2016

Enhanced Hardware Security Using Charge-Based Emerging Device Technology

Yu Bi
University of Central Florida

ENHANCED HARDWARE SECURITY USING CHARGE-BASED EMERGING DEVICE TECHNOLOGY

by

YU BI

B.S. Xidian University, 2010
M.S. New York University, 2012

A dissertation submitted in partial fulfilment of the requirements
for the degree of Doctor of Philosophy
in the Department of Electrical Engineering and Computer Science
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Summer Term
2016

Major Professor: Jiann S. Yuan

ABSTRACT

The emergence of hardware Trojans has largely reshaped the traditional view that the hardware layer can be blindly trusted. Hardware Trojans, which are often in the form of maliciously inserted circuitry, may impact the original design by data leakage or circuit malfunction. Hardware counterfeiting and IP piracy are another two serious issues costing the US economy more than $200 billion annually. A large amount of research and experimentation has been carried out on the design of these primitives based on the currently prevailing CMOS technology.

However, the security provided by these primitives comes at the cost of large overheads mostly in terms of area and power consumption. The development of emerging technologies provides hardware security researchers with opportunities to utilize some of the otherwise unusable properties of emerging technologies in security applications. In this dissertation, we will include the security consideration in the overall performance measurements to fully compare the emerging devices with CMOS technology.

The first approach is to leverage two emerging devices (Silicon NanoWire and Graphene SymFET) for hardware security applications. Experimental results indicate that emerging device based solutions can provide high level circuit protection with relatively lower performance overhead compared to conventional CMOS counterpart. The second topic is to construct an energy-efficient DPA-resilient block cipher with ultra low-power Tunnel FET. Current-mode logic is adopted as a circuit-level solution to countermeasure differential power analysis attack, which is mostly used in the cryptographic system. The third investigation targets on potential security vulnerability of foundry insider's attack. Split manufacturing is adopted for the protection on radio-frequency (RF) circuit design.

To my little angle and my dearest family.

ACKNOWLEDGMENTS

First, I would like to express my special thanks to my advisor, Professor Jiann S. Yuan, for his warm, strong support, consideration, and encouragement throughout my graduate studies. His passion and dedication to research has sound effects on me and will guide me in my future life. His consideration and support has won my greatest respect and sincere friendship. He contributed continuous guidance and suggestions in this work. At the meantime, I have been provided with the essential lab resources and software tools to conduct the research work. His technical and editorial experiences were very critical to the completion of this dissertation too.

My thanks also go to my other four dissertation committee members: Dr. Yier Jin, Dr. Ronald F. DeMara, Dr. Mingjie Lin and Dr. Lee Chow for attending my dissertation defense, reading previous drafts of this dissertation and providing valuable comments that improved the presentation and contents of this dissertation.

I am grateful to all my colleagues: Ekavut (Alex) Kritchanchai, Georgie Brussenskiy, Ursila Khan, Qutaiba Hassan, Shayan Taheri, Jie Lin, Mahed Batarseh, Hojjatollah Fallah, Kiana Montazeri, Aiman Salih. The discussions and exchanges of knowledge enriched my skills and experience. In particular, Alex helped me with LNA circuit design, RF energy harvest design and ADS simulation and optimization. I have collaborated with Qutaiba Hassan and Shayan Taheri in my hardware security research, and they gave me precious inspirations.

Last, but not least, I would like to thank my family, especially my wife Yunshu Wang, for their understanding and support during the past few years. It was their love and support that made this dissertation possible. My parents – Hongxia Yu and Mingcong Bi have my deepest gratitude and love for their dedication and many years of support during my studies.

TABLE OF CONTENTS

LIST OF FIGURES x

LIST OF TABLES xv

CHAPTER 1: INTRODUCTION 1

1.1 Hardware Security 2

1.1.1 Hardware Trojan 2

1.1.2 Physically Unclonable Functions (PUF) 3

1.1.3 Reverse Engineering 4

1.1.4 Side-Channel Attacks 5

1.2 Contribution of the Dissertation 5

1.2.1 Enhanced Security Primitives using Emerging Devices 6

1.2.2 DPA-resilient Block Cipher Design 6

1.2.3 Split Manufacturing on RF Power Amplifier 7

1.3 Dissertation Organization 8

CHAPTER 2: BACKGROUND 9

2.1 Tunnel FET 9

2.2 Silicon NanoWire FET 13

2.3 Graphene SymFET 16

2.4 Other Non-Charge-based Emerging Devices 19

2.4.1 Spin-Transfer Torque RAM (STT-RAM) 19

2.4.2 Resistive RAM (RRAM) 19

CHAPTER 3: ENHANCED HARDWARE SECURITY PRIMITIVES BEYOND PUF . . 21

3.1 SiNW FET based Camouflaging 21

3.2 SiNW FET based Polymorphic Gates 27

3.3 Graphene SymFET based Circuit Protectors 32

3.3.1 Current based Circuit Protector 32

3.3.2 Voltage based Circuit Protector 35

3.4 Graphene SymFET based XOR Logic 38

3.5 Discussion 41

3.6 Summary 41

CHAPTER 4: DPA-RESILIENT BLOCK CIPHER DESIGN 43

4.1 Tunnel FET Circuit Evaluation 43

4.1.1 TFET-based Current Mode Logic 43

4.1.2 Design Optimization 45

4.1.3 TFET-based CML Standard Cells 47

4.1.4 Security Evaluation of TFET-based CML Gates 50

4.2 Implementation of Cryptographic System 52

4.2.1 Overview of the KATAN Cipher 53

4.2.2 CML Implementation on KATAN 56

4.2.3 Power Model and Attack Mechanism 57

4.2.4 Correlation Power Analysis on KATAN32 59

4.3 Discussion 63

4.3.1 Circuit-Level Optimization 64

4.3.2 Encryption Algorithm Consideration 64

4.4 Summery 65

CHAPTER 5: SPLIT MANUFACTRUING ON RF POWER AMPLIFIER 67

5.1 Motivation 67

5.2 RF Design Flow Basics 68

5.2.1 RF Design Procedures 69

5.2.2 Power Amplifier Modeling and Analysis 70

5.3 Split Manufacturing in RF Circuits 72

5.3.1 The First Example 74

Scenario I: Removal of Metal6 Layers (Inductors) 75

Scenario II: Removal of Metal5 and Metal6 Layers (Capacitors and Inductors) 80

Scenario III: Obfuscation Techniques 83

5.4 Experimentation 84

5.4.1 Scenario I: Removal of Metal6 Layers (Inductors) 85

5.5 Discussion 92

5.6 Summery 93

CHAPTER 6: CONCLUSION 94

6.1 Enhanced Hardware Security Primitives beyond PUFs 94

6.2 DPA-resilient Block Cipher Design 95

6.3 Split Manufacturing on RF Power Amplifier 95

LIST OF REFERENCES 96

LIST OF FIGURES

Figure 2.1 3-D Physical Structure of (a) A Tunnel FET [1] vs. (b) A FinFET [2]. . 10

Figure 2.2 TFET Device Modeling: (a) TFET Verilog-A Model (b) I_{DS} vs. V_{GS} [3]. 12

Figure 2.3 3D Sketch of The SiNW FETs Featuring Two Independent Gates and Its Associated Symbol [4] 14

Figure 2.4 Both N and P-type Device Branches Show Subthreshold Slopes $S \leq 70mV/dec$. I_{on}/I_{off} Ratios of $\approx 10^7$ ($\approx 10^6$) Are Obtained Respectively for the N-type (P-type) Conduction Branches. [5] 15

Figure 2.5 Sketch of the SymFET 17

Figure 2.6 I-V Characteristics of SymFET Device for Different Top and Back Gate Voltage Combinations 18

Figure 2.7 IMAMTJ and PMAMTJ 19

Figure 2.8 Bi-polar RRAM operation. 20

Figure 3.1 CMOS Camouflaged Layout for Achieving XOR, NAND or NOR [6] . 22

Figure 3.2 One Tile Layout for Either An NAND or An XOR Gate Under Different Pin Connections [7] 24

Figure 3.3 Camouflaging Layout Performing NAND or NOR 25

Figure 3.4 Camouflaging Layout with Four Possible Functions: NAND, NOR, XOR or XNOR 26

Figure 3.5 (a) SiNW FETs NAND (b) CMOS NAND 29

Figure 3.6 (a) SiNW FETs NOR (b) CMOS NOR 29

Figure 3.7 Original Functionality of A SiNW FET Complex Gate (a) Transistor Schematic (b) Gate Schematic 30

Figure 3.8 Reconfigured Functionality of A SiNW FET Complex Gate (a) Transistor Schematic (b) Gate Schematic 31

Figure 3.9 Schematic of Current based Circuit Protector 33

Figure 3.10 Simulation of Output Current Changing with VDD 34

Figure 3.11 Voltage based Circuit Protector using SymFET (a) Schematic (b) Simulation Results 37

Figure 3.12 Voltage based Circuit Protector on 1-Bit Full Adder (a) Schematic (b) Simulation Results 38

Figure 3.13 Schematic of the SymFET XOR Logic. 40

Figure 3.14 Simulation Results of the SymFET XOR Logic. 40

Figure 4.1 (a) The Universal Diagram of CML Circuits (b) Schematic of the TFET-based CML Inverter. 45

Figure 4.2 Different Configurations of TFET CML Inverter vs. CMOS CML Inverter. 47

Figure 4.3 The Universal Schematics Structure of Four Different CML Circuits: (a) AND (b) Multiplexer (MUX) (c) Exclusive-OR (XOR) (d) D Latch. . . . 48

Figure 4.4 (a) XOR Simulation Results (b) D Latch Simulation results. 49

Figure 4.5 The Power Traces Between Static XOR and CML XOR. 51

Figure 4.6 The Abstract Schematic of the KATAN Cipher. 53

Figure 4.7 Two Additional Hardware Blocks: (a) IR (Counting Cycles) and (b) Key Schedule. 54

Figure 4.8 KATAN32 Power Measurements CML TFET vs. Static TFET. 57

Figure 4.9 The Correlation Power Analysis Flow on KATAN Cipher. 59

Figure 4.10 CPA Attack on One Clock Cycle (a) TFET Static KATAN32 vs. (b) TFET CML KATAN32. 62

Figure 5.1 Standard RF Circuit Design Flow 69

Figure 5.2 Schematic of A Class-AB Power Amplifier 75

Figure 5.3 A Class-AB Power Amplifier With Metal6 Removed (Missing Inductors) 75

Figure 5.4 (a) Supply Voltage and Gate Biasing versus Output Power (b) Supply Voltage and Gate Biasing versus Power-added Efficiency 77

Figure 5.5 (a) Supply Voltage and Frequency versus Output Power (b) Supply Voltage and Frequency versus Power-added Efficiency 77

Figure 5.6 (a) Gate Biasing and Frequency versus Output Power (b) Gate Biasing and Frequency versus Power-added Efficiency 78

Figure 5.7 (a) Output Inductor and RF Choke versus Output Power (b) Output Inductor and RF Choke versus Power-added Efficiency 79

Figure 5.8 Schematic of Class-AB Power Amplifier Without Top Two Metal Layers (Missing Inductors and Capacitors) 80

Figure 5.9 (a) RF Choke and Output Coupling versus Output Power (b) RF Choke and Output Coupling versus Power-added Efficiency 81

Figure 5.10 Four Possible Output Matching Network for the Class-AB Power Amplifier 82

Figure 5.11 Schematic of A Cascode Class-E Power Amplifier 84

Figure 5.12 (a) Layout of Class-E Power Amplifier (b) Microchip View of the Fabricated Class-E Power Amplifier 85

Figure 5.13 Schematic of the Class-E Power Amplifier Without Metal6 86

Figure 5.14 Layout of the Class-E Power Amplifier Without Metal6 86

Figure 5.15 First-stage and Second-stage Gate Biases versus (a) Output Power (b) Power-added Efficiency. 88

Figure 5.16 First-stage and Second-stage Supply Voltages versus (a) Output Power (b) Power-added Efficiency. 88

