p_x$ is defined as (2.3). However, it is very difficult to directly measure the entropy of a PUF. This is because it requires the exact distribution of its CRPs, which is generally unknown. Fortunately, the maximum entropy can be determined by the number of independent output bits of a PUF and used as an estimate of the PUF's unpredictability [12]. For a RO PUF, the number of independent bits that can be generated by the circuit is a function of N_{osc}, where N_{osc} is the number of oscillators. There are $N_{osc}!$ different orderings of ROs based on their frequencies. If the orderings are equally likely, the entropy corresponding to the number of independent bits will be $log_2(N_{osc}!)$ bits. For comparison, the number of independent bits generated by a RO PUF is expressed in terms of the number of transistors required to realize the PUF circuit. Therefore, the number of independent bits is $\log_2(\frac{M}{2N}!)$ for the classic RO PUF if each RO has N inverter stages and M is the total number of transistors. For the proposed hybrid RO PUF, the current

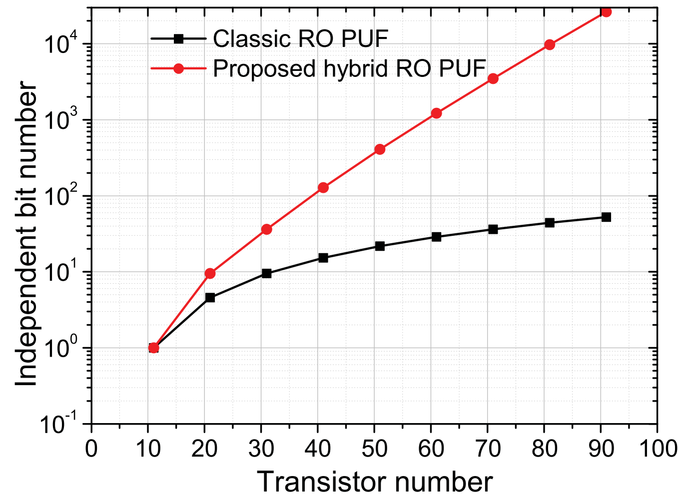

Figure 4.14: *The number of independent bits that can be produced by the classic Suh's RO PUF [12] and the proposed hybrid RO PUF with the same number of transistors.*

starve stage consists of 18 transistors while the regular inverter stage consists of 14 transistors, and the multiplexors are implemented by transmission gates. On average, 16 transistors are used in each inverter stage. Hence, the proposed design can produce $\log_2(2^{\frac{M}{16}}!)$ independent bits with M transistors. Fig. 4.14 compares the number of independent bits that can be produced by the Suh's RO PUF (assuming $N = 5$) and the proposed hybrid RO PUF implemented with the same number of transistors. Based on the larger number of independent bits generated with the same amount of hardware resources, the CRPs of the proposed hybrid RO PUF are more difficult to be predicted.

4.4.4 Attack Analysis

There are two popular methods to predict the CRPs of a PUF. They are modeling attack [74, 75] and side-channel attack [15, 76].

Modeling attack assumes that the adversary can create a model of the target PUF given a number of CRPs. With this model, other CRPs can be predicted. In this chapter, a class of modeling attacks based on the support vector machine

(SVM) classifier is introduced. SVM is a supervised learning model for data analysis and pattern recognition. For binary classification of data, the SVM finds a hyperplane to separate the 0 and 1 responses with a maximum margin. To predict the CRPs with SVM, the attackers need to model the CRP generation accurately. Without considering the reconfigurability, N_{clk} for the LFSR counter is assumed to be a known constant. An additive delay model for the proposed PUF structure can be constructed as follows.

The response corresponding to the challenge C can be expressed as:

$$R = \begin{cases} 1 & \delta(n+1) > \delta'(n+1) \\ -1 & \delta(n+1) < \delta'(n+1) \end{cases}$$

where $\delta(n+1)$ and $\delta'(n+1)$ are the signal delays from the NAND gate input to the output of the last (i.e., the $(n+1)$-th) inverter stage of the hybrid RO in Fig. 4.8 upon the application of the challenge C and the shadow challenge C' after N_{clk} cycles, respectively. These two delays are then written as:

$$\delta(i) = \frac{1+C_i}{2}p_i + \frac{1-C_i}{2}q_i + \delta(i-1) \tag{4.15}$$

$$\delta'(i) = \frac{1+C'_i}{2}p_i + \frac{1-C'_i}{2}q_i + \delta'(i-1) \tag{4.16}$$

where p_i and q_i, $i = 1, 2, \cdots, n+1$, are respectively the top and bottom inverter delays at the i-th inverter stage of the RO, and $C_i, C'_i \in \{-1, 1\}$.

Let $\Delta(i)$ denote the difference between $\delta(i)$ and $\delta'(i)$. Subtracting (4.15) from (4.16):

$$\Delta(i) = \frac{p_i - q_i}{2}(C_i - C'_i) + \Delta(i-1) \tag{4.17}$$

$$\Delta(i) = \frac{p_i - q_i}{2}(C_i - C'_i) + \frac{p_{i-1} - q_{i-1}}{2}(C_{i-1} - C'_{i-1}) \cdots + \Delta(0) \tag{4.18}$$

where $\Delta(0) = 0$. The final delay difference $\Delta(n+1)$ can be represented as an

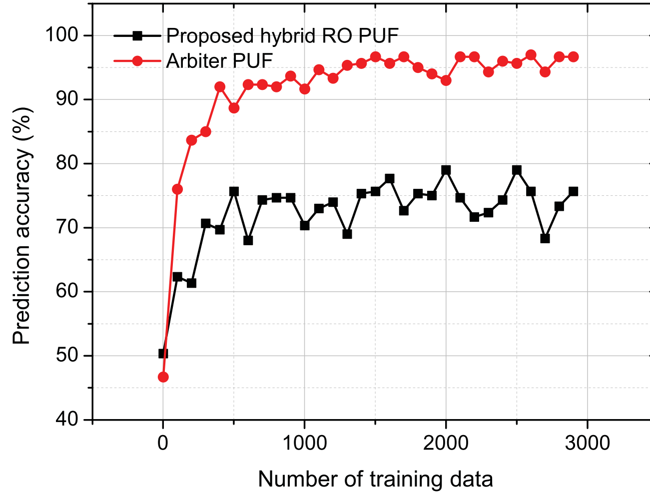

Figure 4.15: *Prediction accuracy by SVM for 64-bit arbiter PUF [13] and the proposed 64-bit hybrid RO PUF.*

inner product:

$$\Delta(n+1) =< \overrightarrow{w}, \overrightarrow{x} > \tag{4.19}$$

where $\overrightarrow{w} = \frac{1}{2}((p_0 - q_0), \cdots, (p_{n+1} - q_{n+1}))$ and $\overrightarrow{x} = ((C_0 - C'_0), \cdots, (C_{n+1} - C'_{n+1}))$.

In this way, a separating hyperplane in the space of all feature vectors $\overrightarrow{x}$ can be determined by the SVM. However, if N_{clk} is not fixed but randomly reconfigurable by the user, $\overrightarrow{x}$ becomes unpredictable. Fig. 4.15 shows the prediction results for a 64-bit arbiter PUF [13] and the 64-bit proposed hybrid RO PUF using the tool SVM^{light} [77]. The prediction accuracy is more than 90% with only about 400 training CRPs for the arbiter PUF. The predictability of the CRPs generated by the proposed PUF is much lower. It turns out that the predication accuracy of the SVM for the proposed PUF response converges to around 78% even with very large training set size of several thousand CRPs.

A side-channel attack is an attack based on measurements made from the physical implementation of a system. The Electro-Magnetic (EM) leak has been successfully utilized to break the RO PUFs [15]. The analysis is based on the study and comparison of the frequency spectrum of the detectable EM emanations for

the working RO. According to Friis transmission equation [78]:

$$P_r = G_t G_r (\frac{\lambda}{4\pi R})^2 P_t \tag{4.20}$$

where G_t and G_r are the antenna gains (with respect to an isotropic radiator) of the transmitting and receiving antennas respectively, λ is the wavelength, R is the distance from the detector probe to the device, P_r is detectable magnitude of the EM radiation and P_t is the device's working power consumption.

The proposed hybrid RO PUF has lower power consumption over the classic RO PUF. Since P_r is proportional to P_t, it will have a lower magnitude of EM radiation. In the next section, measurement results of the physical implementation of the proposed hybrid RO PUF will be presented to corroborate the analysis.

4.5 Experimental Result

The prototype IC of the proposed 9-stage hybrid RO PUF has been implemented in GF 65nm CMOS process. The microphotograph of the fabricated chip is shown in Fig. 4.16. The LFSR counter is not included. The active area of the proposed PUF is only $5 \times 50\mu m^2$, which is even smaller than a digital pad of $50 \times 150\mu m^2$. Five dice are packaged and tested. The setup of the probe station for the post-silicon test is shown in Fig. 4.17, where Agilent oscilloscope with 1GS/s sampling rate is used to capture the output frequencies of the RO and the responses of the PUF. The control signals and the LFSR counter values are generated with a Xilinx Virtex-II Pro FPGA board externally. Fig. 4.18 shows the measured frequency distribution of the hybrid RO's output frequencies in one sample chip.

10000 CRPs generated by the PUFs have been collected from the five dice to evaluate the uniqueness. Fig. 4.19 shows the measured frequency distribution of the inter-die HDs. The uniqueness calculated from the inter-die HD of the proposed PUF is 50.42%, which is very close to the ideal value of 50%. The reliability is measured using 1000 CRPs generated by the PUF under varying supply voltages and temperatures. Fig. 4.20(a) shows the reliability of the fabricated hybrid

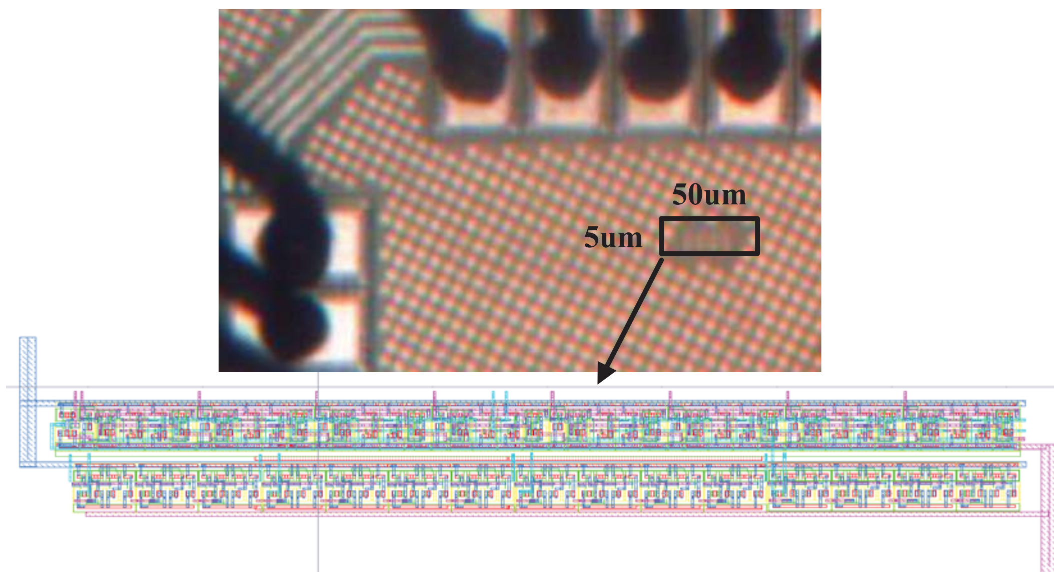

Figure 4.16: *The microphotograph of the proposed hybrid RO PUF chip.*

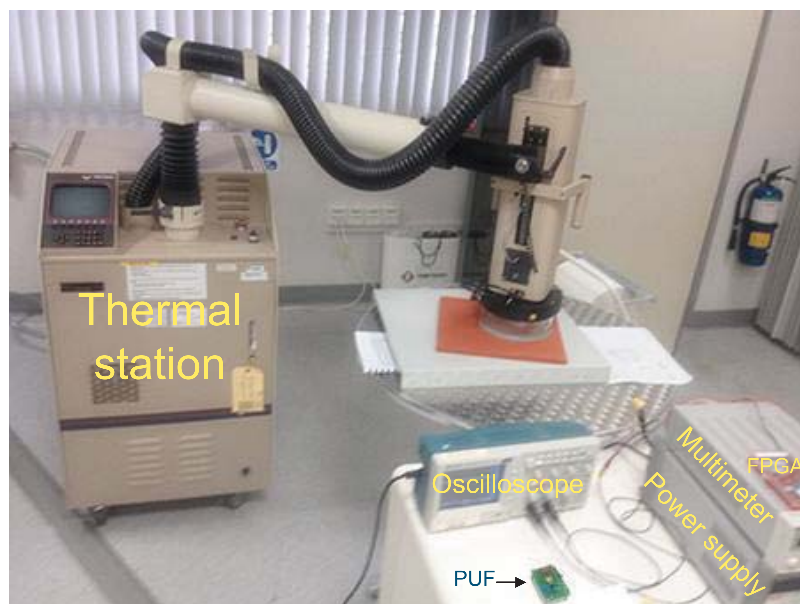

Figure 4.17: *The probe station for the testing of the sample chips.*

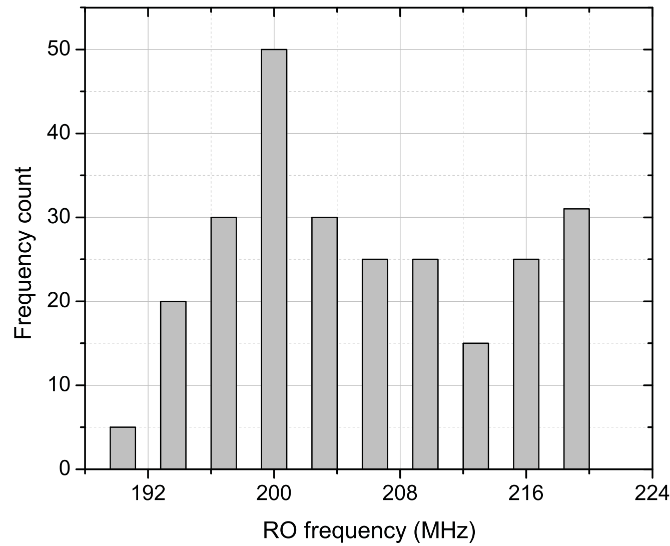

Figure 4.18: *The distribution of hybrid RO's oscillation frequency of one sample chip.*

RO PUF against the voltage variations. The nominal power supply for the GF 65nm CMOS technology is $1.2V$ and the CRPs collected under this supply voltage are used as the reference. The supply voltage is varied from $1V$ to $1.4V$. The average reliability of the CRPs obtained from the five test chips is 87.87%. The worst reliability within the range of $\pm 2\% V_{DD}$ is 98.26%. The reliability of the CRPs generated by the hybrid RO PUF for different operating temperature is also measured by the thermal station shown in Fig. 4.17. The working temperature is varied from $-40°C$ to $120°C$. The CRPs collected under $27°C$ are used as the reference. Fig. 4.20(b) shows the average reliability of the five hybrid RO PUF chips under different operating temperatures. The average reliability measured from the hybrid RO PUF chips is as high as 99.84% and the worst-case reliability is 97.28% at $-40°C$. The results attest that the frequency of hybrid RO is much less susceptible to temperature fluctuation.