Figure 5.17 (a) Output Power versus L_{in} and L_{d1} (b) Power-added Efficiency versus L_{in} and L_{d1} 90

Figure 5.18 (a) Output Power versus L_s and L_{d2} (b) Power-added Efficiency versus L_s and L_{d2} 91

Figure 5.19 Overall Performance versus L_{tr} 92

LIST OF TABLES

Table 2.1 InAs Homo-junction TFET Device Parameters [8]. 11

Table 3.1 List of True and Dummy Contacts to Realize Three Functions for the Camouflaged Layout Presented in Figure 3.1 23

Table 3.2 List of Possible Functions from One Tile Layout 24

Table 3.3 List of True and Dummy Contacts To Realize Basic Functions for The Layout in Figure 3.3 25

Table 3.4 List of True and Dummy Contacts To Realize Complex Functions for Layout in Figure 3.4 27

Table 3.5 A Summary of Developed Polymorphic Gates 28

Table 3.6 Simulation Results for NAND/NOR Gates 30

Table 3.7 Simulation Results of the SiNW FET and CMOS 5-input Polymorphic Function 32

Table 3.8 Power Provided by Current based Circuit Protector 34

Table 3.9 Power Measurement of SymFET Voltage based Circuit Protector 38

Table 3.10 Summary of SiNW FET and SymFET in Security Applications 42

Table 4.1 Area, Delay and Power of the TFET-based CML Standard Cells 50

Table 4.2 Power Consumption Comparison Among Different Implementations on KATAN32. 56

CHAPTER 1: INTRODUCTION

With the emergence of information technology and its critical role in our daily lives, the risk of cyber attacks is larger today than ever before. Many security systems or devices have critical assurance requirement. Their failure may endanger human life and environment (as with military and transportation system), do serious damage to major financial infrastructure, endanger personal privacy, and undermine the viability of whole business sectors (cable service). Even the perception that a system is more vulnerable than it really is (paying with a credit card over the Internet) can significantly impede economic development. Information security engineering focuses more on the defense against intrusion and unauthorized use of resources with software in the past, such as antivirus, firewall, security information management, virtualization, cryptographic software, and security protocol. While the battle between software developers and hackers has raged since the 1980s, the underlying hardware was generally considered safe, though not perfectly reliable.

However, in the last decade or so, this assumption is increasingly questionable. The battle field extends to hardware domain because more attacks on hardware are discovered and they are shown to be more effective and efficient than traditional software attacks. Additionally, the complexity of the design, fabrication, and distribution of electronics has caused a shift throughout the industry towards a global business model. In such a model, untrusted entities participate either directly or indirectly in all phases in the life of an electronic device or integrated circuit (IC), which provides more poten- tial opportunities for adversaries to perform their attacks. The use of untrusted (and potentially malicious) third parties into the development flow also increases the security concerns as designs and devices pass through deeper supply chains. Therefore, the IC development supply chain is now considered susceptible to various attacks, such as hardware Trojan attacks, reverse-engineering, side-channel attacks, counterfeiting, and so forth. This disseration will discuss the partial solutions on those potential security concerns.

1.1 Hardware Security

1.1.1 Hardware Trojan

Trusted Integrated Circuit design is a newly proposed topic due to the progress of globalization and the fast improving IC manufacturing technology. Because of global economic pressures, the development and fabrication of advanced ICs are migrating offshore in order to lower the cost. As a result, the whole IC supply chain once located in one country can be spread globally now. To control all these manufacturing facilities is almost impossible while on the other hand, to compromise the IC supply chain for sensitive commercial and defense applications becomes easier. Also, under the pressure of market requirements, auto-placement and auto-routing tools are widely used in modern IC design to deal million-gate level circuits in order to reduce product developing cycle time. These tools, however, are not optimal and leave plenty of chip space unused. Based on the advanced IC manufacturing technology, it is much easier for attackers to embed some malicious circuits, so-called Trojan circuits, in the unused space, or other parameters without changing the area of the whole chip.

Traditional function testing is less effective in detecting Trojan circuit for the following reasons, 1) the trigger condition of a Trojan rarely appears, 2) Trojan inputs could be any patterns in the gap between the vast amount of exhaustive input patterns and the relatively small amount of testing patterns actually used, 3) the harm of Trojan circuits may emerge after a long time after chips are implemented. For example, the Trojan can be a series of XOR gates to compare some inner signals with a preset value, a value that will not appear under normal testing patterns. Only if the attacker loads a special test pattern could the Trojan be triggered to do harm to the circuit.

A lot of research has been done concerning the security of cryptographic IP cores and embedded systems with various design methods and hardware-based approaches. For example, in [9]

a root-of-trust model together with a security policy was proposed. The authors paid attention on the security of ubiquitous embedded devices at the design methodology level to prevent the system from side-channel attacks. Also, another common approach to implement tamper-resistance is to use a separate secure co-processor module [10]. Other methods to counter probing attacks, side-channel attacks are proposed in [11, 12].

1.1.2 Physically Unclonable Functions (PUF)

Classic cryptographic mechanisms and protocols are among the most surprising and elegant algorithms within the wide spectrum of computer science tasks. Although their mathematical correctness is still not proved, it is widely considered that they are secure. However, it has also been demonstrated that classic cryptographic systems are easily compromised using side-channel techniques and physical attacks. More recently, a new type of security primitive, the physical unclonable functions (PUFs), has attracted a great deal of attention.

A PUF is a multiple-input–multipleoutput function that has hard-to-predict dependency between the outputs and the inputs. While the initial proposal used an optical mesoscopic system for demonstration, the tremendous growth in interest in PUFs is due to its standard semiconductor integrated circuit (IC) implementation. The uniqueness of identical PUF design is provided by currently ubiquitous process variation. Several PUF architectures (e.g., arbiter based, ring oscillator, and SRAM) have been proposed, implemented, and analyzed. The initial security protocol was secret key in which one party collects a set of challenge–response pairs before releasing the PUF to another party. The authentication of the second party can now be done by the first party by issuing a challenge. Only the entity with the PUF can respond to an unknown challenge fast.

In the past few years, several PUF primitives in silicon CMOS technologies have been proposed and demontrated [13]. These include delay-based PUFs such as Arbiter or Ring Oscillator

PUF and memory-based PUFs such as SRAM or Flip-Flop PUF. However, it has been proved that none of these PUF primitives are completely immune to different types of attacks. For example, the Arbiter PUF and its variants all suffer from the modeling attacks (e.g. the machine learning alogrithm) [14], and the SRAM PUF can be characterized by photon emission analysis and cloned by Focused Ion Beam Circuit Edit [15].

1.1.3 Reverse Engineering

Reuse-based system-on-chip design using hardware intellectual-property cores has become a pervasive practice in the industry. The IP cores usually come in the form of synthesizable register-transfer-level descriptions (Soft IP), gate-level designs directly implementable in hardware (Firm IP), or GDS-II design database (Hard IP).

RE of an IC involves 1) identifying the device technology used in it [16]; 2) extracting its gate-level netlist [17]; and/ or 3) inferring its functionality [18]. Several techniques and tools have been developed to reverse engineer1 ICs [19]. RE can be misused to steal and/or pirate a design, identify the device technology, or illegally fabricate the target IC. The objective of the attacker is to successfully reverse engineer a design to a desired abstraction level. He can use the known input–output pairs to verify the functional correctness of the reverse-engineered design and/or to guide RE to extract the gate-level netlist of a competitor's IP and use it in one's own IC or illegally sell it as an IP.

The objective of the attacker is to successfully reverse engineer a design to its target abstraction level. The target level can vary depending on the objective of the attacker. If the objective is to pirate the design, the target abstraction level can be either the physical design level, the gate level, or the RT level. If the goal is to insert Trojans, the target abstraction level can be either the gate level or the RT level.

1.1.4 Side-Channel Attacks

Side-channel attacks exploit the leakage of secret informatio through a physical modality when an application is being executed on a system. Side-channel attacks are powerful and have been able to break most existing important cryptographic algorithms [20]. Consider the RSA encryption algorithm which uses modular exponentiation with large exponents. An essential step in RSA encryption and decryption is computing m^e, where m is the message and e is either the pubic or private key. For an acceptable security level, m and e are required to be at least 1024-b numbers [21]. A naive approach to calculate m^e involves multiplying m by itself $e-1$ times. This approach requires $e-1$ multiplications, which is prohibitive.

Power consumption [12], electromagnetic (EM) emanations [22], photonic emissions [23], and acoustic noise of the system [24] are all correlated with the exponent, and can be used to extract the secret. Another side-channel attack against RSA exploits the Chinese reminder theorem (CRT) that is typically used to speed up its computation. If an adversary induces a fault during the CRT computation, the secret information can be obtained. Fault attacks can be launched using lasers, glitches in power supplies and clocks, and X-rays [25].

1.2 Contribution of the Dissertation

With the above motivation, this dissertation is devoted to the development of a series of low-cost and effective techniques for secure and trustworthy integrated circuits. All the security issues discussed above will be dealt with from three subjects: enhanced security primitives using emerging devices, robust and energy-efficient block cipher, and emerging split manufacturing methodology.

1.2.1 Enhanced Security Primitives using Emerging Devices

While most work with emerging technologies for security purposes to date has been with implementations like Physical Unclonable Functions (PUFs) [26], PUFs essentially leverage device-to-device process variation. In some sense this suggests that noisier devices are more useful. Orthogonal to these efforts, in this chapter, we present a collection of design concepts that leverage the unique properties of emerging technologies, other than relying on noisy devices, for IP protection and hardware attack prevention. Specifically, this chapter considers two emerging technologies: silicon nanowire (SiNW) FETs [4] and Graphene SymFETs [27], and makes the following contributions.

- To assist IP protection, we introduce SiNW FET based camouflaging layout and polymorphic gates to help obfuscate layouts and netlists. Hamming distance (50%) can be accomplished by a smart placement alogrithm, thereby improving the security of IP protection.
- We further propose Graphene SymFET circuit protectors to counter fault injection attacks. Two circuit protectors, voltage and current-based schemes, are presented in details.
- Last, we present a lightweight SymFET based XOR for implementing cryptographic functions, which consumes less transistor counts and energy consumption against CMOS counterparts.

1.2.2 DPA-resilient Block Cipher Design

In this work, we further extend research in this direction to use emerging devices to preserve low power consumption but achieve the goal of DPA-resilience. More specifically, we will demonstrate that by implementing CML with emerging tunnel transistors (TFETs) for lightweight encryption

algorithms, one can significantly improve the circuit security at a fraction of the power when compared to CMOS equivalents. Our contributions are as follows:

- We introduce a library of TFET-based current mode logic components that cover all basic logic gates. This is the first work to introduce a full set of designs and measurements of TFET-based CML gates.
- We then use the TFET based CML gates to design a 32-bit, lightweight KATAN cipher. To the best of our knowledge, this is also the first attempt to use CML gates based on emerging technologies for lightweight cryptography implementations.
- Finally, we present correlation power analysis on the TFET CML KATAN cipher, which shows that TFET CML is better than MOS CML in terms of the power consumption and area usage when achieving similar security levels.

1.2.3 Split Manufacturing on RF Power Amplifier

The fundamental difference between digital design flow and RF design process has already raised the concern whether it is still applicable to apply split manufacturing in RF design. A deep look into both design flows proves us that it would be more suitable to apply split manufacturing in RF circuits than in digital circuits because of the unique functionality metal layers play in RF designs:

- Approach I: Remove only the top metal layer from the layers to generate FEOL. Since the inductors are often located in the top layer, the FEOL foundry does not have the information of interconnections through top metal layer as well as the inductor locations and sizes.
- Approach II: Remove the top and the second to the top metal layers. In this approach, two upper metal layers are removed so that both inductors and capacitors are missing from the

FEOL layout because the capacitors are often built through the top two metal layers.

- Design obfuscation. For RF designs, inductors are always located in metal rings and lower metal layers will be removed inside the rings for performance optimization. Therefore, the rings themselves, which contain multiple metal layers, would indicate positions and approximate sizes of inductors. Similarly, the lower metal layers will not be used where capacitors are located. Therefore, attackers in both approaches I and II may learn the precise positions of the removed inductors/capacitors and may even further estimate their sizes. To further increase the security level but still to avoid performance overhead, we propose an obfuscation technique during the design phase to insert non-functional rings and to create empty zones in the original design. Using this method, it becomes more difficult for attackers to pin down the location, the count, and the sizes of passive components.

1.3 Dissertation Organization

The outline of this dissertation is summarized as follows: Chapter 1 summarizes the overall picture of this dissertation, including the introduction, research contribution and the dissertation outline; The device backgrounds used in this dissertation is discussed in Chapter 2; Chapter 3 presents a group of hardware security primitives using emerging device technologies, such as Silicon NanoWire FET and Graphene SymFET; Chapter 4 proposes a DPA-resilient block cipher design with tunnel FET; Chapter 5 demonstrates the benefits of proposed IP protection scheme leveraging the split manufacturing technique; Finally, Chapter 6 concludes the research work and future research directions.

CHAPTER 2: BACKGROUND

In this chapter, we review several emerging device technologies, including Tunnel FET, Silicon NanoWire FET and Graphene SymFET. The associated underlying physical phenomena in these different emerging devices are also explained. In the latter chapters, the fundamental phenomena presented in this chapter will be employed as the building blocks in enhanced hardware security primitives.

2.1 Tunnel FET

Different types of tunneling FETs (TFETs) have been developed and fabricated [28, 29]. Among them, III-V TFETs appear more promising due to their higher conduction current. More specifically, InAs homo-junction TFETs [8] and GaSb-InAs hetero-junction TFETs [30] have been the subject of much study. Considering that the InAs homo-junction is the more mature of these two devices, we will employ it as our TFET transistor model in this work. FinFET 20 nm technology is also adopted for comparison. The physical structures (used in Synopsys TCAD simulation) of both the homo-junction TFET and FinFET are depicted in Figure 2.1 [1, 2].

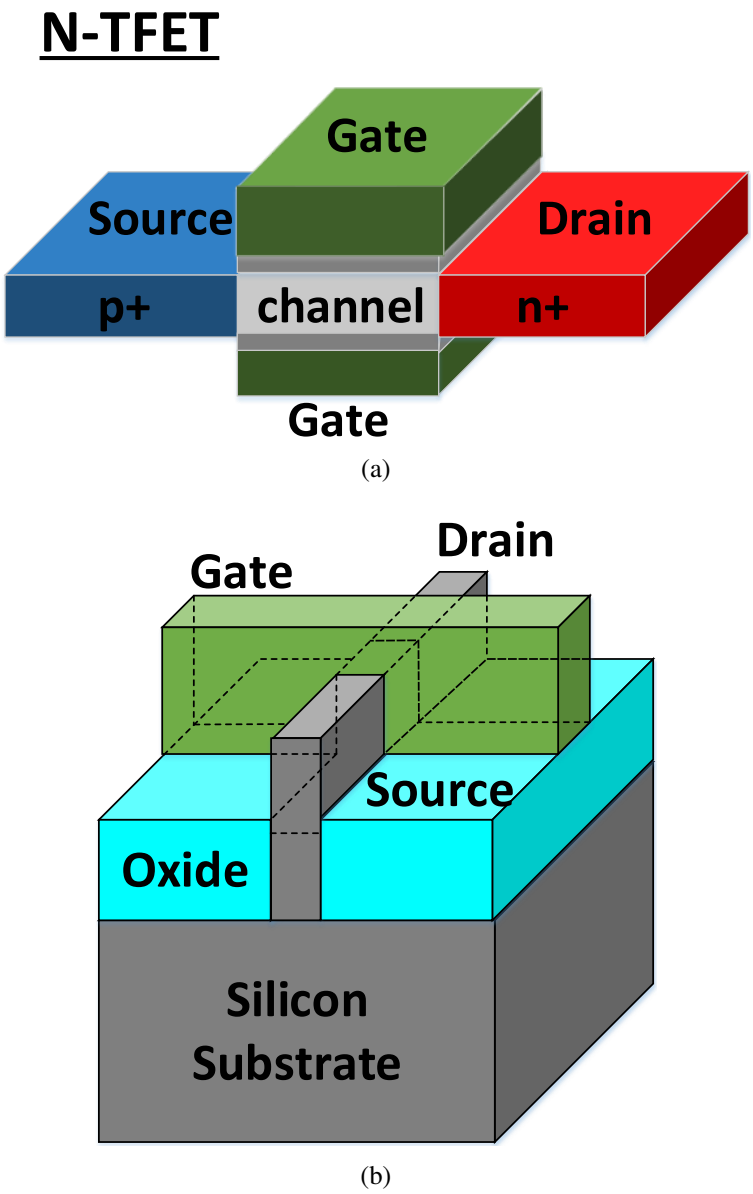


Figure 2.1: 3-D Physical Structure of (a) A Tunnel FET [1] vs. (b) A FinFET [2].

It is apparent that TFETs have asymmetrical doping where source and drain are p-type and n-type doping, respectively. A gate voltage can induce band-to-band tunneling at the channel to control the tunneling current. In contrast, in a conventional CMOS transistor, current conduction

occurs via electron carriers with enough energy to surmount the channel thermal barrier. The Fermi-Dirac distribution limits the sub-threshold slope (SS) to 60 mV/decade. However, the high energy carriers in TFETs can be filtered by the gate-voltage-controlled tunnel such that a sub-60 mV/decade subthreshold swing is achievable at the room temperature [28]. With improved steep slope and high on-current at a low supply voltage, TFETs could enable supply voltage scaling to further address challenges such as undesirable leakage currents, threshold voltage reduction, etc.

The device parameters assumed for the InAs homo-junction TFET (that we will employ in our circuit simulations) are listed in Table 2.1. A Si FinFET is also included as the baseline.

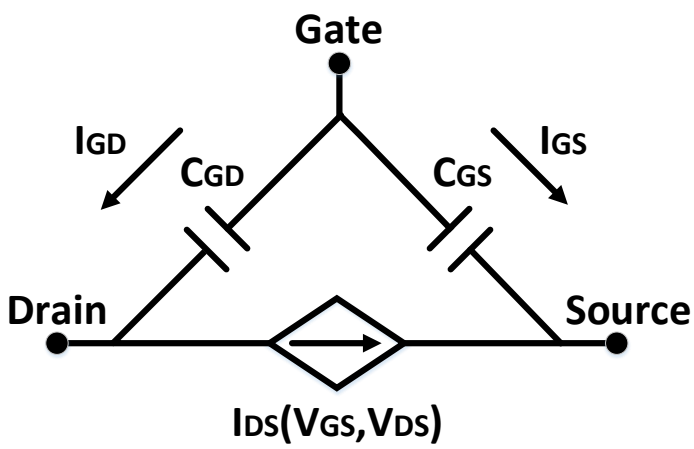
Table 2.1: InAs Homo-junction TFET Device Parameters [8].

Gate Length (L_G)	20 nm
Body Thickness (T_{ch})	5 nm
Dielectric Thickness (HfO_2)	5 nm
Source Doping (p+)	$4 \times 10^{19}\ cm^{-3}$
Drain Doping (n+)	$6 \times 10^{17}\ cm^{-3}$
Si FinFET S/D Doping	$1 \times 10^{20}\ cm^{-3}$

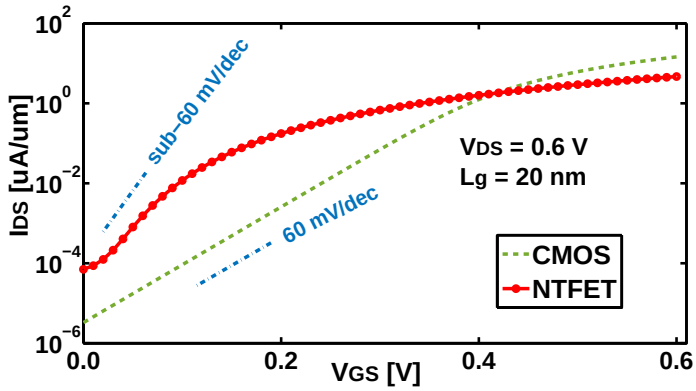
While a compact SPICE model has been recently developed for TFETs [31, 32], in this work, we employ a look-up table based Verilog-A model derived from TCAD Sentaurus for our simulations as this model has been widely used and validated [33]. Figure 2.2a depicts the structure of the TFET Verilog-A model [3]. It is composed of three parts: gate-drain capacitance C_{GD}, gate-source capacitance C_{GS} and the transfer characterisitics $I_{DS}(V_{GS}, V_{DS})$. The current models of different paths are also listed in Equation (2.1). The calculation of three current models refers to

the look-up table that includes a range of fine-step voltage bias and capacitance.

$$\text{Look Up Table} = \begin{cases} I_{GD} = \dfrac{d}{dt}(C_{GD} * V_{GD}) \\ I_{GS} = \dfrac{d}{dt}(C_{GS} * V_{GS}) \\ I_{DS} \rightarrow (V_{GD}, V_{GS}) \end{cases} \tag{2.1}$$



(a)



(b)

Figure 2.2: TFET Device Modeling: (a) TFET Verilog-A Model (b) I_{DS} vs. V_{GS} [3].

By employing the TFET Verilog-A model, we evaluate the DC performance of an N-type TFET as shown in Figure 2.2b, where the on-current I_{DS} varies with gate-source voltage V_{GS}. CMOS data is also included for comparison. Both CMOS and TFET devices assume 20 nm technology with V_{DS} = 0.6 V. A TFET's sub-threshold slope is improved when compared to CMOS. Notably, when the gate-source voltage is less than 0.4 V, the conducting current of TFETs outperforms the CMOS counterpart. (However, when $V_{GS} > 0.4\ V$, the CMOS device exhibits a better on-current.) As a result, TFETs represent promising ultra low-power features that provide further V_{DD} scaling in integrated circuit designs.

2.2 Silicon NanoWire FET

In several nanoscale FET devices (45nm and below), the superposition of n-type and p-type carriers is observable under normal bias conditions. The phenomenon, called ambipolarity, exists in various materials such as silicon [34], carbon nanotubes [35] and graphene [36]. Through the control of this ambipolarity, we can adjust the device polarity during the post-deployment stage. Transistors with a controllable polarity have already been experimentally fabricated in several novel technologies, such as carbon nanotubes [37], graphene [38] and Silicon NanoWires (SiNWs) [39, 40]. Given an additional gate, the operation of these FETs is enabled by the regulation of Schottky barriers at the source/drain junctions. The example emerging device considered in this chapter is a vertically-stacked silicon nanowire (SiNW) FET, featuring two Gate-All-Around (GAA) electrodes [4]. Figure 2.3 shows the 3D structure of the SiNW FET. Vertically-stacked GAA SiNWs represent a natural evolution of FinFET structures, providing better electrostatic control over the channel and, consequently, superior scalability properties [4].