In the classic RO PUF, the RO consumes the most power, as it has the greatest switching activities. In the proposed design, the current starved inverters are biased in the subthreshold region, which reduces the power consumption of the

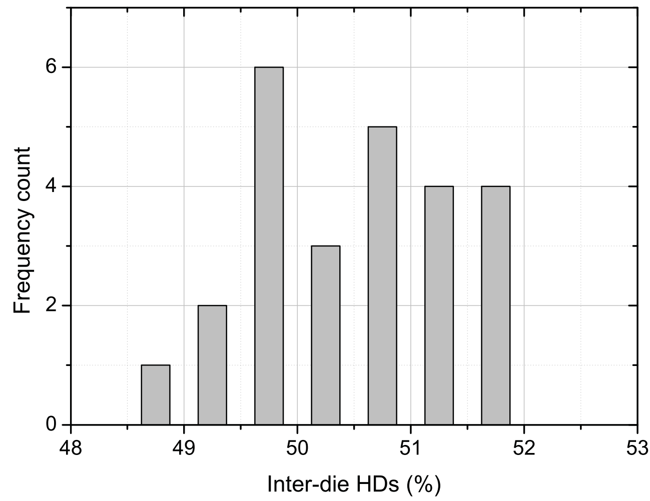

Figure 4.19: *Inter-die HD distribution measured from the hybrid RO PUF chips.*

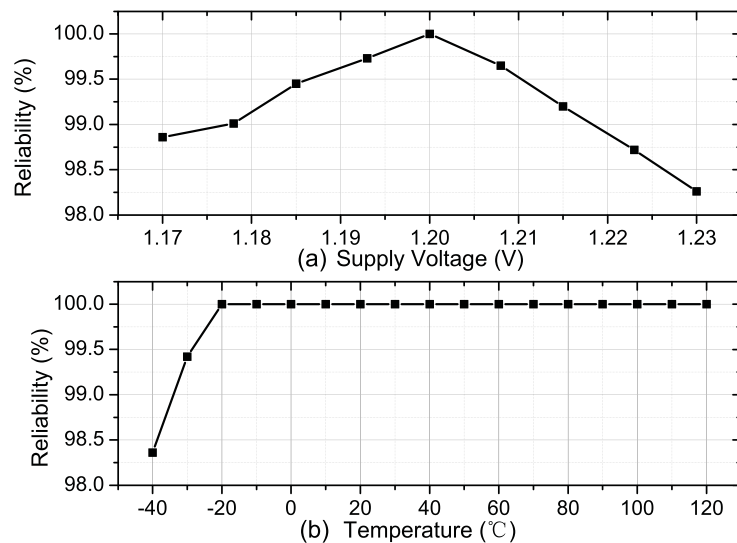

Figure 4.20: *The measured average reliability of hybrid RO PUF against (a) voltage variations, (b) temperature variations.*

Table 4.2: *Comparison of power consumption per CRP of the proposed hybrid RO PUF with other temperature invariant RO PUFs.*

Architecture	Technology	Power/CRP
Optimized supply voltage	$45nm$	$82\mu W$
Negative TCR feedback resistance	$45nm$	$98\mu W$
Phase Differential	$45nm$	$80\mu W$
Proposed	$65nm$	$\mathbf{32.3\mu W}$

RO. Besides, only one “RO” is active (by selecting one of the two inverters in each stage of the RO) at any time. A power analysis is carried out by applying 1000 random challenges to a prototype PUF IC. The power consumption is averaged over all the challenges. The average power consumption measured for each CRP generated by the PUF is $32.3\mu W$ at a power supply voltage of 1.2V and an operating frequency of $230MHz$. The actual power consumption per CRP for the proposed hybrid RO PUF are compared against the simulated power consumptions of other temperature invariant RO PUFs excerpted from [66] in Table 4.2. It should be noted that the power per CRP values of other RO PUFs shown in Table 4.2 are based on pre-layout simulation of a more advanced technology and operating at a slightly lower supply voltage. Even then, the physically measured power consumption per CRP of the chip is less than half of theirs, thanks to the current starved inverter stages of the RO. In order to study the relationship between the power consumption and the working frequency, the same structure of hybrid RO PUF is also fabricated using the same CMOS process but with V_p and V_n of all current starved inverters connected to two external pins in order to adjust the RO's frequency. The measured power consumption is plotted against the RO's frequency (in logarithmic scale) in Fig. 4.21. The minimum measurable oscillation frequency is $100KHz$ and the power consumption at this RO's frequency is only $5.16\mu W$. The ultra-low power consumption makes the proposed hybrid RO PUF attractive for security application in mobile devices.

To validate the resilience of the proposed PUF against EM attack, larger FLS 106 IC scanner is used to capture the EM radiation close to the fabricated chip's surface. Fig. 4.22 illustrates the measured spectrum of the proposed hybrid RO

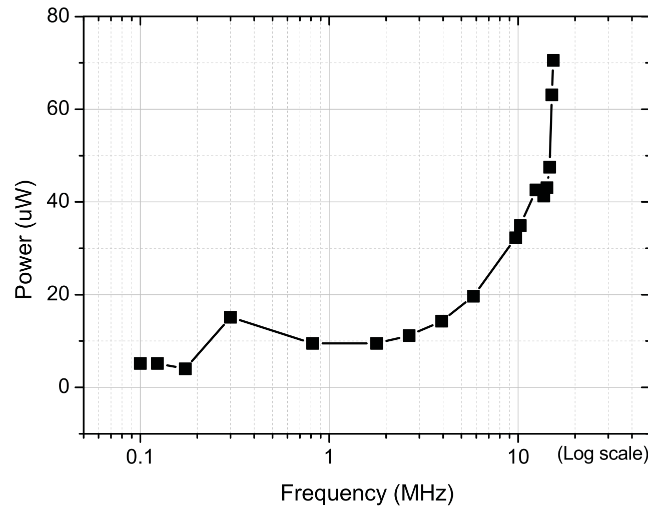

Figure 4.21: *The measured power consumption per CRP of the proposed PUF chip at different RO's frequency.*

and the regular RO fabricated in the same chip. It is obviously that the magnitude of EM radiation of the proposed hybrid RO is too small to be distinguished from the noise floor, whereas an EM radiation of $64dB\mu V$ at $278MHz$ is detected from the regular RO. In addition, as the proposed hybrid PUF occupies only a tiny area and has an interleaving structure, it is very difficult to locate the active RO in the chip [79].

A comparison of the qualities and costs of implementation of different PUFs reported in the literature is summarized in Table 4.3. Except the results of RO [12], Arbiter [12] and Bistable ring [80], which are reported based on FPGA implementation, the results of the remaining PUFs are obtained from custom chip implementation. The proposed PUF has great advantages for lightweight application due to its tiny footprint and very low power consumption. Its uniqueness and reliability are also competitive, particularly the thermal stability of its CRP. The fabricated prototype PUF exhibits a measured reliability of 100% over a temperature range of $-20°$ to $120°C$, as depicted earlier in Fig. 4.20(b).

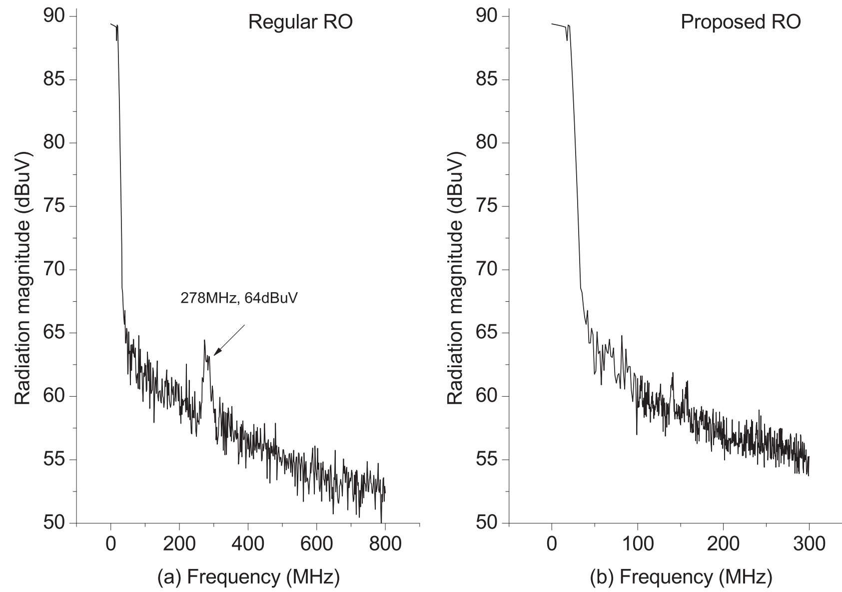

Figure 4.22: *The measured EM radiation from (a) the regular RO, (b) the proposed hybrid RO.*

Table 4.3: *Comparison of the qualities and costs of the proposed PUF with other PUFs.*

PUF	Power (μW)	Technology (nm)	Area (μm^2)	Uniqueness (%)	Worst-case reliability (%)	Reliability conditions
Lofstrom [81]	250	350	23,436	NA	95.00	$1.5 \sim 5V, -25 \sim 125°C$
Arbiter [7, 12]	NA	180	1,470,000	40.00	95.20	$\pm 2\% V_{DD}, 40 \sim 67°C$
RO [12]	NA	90	NA	46.14	99.52	$1.2 \sim 1.08V, 20 \sim 120°C$
SRAM [9]	0.93	130	15,288	64.70	96.96	$0.9 \sim 1.2V$
Bistable ring [80]	NA	NA	NA	50.90	98.70	$-55 \sim 125°C$
This work	**32.3**	65	**250**	**50.42**	97.22	$\pm 2\% V_{DD}, -40 \sim 120°C$

4.6 Summary

A low-cost and reconfigurable RO PUF with improved response stability has been presented. The proposed PUF utilizes the positive temperature coefficient of the current starved inverters to offset the response instability due to the negative temperature coefficient of the regular inverters used in the classic RO PUF. The prototype PUF chip fabricated in GF 65nm CMOS technology consumes only $32.3\mu W$ per CRP at 1.2 V with a working frequency of $230MHz$. The measured CRPs show a nearly perfect average inter-die HD of 50.46% and an average BER of 0.16% with temperature varied from −40°C to 120°C. The analysis shows that with the LFSR counter incorporated to randomize the external challenge, the re-

configurable CRPs offer substantial resistance to the modeling attacks by SVM. The ultra-low power consumption of the current starved inverter stages and the reduced number of inverters also makes it more immune to EM based side-channel attacks. The proposed PUF stands out as an ideal candidate for lightweight security applications by comparing its overall figures of merit with other existing PUFs.

Chapter 5

CMOS Image Sensor based Physical Unclonable Function for Coherent Sensor-level Authentication

5.1 Introduction

Driven by the Internet of Things (IoT) and smartphone industry, the CMOS image sensor market is expected to hit a total value of $10,172 million by 2020 [82]. A noteworthy growth is envisaged from the proliferation of CMOS image sensors into emerging security applications in biometric authentication, reconnaissance and surveillance [83,84]. To prevent attackers from exploiting the image sensing system by inserting the unauthorized nodes, the image sensor itself should be trusted [83]. Recently, phishers have also begun to use images to evade detection by text-based anti-phishing filters. While certified cryptographic protocols and infrastructures have been developed for securing the communication channels [85], they cannot prevent false pretenses from masquerading as trustworthy imaging devices in the electronic communications. This security hole can be closed up by integrating dedicated security functions into the image sensor [86]. If the authentication is assured at the sensor level, the camera and its relatively large software stack would no longer need to be implicitly trusted [86]. Researchers have proposed a few sensor-level authentication schemes to provide the integrity and authenticity of

the image sensors [87–89]. The encryption techniques are performed on-chip to guarantee a real end point security, i.e., security that actually starts at the data source and ends at the data receiver. However, this is very demanding and costly. Another drawback about this method is that the private key used for the encryption is generally stored in a non-volatile memory (NVM), such as EEPROM or polysilicon fuses [87]. Unfortunately, these NVM technologies are often vulnerable to invasive attacks as the secrets have to be preserved instead of generated upon demand, and often reside persistently in a digital form [12].

A physical unclonable function (PUF) is a circuit module that generates chip signatures relying on the uncontrollable and unpredictable process variations. The mapping of challenge and response pairs (CRPs) is unique to each PUF instance. The response of the silicon PUF is usually a binary string generated by applying its corresponding challenge. PUF provides a secure and low-cost solution for key generation, device authentication, counterfeit detection and prevention [12]. The small footprint makes it promising for the cost-sensitive sensor market and remote trusted sensing system. In contrast to the IDs stored in NVM, the signatures produced by the PUF cannot be easily removed, copied or compromised, as the secrets are inherent in the physical structure of the PUF. Any invasive or semi-invasive attack on the chip can easily destroy the original secrets. Many silicon PUFs have been proposed and successfully implemented in secure applications owing to the simplicity of their design and fabrication, as well as their compatibility with modern integrated systems [7, 9, 12, 13, 80, 81, 90, 91].

In this chapter, we proposed a new CMOS image sensor based PUF for on-chip authentication and identification. It exploits the dark signal non-uniformity (DSNU) of the fixed pattern noise (FPN) in a CMOS image sensor to generate a unique and reliable signature. FPN as a whole refers to the variations in the output pixel voltage values, under uniform illumination, due to the device and interconnect mismatches across an image sensor [92]. It consists of two parameters, DSNU and photo response non-uniformity (PRNU) [93]. The former refers to the offset from the average pixel intensity across the array at a specified setting of temperature and integration time in the absence of external illumination, whereas

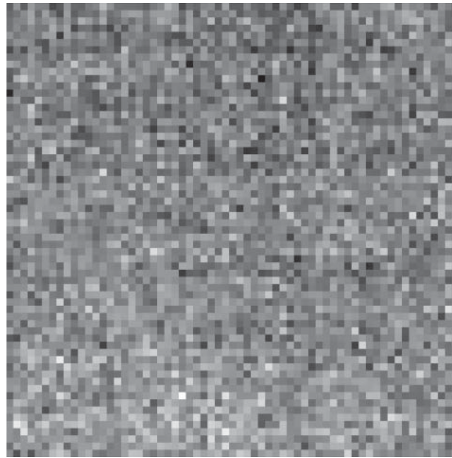

Figure 5.1: *A typical FPN image of a CMOS image sensor [14].*

the latter relates the optical power on a pixel to the electrical signal output. A typical FPN image of a CMOS image sensor taken without illumination (dark) is shown in Fig. 5.1 [14]. Unfortunately, these patterns are susceptible to the changes in the operating environments such as power supply voltage, temperature and ambient noise. A differential readout is proposed to desensitize the impact of environment variations on the PUF response. This readout scheme enables the PUF reliability and demand on security protocol efficiency to be optimized by a thresholding parameter, making it adaptable for use in different applications. It can be easily implemented on existing image sensors without affecting their original functionality and performance. It eliminates the potential security flaws and vulnerability caused by the separation of image sensing and authentication module without the need for additional encryption module or ancillary PUF circuitry.

The rest of the chapter is organized as follows. Related works on sensor-level authentication is reviewed in Section 5.2. In Section 5.3, the design and operations of the proposed PUF are elaborated. The figures of merit and experimental results of the proposed image sensor based PUF are analyzed in Section 5.4. Promising emerging trusted sensing system applications are identified and discussed in Section 5.5. Finally, the summary is given in Section 5.6.

5.2 Related Works

The method to identify a camera by the image sensor's imperfection during manufacturing is not new. Related works can be found in the area of image forensics. Previously, the defective pixels (including hot pixels and dead pixels) are used for camera identification [94]. Advanced methods [95, 96] utilize the pixel non-uniformity noise caused by different sensitivity of pixels to light to characterize the individual cameras. These methods can extract unique property of an image sensor, but they do not fulfill the definition and criteria of a PUF. The lack of a native challenge-response mapping makes them incompatible with modern PUF based security protocols such as [97].

Recently, a sensor PUF was proposed in [98]. It is different from the conventional PUFs in that it includes two inputs: a traditional binary challenge and a physical quantity being sensed. An example of a light level sensor PUF based on the optical system similar to the optical PUFs [37] was illustrated. In [99], the notion of virtual proofs (VP) of the reality is introduced. Its basic idea is to convert certain external physical property into digital data for authentication. The conversion is accomplished by the so called "witnessed objects" without any secret keys or tamper-proof hardware. The generic concept of VP is extended to a camera of p pixels. As each pixel can have s states, there are p^s possible images. The VP of reality is constructed from the response bits generated from an input image sensed with the help of a light sensor PUF similar to that of [98]. A SIMPL camera was patented in [100]. SIMPL, stands for "SIMulation Possible, but Laborious" [101], is a PUF that comes with a digital simulation and prediction model. The response to a challenge can be simulated by the public simulation model with a significantly lower speed than the real-time response of its physical device. Other than exploiting the execution and simulation time gap to achieve the public-key equivalent cryptography, the SIMPL camera is similar to the PUF based cameras of [98] and [99] in other aspects. It also measures the analog signal of the incoming light intensity from the image to generate the digital bits.

Instead of introducing a new and more robust PUF, these methods actually ex-

ploit the new features (the sensing functions) of existing PUFs [99] for sensor-level authentication. For example, the light sensor PUF [98] and VPs of destruction and distance in [99] are built upon an optical system likes the optical PUF [37], and the VP of temperature [99] is designed based on a temperature dependent system similar to the Bistable Ring PUF [80]. A conventional PUF was used in [98] to transform the public challenge into a volatile secret initialization vector for the stream cipher and in [100] to realize the SIMPL based public-key authentication. These ancillary PUFs add extra hardware area, power and operational complexity to the sensor chip of the camera. As the extraneous witness objects are not physically unclonable and are not entropy sources derived from the manufacturing process variations, they do not augment the randomness and reliability of the exploited PUFs. On the contrary, by integrating a physical quantity, e.g., light, temperature, etc., sensed or measured by the original PUF into the challenge-response processing, the reliability of the original PUF can be jeopardized. This is because the extraneous analog input signals are more susceptible to environmental factors, which is more difficult to control than the digital challenge input. More importantly, the sensed physical quantity for authentication can be easily decoupled from the sensor, which makes them vulnerable to sensor decoupling attack [98]. The light senor PUF [98] makes use of non-homogeneous coatings to achieve uniqueness and unclonability, which incur additional processing steps, and are not standard CMOS compatible. The non-uniform optical transmittance of the coating applied on the sensor area can reduce its sensitivity and degrade the image quality. Unfortunately, there is no physical implementation reported for all these camera-based PUFs to assess their costs and performances.

Our proposed sensor PUF is different from the above in that it extracts the digital signature intrinsically from the DSNU of FPN resulting from the manufacturing process variations of CMOS image sensor. As the PUF itself is a monolithic CMOS imager, its device signature can be spontaneously imbedded into the images it took. This offers greater flexibility to use the imaging device for versatile security applications as the camera can be identified reliably independent of lighting conditions. The images taken by the camera can also be directly encrypted

or watermarked by the unique signature of the CMOS imager within the camera system. The proposed PUF is resilient against the sensor decoupling attack as its input challenges are the digital addresses of the pixels, which are not taken from the measurement of any incident illumination intensity. The image sensor can be fabricated by standard CMOS process without additional processing steps. The only modification required from the commercial CMOS image sensor core is a switch transistor for bypassing the correlated double sampling (CDS) circuit. This makes it feasible to be implemented on existing cameras that use CMOS active pixel sensor, and easily integrated with other CMOS functional blocks for digital image processing.

5.3 Circuits and Operations

5.3.1 CMOS Image Sensor Fundamentals

Fig. 5.2 shows a typical architecture of a CMOS image sensor, which consists of a pixel array, vertical and horizontal scanners, and readout circuits. The pixel array is the key region of an image sensor and the imaging quality is mostly determined by the performance of this array. There are two popular types of pixel structure: 3T-APS and 4T-APS.

Fig. 5.3 shows the transistor-level implementations of 3T-APS and 4T-APS [102]. In the 3T-APS, each pixel cell consists of a photodiode (PD), a reset transistor M_{RS}, a select transistor M_{SEL} and a source follower readout transistor M_{SF}. When M_{RS} is turned on, the voltage on the PD is reset to the value:

$$V_{PD} = V_{dd} - V_{th,RS} \tag{5.1}$$

where $V_{th,RS}$ is the threshold voltage of M_{RS}. When M_{RS} is turned off, the PD is electrically floated. The photocurrent I_{ph} due to the incident illumination discharges the PD (omitting the small dark current). After an exposure time t, M_{SEL} is turned on. The output voltage of this pixel is read out. This voltage can be expressed as:

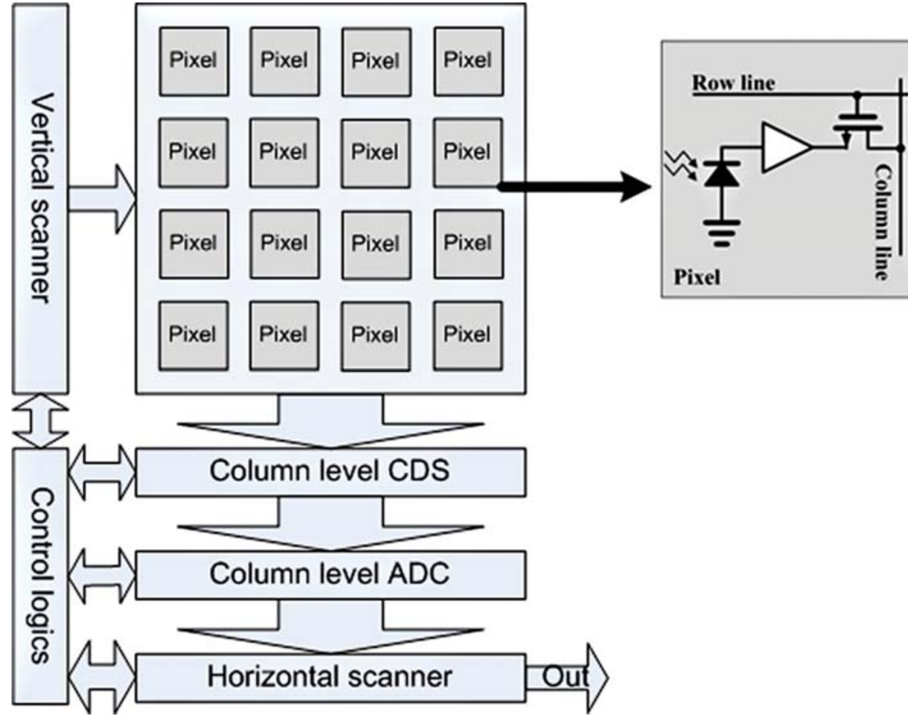

Figure 5.2: *Typical CMOS image sensor architecture.*

$$V_{out} = V_{dd} - V_{th,RS} - V_{th,SF} - \frac{I_{ph} \times t}{C_{PD}} \tag{5.2}$$

where $V_{th,SF}$ and C_{PD} are the threshold voltage of M_{SF} and the PD junction capacitance, respectively. The output voltage V_{out} is linearly proportional to I_{ph}. From (5.2), the variations in pixel output values are mainly caused by the variations in the size and capacitance of the photodiode, as well as the threshold voltages of M_{RS} and M_{FS}.

The 4T-APS is shown in Fig. 5.3(b). It consists of the same components as 3T-APS except for the transfer gate M_{TG} and the pinned PD. The operation of 4T-APS is explained as follows. Assume that there is no accumulated charge in the PD initially. The floating diffusion (FD) is reset by turning on M_{RS}. The voltage on the FD is the same as that expressed in (5.1). It can be read out by turning on M_{SEL}. The photocurrent I_{ph} is accumulated in the PD for an exposure time t. The accumulated charge is transferred to the FD by turning on M_{TG}, followed by turning on M_{SEL} to readout the signal. This output voltage can also be expressed

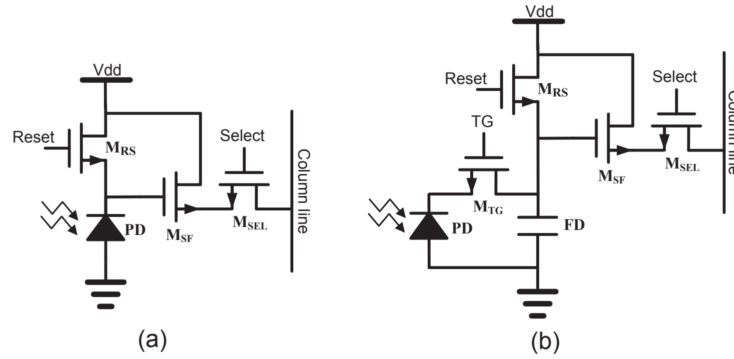

Figure 5.3: *The schematic of (a) 3T-APS pixel, (b) 4T-APS pixel.*

by (5.2), if the charge in the FD is completely depleted. This process is repeated to read the reset voltage and signal voltage successively.

Irrespective of 3T- or 4T-APS, the pixel voltage of the CMOS image sensor is preserved during the readout, which makes it possible to read the pixel voltage value multiple times. As FPN can badly degrade the image qualities, noise cancelation circuits, such as CDS, are employed in the readout circuits [14]. The output of the pixel is measured twice to obtain the reference voltage (i.e., the pixel voltage after reset) and the signal voltage (i.e., the pixel voltage after exposure). The reset noise is reduced by taking the difference between these two voltages. It is noted that the signal voltage can be read out just after the reset voltage is read out from the 4T-APS. This is essential for the CDS operation and it is achieved by separating the charge accumulation region (PD) from the charge readout region (FD). Due to the more effective cancellation of reset noise, 4T-APS provides better image quality but 3T-APS has lower processing cost and more compact pixel layout [102].

5.3.2 Proposed Image Sensor based PUF

The response of the proposed PUF is a binary string extracted from the pixel array. Each response bit is obtained by comparing the reset voltages of two pixels. The output bit is '0' or '1' depending on which reset voltage is larger. The address of the selected pixel pair is determined by a digital input challenge. As the CMOS

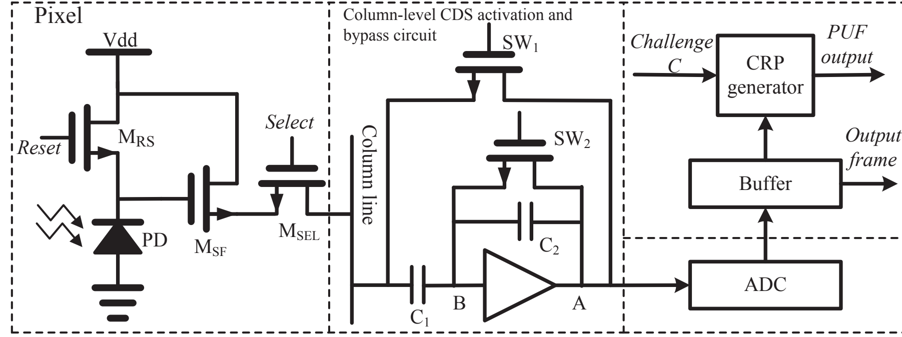

Figure 5.4: *Architecture of the proposed CMOS image sensor based PUF.*

image sensor has non-destructive readout, the original function will not be affected by operating the image sensor in the PUF mode. Fig. 5.4 shows the architecture of the proposed CMOS image sensor based PUF with CDS enabling and disabling switches for regular sensing and PUF modes. Although 3T-APS is illustrated, other pixel structure is equally applicable as long as the random reset voltage of the pixel can be accessed before it is suppressed by the CDS. The CDS can be bypassed in PUF mode by inserting a bypass transistor (i.e., SW_1) in parallel with the CDS circuit. During normal sensing mode, SW_1 is turned off and the reference signal (i.e., reset signal) on the capacitor C_1 is subtracted from the column level CDS [102] to reduce the FPN. The operation of the column level CDS can be explained as follows. In the first phase, the pixel signal value on the capacitor C_1 is sampled. The switch SW_2 is closed to reset the capacitor C_2 and the operational amplifier input offset is sampled. In the second phase, SW_2 is open to reset the pixel. The reset pixel voltage on C_1 is sampled. The output of the amplifier is the difference between the reset and signal values. During the PUF mode, the reset pixel output voltage is directly read out by turning on SW_1. Otherwise, the CDS may bias the FPN and impact the randomness of PUF response. The digitized sensor outputs are buffered and fed into the CRP generator to produce the stable response bits to the applied challenges.

Based on (5.1), the pixel output voltage during the reset phase can be written as:

$$V_{rst} = V_{dd} - V_{th,RS} - V_{th,SF} \tag{5.3}$$

V_{rst} can be varied due to the variations of $V_{th,RS}$ and $V_{th,SF}$. The variation of V_{rst} generates a unique pattern for each pixel array. However, as V_{rst} is sensitive to the random reset noise and the variations of supply voltage and temperature, the IC signature produced directly from V_{rst} is unstable. To obtain a more reliable signature from the image sensor, a differential readout scheme is proposed. The architecture of the proposed CRP generator is shown in Fig. 5.5, and the process of its CRP generation is shown in Fig. 5.6. First, the bypass transistor is turned on to skip the column-level CDS. V_{rst} of each pixel is then scanned out and stored in the frame memory after it is digitized. For ease of exposition, the entire image of V_{rst} is called the "reset image". The address decoder decodes an n-bit address C to read out a pixel voltage value P_C of the "reset image". The bit length n of the challenge can be determined by:

$$n = \log_2 (H \times V) \tag{5.4}$$

where H and V are the numbers of rows and columns of the image sensor, respectively.

Another challenge (address) C' can be generated from C through an n-bit linear feedback shift register (LFSR) counter. The LFSR is initialized by an arbitrary user selectable n-bit seed N $(0 < N < 2^n)$, i.e.,

$$C' = C \oplus N \tag{5.5}$$

where $\oplus$ denotes a bitwise XOR operation.