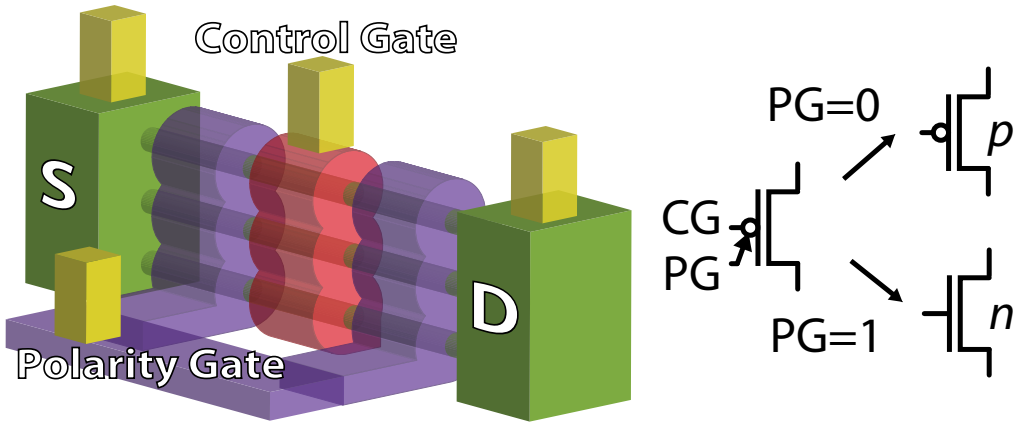


Figure 2.3: 3D Sketch of The SiNW FETs Featuring Two Independent Gates and Its Associated Symbol [4]

In this device, one gate electrode, the Control Gate (CG), acts conventionally by turning on and off the device depending on the gate voltage. The other electrode, the Polarity Gate (PG), acts on the side regions of the device, in proximity to the Source/Drain (S/D) Schottky junctions, switching the device polarity dynamically between n- and p-type (2.4). The input and output voltage levels are compatible, enabling directly-cascadable logic gates [4, 7]. It should be noted that owing to the device geometries, the two gates are not identical from a size standpoint. Indeed, the PG is roughly two times bigger than the CG, leading to differences in their timing responses. Such a behaviour can be easily compensated at the design level by assigning the signal with the lowest frequency/switching activity to the slowest gate terminal.

Thanks to their one-dimensional structure, DG-SiNWFETs demonstrate remarkable electrostatic performances. Figure 2.4 depicts the subthreshold slopes of 64 mV/dec and 70 mV/dec for the p-type and n-type parts of the characteristic, respectively, hence competing with the most advanced FinFET technologies [41]. In addition, the one-dimensional electrostatic control over the channel coupled to the use of a Schottky barrier-based injection mechanism enables very low off-current densities of a few ρA per μm when compared with few tens of ρA per μm for low-power

FinFETs [41]. These combined facts qualify the presented device technology as high-performance low-standby-power technology.

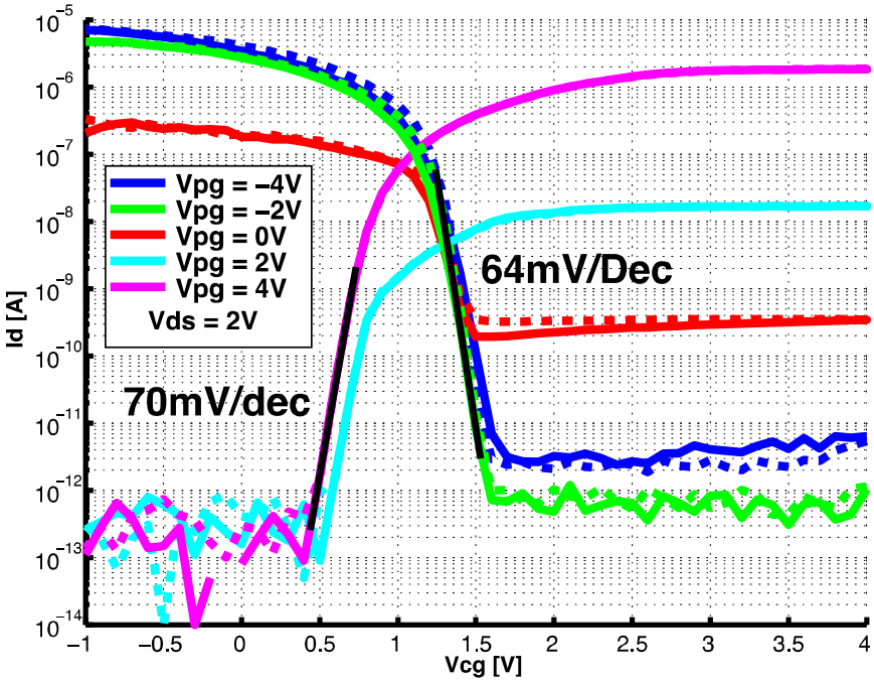


Figure 2.4: Both N and P-type Device Branches Show Subthreshold Slopes $S \leq 70mV/dec$. I_{on}/I_{off} Ratios of $\approx 10^7$ ($\approx 10^6$) Are Obtained Respectively for the N-type (P-type) Conduction Branches. [5]

While many emerging devices demonstrates the polarity control property (SiNWFETs, Graphene transistors, CNTFETs, NEM relays, etc.), we focus on SiNW FET due to their full process compatibility with the current silicon technology and their high probability of industrial transfer in the near term. In addition, both single transistors and basic logic gates for SiNWFETs have been experimentally demonstrated. Furthermore, a simple compact model is available. However, note that the techniques presented in this chapter are not limited only to this device, but rather can be applied to any other polarity controllable transistor devices.

2.3 Graphene SymFET

As MOSFET alternatives, tunneling based transistor technologies (e.g., [29,42]) are being actively investigated by device scientists. Among these devices is a double-layer graphene transistor – often referred to as SymFET [43]. In the SymFET device, tunneling occurs between the two graphene sheets – which are separated by insulating and oxide layers. Possible $I_{DS} - V_{DS}$ characteristics of a SymFET – which are a function of a top gate voltage (V_{TG}) and back gate voltage (V_{BG}) (see the device symbol in the Figure 2.6 inset) – are illustrated in Figure 2.6. Similar characteristics have also been observed experimentally [44]. More specifically, V_{TG} and V_{BG} change the carrier type/density of the drain and source graphene layers by electostatic field, which can modulate I_{DS}. Per Figure 2.6, the value and position of the peak current depends on the values of V_{TG} and V_{BG}. Note that the I-V curves illustrated in Figure 2.6 assume a SymFET device with a 100 nm $\times$ 100 nm footprint with a coherence length of 0.75X of the edge side, and an insulating layer of boron nitride (h-BN) that is 1.34 nm (or 4 h-BN layers) thick. While further study is required, tuning the insulator thickness could represent another design lever at the device-level. For example, theoretically, by reducing barrier thickness to 2 layers of h-BN, tunneling current could be increased substantially – albeit at the expense of higher leakage current [27].

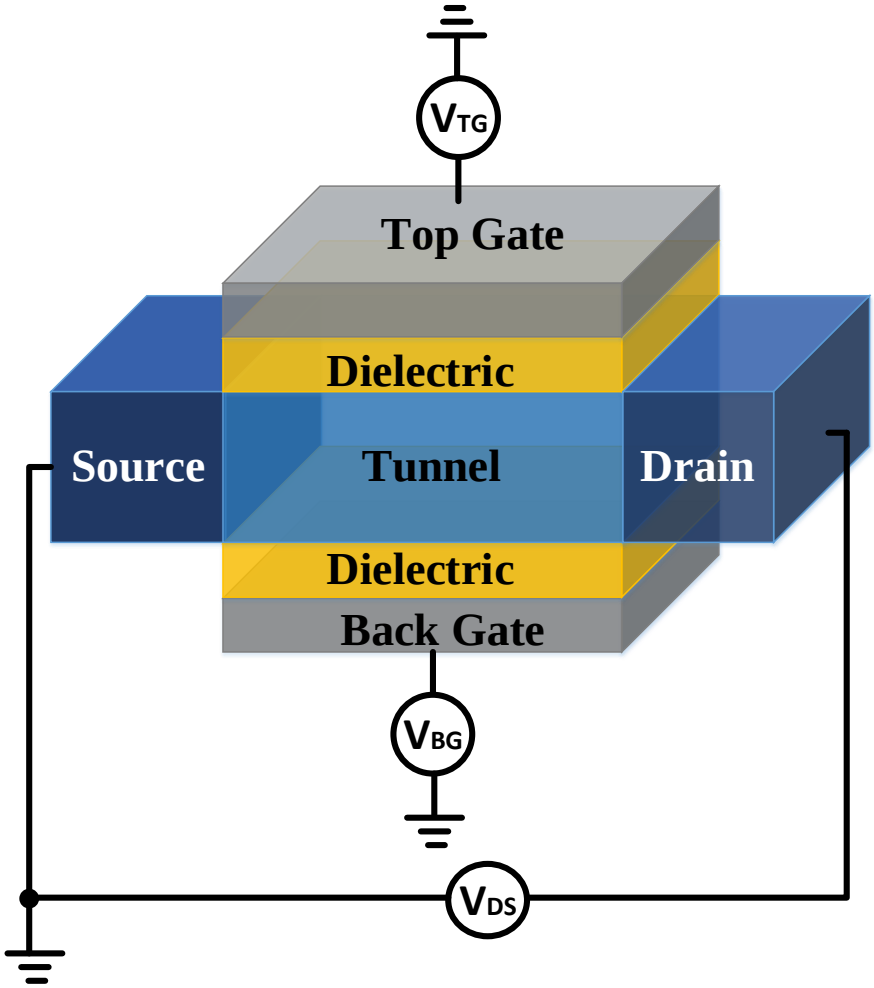


Figure 2.5: Sketch of the SymFET

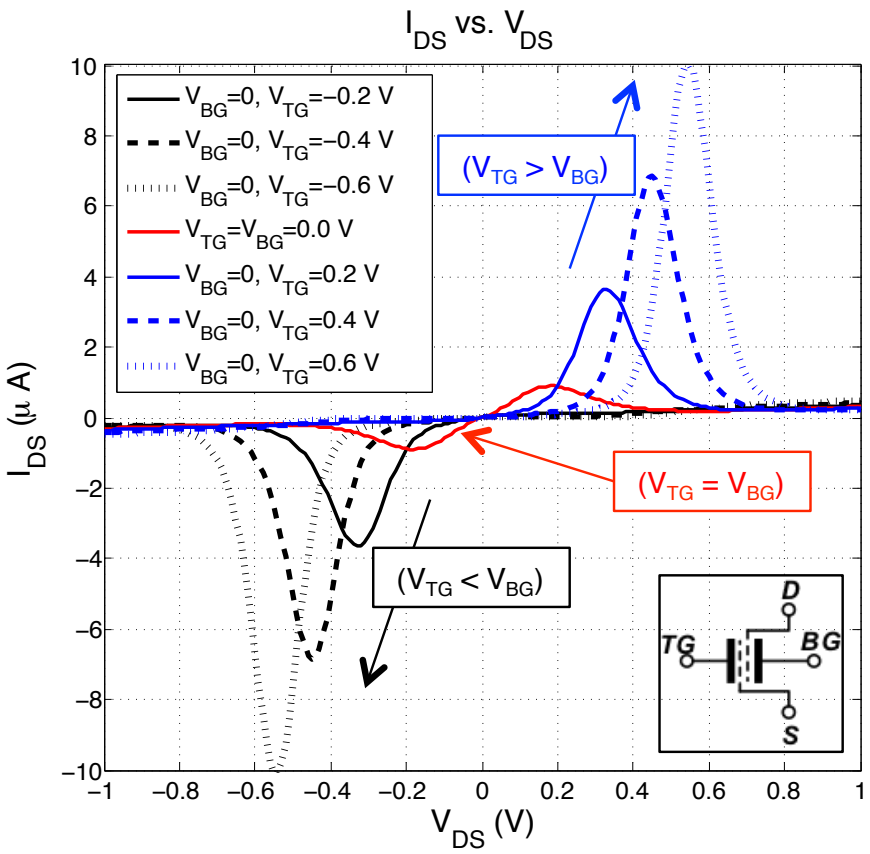


Figure 2.6: I-V Characteristics of SymFET Device for Different Top and Back Gate Voltage Combinations

The unique I-V characteristics of SymFET offer some interesting circuit-level alternatives for realizing both analog and digital circuits [27, 45]. For example, simply cascading SymFET devices leads to an extremely small majority gate design. Furthermore, different combinations of V_{TG} and V_{BG} can change the shape of the I-V curve dramatically. Devices such as the interlayer tunnel FET (ITFET) have similar behaviors as the SymFET. We use SymFETs as a proxy for all these types of devices.