Since $N \neq 0$, $C \neq C'$. A different pixel voltage value $P_{C'}$ is read out by the challenge C' and compared with P_C by a binary subtractor and a binary comparator. The PUF output bit is either 0 or 1 depending on which pixel voltage value is larger. When the difference between P_C and $P_{C'}$ is sufficiently large, i.e., the absolute value of $P_C - P_{C'}$ is larger than a predefined threshold P_{th}, the

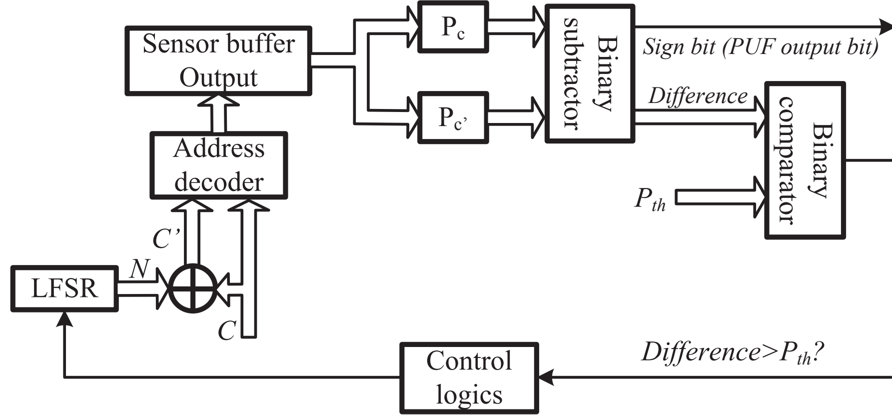

Figure 5.5: *Architecture of CRP generator circuit.*

generated bit is considered stable and will be retained as the response bit to the input challenge C. Otherwise, another pair of pixels will be sought by shifting the content N of the LFSR by one more clock cycle to generate a new C'. This procedure is repeated until a stable CRP is found or the entire pixel array has been exhausted. The threshold of difference P_{th} is process technology dependent and is determined empirically. P_{th} provides a knob to tune the noise margin of the pixel pairs to stabilize the response bit against temperature and voltage variations. Besides, the entire CRP mappings of the PUF can be reconfigured by selecting a different value of N to initialize the LFSR counter. With a different seed value N, the mapping of the CRPs can be changed. This is particularly useful when the original CRP mapping is suspected to be compromised or the CRP can be periodically refreshed to thwart modeling attacks [103].

5.3.3 Reliability Enhancement

It can be shown that the proposed differential readout scheme can improve the PUF's reliability against temperature and supply voltage variations. Let V_{sig} denote the signal voltage $P_C - P_{C'}$, where P_C and $P_{C'}$ are the two reset voltages of the pixels selected by the addresses, C and C', respectively. From (5.3), V_{sig} can

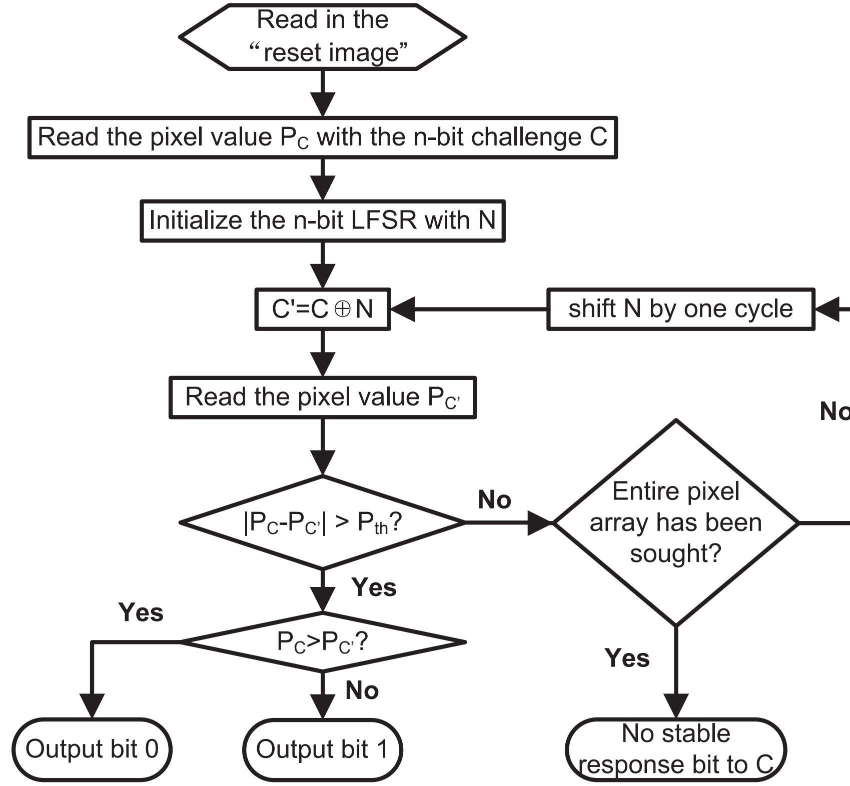

Figure 5.6: *Procedure for CRP generation.*

be expressed as:

$$\begin{aligned} V_{sig} &= V_{rst} - V'_{rst} \\ &= V'_{th,RS} + V'_{th,SF} - V_{th,RS} - V_{th,SF} \end{aligned} \tag{5.6}$$

Equation (5.6) indicates that V_{sig} is insensitive to the supply voltage variations V_{dd}.

The threshold voltage is temperature dependent and can be expressed as [69]:

$$V_{th}(T) = V_{th}(T_0) + \sigma_{th}(T - T_0) \tag{5.7}$$

where T_0 is the reference temperature and σ_{th} is the threshold voltage temperature coefficient in the range of 0.5$\sim$ 3 mV/K.

Taking the partial derivative of V_{sig} with respect to T,

$$\frac{\partial V_{sig}}{\partial T} = \sigma'_{th,RS} + \sigma'_{th,SF} - \sigma_{th,RS} - \sigma_{th,SF} \tag{5.8}$$

The differential readout voltage V_{sig} is less sensitive to temperature variation than any single pixel reset voltage V_{rst} as

$$\left|\frac{\partial V_{sig}}{\partial T}\right| < \left|\frac{\partial V_{rst}}{\partial T}\right| = |\sigma_{th,RS} + \sigma_{th,SF}| \tag{5.9}$$

To show the robustness of the differential readout scheme against supply voltage and temperature variations, 50 runs of Monte Carlo simulation of a 3T-APS are performed at the transistor-level using 180 nm CMOS process design kit (PDK). The PDK provided by the foundry contains the variation profile of key parameters in 180 nm CMOS technology. It can well represent the ranges of parameter values of the physical design due to the manufacturing process variations. The Monte Carlo simulation method [13] is used to introduce randomly sampled device parameter variations from a normal distribution. The results are shown in Fig. 5.7 for the pixel reset output voltage V_{rst} and the differential output signal voltage V_{sig} with the supply voltage varies by ±20% and the temperature varies from 0 to $100°C$. Each line in the figure represents an instance of the Monte Carlo simulation. It is evident that the noises induced by the variations of the supply voltage and the temperature are well suppressed by the differential readout method.

The differential readout scheme is inadequate to mitigate other random effects due to KTC noise (thermal noise), shot noise (noise due to the dark current and photocurrent), 1/f noise, column switch noise, etc.. Since the response of our PUF is generated during reset, the KTC noise dominates [92]. The root mean square (RMS) voltage of the KTC noise is given by [102]:

$$\overline{V_n^2} = \frac{KT}{C5 - C} \tag{5.10}$$

where K is the Boltzmann constant, T is the temperature in Kelvin and C is the photodiode junction capacitance for a 3T-APS or the floating diffusion capacitance

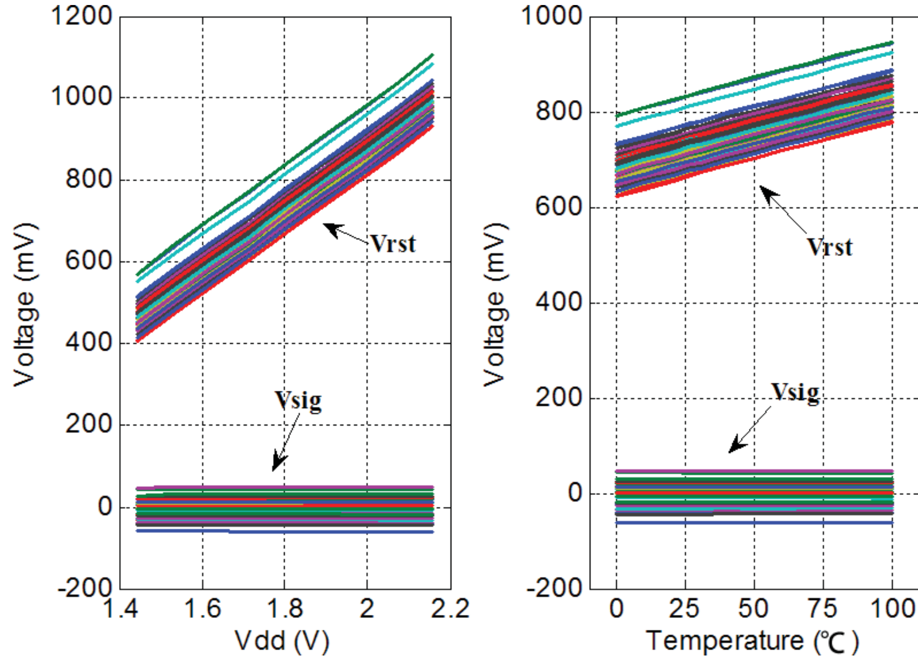

Figure 5.7: *Monte Carlo simulation results of V_{rst} and V_{sig} against the variations of (a) supply voltage, and (b) temperature.*

for a 4T-APS. For $C = 22$ fF, the input referred RMS KTC noise voltage is 414 μV at room temperature. Owing to the fact that the reset time is not long enough for the circuit to be in steady state, the actual reset noise is closer to half the commonly quoted KTC value [92]. The RMS voltage induced by the process variations is much larger. Based on the extracted parameters from the PDK of 180nm CMOS process, a Monte Carlo simulation of 1000runs shows that V_{sig} is Gaussian distributed with mean $\mu = 250$ μV and standard deviation $\sigma = 22.55$mV. According to [104],

$$\overline{V^2} = \mu^2 + \delta^2 \tag{5.11}$$

The RMS voltage contributed by the process variation is calculated to be 22.55 mV. This is two orders of magnitude larger than the KTC noise. The margin is more than sufficient for them to be segregated by comparing V_{sig} with a predefined threshold P_{th}, which can be empirically determined and adjusted based on the characterization model of target fabrication process. If the difference exceeds P_{th}, the response bit generated by this pair of pixels is discarded for use as CRP. The

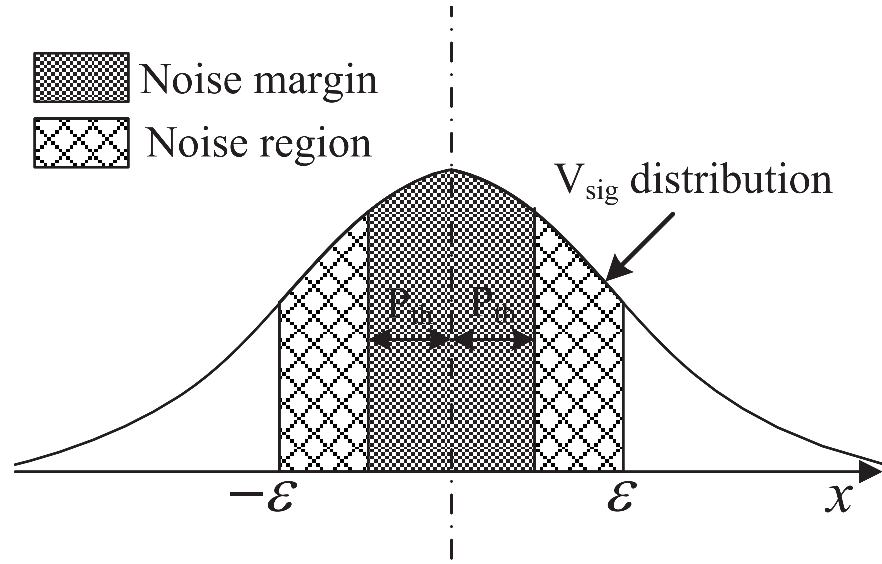

Figure 5.8: *Effects of P_{th} on PUF reliability and the number of CRPs.*

reliability is increased at the cost of a reduction in the total number of CRPs. Fig. 5.8 depicts the effect of changing P_{th} on the PUF reliability. Assuming that the threshold voltage V_{th} of the transistors in each pixel are Gaussian distributed, then V_{sig} is also Gaussian distributed. With ε representing the overall noise voltage, the CRPs located in the noisy region are considered to be unstable. If the CRPs with V_{sig} lying in the range between $-P_{th}$ and $+P_{th}$ are discarded, the statistic mean of the bit error rate (BER) can be calculated by:

$$\overline{BER} = \frac{1}{n}\sum_{i=1}^{n} \Pr(|V_{sig} - P_{th}| < \varepsilon_i) \tag{5.12}$$

Fig. 5.9 plots the BER against the parameters P_{th} and $\overline{\varepsilon}$, where $\overline{\varepsilon}$ is the mean of ε. The BER is calculated from one thousand V_{sig} voltages generated by the Monte Carlo simulation using the PDK. Fig. 5.9 shows the BER decreases with increasing P_{th}. In principle, a BER of 0% can be obtained when $P_{th} > \overline{\varepsilon}$.

Based on the above analysis, the noise margin P_{th} provides a trade-off between the reliability of PUF as a whole and the number of CRP pairs. Decreasing P_{th} will enable more CRP pairs to be extracted but with lower overall reliability. On the other hand, increasing P_{th} will result in higher reliability but less number of extractable CRPs. This trade-off will be further evaluated in our experimental

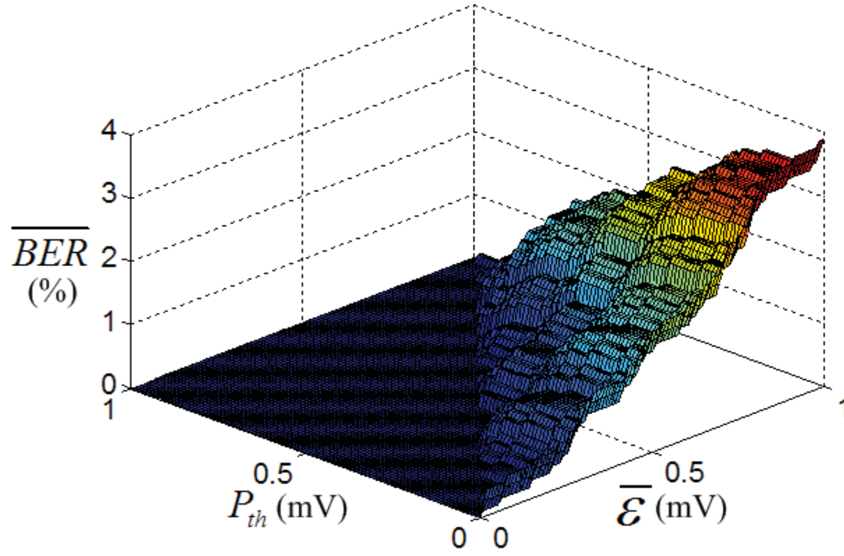

Figure 5.9: *Simulation results of BER for different parametric combinations of P_{th} and ε.*

results.

5.4 Experimental Results and Discussions

The raw reset voltages required for CRP generation cannot be read out directly from commercially available CMOS image sensors due to the built-in CDS. To evaluate the quality of the proposed PUF, a switch transistor was added into the column-level CDS circuit (see Fig. 5.4) to bypass the CDS of a 180 nm CMOS image sensor chip, which was originally designed for another high-speed imaging project. The CRP generator shown in Fig. 5.5 was implemented on an off-chip Xilinx Virtex-6 ML605 FPGA board to simplify its communication with the personal computer. The raw data from the CMOS image sensor during the reset phase are read out and processed by the MATLAB scripts. The image sensor ASIC mainly consists of a 64×64 3T-APS array, a column level CDS, an on-chip column level 10-bit ADC, and a readout buffer. The chip microphotograph is shown in Fig. 5.10. Its active area is 2.5 mm × 5 mm. Five chips have been packaged and tested. The measured FPN without CDS is 9.82%. To show the higher non-uniformity

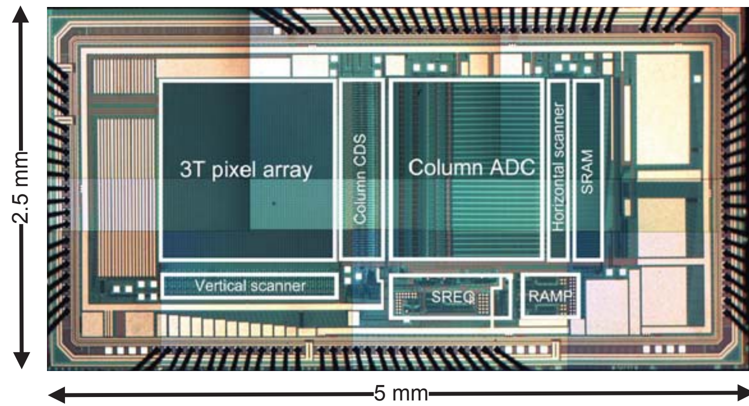

Figure 5.10: *The microphotograph of the image sensor used for the validation of the proposed PUF.*

of the image taken before the FPN is suppressed by the on-chip CDS, the reset image and the pixel voltages of a plain image taken under office lighting after the CDS are measured and compared in the histograms of Fig. 5.11. The standard deviation of the pixel voltages has been reduced by 68.5% by the CDS from 99.09 in Fig. 5.11(a) to 31.24 in Fig. 5.11(b).

Uniqueness, reliability and unpredictability are the three most important figures of merit (FOMs) of a PUF. These FOMs are analyzed in the following experiments.

5.4.1 Uniqueness Assessment

The uniqueness of the proposed PUF can be efficiently estimated by simulating the CRPs generated from a reasonably large number of image sensors by Monte Carlo simulation. The simulation is carried out at the transistor-level by Cadence Virtuoso Spectre using the PDK of 180 nm CMOS process technology. Each iteration of the Monte Carlo simulation represents a unique set of variations applied to a PUF instance. The simulated CRPs of the proposed PUF based on a 64×64 image sensor are collected and processed by the MATLAB scripts. Based on the CRPs collected from 100 PUF instances, with 120 CRPs generated for each instance, the frequency distribution of the inter-die HDs is obtained in Fig. 5.12(a). The uniqueness of these 100 instances is calculated to be 50.12%. The best fit

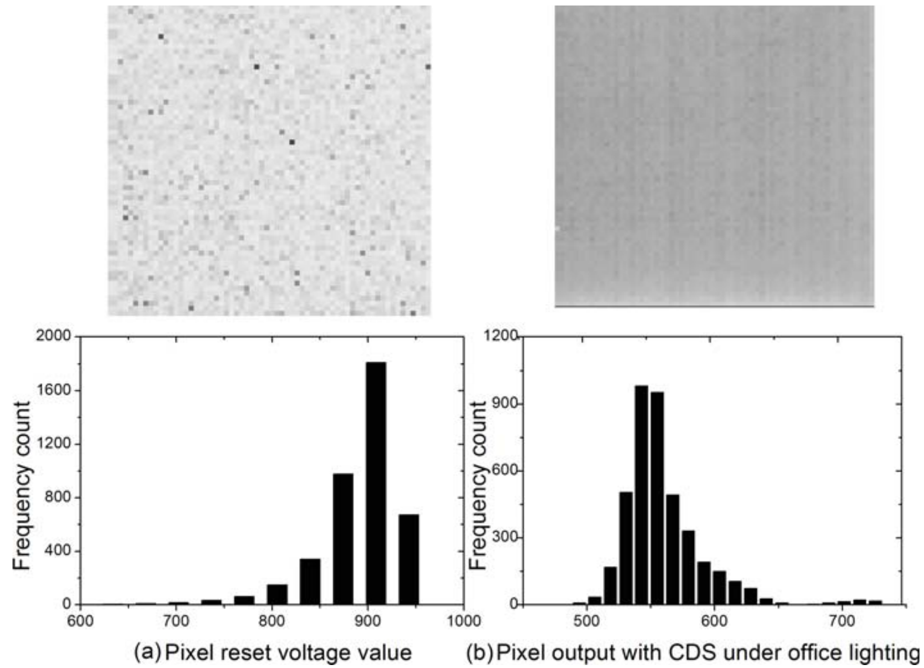

Figure 5.11: *The distribution of pixel voltage values of the image (a) without CDS and (b) with CDS under office lighting.*

Gaussian curve to the histogram has mean $\mu = 50.12\%$ and standard deviation $\sigma = 4.42\%$. The 3σ variation of 13.26% accounts for 99.92% of its statistical population.

Physical measurements obtained from the five dice were also used for this evaluation. A total of 8000 CRPs were generated by the five PUFs. Fig. 5.12(b) shows the measured frequency distribution of the inter-die HDs. The uniqueness calculated from the inter-die HDs of the proposed PUF is 49.37%, which is very close to the ideal value of 50%. The histogram is well fitted by a Gaussian curve with $\mu = 49.37\%$ and $\sigma = 6.48\%$. The measured results show a good uniqueness and are consistent with the Monte Carlo simulation.

5.4.2 Reliability Assessment

Fig. 5.13(a) shows the reliability measured using 1000 CRPs generated by each image sensor based PUF under varying supply voltages with different P_{th}. The nominal power supply for this CMOS technology is $3.3V$ and the CRP collected under this supply voltage is used as a reference. The supply voltage is varied

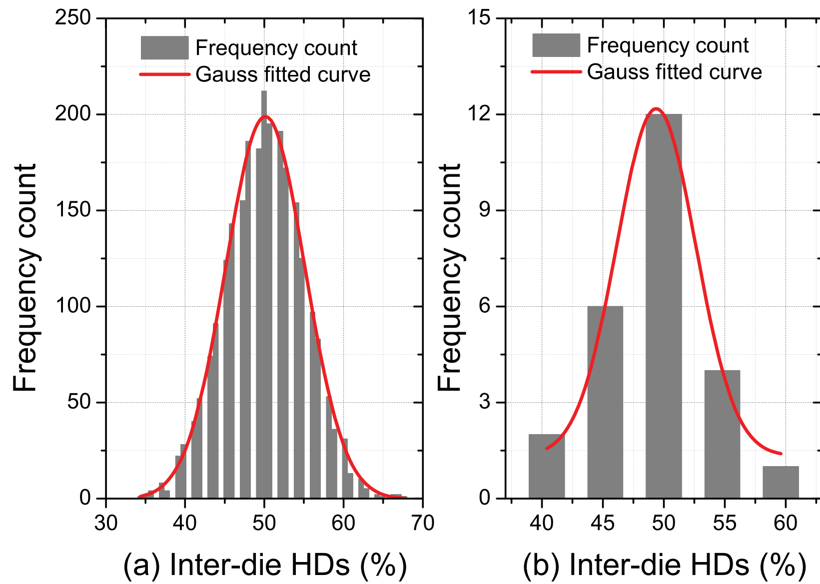

Figure 5.12: *Frequency distribution of (a) the simulated inter-die HDs for 100 PUF instances and (b) the measured inter-die HDs from the five image sensor based PUF chips.*

from 3 to 3.6 V. The average reliability of the CRPs obtained from the five test chips is 97.66% with $P_{th} = 0$. With $P_{th} = 30$, the average reliability and the worst reliability can still be maintained at 99.77% and 99.10%, respectively when $V_{dd} = 3.6$ V. The reliability of the proposed PUF operating at different temperature is also measured. The operating temperature was increased by generating heated air around the die and the ambient temperature was measured by the TK-610B thermometer. The working temperature was varied from 15°C to 115°C. The CRP collected under 27°C is used as a reference. Fig. 5.13(b) shows the average reliability of the five PUF chips under different operating temperatures. The average reliability measured from the PUF chips is 95.97% with $P_{th} = 0$. The reliability can be increased to 100% when $P_{th} = 30$. The results corroborate that the proposed image sensor based PUF can be made much less susceptible to power supply and temperature fluctuations by increasing P_{th}. Fig. 5.14 shows the measured relationship of the threshold voltage P_{th} versus the number of valid pixels and the reliability of the fabricated 64×64 image sensor. As discussed in Section 5.3.3, the number of valid bits decreases with P_{th}, while the reliability increases

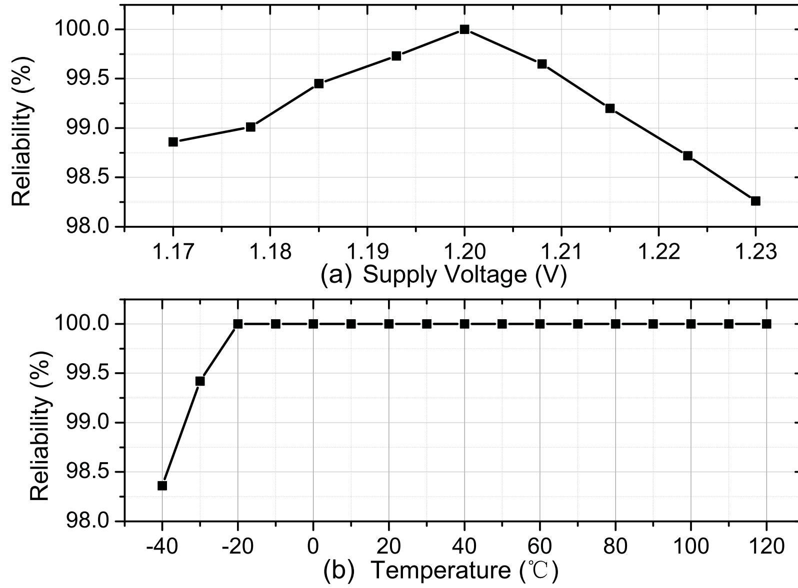

Figure 5.13: *The measured average reliability of hybrid RO PUF against (a) voltage variations, (b) temperature variations.*

with P_{th}. Due to the demand for high resolution imaging, modern CMOS image sensors usually have a large number of pixels, which provide enough headroom to have a high P_{th} for enhanced reliability while still preserving a large CRP space.

5.4.3 Unpredictability Assessment

For the proposed PUF, the number of independent bits that can be generated is a function of N_{pixel}. N_{pixel} is the total number of pixels of the image sensor. There are $N_{pixel}!$ different orderings of pixels based on their reset voltages. If the orderings are equally likely, the entropy corresponding to the number of independent bits will be $log_2(N_{pixel}!)$ bits. For example, in the 64×64 sensor, $\log_2(4096!) = 43,250$ independent bits can be found. This is equivalent to 10.56 bits/pixel, which is more than 10 times that of cell based PUF (e.g., SRAM PUF, latch PUF).

While the maximum number of independent CRPs is intended as the primary assurance of unpredictability, these generated random output bits are also tested by the NIST suite [105]. If they fail to pass the NIST test, the responses are considered as not random enough and may be vulnerable to cryptanalysis. 500,000

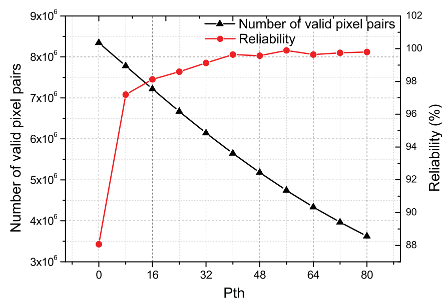

Figure 5.14: *The measured relationship between P_{th} versus the number of valid pixels and the reliability.*

Table 5.1: *NIST test results on the random sequences generated by the proposed image sensor based PUF.*

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P VAL	PROP	TEST
11	5	13	8	14	7	15	10	9	8	0.401199	100/100	Frequency
11	13	11	12	11	2	6	7	11	16	0.115387	97/100	BlockFrequency
11	9	3	15	12	11	12	11	12	4	0.181557	100/100	CumulativeSums
10	7	7	15	10	14	7	13	6	11	0.401199	100/100	CumulativeSums
19	9	18	8	8	8	6	9	9	6	0.023545	99/100	Runs
12	11	11	12	9	10	13	6	11	5	0.719747	100/100	LongestRun
5	9	14	6	8	9	18	11	12	8	0.137282	100/100	FFT
12	20	9	8	12	11	11	6	6	5	0.045675	96/100	ApproximateEntropy
11	9	14	7	11	12	13	12	7	4	0.437274	100/100	Serial(forward)
11	11	11	7	15	8	11	12	7	7	0.699313	99/100	Serial(backward)
18	6	4	7	8	12	7	8	13	17	0.015598	97/100	LinearComplexity

response bits generated from the five dies are collected and divided into 100 blocks of 5,000 bits each. Table 5.1 shows the results of NIST tests. The uniform distribution across columns C1 through C10 indicates a uniform distribution of the frequency of various P-values. The 11th column indicates the P-value obtained via a chi-square test. The 12th column indicates the proportion of binary sequences that passed testing. The results show that the random numbers generated by the proposed image sensor based PUF have passed all tests, and support the extraction of statistically random numbers from the proposed PUF.

A comparison of the FOMs for the silicon PUFs reported in the literature is summarized in Table 5.3. Except the results of RO [12] and Bistable ring [80], which are reported based on FPGA implementation, the results of the remaining PUFs are obtained from custom chip implementation. Our proposed PUF has great advantage of high reliability by virtue of the differential readout method. By increasing the adaptive threshold P_{th} to 80, the worst reliability for our proposed image sensor PUF can still be maintained at 99.80% with ±10% supply

Table 5.2: *Resources consumed by CRP generator in FPGA implementation.*

Component	Number of slice LUTs	Number of slice registers
Subtractor	19	0
Comparator	9	0
Control logics	31	11
LFSR	1	12
Address decoder	134	0
Total	194	23

voltage variations from 3.0∼3.6 V and a temperature variations of 15∼115 °C. This is highly competitive for the hostile operating condition variations that can be achieved among all PUFs in comparison.