2.4 Other Non-Charge-based Emerging Devices

2.4.1 Spin-Transfer Torque RAM (STT-RAM)

The magnetic tunneling junction (MTJ) is the essential element of spintronics. In essence, an MTJ is an insulator sandwiched between two ferromagnetic layers that form a two terminal device. While one ferromagnetic layer is magnetically pinned to a fixed direction, the other layer's magnetization can be altered. Interestingly, passing current through the MTJ itself, in different directions can alter the magnetization polarity through a spin-charge interaction process called Spin-Transfer Torque (STT) [46]. This is the basis for write operation in STT-MRAMs. MTJ device technology has consistently advanced over the past decade [47]. Recent efforts have advanced from devices with in-plane magnetization states (Fig. 2.7a) to devices with perpendicular magnetic anisotropy (PMA) (Fig. 2.7b) [48] – e.g., based on CoFeB/MgO/CoFeB material stacks. PMAMTJs demonstrate superior switching and retention properties as compared to earlier in-plane anisotropy MTJs.

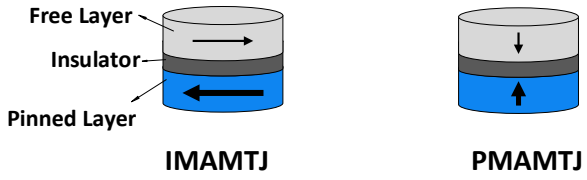


Figure 2.7: IMAMTJ and PMAMTJ

2.4.2 Resistive RAM (RRAM)

Resistive switching in metal-insulator-metal (MIM) nano-pillars is the operational principle for RRAMs [49]. While the exact switching physical process is still under debate, it is agreed that the formation and dissolution of conductive filaments (CF) under electric potential results in the switching of resistive states [50–52]. As shown in Fig. 2.8 in a bi-polar RRAM element a pos-

itive voltage (V_{form}) across a fresh device results in the formation of a CF, taking the device to a low-resistance-state (LRS). A negative voltage can dissolve the CF, restoring the device to the high-resistance-state (HRS). Among the vast variety of materials reported in literature, transitional metals (HfO_x and/or TiO_x-based) show the best performance [51]. In this paper, we focus on bi-polar RRAM devices that are accessed with a transistor [53].

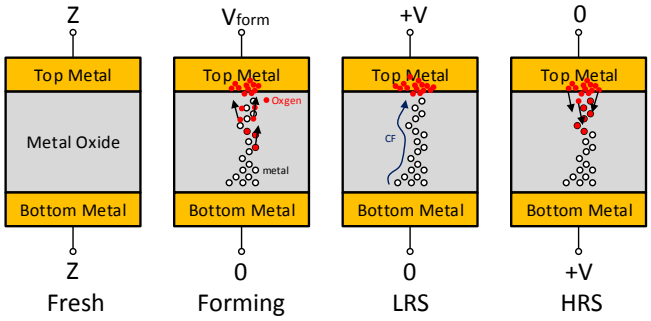


Figure 2.8: Bi-polar RRAM operation.

CHAPTER 3: ENHANCED HARDWARE SECURITY PRIMITIVES BEYOND PUF

The development of emerging technologies provides hardware security researchers with opportunities to utilize some of the otherwise unusable properties of emerging technologies in security applications. Originally developed as alternatives to CMOS technology to overcome the scaling limit, emerging technologies also demonstrated their unique features which, besides improving circuit performance, can simplify circuit structure for security purposes such as IP protection and Trojan detection [54,55]. While traditional metrics, such as power, delay etc., are the major criteria to evaluate the merits of emerging devices, in this chapter, we will include the security consideration in the overall performance measurements to fully compare the emerging devices with CMOS technology.

3.1 SiNW FET based Camouflaging

Counterfeiting and IP piracy are among the most serious security threats to the IC industry. In order to prevent attackers from learning the circuit schematic through reverse engineering, various protection methods have been developed among which camouflaging is a popular solution [56–58]. This method relies on layout-level obfuscation with similar layouts for different gates. As a result, attackers cannot easily recover the circuit structure through reverse engineering [6]. However, the overhead in applying CMOS camouflaging gates can be rather high such that both power consumption and area would increase significantly for high level protection.

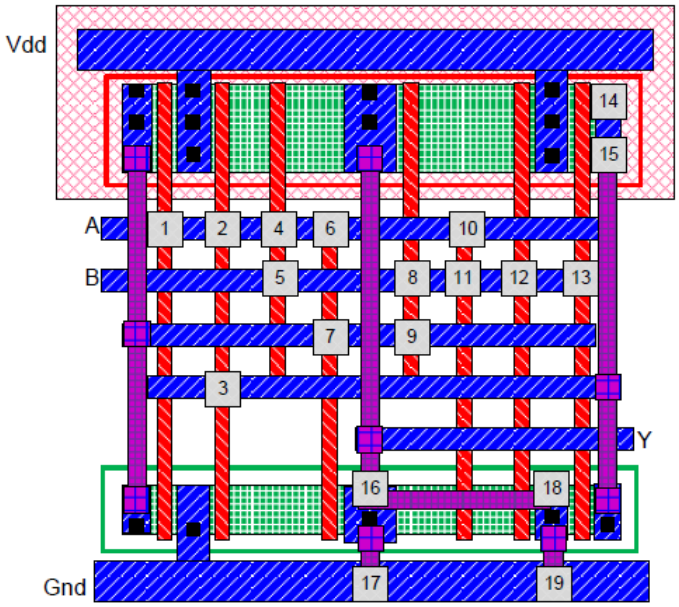


Figure 3.1: CMOS Camouflaged Layout for Achieving XOR, NAND or NOR [6]

In [6], a CMOS camouflaging standard cell utilizes 12 transistors and a group of contacts to achieve three logic functions, as shown in Figure 3.1. There are more contacts than normal standard cell, since some of the contacts work as dummies to camouflage the functionality of this logic cell. More specifically, in Table 3.1, different combinations of true and dummy contacts deliver three different logic functions. For example, when contacts 2,4,6,8,11,12,16,17 are true and contacts 1,3,5,7,9,10,13,14,15,18,19 are fake, the camouflaging layout performs the NAND functionality. With more functionalities being achieved by a camouflaging gate, it becomes more difficult for attackers to recover the gate functionality through reverse engineering. Compared to the 4-T NAND, 4-T NOR and 8-T XOR gates, the area overhead of CMOS camouflaging layout ranges from 50% to 200%.

Table 3.1: List of True and Dummy Contacts to Realize Three Functions for the Camouflaged Layout Presented in Figure 3.1

Function	Contacts	
	True	Dummy
NAND	2,4,6,8,11,12,16,17	1,3,5,7,9,10,13,14,15,18,19
NOR	2,5,6,11,12,18,19	1,3,4,7,8,9,10,13,14,15,16,17
XOR	1,3,4,7,9,10,12,13,14,15,18,19	2,5,6,8,11,16,17

It is not surprising that CMOS camouflaging gates consume significantly larger area than normal gates. Because of the fixed polarities of both PMOS and NMOS, designers must prepare spare transistors in order to build a camouflaging gate. However, the polarity controllable SiNW FETs, with their unique property, can help build camouflaging gates without using extra FETs. As demonstrated in [7], only four SiNW FETs are required to build an XOR or a NAND gate (See Figure 3.2). This one tile layout includes four SiNW FETs where circles stand for drain/source pins and bars represent the polarity gate (or control gate). A further analysis reveals that by connecting pins with different signals, the four SiNW FETs in Figure 3.2 can perform five other meaningful functions besides the NAND and XOR. A list of all these connections as well as the corresponding output functions are presented in Table 3.2.

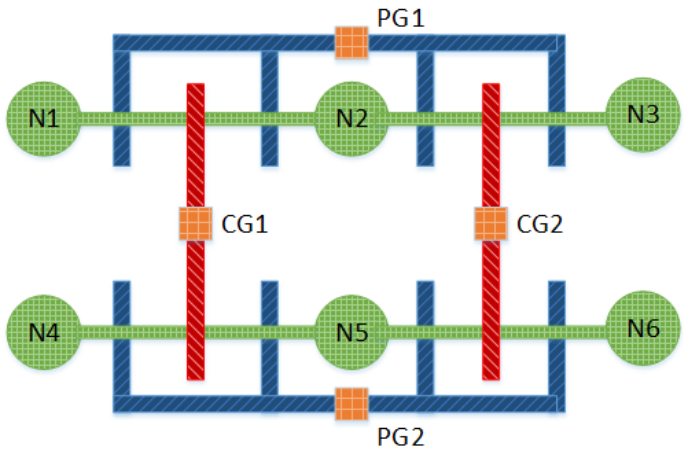


Figure 3.2: One Tile Layout for Either An NAND or An XOR Gate Under Different Pin Connections [7]

Table 3.2: List of Possible Functions from One Tile Layout

PG1	PG2	CG1	CG2	N1	N2	N3	N4	N5	N6	Function (Y)
GND	VDD	A	B	Y	VDD	Y	GND	N/A	Y	NAND
GND	VDD	A	B	VDD	N/A	Y	Y	GND	Y	NOR
Bbar	B	A	Abar	VDD	Y	GND	GND	Y	VDD	XOR
Bbar	B	A	Abar	GND	Y	VDD	VDD	Y	GND	XNOR
Bbar	B	A	Abar	Cbar	Y	C	C	Y	Cbar	XOR3
Bbar	B	A	Abar	C	Y	Cbar	Cbar	Y	C	XNOR3
GND	VDD	A	X	X	VDD	Y	X	GND	Y	Buffer

Note that the functionality of the gate is fixed post-fabrication with gate signals being connected to physical terminals. After these connections, the polarity gates perform as normal input gates and no extra control circuitry is required to maintain the functionality. This structure, or more precisely the polarity controllable feature, provides an ideal candidate for camouflaging gates since all these gates share the same structure with only four SiNW FETs used. In fact, the additional polarity gate is leveraged in the camouflaging gate layout to reduce the transistor count. The overhead of this SiNW based camouflaging layout is negligible, which is mainly caused by additional

insignificant dummy contacts.

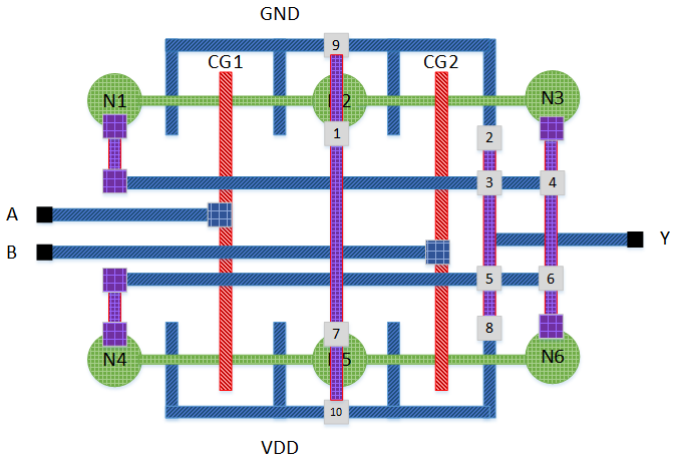


Figure 3.3: Camouflaging Layout Performing NAND or NOR

Table 3.3: List of True and Dummy Contacts To Realize Basic Functions for The Layout in Figure 3.3

Function	Contacts	
	True	Dummy
NAND	1,2,4,5,10	3,6,7,8,9
NOR	3,6,7,8,9	1,2,4,5,10

Following this concept, two SiNW FETs based camouflaging gates are built of different complexities. The first camouflaging gate performs either NAND or NOR functionality if different sets of dummy contacts are selected. Figure 3.3 shows the layout of the gate where 10 dummy/real contacts are used. As presented in Table 3.3, if we leave No. 3,6,7,8,9 as dummy contacts, the gate is a NAND gate. If we make No. 1,2,4,5,10 contacts as dummy contacts, the gate will then perform NOR logic.