5.4.4 Implementation Overheads

5.4.4.1 Area overhead

The area overhead of our proposed CMOS image sensor based PUF is mainly contributed by the switch transistors and the CRP generator. One switch transistor per column is added to bypass the column level CDS circuitry. This area is negligible as it can be minimized by sizing the transistors with the minimum feature size of the target process technology. In our design, the size of the switch transistor is $W = 460nm$ and $L = 350nm$. The CRP generator contributes a fixed overhead irrespective of the pixel array size. Table 5.2 shows the resources consumed (estimated by the Xilinx ISE 14.4) for its implementation on FPGA. The total number of LUTs and registers required are 196 and 27, respectively. The CRP generator is also synthesized by Synopsys Design Compiler using the standard cell library of 180nm process PDK. The total area including the cell area and interconnect area is 63540 μm^2. This cost is small and does not increase when more independent cells are added.

5.4.4.2 Power overhead

The baseline CMOS image sensor was designed for a high-speed imaging application, which operates at 780 frames per second (fps) at 3.3 V with a power consumption of 300.5mW. The energy consumption per CRP can be calculated as follows. Each frame of 64 $\times$ 64 pixel resolution produces 43,250 independent

Table 5.3: *Comparison of qualities of our proposed PUF with other PUFs.*

PUF	Technology (nm)	Uniqueness (%)	Worst case reliability (%)	Reliability conditions
ISSCC'00 [81]	350	NA	95.00	$1.5 \sim 5V, -25 \sim 125°C$
DAC'07 [12]	90	46.14	99.52	$1.2 \sim 1.08V, 20 \sim 120°C$
VLSI'04 [7, 12]	180	23.00	95.20	$\pm 2\% V_{DD}, 20 \sim 70°C$
Subthreshold arbiter [13]	45	42.70	82.00	$\pm 10\% V_{DD}, 75°C$
ISSCC'07 [9]	130	64.70	96.96	$0.9 \sim 1.2V$
HOST'08 [42]	65	45.00	94.00	$-20 \sim 80°C$
HOST'11 [80]	NA	50.90	98.70	$-55 \sim 125°C$
VLSI'10 [107]	65	49.95	100	$\pm 10\% V_{DD}, 0 \sim 85°C$
JSSC'11 [108]	90	NA	99.90	$\pm 10\% V_{DD}, 25 \sim 115°C$
ISSCC'14 [47]	22	NA	99.03*	$0.7 \sim 0.9V, 25 \sim 55°C$
This work	180	**49.37**	88.00 ($P_{th} = 0$) 99.10 ($P_{th} = 30$) **99.80** ($P_{th} = 80$)	$3.0 \sim 3.6V, 15 \sim 115°C$

* Reliability is 100% after ECC.

bits, which gives a bit rate of 43,250 b/frame × 780 fps = 33.735 Mb/s. The energy per CRP is 300.5 mW ÷ 33.735 Mb/s = 8.9077 nJ/b. This can be reduced substantially if the PUF is piggybacked on an image senor targeting for low-power instead of high-speed application. For example, if our proposed PUF is applied on a low-voltage 176 × 144 3T-APS CMOS image sensor [106], which operates at 20 fps and dissipates only 48 μW at 1.2 V, the energy per CRP will be reduced to 23.9 pJ/b. The power consumed by our proposed PUF is only a fraction of the total power consumed by the baseline CMOS image sensor. With additional capacitance added onto the column bus, the extra power contributed by the bypass transistor simulated using the 180nm process PDK is 0.33 μW per column. The power consumption due to the bypass transistors in the sensor chip is 0.33 μW × 64 = 21.12 μW. The total power consumed by the CRP generator reported by Synopsys Design Compiler using the same 180nm CMOS process is 242.59 μW. Hence, the total power overhead due to the proposed PUF is estimated to be 263.71 μW.

5.4.5 Attack Analyses

5.4.5.1 Modeling attack

Modeling attack assumes that the adversary can create a model of the target PUF with a given number of CRPs. With the derived model, other CRPs can be predicted with a high accuracy. The basic arbiter PUF is vulnerable to the modeling attack because an additive linear delay model can be constructed [109],

the delay of a path is assumed to be a linear sum of each segment delay along the path. Modern machine learning tool can find a maximum-margin hyperplane to separate the 0 and 1 responses. Successful prediction rate of greater than 95% with 640 training CRPs for a 64-bit arbiter PUF was reported [109]. It is not possible to derive an additive linear model from our proposed PUF because the reset voltages of every pixels in the pixel array are independent of each other. The RO PUF in [12] is also vulnerable to the modeling attack [109] due to the correlation of the RO frequency deviations obtained from different RO pairs. A smart adversary can attack the RO PUF by adaptively reading the CRPs. By sorting the collected ROs frequencies in ascending order with a fast algorithm, the adversary can predict other outputs without knowing the exact frequencies of the ROs. As the response of our proposed PUF is obtained by comparing the reset voltages of two pixels selected by the challenge, to thwart modelling attack, correlated outputs should be discarded as discussed in Section 5.4.3. Since the layout of a pixel is more compact than an RO, more independent bits per unit area can be obtained from our proposed PUF. Besides, there is one subtle difference in the challenge-response generation of our proposed image sensor based PUF that constitutes to its greater resiliency against modeling attack. The address to select the second pixel in the pair is obtained by encrypting (XORing) the input challenge by a LFSR-based stream cipher (see Section 5.3.2). Different seed value of LFSR produces different random number, which causes the original CRPs collected by the attacker to be invalid after the seed value has been changed. Furthermore, the characteristic polynomial can be changed by reconfiguring the properties of LFSR [110]. Such capability makes it extremely difficult for an adversary to predict the proposed PUF output with the currently available modeling attack methodologies [103,110].

5.4.5.2 Sensor decoupling attack [98]

Sensor decoupling refers to the separation of the sensor from its measured physical quantity. This attack can be easily mounted on the sensor PUFs proposed in [98–100]. For example, the light sensor PUF can be deployed in a black box to cause an authentication failure or make it reporting the wrong light level. In

contrast, our proposed PUF does not mix the measured light level of an image with an input challenge to produce its response. Since the response generated based on the DSNU of FPN is independent of the external illumination, sensor decoupling attack is infeasible for our proposed PUF.

5.5 Emerging Applications

5.5.1 Smart phone authentication and anti-counterfeiting

The proposed image sensor based PUF has opened new avenues for low-cost, secure and robust solution for on-chip CMOS image sensor device authentication and key generation. Besides surveillance cameras, one attractive application for this new form of PUF is the smart phone authentication and counterfeit prevention. Presently, device-specific IDs such as IMEI (device ID), IMSI (subscriber ID) and ICC-ID (SIM card serial number) are used for the identification and authentication of mobile phones. As these digital device IDs are normally kept in the NVM in SIM cards, the hackers can easily copy them to another low-cost refurnished or knockoff cell phones [111]. These cloned phones are virtually indistinguishable from the authentic ones. The proposed PUF is advantageous over the standard secure digital storage for the following reasons:

- Most smart phones are integrated with more than one CMOS image sensor (back and front). As modern integrated CMOS image sensors have high resolution, it can provide an enormously large CRP space. For example, the back camera in iPhone 5s has 8×10^6 pixels, which is capable of providing $\log_2(8 \times 10^6!) = 1.72 \times 10^8$ independent CRPs. A larger CRP space is advantageous in enhancing the security of the PUF [40].

- The proposed PUF can generate highly reliable response by tuning P_{th}. Unlike the ID stored in NVMs, it cannot be easily copied, compromised or removed as the secrets are integral parts of the structure inherited from its manufacturing process and can only be generated when the chip is powered

on. Any invasive attack to steal the secret will destroy the original secrets and render the chip inoperable.

- The proposed PUF can be easily implemented with a negligible hardware cost and does not affect or compromise the original functionality and performance of CMOS image sensor.
- The proposed PUF can be seamlessly integrated into the image sensor. No extra expensive secure EEPROM/RAM, dedicated encryption module or other auxiliary PUF module is required for the purpose of device authentication, which can further reduce the total cost of the system.

5.5.2 Against Virtual Camera Attack

Another promising application for the proposed PUF is the fortification against virtual camera attack [84]. Virtual camera is a software tool that could not only modify the face look, hair and backgrounds, but also stream a pre-recorded video to spoof the operating system into believing that the image is captured by the physical webcam in real time. Examples of such cameras are Virtual Webcam, ManyCam, Magic Camera, etc [84]. Virtual cameras pose a severe threat to the surveillance camera system, image sensor based biometric authentication, etc.. Even though the communication between devices and users can be encrypted with provable secure algorithms like AES and DES, the attacker can easily copy the message authentication code (MAC) stored in EEPROM or fuses [112]. The virtual cameras can then use the cloned MAC to masquerade as the device to deliver the fake image or video to gain access to a restricted area or the confidential information. The proposed PUF can be used to tag the images and video streams produced by its image sensor with a unique and trusted signature which is extremely hard to be copied and compromised by videos or images taken from any other image sensors. Being an intrinsic function of a CMOS image sensor, it avoids the risks of man-in-the-middle, replay and masquerade attacks as the sensor and the authentication module are inseparable [89].

5.5.3 Optimize P_{th} for Different Applications

Modern PUF based secure protocols [12,113] can be used with our proposed image sensor based PUF for authentication. A secure database is required to store a set of CRPs from each image sensor PUF before the use of the sensor. When the authenticity of the sensor is queried, a set of CRPs are chosen randomly from this database and applied to the PUF circuit. The obtained response is compared with the responses stored in the database to authenticate the IC. The authentication is successful when the HD between the CRP stored in the database and the CRP generated by the PUF in use is lower than a predefined value. For strong resilience against masquerade attacks, it is highly desirable that the challenges are never reused [12]. This case mandates a lower P_{th} to support a large number of CRPs as a lower reliability is tolerable by the augmented authentication protocol. On the other hand, when the proposed PUF is used as encryption primitives for secret key generation, a high reproducibility of responses is required under all circumstances including operating in noisy and harsh environments [113]. In this case, a larger P_{th} is required to achieve a high reliability. In summary, the trade-off between the reliability and number of CRPs of our proposed PUF provides an adaptable solution for different security applications.

5.6 Summary

This chapter presents a new CMOS image sensor based PUF. The proposed PUF has been validated on a CMOS image sensor fabricated in 180 nm CMOS technology. The intrinsic IDs measured from the imager core have a uniqueness of 49.37%. A high reliability of 99.80% with ±10% supply voltage variations and temperature range of 15∼115 °C can be attained by tuning the differential threshold P_{th}. As a standard and indispensable component of the surveillance camera and smart phones, the introduction of this integrated security primitive for device identification and authentication has not only enhanced the security of existing sensor level applications but also created exciting new opportunities for the devel-

opment of security, privacy and trust protocols in distributed and mobile sensing applications.

Chapter 6

Conclusion

6.1 Conclusion

Hardware security has recently emerged as a hot research topic of great societal impact due to the paradigm change in the integrated circuit (IC) design and fabrication flow. Modern ICs are becoming increasingly more susceptible to the diverse forms of hardware-based attacks. This is because of the worldwide outsourcing of external facilities, such as IP blocks, CAD software tools and IC fabrication by the semiconductor industry as an effective economic cost saving strategy to deal with the increasing complex and interalliance IC design business support solutions. These practices relinquish the control of a designer on the core design, integration, verification, testing and manufacturing processes in the complete IC design chain, and open the door to various security threats. For instance, a chip may be maliciously modified at different stages of the design flow by the implantation of "hardware Trojans" by a third party or an insider by bribery or collusion. The Trojans can subvert the security and reliability of the entire electronic systems. Besides, an illegally "cloned" ICs can extort a big market share from the original IC design house. Unauthorized or insecured transaction of IP modules to unscrupulous system integrators will also increase the vulnerability of infringement of IP rights and resulted in great loss of the IP vendors.

This dissertation aims to address some of these hardware-based attacks by low-cost and comprehensive techniques to ensure the security and integrity of the

hardware platforms. The research mainly contributes to two key fields of hardware security, namely hardware Trojan (HT) detection and physical unclonable functions (PUFs).

In Chapter 3, a new cluster-based distributed active current sensor for hardware Trojan detection has been proposed. This sensor exploits both the amplitude and timing of the switching current of an IC to facilitate the monitoring and screening of IC for HT infection. The proposed technique utilizes the industrial power gating scheme to reduce the power consumption and convert the switching current on the local power grid into a timing pulse. Then, the timing and power side channel signals of the pulse can be detected by the existing scan test architecture. The effect of the process variations is reduced through the adjustment of the current comparator threshold in the sensor. The post-layout Monte Carlo simulations on the state-of-art hardware Trojan benchmarks have demonstrated the effectiveness of the current sensor for the detection of delay-invariant and rarely switched Trojans. Its capability to detect the Trojan at speed without affecting the original functionality makes it possible to be integrated into a trusted platform to monitor the anomaly of an IC in operation to limit the damage of a dreadful Trojan that has evaded detection at post-manufacturing test.

A hybrid RO PUF with enhanced thermal stability is proposed in Chapter 4. The current starved inverter stages in the proposed RO PUF not only compensate the temperature variations of the regular inverter stages, but also reduce the overall power consumptions. The measurement results of the proposed 9-stage PUF prototype fabricated in 65 nm 1.2 V CMOS process possess a uniqueness of 50.46% and a very high reliability of 99.84% against a wide range of temperature variations from −40 °C to 120 °C. The entropy of its CRPs per unit area is much larger than that of the classic RO PUF. Its robustness against machine learning and side-channel attacks has also been successfully demonstrated in the experiments. The core of the PUF has a small active area of 250 μm^2 and a low power consumption of 32.3 μW per CRP at 1.2 V and 230 MHz. Due to the very low overhead on power consumption and hardware area, the proposed PUF is a promising candidate for the secret key generation and secure authentication in

mobile applications.

In Chapter 5, a new low-cost CMOS image sensor based PUF is also presented to provide the trusted authentication at the sensor-level. It exploits the fixed pattern noise (FPN) in a CMOS image sensor to generate random and stable response bits. The proposed differential readout method reduces the effects of temperature and supply voltage variations. In addition, the readout scheme enables the PUF reliability and the efficiency of security protocol to be optimally traded through a thresholding parameter to adapt to different applications or used environments. The proposed PUF has been validated on a pre-fabricated CMOS image sensor in 180 nm CMOS technology. The measurement results showed that the PUF extracted from the imager core have a uniqueness of 49.37% and a high reliability of 99.10% with ±10% supply voltage variation and a temperature range of 15∼115 °C by tuning the differential threshold P_{th}. As a standard component in smart phones, tablets and surveillance cameras, the proposed image sensor based PUF can be used to provide the Root of Trust (RoT) for further development of mobile security applications.

6.2 Future Work

Based on the above accomplishments, the following ideas worthy of further investigation are suggested for future research.

6.2.1 Temperature and Voltage Invariant Hybrid RO based PUF with Adaptive Self Biasing

Chapter 4 has presented a hybrid RO PUF with high temperature stability. As shown in Fig. 4.3(b), the two biasing voltages (i.e., V_p for PMOS and V_n for NMOS) are currently fixed in the given current starved inverter stage. However, the original current starved inverter is designed with a bias control voltage V_{ctrl} [114] as shown in Fig. 6.1. In fact, some preliminary results in the latest stage of our research indicated that it may be feasible to use V_{ctrl} to improve the reliability of the

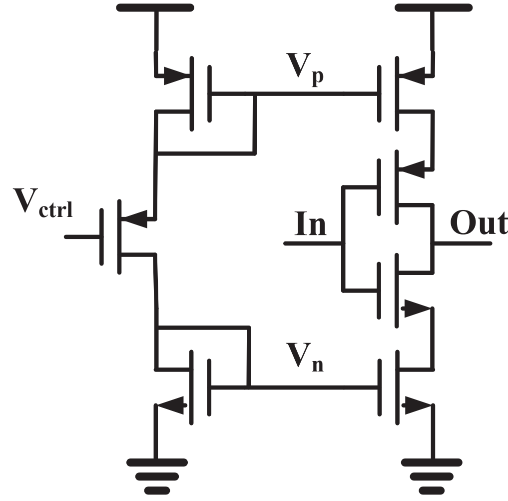

Figure 6.1: *Current starved inverter with external bias V_{ctrl}.*

proposed PUF against supply voltage variations. The two biasing voltages, V_p and V_n can be adjusted by V_{ctrl} to tune the oscillation frequency. The simulation results using GF 65nm CMOS process for the 9-stage hybrid RO's frequencies against V_{ctrl} and V_{DD} variations are shown in Fig. 6.2 and Fig. 6.3, respectively. The oscillation frequency of the hybrid RO decreases with the bias control voltage V_{ctrl} but increases with the supply voltage V_{DD}. Therefore, it is possible to design a negative feedback from the supply voltage V_{DD} to V_{ctrl} to cancel out the effect of supply voltage variations on the hybrid RO's oscillation frequency.

6.2.2 Cognitive Image Sensor Based PUF

In Chapter 5, the user defined threshold P_{th} provides a tradeoff between the PUF reliability and the number of valid CRPs. The optimization of P_{th} has already been discussed in Section 5.5.3. It may also be possible to autonomously adjust P_{th} in a more intelligent way depending on the different application contexts. The basic concept of this smart PUF is to sense the environmental conditions and adopt an optimal P_{th} based on the targeted applications. The environmental conditions include not only the temperature, supply voltage and ambient noise level, but also the location information, image content, CPU status and so on. For example, the image sensor based PUF which is built in a smartphone can change the security

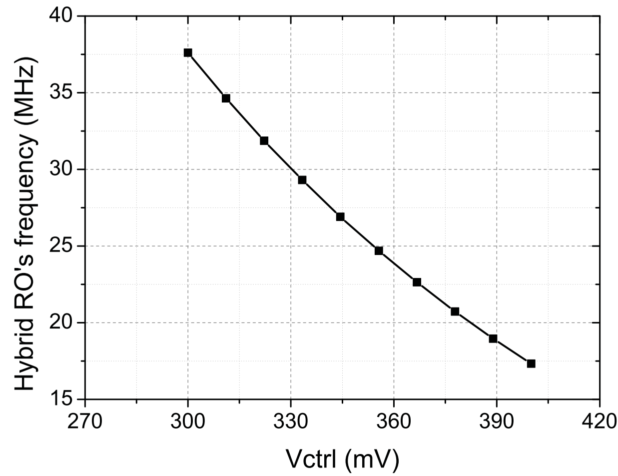

Figure 6.2: *Simulation results of the 9-stage hybrid RO's frequency versus* V_{ctrl}.

level for authentication when the device is located in different places. It would allow a fast authentication when the user is sensed to be located in the comfort and less vulnerable zone of his home, but a more rigorous authentication is set when the device is accessed in a public location, such as a cafe. Such smartness in a PUF can be especially useful in biometric authentication with the help the captured image. If the captured image has been processed and recognized to be a "familiar" scene or feature such as the device owner's face, then subsequent authentications will be carried out with a relatively larger HD tolerance (smaller P_{th}) to speedup authentication or conserve energy. On the other hand, if the feature is categorized as a stranger, the HD tolerance is set to a lower value (larger P_{th}) to increase the vigilance in any access to the information on the device.

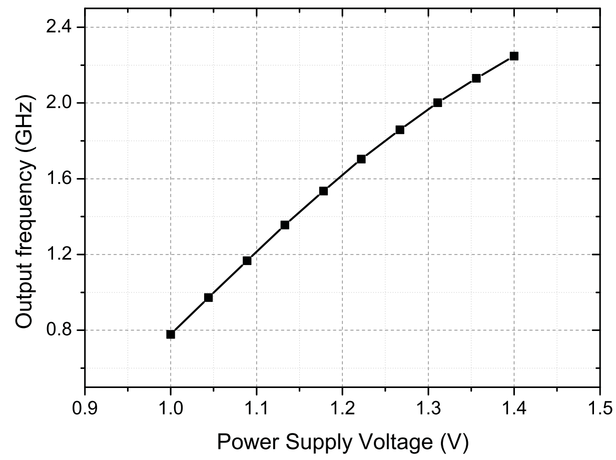

Figure 6.3: *Simulated results of 9-stage hybrid RO's frequency versus the supply voltage* V_{DD}.

List of Publications

Journal Paper Published:

Yuan Cao, Chip-Hong Chang, and Shoushun Chen, "Cluster-based Distributed Active Current Sensing Circuit for Hardware Trojan Detection", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2220-2231, Sep. 2014.

Yuan Cao, Zhang Le, Chip-Hong Chang, and Shoushun Chen, "A Low-power Hybrid Ring Oscillator Physical Unclonable Function with Improved Thermal Stability for Lightweight Applications", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Accepted.

Conference Paper Published:

Yuan Cao, Zhang Le, Siarhei S. Zalivaka, Chip-Hong Chang and Shoushun Chen, "CMOS Image Sensor Based Physical Unclonable Function for Smart Phone Security Applications", *IEEE International Symposium on Integrated Circuits (ISIC)*, Singapore, Dec. 2014, pp. 392-395.

Yuan Cao, Chip-Hong Chang and Shoushun Chen, "Cluster-based Distributed Active Current Timer for Hardware Trojan Detection," *IEEE International Symposium on Circuits and Systems (ISCAS)*, Beijing, China, May 2013, pp. 1010-1013.

Journal Paper Submitted:

Yuan Cao, Zhang Le, Siarhei S. Zalivaka, Chip-Hong Chang, and Shoushun Chen, "CMOS Image Sensor based Physical Unclonable Function for Coherent Sensor-level Authentication", *IEEE Transactions on Circuits and Systems I: Regular Papers*.

Bibliography

[1] B. Sharkey, "Trust in integrated circuits program," DARPA, Tech. Rep., Mar. 2007.

[2] [Online]. Available: http://www.ece.unm.edu/~jimp/HOST/slides/Trojans1.pdf

[3] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Des. Test. Comput.*, vol. 27, no. 1, pp. 10–25, Jan. 2010.

[4] J. Li and J. Lach, "At-speed delay characterization for IC authentication and Trojan horse detection," in *Proc. IEEE Int. Workshop on Hardware-Oriented Security and Trust*, San Francisco, USA, June 2008, pp. 8–14.

[5] Y. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in *Proc. 16th Usenix Security Symp.*, Boston, USA, Aug. 2007, pp. 291–306.

[6] M. Banga and M. Hsiao, "A region based approach for the identification of hardware Trojans," in *Proc. IEEE Int. Workshop on Hardware-Oriented Security and Trust*, San Francisco, USA, June 2008, pp. 40–47.

[7] J. Lee *et al.*, "A technique to build a secret key in integrated circuits for identification and authentication application," in *Proc. Symp. VLSI Circuits*, Hawaii, USA, June 2004, pp. 176–179.

[8] A. Garg and T. Kim, "Design of sram puf with improved uniformity and reliability utilizing device aging effect," in *Proc. 2014 IEEE Int. Symp. on Circuits and Systems (ISCAS)*, Melbourne, June 2014, pp. 1941–1944.

[9] Y. Su, J. Holleman, and B. Otis, "A 1.6 pj/bit 96% stable chip-ID generating circuit using process variations," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, USA, Feb. 2007, pp. 406–407.

[10] H. Traff, "Novel approach to high speed CMOS current comparators," *Electron. Lett.*, vol. 28, no. 3, pp. 310–312, Jan. 1992.

[11] C. E. Liu, Y. J. Hsieh, and J. F. Kiang, "RFID regulator design insensitive to supply voltage ripple and temperature variation," *IEEE Trans. Circuits and Systems II: Express Briefs*, vol. 57, no. 4, pp. 255–259, April 2010.

[12] G. Suh and S. Devadas, "Physical unclonable function for device authentication and secret key generation," in *Proc. Design Automation Conf. (DAC 07)*, San Diego, USA, June 2007, pp. 9–14.

[13] L. Lang *et al.*, "Design and validation of arbiter-based PUFs for sub-45-nm low-power security applications," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 4, pp. 1394–1403, Aug. 2012.

[14] A. E. Gamal *et al.*, "Modeling and estimation of FPN components in CMOS image sensors," in *Proc. the Int. society for optics and photonics (SPIE)*, San Jose, USA, Jan. 1998, pp. 168–177.

[15] D. Merli *et al.*, "Localized electromagnetic analysis of RO PUFs," in *Proc. Hardware-Oriented Security and Trust (HOST)*, Austin, TX, USA, June 2013, pp. 19–24.

[16] "Report of the defense science board task force on high performance microchip supply," Defense Science Board, US DoD, Tech. Rep., Feb. 2005.

[17] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *Proc. IEEE Symposium on Security and Privacy*, Berkeley, USA, May 2007, pp. 296–310.

[18] G. Suh, D. Deng, and A. Chan, "Hardware authentication leveraging performance limits in detailed simulations and emulations," in *Proc. 46th Design Automation Conf.*, San Francisco, USA, July 2009, pp. 682–687.

[19] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: challenges and solutions," in *Proc. IEEE Int. Workshop on Hardware-Oriented Security and Trust*, San Francisco, USA, June 2008, pp. 15–19.

[20] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *Proc. IEEE Int. Workshop on Hardware-Oriented Security and Trust*, San Francisco, USA, June 2008, pp. 51–57.

[21] M. Li, A. Davoodi, and M. Tehranipoor, "A sensor-assisted self-authentication framework for hardware Trojan detection," in *Proc. Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Dresden, German, March 2012, pp. 1331 – 1336.

[22] B. Cha and S. Gupta, "Efficient Trojan detection via calibration of process variations," in *Proc. 2012 IEEE 21st Asian Test Symposium (ATS)*, Niigata, Japan, Nov. 2012, pp. 19–22.

[23] B. Cha and S. K. Gupta, "Trojan detection via delay measurements: A new approach to select paths and vectors to maximize effectiveness and minimize cost," in *Proc. Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, France, Mar. 2013, pp. 18–22.

[24] R. Rad, J. Plusquellic, and M. Tehranipoor, "A sensitivity analysis of power signal methods for detecting hardware Trojans under real process and environmental conditions," *IEEE Trans. on Very Large Scale Integr. (VLSI) Syst.*, vol. 18, no. 12, pp. 1735–1744, 2010.

[25] S. Wei and M. Potkonjak, "Scalable segmentation-based malicious circuitry detection and diagnosis," in *Proc. Int. Conf. on Computer-Aided Design*, San Jose, USA, Nov. 2010, pp. 483–486.

[26] I. Verbauwhede and P. Schaumont, "Design methods for security and trust," in *Proc. Design, Automation and Test in Europe Conf.*, Nice, France, April 2007, pp. 672–677.

[27] S. Wei and M. Potkonjak, "Integrated circuit security techniques using variable supply voltage," in *Proc. Design Automation Conf.*, San Diego, USA, June 2011, pp. 248–253.

[28] H. Salmani and M. Tehranipoor, "Layout-aware switching activity localization to enhance hardware Trojan detection," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 1, pp. 76–87, Feb. 2012.

[29] S. Narasimhan, X. Wang, D. Du, R. Chakraborty, and S. Bhunia, "TeSR: A robust temporal self-referencing approach for hardware Trojan detection," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*, San Diego, USA, June 2011, pp. 71–74.

[30] S. Wei, K. Li, F. Koushanfar, and M. Potkonjak, "Hardware Trojan horse benchmark via optimal creation and placement of malicious circuitry," in *Proc. of the 49th Annual Design Automation Conf. (DAC)*, San Francisco, USA, June 2012, pp. 90–95.

[31] Y. Jin and D. Sullivan, "Real-time trust evaluation in integrated circuits," in *Prrc. Design, Automation and Test in Europe Conference and Exhibition (DATE)*, Dresden, German, Mar. 2014, pp. 1–6.

[32] C. Lamech, R. Rad, M. Tehranipoor, and J. Plusquellic, "An experimental analysis of power and delay signal-to-noise requirements for detecting Trojans and methods for achieving the required detection sensitivities," *IEEE Trans. Inform. Forensics and Security*, vol. 6, no. 3, pp. 1170 – 1179, 2011.

[33] S. Wei and M. Potkonjak, "Scalable consistency-based hardware Trojan detection and diagnosis," in *Proc. Int. Conf. on Network and System Security (NSS)*, Milan, Italy, Sep. 2011, pp. 176–183.

[34] S. Wei, S. Meguerdichian, and M. Potkonjak, "Gate-level characterization: foundations and hardware security applications," in *Proc. Design Automation Conf. (DAC 10)*, Anaheim, USA, June 2010, pp. 222–227.

[35] K. Hu, A. Nowroz, S. Reda, and F. Koushanfar, "High-sensitivity hardware trojan detection using multimodal characterization," in *Proc. Design, Automation & Test in Europe Conference & Exhibition (DATE 2013)*, Grenoble, France, Mar. 2013, pp. 1271–1276.

[36] S. W. J. Herschel, *The origin of finger-printing.* Oxford University Press, 1916.

[37] R. S. Pappu, "Physical one-way functions," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, 2001.

[38] B. Gassend, "Physical random functions," Master's thesis, MIT, MA, USA, 2003.

[39] J. Guajardo *et al.*, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Cryptographic Hardware and Embedded Systems Workshop*, Viena, Austria, Sep. 2007, pp. 63–80.

[40] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[41] U. Ruhrmair *et al.*, "Modeling attacks on physical unclonable functions," in *Proc. ACM Conf. on Comput. and Communications Security*, Chicago, USA, Oct. 2010, pp. 237–249.

[42] S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE*

Int. Symp. on Hardware-Oriented Security and Trust (HOST), Anaheim, CA, June 2008, pp. 67–70.

[43] J. Huang and J. Lach, "IC activation and user authentication for security-sensitive systems," in *Proc. IEEE Int. Workshop on Hardware-Oriented Security and Trust*, Anaheim,CA, June 2008, pp. 76–80.