Furthermore, Figure 3.4 shows a more complex camouflaging gate which can act as NAND, NOR, XOR or XNOR given different sets of dummy contacts. As described in Table 3.4, different

connections can result in four different operations for the same input signals. Again, only four SiNW FETs are used in this camouflaging gate. Compared to the CMOS-based camouflaging gate which needs 12 transistors for a NAND-NOR-XOR gate, the proposed circuit structure can reduce two-thirds of the transistor count. However, five more contacts are used in the SiNW FET based camouflaging gate although the area overhead incurred by the extra contacts are negligible considering the transistor count reduction. To further evaluate the security improvement, the security metric has been used to check how easily an attacker can guess the full functionality of a given designs containing camouflaging gates. That is, if one camouflaging layout can achieve four functions, the chance that the attacker can retrieve the correct result is 25%. Therefore, assuming that there are N SiNW FET camouflaging layouts incorporated in the design, the attacker may have to try up to 4^N times to get the correct design layout. As a consequence, it is promising that the SiNW FET based camouflaging layout which has more functionality and less area consumption compared to CMOS counterparts can achieve higher level of protection to circuit designs.

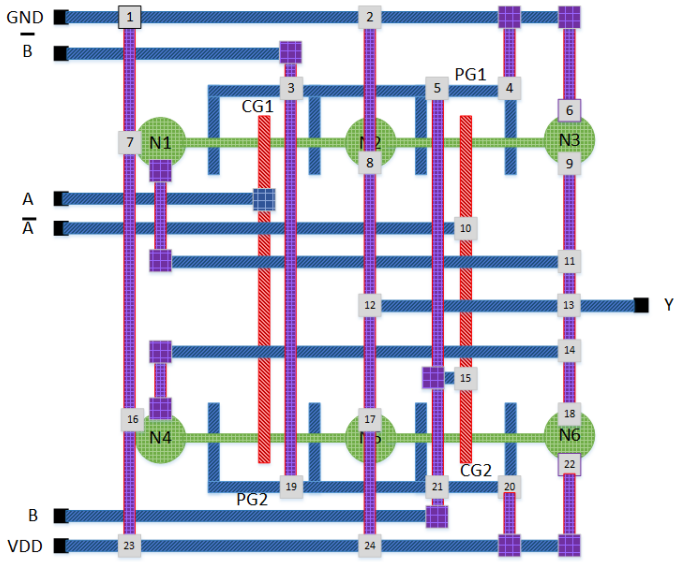


Figure 3.4: Camouflaging Layout with Four Possible Functions: NAND, NOR, XOR or XNOR

Table 3.4: List of True and Dummy Contacts To Realize Complex Functions for Layout in Figure 3.4

Function	Contacts	
	True	Dummy
NAND	1, 4, 8, 9, 11, 13, 15, 16, 18, 20, 24	2, 3, 5, 6, 7, 10, 12, 14, 17, 19, 21, 22, 23
NOR	2, 4, 7, 9, 13, 14, 15, 17, 18, 20, 23	1, 3, 5, 6, 8, 10, 11, 12, 16, 19, 21, 22, 24
XOR	1, 3, 6, 8, 10, 11, 12, 16, 17, 18, 21, 22	2, 4, 5, 7, 9, 13, 14, 15, 19, 20, 23, 24
XNOR	1, 5, 6, 8, 10, 11, 12, 16, 17, 18, 19, 22	2, 3, 4, 7, 9, 13, 14, 15, 20, 21, 23, 24

3.2 SiNW FET based Polymorphic Gates

Polymorphic electronics, which were firstly introduced in [59], are based on the idea of having multiple functionalities built in the same cell and deciding the input-output relation by means of a controllable factor in the circuit. For instance, a polymorphic gate presented in [59] would be an AND gate when the VDD is 3.3 V and function as an OR gate when VDD is lowered to 1.5 V. Such multi-functional gates would prove useful in a number of applications. Circuits that change functionality with temperature variation can find use in aerospace applications, or those that respond to VDD variation could be used to change functionality when the battery is low. Also, polymorphic electronics could prove useful in evolvable, intelligent or self-checking hardware [60]. For security purposes, adding polymorphic gates to a digital circuit can hide the real functionality of the circuit. Since the circuit functions correctly only in a certain configuration of the control signals known to the designer, even if the adversary knows the whole netlist (including the dummy and true contacts), he or she will not be able to utilize the circuit in his or her own

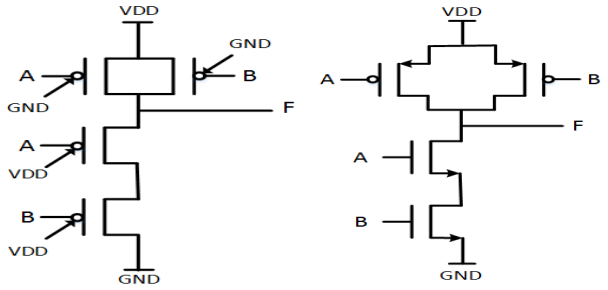
design. Carefully encrypting a logic in this way, can ensure that it will take too long for the adversary to find the key (a vector constructed from all the morphing signals of the polymorphic gates) [61]. Therefore, the polymorphic gate becomes a good candidate for integrated circuits protection against IP piracy.

Table 3.5: A Summary of Developed Polymorphic Gates

Function	Morph Method	Number of Transistors	Published in
AND/OR	27/125 C Temperature	6	[62]
AND/OR/XOR	3.3/0.0/1.5V External Signal	10	[62]
AND/OR	3.3/0.0V External Signal	6	[62]
NAND/NOR/XOR/AND	0.0/0.9/1.1/1.8V External Signal	11	[62]
AND/OR	1.2/3.3V Vdd	8	[62]
NAND/NOR	3.3/1.8V Vdd	6	(Fabricated) [59]
NAND/XOR	0/3.3V External Signal	9	[60]
NAND/NOR	VDD and GND Interchange	4	This Work

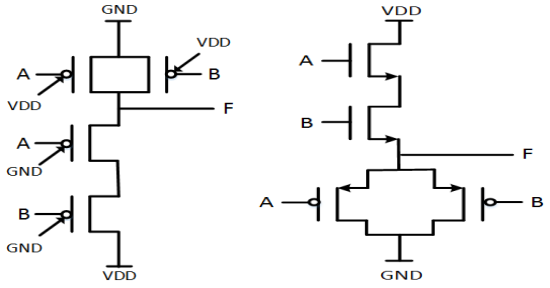
Here we present a novel approach to designing polymorphic gates using polarity controllable FETs. The ability to control the polarity of a transistor enables us to build polymorphic cells with a much less number of transistors. As shown in Figures 3.5 and 3.6, the basic NAND and NOR gate structure is similar for both the CMOS and the SiNW FET. The polarity control gate does not reduce the number of transistors required to implement NAND and NOR using SiNW FET technology. However, this unique property allows us to change the functionality of the gate simply by interchanging the VDD and GND. Note that interchanging the VDD and GND connections in any CMOS based logic will produce the complement of the original function at the output but full voltage swing at the output will not be achieved due to the presence of PMOS in the pull-down network or NMOS in the pull-up network. Therefore, using this method one can gather the VDD and GND terminals of the NAND and NOR gates in a combinational logic into a vector and construct a “logic encryption key”. As opposed to the work presented in [61], which adds additional XOR or XNOR gates into a logic gate to realize the logic encryption scheme and thus incurs performance overhead, this approach has zero overhead in terms of gate count and trivial

wiring cost due to the switching of VDD/GND. The comparison of transistor counts for different polymorphic gates is listed in Table 3.5.



(a) (b)

Figure 3.5: (a) SiNW FETs NAND (b) CMOS NAND



(a) (b)

Figure 3.6: (a) SiNW FETs NOR (b) CMOS NOR

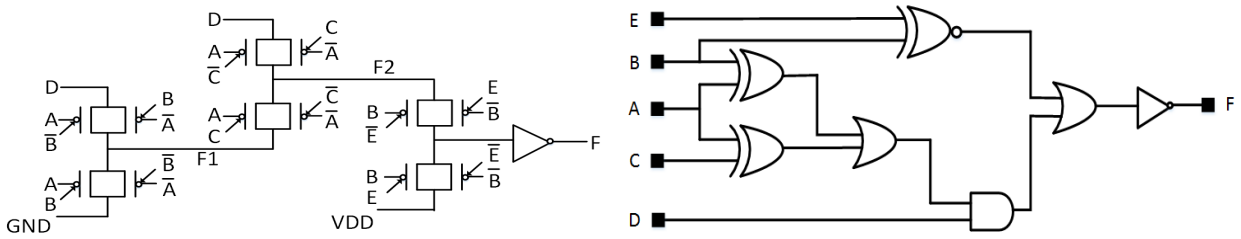
The simulation results for the NAND and NOR generic cells using the EPFL SiNW FET model [7] and the FinFET 22nm Low Standby Power (LSTP) and High Performance (HP) configurations of the PTM model [63], can be viewed in Table 3.6. It is not surprising to see that SiNW FET based NAND (or NOR) gate consumes more dynamic power and has longer delay than the CMOS NAND (or NOR) gate, mainly because of the immaturity of the SiNW FET technol-

ogy. Note that the leakage power of the SiNW FET is drastically reduced compared to FinFET technology.

Table 3.6: Simulation Results for NAND/NOR Gates

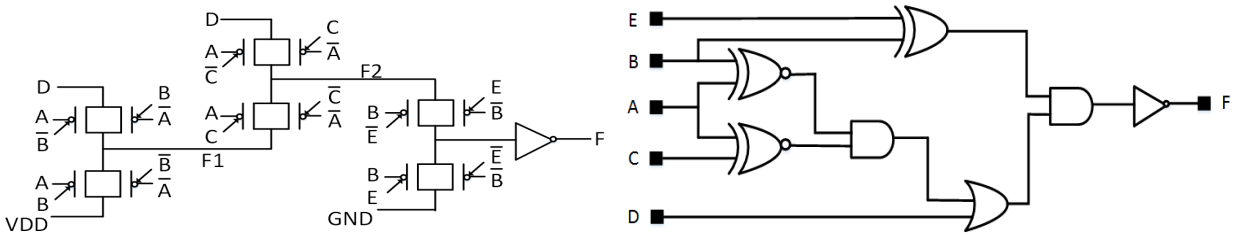
Gate	Static Power(pW)	Dynamic Power at 1GHz(uW)	Delay Averaged Delay(ps)
FinFET 22nm LSTP NOR	52.19	0.19	28
FinFET 22nm HP NOR	30360	0.67	23.5
FinFET 22nm LSTP NAND	27.19	0.15	23
FinFET 22nm HP NAND	1650	0.652	15.5
SiNW FET 20nm NAND/NOR	8.037	1.77	42
SiNW FET 20nm NAND/NOR	4.127	1.13	56

The performance comparison in Table 3.6 does not take the SiNW FET unique property into consideration. In fact, the benefits of using SiNW FETs can be revealed if the polarity controllable property is leveraged, e.g., sophisticated polymorphic gates. To validate our claim, a sample polymorphic gate is designed (see Figure 3.7). The two separate functions shown in Figures 3.7(b) and 3.8(b) can be implemented by the SiNW FET circuit in its different VDD and GND configurations depicted in Figures 3.7(a) and 3.8(a).



(a) (b)

Figure 3.7: Original Functionality of A SiNW FET Complex Gate (a) Transistor Schematic (b) Gate Schematic



(a) (b)

Figure 3.8: Reconfigured Functionality of A SiNW FET Complex Gate (a) Transistor Schematic (b) Gate Schematic

Table 3.7 lists the simulation results of the designed SiNW FET polymorphic logic and a MUX-based CMOS polymorphic gate which achieves the same functionality. As the results suggest, the SiNW FET approach reduces the total dynamic power due to the less number of cells while suffering from a longer delay because of the same number of cells available in the critical path. Besides the extremely low leakage power, the overall performance of the SiNW FET polymorphic logic is better than its CMOS counterpart. Consequently, SiNW FET circuits outperform CMOS circuits in terms of power and delay while achieving similar level of circuit protection. The security metric that we applied measures the difficulty level if attackers want to learn the circuit structure using the brute force method. That is, if there are N gates each with 2 possible functions in the schematic, it would take 2^N trials for an attacker to determine the exact functionality of the circuit. The benefits can be more significant in more complex polymorphic logic for large-scale circuits protections.