[44] [Online]. Available: http://www.verayo.com

[45] [Online]. Available: http://www.intrinsic-id.com

[46] A. Maiti, I. Kim, and P. Schaumont, "A robust physical unclonable function with enhanced challenge-response set," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 1, pp. 333–345, Feb. 2012.

[47] S. Mathew *et al.*, "A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100in 22nm CMOS," in *Proc. 2014 IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, CA, Feb. 2014, pp. 278–279.

[48] I. Verbauwhede and R. Maes, "Physically unclonable functions: manufacturing variability as an unclonable device identifier," in *Proc. the 21st edition of the great lakes symposium on Great lakes symposium on VLSI*, Lausanne, Switzerland, May 2011, pp. 455–460.

[49] E. Pakbaznia and M. Pedram, "Coarse-grain MTCMOS sleep transistor sizing using delay budgeting," in *Proc. Design, Automation and Test in Europe Conf. (DATE)*, Munich, Germany, Mar. 2008, pp. 385–390.

[50] S. Bhunia, H. Mahmoodi, D. Ghosh, and K. Roy, "Power reduction in test-per-scan BIST with supply gating and efficient scan partitioning," in *Proc. Sixth International Symposium on Quality of Electronic Design, ISQED*, San Jose, USA, Mar. 2005, pp. 453–458.

[51] A. Bsoul and S. Wilton, "An FPGA architecture supporting dynamically controlled power gating," in *Proc. IEEE Int. Conf. on In Field-Programmable Technology (FPT)*, Beijing, China, Dec. 2010, pp. 1–8.

[52] L. Whetsel, "Adapting scan architectures for low power operation," in *Proc. International Test Conference*, Atlantic City, USA, Oct. 2000, pp. 863–872.

[53] Y. Cao, C. Chang, and S. Chen, "Cluster-based distributed active current timer for hardware Trojan detection," in *Proc. 2013 IEEE Int. Symp. on Circuits and Systems*, Beijing, China, May 2013, pp. 1010–1013.

[54] S. Wei and M. Potkonjak, "Scalable hardware Trojan diagnosis," *IEEE Trans. on Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 6, pp. 1049–1057, 2012.

[55] Y. Jin, N. Kupp, and Y. Makris, "Experiences in hardware Trojan design and implementation," in *Proc. IEEE International Workshop on Hardware-Oriented Security and Trust*, Francisco, USA, July 2009, pp. 50–57.

[56] I. Pecuh, M. Margala, and V. Stopjakova, "1.5 Volts Iddq / Iddt current monitor," in *Proc. IEEE Canadian Conf. on Electrical and Computer Engineering*, Alberta, Canada, May 1999, pp. 472–476.

[57] M. Anis, S. Areibi, M. Mahmoud, and M. Elmasry, "Dynamic and leakage power reduction in MTCMOS circuits using an automated efficient gate clustering technique," in *Proc. IEEE Design Automation Conference (DAC 02)*, New Orleans, USA, June 2002, pp. 480–485.

[58] I. Park and E. McCluskey, "Launch-on-shift-capture transition tests," in *Proc. IEEE Int. Test Conf.*, Santa Clara, USA, Oct. 2008, pp. 1–9.

[59] "ISCAS'85 benchmarks circuits." [Online]. Available: http://web.eecs.umich.edu/~jhayes/iscas.restore/

[60] D. Rai and J. Lach, "Performance of delay-based trojan detection techniques under parameter variations," in *Proc. IEEE Int. Hardware-Oriented Security and Trust (HOST)*, Francisco, USA, July 2009, pp. 58–65.

[61] M. Saint-Laurent and M. Swaminathan, "A digitally adjustable resistor for path delay characterization in high-frequency microprocessors," in *Proc. 2001 Southwest Symposium on Mixed-Signal Design*, Austin, USA, Feb 2001, pp. 61–64.

[62] S. Borkar *et al.*, "Parameter variations and impact on circuits and microarchitecture," in *Proc. Design Automation Conference (DAC 03)*, San Francisco, USA, June 2003, pp. 338–342.

[63] S. Devadas *et al.*, "Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications," in *Proc. IEEE Int. Conf. on RFID*, Las Vegas, USA, April 2008, pp. 58–64.

[64] L. Dung and C. Chen, "A VLSI implementation of variation-free PUF based processor for RFID applications," in *Proc. IEEE Int. Automatic Control Conf. (CACS)*, Nantou, Taiwan, Dec. 2013, pp. 120–123.

[65] D. Merli, F. Stumpf, and C. Eckert, "Improving the quality of ring oscillator PUFs on FPGA," in *Proc. Workshop on Embedded Systems Security (WESS 2010)*, Scottsdale, USA, Oct. 2010, pp. 1–9.

[66] R. Kumar, V. Patil, and S. Kundu, "On design of temperature invariant physically unclonable functions based on ring oscillators," in *Proc. IEEE Computer Society Annual Symp. on VLSI (ISVLSI)*, Amherst, MA, USA, Aug. 2012, pp. 165–170.

[67] C. Yin and G. Qu, "Temperature-aware cooperative ring oscillator PUF," in *Proc. IEEE Int. Workshop on Hardware-Oriented Security and Trust*, Francisco, CA, USA, July 2009, pp. 36–42.

[68] S. Mansouri and E. Dubrova, "Ring oscillator physical unclonable function with multi level supply voltages," in *Proc. IEEE 30th Int. Conf. on Computer Design (ICCD)*, Montreal, Canada, Sep. 2012, pp. 520–521.

[69] E. Socher, S. Beer, and Y. Nemirovsky, "Temperature sensitivity of SOI-CMOS transistors for use in uncooled thermal sensing," *IEEE Trans. Electron Devices*, vol. 52, no. 12, pp. 2784–2790, 2005.

[70] Y. Taur and T. Ning, *Fundamentals of modern VLSI devices.* Cambridge Univ. Press, 1998.

[71] S. Mondal, S. Talapatra, and H. Rahaman, "Analysis, modeling and optimization of transmission gate delay," in *Proc. Asia Symposium on Quality Electronic Design (ASQED)*, Kuala Lumpur, Malaysia, July 2011, pp. 246–253.

[72] G. Komurcu, A. Pusane, and G. Dundar, "Analysis of ring oscillator structures to develop a design methodology for RO-PUF circuits," in *Proc. Int. Symp. on Very Large Scale Integration(VLSI-SoC)*, Istanbul, Turkey, Oct. 2013, pp. 332–335.

[73] S. Katzenbeisser *et al.*, "Recyclable PUFs: logically reconfigurable PUFs," *Journal of Cryptographic Engineering*, vol. 1, no. 3, pp. 177–186, 2011.

[74] D. Lim, "Extracting secret keys from integrated circuit," Master's thesis, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technology, Cambridge, 2004.

[75] H. G, R. Maes, and I. Verbauwhede, "Machine learning attacks on 65nm arbiter PUFs: accurate modeling poses strict bounds on usability," in *Proc. IEEE Int. Workshop on Information Forensics and Security (WIFS)*, Tenerife, Spain, Dec. 2012, pp. 37–42.

[76] J. Delvaux and I. Verbauwhede, "Side channel modeling attacks on 65nm arbiter PUFs exploiting CMOS device noise," in *Hardware-Oriented Security and Trust (HOST)*, Austin, TX, USA, June 2013, pp. 137–142.

[77] T. Joachims, "Learning to classify text using support vectormachines," Ph.D. dissertation, Univ. Dortmund, Dortmund, Germany, 1999.

[78] D. Hogg, "Fun with the Friis free-space transmission formula," *IEEE Antennas and Propagation Magazine*, vol. 35, no. 4, pp. 33–35, 1993.

[79] W. He, E. de la Torre, and T. Riesgo, "An interleaved EPE-immune PA-DPL structure for resisting concentrated EM side channel attacks on FPGA implementation," in *Proc. Int. Conf. on Constructive Side-Channel Analysis and Secure Design, ser. COSADE*, armstadt, Germany, May 2012, pp. 39–53.

[80] Q. Chen *et al.*, "The bistable ring PUF: A new architecture for strong physical unclonable functions," in *Proc. IEEE Int. Symp. on Hardware-Oriented Security and Trust (HOST)*, San Diego, CA, USA,, June 2011, pp. 134–141.

[81] K. Lofstrom, W. Daasch, and D. Taylor, "IC identification circuit using device mismatch," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, USA, Feb. 2000, pp. 372–373.

[82] "CMOS image sensors market analysis and segment forecasts to 2020," Grand View Research, Inc., San Franccisco, USA, Tech. Rep., May 2014.

[83] D. Serpanos and A. Papalambrou, "Security and privacy in distributed smart cameras," *Proceedings of the IEEE*, vol. 96, no. 10, pp. 1678–1687, Oct. 2008.

[84] S. Chen *et al.*, "Sensor-assisted facial recognition: an enhanced biometric authentication system for smartphones," in *Proc. 12th annual Int. Conf. on Mobile systems, applications, and services*, Bretton woods, USA, June 2014, pp. 109–122.

[85] F. Bagci, T. Ungerer, and N. Bagherzadeh, "SecSens - security architecture for wireless sensor networks," in *Proc. 3rd Int. Conf. on Sensor Technologies and Applications, 2009. SENSORCOMM '09*, Athens, Glyfada, June 2009, pp. 18–23.

[86] T. Winkler and B. Rinner, “Security and privacy protection in visual sensor networks: A survey,” *ACM Computing Surveys (CSUR)*, vol. 47, no. 1, p. 2, July 2014.

[87] P. Stifter, K. Eberhardt, A. Erni, and K. Hoffmann, “Image sensor for security applications with on-chip data authentication,” *Proc. the Society of Photo-Optical Instrumentation Engineers*, vol. 6241, p. 8, April 2006.

[88] S. P. Mohanty, “Secure digital camera architecture for integrated real-time digital rights management,” *Journal of Systems Architecture*, vol. 55, no. 10-12, pp. 468–480, Oct. 2009.

[89] T. Winkler and B. Rinner, “Sensor-level security and privacy protection by embedding video content analysis,” in *Proc. Int. Conf. on Digital Signal Processing (DSP)*, Fira, July 2013, pp. 1–6.

[90] T. Addabbo, A. Fort, M. Di Marco, L. Pancioni, and V. Vignoli, “Physically unclonable functions derived from cellular neural networks,” *IEEE Trans. Circuits and Systems I: Regular Papers*, vol. 60, no. 12, pp. 3205–3214, Dec. 2013.

[91] R. Maes and I. Verbauwhede, “Physically unclonable functions: a study on the state of the art and future research directions,” in *Proc. Towards Hardware-Intrinsic Security*. Heidelberg, Berlin: Springer-Verlag, 2010.

[92] H. Tian *et al.*, “Analysis of temporal noise in CMOS photodiode active pixel sensor,” *IEEE Journal of Solid-State Circuits*, vol. 36, no. 1, pp. 92–101, 2001.

[93] H. Gou, A. Swaminathan, and M. Wu, “Intrinsic sensor noise features for forensic analysis on scanners and scanned images,” *IEEE Transactions on Inf*, vol. 4, no. 3, pp. 476–491, July 2009.

[94] K. Kurosawa, K. Kuroki, and N. Saitoh, “CCD fingerprint method c identification of a video camera from videotaped images,” in *Proc ICIP 99*, Kobe, Japan, Oct. 1999, pp. 537–540.

[95] J. Lukas and J. Fridrich, "Digital camera identification from sensor pattern noise," *IEEE Trans. Inform. Forensics and Security*, vol. 1, no. 2, pp. 205–214, June 2006.

[96] X. Kang, Y. Li, Z. Qu, and J. Huang, "Enhancing source camera identification performance with a camera reference phase sensor pattern noise," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 2, pp. 393–402, April 2012.

[97] M. van Dijk and U. Ruhrmair, "Protocol attacks on advanced PUF protocols and countermeasures," in *Proc. Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*, Dresden, German, March 2014, pp. 1–6.

[98] K. Rosenfeld, E. Gavas, and R. Karri, "Sensor physical unclonable functions," in *Proc. 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Anaheim, CA, June 2010, pp. 112–117.

[99] U. Ruhrmair, "Virtual proofs of reality," IACR Cryptology ePrint Archive, 2013. [Online]. Available: https://eprint.iacr.org/2014/415.pdf

[100] M. Stutzmann *et al.*, "Method for security purposes," Europe Patent, 2013, eP Patent 2,237,183. [Online]. Available: http://www.google.com/patents/EP2237183B1?cl=en

[101] U. Ruhrmair, "SIMPL systems: On a public key variant of physical unclonable functions," IACR Cryptology ePrint Archive, 2009. [Online]. Available: https://eprint.iacr.org/2009/255.pdf

[102] J. Ohta, *Smart CMOS Image Sensors and Applications.* London, New York: CRC Press, 2007.

[103] L. Zhang, Z. H. Kong, C. H. Chang, A. Cabrini, and G. Torelli, "Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions," *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 6, pp. 921–932, June 2014.

[104] C. C. Bissell and D. A. Chapman, *Digital Signal Transmission.* Cambridge University Press, 1992.

[105] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *NIST Special Publication 800-22 (revised May 15, 2002)*, 2010.

[106] K.-B. Cho, A. Krymski, and E. Fossum, "A 1.2 V micropower CMOS active pixel image sensor for portable applications," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, CA, Feb. 2000, pp. 114–115.

[107] N. Liu, S. Hanson, D. Sylvester, and D. Blaauw, "OxID: On-chip one-time random ID generation using oxide breakdown," in *Proc. 2010 IEEE Symp. on VLSI Circuits*, Honolulu, HI, June 2010, pp. 231–232.

[108] S. Stanzione, D. Puntin, and G. Iannaccone, "CMOS silicon physical unclonable functions based on intrinsic process variability," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 6, p. 14561463, April 2011.

[109] U. Ruhrmair *et al.*, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inform. Forensics and Security*, vol. 8, no. 11, pp. 1876–1891, August 2013.

[110] L. Alaus, D. Noguet, and J. Palicot, "A reconfigurable linear feedback shift register operator for software defined radio terminal," in *Proc. 3rd Int. Symp. on Wireless Pervasive Computing*, Santorini, May 2008, pp. 319–323.

[111] "Free tool can change SN and IMEI to unlock iphone," 2013. [Online]. Available: http://yjjhen.sinaapp.com/

[112] Y. S. Lee, H. J. Lee, and E. Alasaarela, "Mutual authentication in wireless body sensor networks (WBSN) based on Physical Unclonable Function (PUF)," in *Proc. 9th Int. Wireless Communications and Mobile Computing Conf. (IWCMC)*, Sardinia, Italy, July 2013, pp. 1314–1318.

[113] S. K. Srivathsa, “Secure and energy efficient physical unclonable functions,” Ph.D. dissertation, University of Massachusetts Amherst, Feb. 2012.

[114] N. Pathak and R. Mohan, “Performance analysis and implementation of CMOS current starved voltage controlled oscillator for phase locked loop,” *International Journal of Emerging Technology and Advanced Engineering*, vol. 4, no. 3, pp. 365–369, March 2014.