We would like to point that machine learning attacks may be used to speed up the hacking of encryption [64]. Thus, judicious placement of these SiNW FET polymorphic gates in a circuit should also be considered to impede such attacks.

Table 3.7: Simulation Results of the SiNW FET and CMOS 5-input Polymorphic Function

Technology	Static Power(nW)	Switching Average Power(uW)	Average Delay(ps)
FinFET 22nm LSTP	0.755	4.04	80
FinFET 22nm HP	491	5.4	60
SiNW 20nm	0.01	2.5	100

3.3 Graphene SymFET based Circuit Protectors

Besides the above-mentioned IP protection, emerging devices may also help improve circuit resilience to counter various hardware attacks such as fault injection, side-channel signal analysis, etc. with extremely low performance overhead and little circuit redesign. For example, cryptographic circuits are often vulnerable to power supply-based fault injections [65]. The manipulation of the power supply causes faults due to the raise of the setup time needed for registers to switch into the correct state: this phenomenon particularly affects high capacitance paths, which are often the slowest paths of the circuit. In this section, we introduce two SymFET based circuit protectors which leverages the unique I-V characteristics of SymFETs to protect circuits from power supply fault injections.

3.3.1 Current based Circuit Protector

As shown in Figure 2.5, the I-V curve of a SymFET indicates that the I_{DS} only exists for a narrow band of V_{DS}. Supported by this property, we propose a current based circuit protector, which can effectively prevent supply voltage based fault injection. Figure 3.9 shows the proposed structure relying on the unique properties of SymFETs. As shown in the schematic, SymFET M1 is the only transistor directly connected to the power supply VDD, which is also the source to launch a

voltage based fault injection attack.

We use a specific parameter setting to explain how the circuit protector works. In our experiment, V_{TG} is set to 0.6 V and V_{BG} is set to 0 V for all three SymFETs. These gate voltages can be adjusted so that the peak current will appear in different power supply ranges than the one showed in Figure 3.10. Since M2 and M3 are connected in parallel, source-to-drain voltage V_{DS2} for M2 is equal to V_{DS3} for M3, which makes the output current I_{OUT} the same as the input current I_{IN}. The output current I_{OUT} is basically a current source for the circuit under protection. For this SymFET based circuit protector, the output current can only exist for a specific drain-source voltage of SymFET M3. If V_{DS3} is out of this range, either higher or lower than the pre-defined range, the SymFET M3 will be cut off. As a consequence, the circuit under protection will be totally shut down.

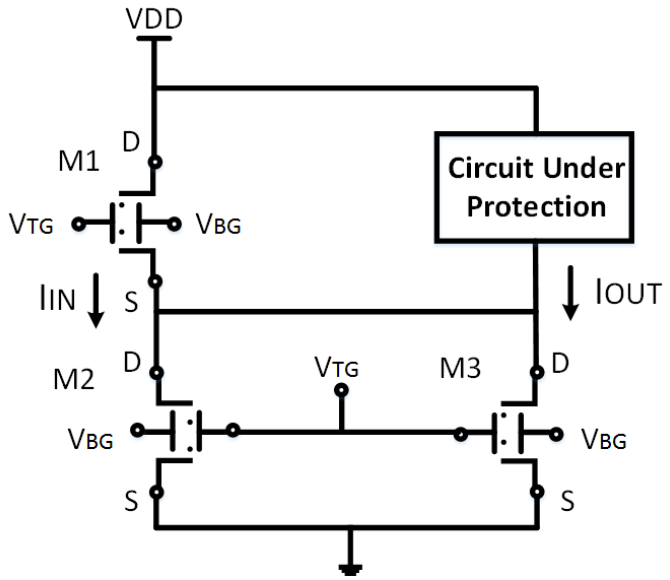


Figure 3.9: Schematic of Current based Circuit Protector

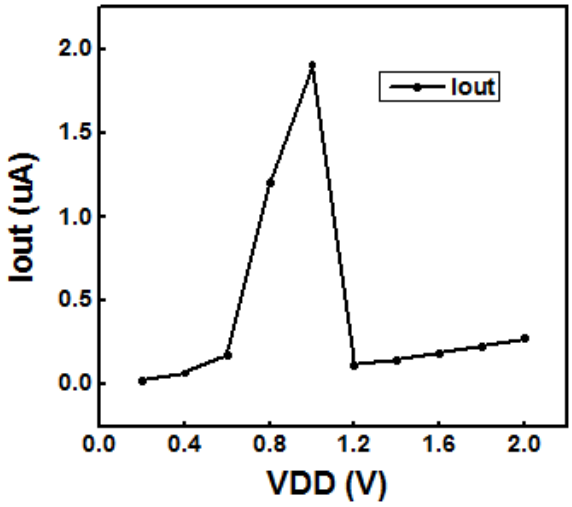


Figure 3.10: Simulation of Output Current Changing with VDD

Table 3.8: Power Provided by Current based Circuit Protector

VDD (V)	0.2	0.4	0.6	0.8	1.0	1.2	1.4	1.6	1.8	2.0
Iout (uA)	0.022	0.067	0.176	1.205	1.904	0.114	0.145	0.184	0.227	0.272
Power (uW)	0.009	0.054	0.211	1.928	3.808	0.273	0.406	0.588	0.817	1.087

The simulation results of the current based circuit protector in Figure 3.10 show that only if the VDD is in the range from 0.8 V to 1 V, the output current will be at its peak values, e.g., 1.928 uA when VDD is 1 V. The power consumption is also derived and listed in Table 3.8. When the supply voltage deviates from its normal value, e.g., 0.6 V, the output current will drop down to 0.176 uA. This feature can be directly exploited in circuit protection, countering side-channel attacks and fault injections. However, due to the limited maximum current, the current protector can mainly be applied for relatively lightweight cryptographic circuits to prevent fault injections. To handle relatively larger loads, either larger SymFET devices or multiple protectors are needed. If the attackers intend to lower the supply voltage to trigger a single-bit error of an encryption

design, the entire circuit can be automatically shut down by the proposed circuit protector before a single-bit error could occur.

Traditionally, power regulators are often used in CMOS technology to protect the main circuit, but they suffer from large area and power consumption. For example, the authors in [66–68] proposed an area-efficient regulator based on the 90nm CMOS technology. The regulator includes more than 20 transistors, 3 capacitors, and 1 resistor with a total area of 0.019 mm^2 and power consumption of 6 μW. However, in our proposed structure, only three SymFET transistors are utilized, leading to an area reduction even though one SymFET consumes larger area than one MOSFET in similar process. The main drawback of the designed circuit protector is the positive voltage at the virtual ground of the main circuit, i.e., the drain voltage of M3 may be larger than 0 V. However, the proposed circuit protector can be used as an alternative to the current source, which acts as both a current source and a circuit protector [69].

3.3.2 Voltage based Circuit Protector

Besides the current based circuit protector which protects the circuit through current manipulation, SymFETs can also be used to control the supply voltage for fault injection prevention. Figure 3.11(a) shows the schematic of the proposed voltage based circuit protector, which is similar to an inverter design [27]. However, in this circuit protector, the top gates of the two SymFETs are connected to the voltage source, while V_B can be manipulated for different cut-off voltage levels for output V_{out}. For instance, in Figure 3.11(b), in the case of V_B equal to 0.8 V, the output voltage quickly drops to nearly zero when VDD is lowered down to 0.65 V, therefore cutting off the voltage supply for the circuit under protection.

To further demonstrate the functionality of the proposed circuit protector, a full adder in the 20nm FinFET technology combined with the protector is implemented and simulated as shown

in Figure 3.12. Note that since the current SymFET technology is not CMOS compatible, 3D stacking is needed to protect a CMOS circuit with the developed protector. That said, we have shown the feasibility of building digital circuits (Inverter, NAND, NOR, etc.) using SymFETs in [27]. Thus, one can ultimately envision a chip comprised entirely of SymFETs. One input of the full adder is set to logic '1', and the other input is given as a periodic pulse signal. As we can see in Figure 3.12(b), the universal VDD is manipulated to decrease gradually. When it reaches 0.65 V, the output voltage of the circuit protector quickly drops to zero. Consequently, both the sum and carry-out in the full adder output zero. We also measured the power consumption by the circuit protector and summarized the results in Table 3.9. Because the dynamic power is frequency dependent, input switching is set at 1 GHz in the simulation. The leakage current shown here is the current flowing through the two SymFETs instead of the circuit under protection. As shown in Table 3.9, when the power supply is large enough to make the full adder operate normally, power consumption by the full adder dominates the overall power consumption. However, if the full adder is completely shut off when the supply voltage becomes lower than 0.65 V, majority of the total power is attributed to the static power of the circuit protector. Though high leakage may not be desired in low-power applications, for circuit protection purpose, the power overhead is bearable as long as it can prevent the intentional injection from the supply voltage. More research is needed along this direction to lower the leakage power.

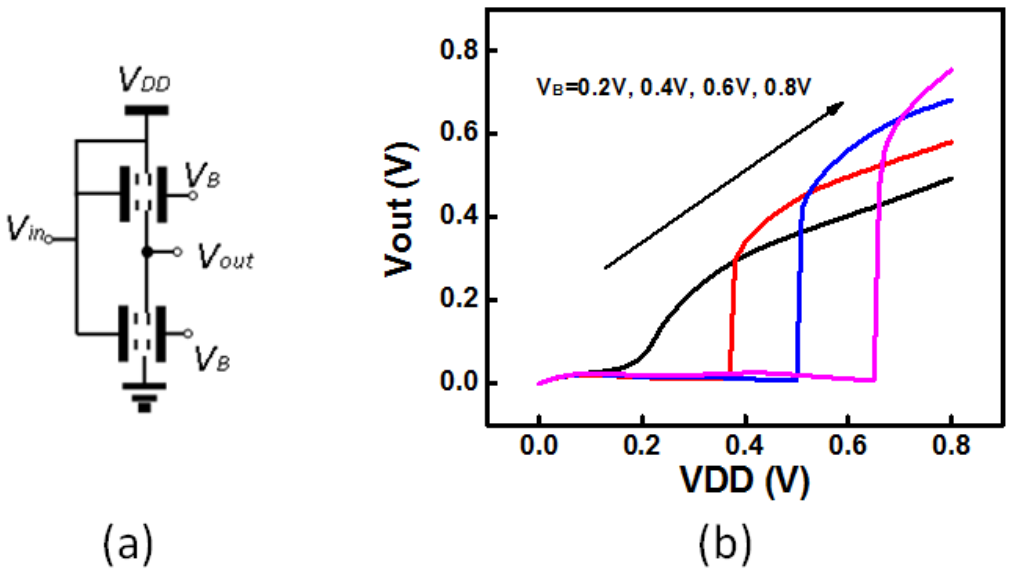


Figure 3.11: Voltage based Circuit Protector using SymFET (a) Schematic (b) Simulation Results

Authors in [70] evaluated the impacts of power supply attacks, where the voltage sensitivity margin is 0.4V. That is, a bit flip error would only happen if the power supply glitch is larger than 0.4V. As what we have presented, the voltage sensitivity of our designs are less than 0.2V. Before the power glitch attack can be triggered, the SymFET circuit protector already shuts down the circuit to prevent such attacks. Note that the sensitivity of the SymFET projector can be adjusted by altering the top/back gate voltages. Another factor to consider is noise in power supply. It may be possible that due to environmental variations, e.g., temperature variation and power noise, the supply voltage may fluctuate. If the voltage variation is larger than the design margin, a false alarm will be triggered and the circuit will be shutdown even though no attacks are launched. For circuits working under the extreme conditions, we may need to tune the circuit protector to increase the allowed supply voltage noise margin.

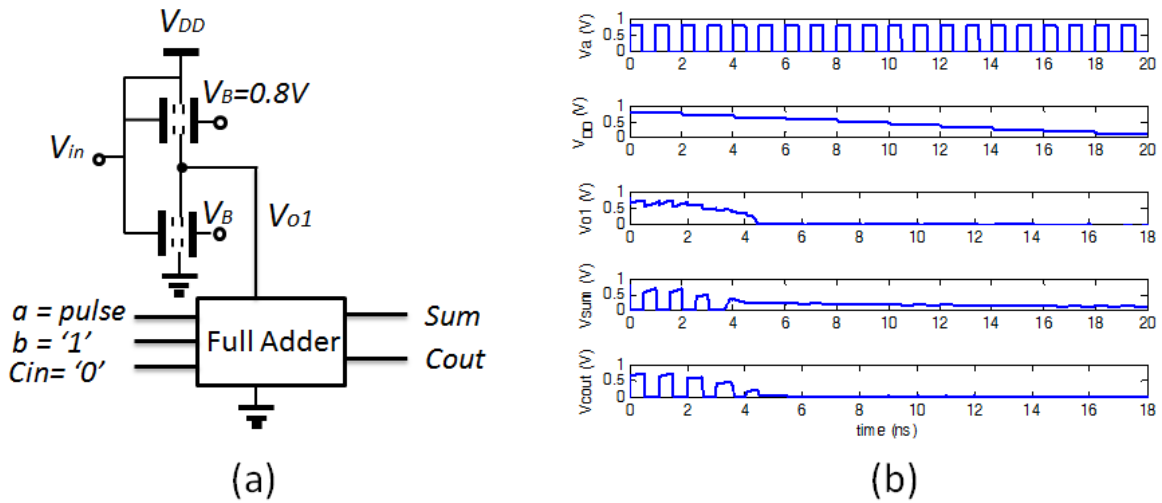


Figure 3.12: Voltage based Circuit Protector on 1-Bit Full Adder (a) Schematic (b) Simulation Results

Table 3.9: Power Measurement of SymFET Voltage based Circuit Protector

Voltage Supply (V)	0.8	0.72	0.64	0.56	0.48	0.40	0.32	0.24
Leakage Current (nA)	527	220	219	208	179	80.3	20.9	4.33
Power of the Protector (nW)	250.5	135.7	142.9	110.3	76.1	30.3	5.9	0.4
Power of the Full Adder (nW)	310.9	117.0	1.0	<0.03	<0.02	<0.02	<0.02	<0.02

3.4 Graphene SymFET based XOR Logic

In the cryptographic systems, XOR logic serves as a basic computation unit for many of the encryption algorithms. Since CMOS XOR gates often take at least 8 transistors, area and power consumption of XOR network becomes the bottleneck to further improve the performance of cryptographic designs. However, in terms of the unique I-V characteristic and low-power feature, the SymFET brings in a new opportunity for hardware security implementation. In [27], a group of SymFET-based generic logic gates have been investigated, such as inverter, NAND and majority gates.

Following a similar design method, a light-weight current-based XOR gate is then developed which uses only two SymFETs. As we can find in Figure 3.13, the Vtg of the upper SymFET is connected to input signal A, while the V_{bg} is connected to input signal B. The drain and source of upper SymFET are connected to the voltage supply and the output port, respectively. In the lower SymFET, the V_{tg} and V_{bg} are tied up to complement A and complement B, respectively. The drain and source connections of lower SymFET are the same as the upper one. The simulation results are shown in Figure 3.14. It illustrates that when input signal A and B are different, there will be a steady output current through the output port. When A and B are of equal values, the output current drops to nearly zero. In this demonstration, input signals are set as square pulses with the peak voltage of 2 V, while the supply voltage keeps at 500 mV. Since the peak current happens due to the different configurations of drain-source voltage and gate voltage (see Figure 2.5), the design also works with the settings of lower VDD and top/back-gate voltage through the same configuration on all terminals.

To fully compare the performance between CMOS XOR and SymFET XOR, delay and power consumption of both gates are also measured. We implemented an 8-transistor XOR gate in CMOS 130nm technology with the nominal voltage of 1.5V [27]. (The 130nm CMOS technology is chosen since this feature size is close to the feature size used by the SymFET device, 100nm $\times$ 100nm.) The CMOS XOR gate consumes 0.632μW. While the SymFET based XOR gate consumes 0.68μW, both gates are comparable in power consumption. However, the average delay of the SymFET XOR gate is 48ps. Compared to the 135ps delay of CMOS XOR gate, the speed of SiNW FET XOR gate is much faster. With slightly larger power consumption, the SymFET XOR gate outperforms CMOS XOR gate significantly in delay and area. Moreover, the power consumption of SymFET XOR gate can be further reduced by lowering the nominal voltage to less than 2.0V.

Although XOR gate is the basic gate for many cryptographic circuits, other gates such as

inverter and NAND gate may also be required. Authors in [27] and [71] have already developed logic gates using SymFET and SiNW FET, respectively. Therefore, the developed XOR gate along with other logic gates can make the cryptographic circuits perform better than their CMOS counterparts.

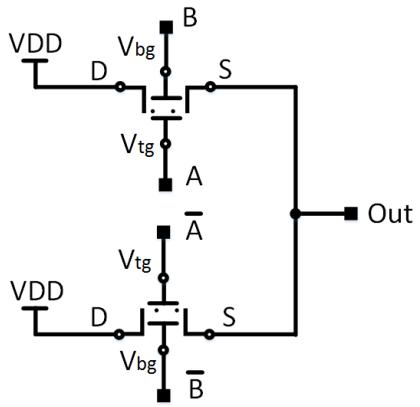


Figure 3.13: Schematic of the SymFET XOR Logic.

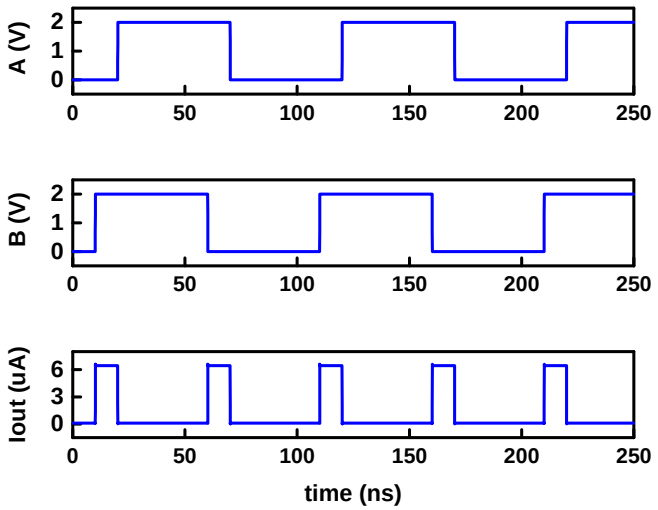


Figure 3.14: Simulation Results of the SymFET XOR Logic.

3.5 Discussion

Emerging technologies, acting as alternatives to CMOS logic, have already shown promising features for high performance circuit design. However, the metrics to evaluate different technologies often follow the traditional criteria, focusing only on power, delay, area, etc. for general-purpose computation modules. Special applications, such as hardware security, are rarely considered mainly because MOSFETs do not support security and circuit protection naturally.

In this chapter, we presented security primitives on how the unique features of emerging technologies can help protect circuits and prevent IP piracy. Unlike CMOS logic, the proposed protection schemes are of much lower overhead because security is not an add-on feature, but a built-in feature. Through the simulation results, the two example devices are proved to be efficient in hardware security applications. These preliminary results lead us towards a new metric for the comparison between CMOS logic and emerging technologies, While traditional metrics, such as power, delay etc., are the major criteria to evaluate the merits of emerging devices, in this chapter, we include the security metric in the overall performance evaluation to fully compare the emerging devices with CMOS technology. A summary of the two emerging devices in hardware security applications is shown in Table 3.10. This table lists the benefits and challenges of the emerging-device based designs compared to CMOS designs and can help guide future designs in the hardware security area.

3.6 Summary

Emerging technologies were investigated in this chapter for their applications in the hardware security domain. Instead of simply replacing CMOS transistors with emerging devices, our work, for the first time, evaluated the unique properties of new devices in helping protect circuit designs and

countering IP piracy. Two emerging technologies were used including SiNW FETs and graphene SymFETs. Five different security applications were designed and verified, ranging from IP protection to efficient cryptographic computation. Through these examples we demonstrated that the unique properties of emerging technologies, if used properly, can provide high level circuit protection with extremely low performance overhead. Along this direction, new evaluation metrics will be developed in our future work to better evaluate the merits of emerging devices. Besides the simulation results, as emerging technologies become more mature, measurements from fabricated devices will also be collected to verify the claim that circuit protection methods can benefit from emerging technologies.

Table 3.10: Summary of SiNW FET and SymFET in Security Applications

	SiNW FETs	Graphene SymFETs
Benefits Over CMOS	Polarity Configurable, Low Static Power Less Transistors for Applications	Low Power, Built-in Negative Differential Resistance
Challenges	Larger Area Per-transistor Large Dynamic Power	Current based Designs, Non-boolean Computation
Opportunities	IP Protection, Logic Encryption, Other Security Applications	Side-channel Attack Prevention, Cryptographic Circuits

CHAPTER 4: DPA-RESILIENT BLOCK CIPHER DESIGN

Orthogonal to current approaches of circuit level optimization, in this chapter we consider how emerging transistor technologies could help mitigate risks of side channel attacks while maintaining low power consumption. Emerging devices have been proven to have unique applications in the hardware security domain [54, 55]. In this work, we further extend research in this direction to use emerging devices to preserve low power consumption but achieve the goal of DPA-resilience [72, 73]. More specifically, we will demonstrate that by implementing CML with emerging tunnel transistors (TFETs) for lightweight encryption algorithms, one can significantly improve the circuit security at a fraction of the power when compared to CMOS equivalents.

4.1 Tunnel FET Circuit Evaluation

Here, we discuss our TFET CML standard cell designs. We begin by discussing a ”generic” TFET-based CML circuit. We then present design specific criteria for TFET-based CML (i.e., required supply voltage values, etc.). After reviewing the power/performance of other TFET CML standard cells, we conclude this section with an initial evaluation of how resilient a TFET CML design might be to DPA.

4.1.1 TFET-based Current Mode Logic

One major difference between CML circuits and single-ended circuits is that the voltage swing of CML is smaller than that of static logic. Thus, differential logic styles were originally designed for high speed communication. Due to invariant power consumption, researchers adopted this circuit-level method as a countermeasure against differential power analysis [74–76]. A “generic”

TFET-based CML circuit is shown in Figure 4.1a. The schematic is divided into two parts: a pull-up network and pull-down network.

For TFET CML, the pull-up network is constructed by either two resistors or two P-type TFETs (PTFETs). Since the consumption of power and area of the resistor is dramatically larger than a FET using modern technology, the FET-based pull-up network dominates. In CML the pull-up network mainly works as the load device to manage the DC voltage drop on the output. By simply tuning the gate bias of a P-type FET, the on-resistance of PTFETs can be adjusted, thereby altering output voltage accordingly. At the bottom of Figure 4.1a, one N-type FET (NTFET) is included to serve as a current source, which can determine the value of output voltage swing. On the other hand, the pull-down network that is composed of NTFETs mainly serves as the major functional unit in the CML circuit. The different logic functions can be achieved by distinct combinations of a group of NTFETs. Note that the inputs of the pull-down network are required to be differential pairs.

Figure 4.1b shows a schematic of a TFET-based current mode inverter/buffer. One pair of transistors is controlled by the differential inputs, IN and IN_b, respectively. The constant driving current is provided by the transistor M5, which is also tunable by the gate bias voltage V_{bias}. Together with M5, transistors M3 and M4 are employed to charge and discharge the output pair, OUT1 and OUT2. When IN is logic 1, M1 is turned on, and the constant current I_C flows through the left-handed path. Thus, OUT1 discharges to a certain value between VDD and GND, and OUT2 alternatively charges to quasi VDD. Note that in the CML design, logic 0 is commonly defined as half VDD, and logic 1 is close to VDD. In this case, OUT1 voltage is less than logic 1, which is treated as logic 0. If OUT1 is extracted as the output pin and the inverted OUT2 is extracted as complementary output pin, the schematic achieves the inverter function. On the contrary, if OUT1 is treated as the complementary output pin and OUT2 is treated as the output pin, the circuit performs the buffer function.

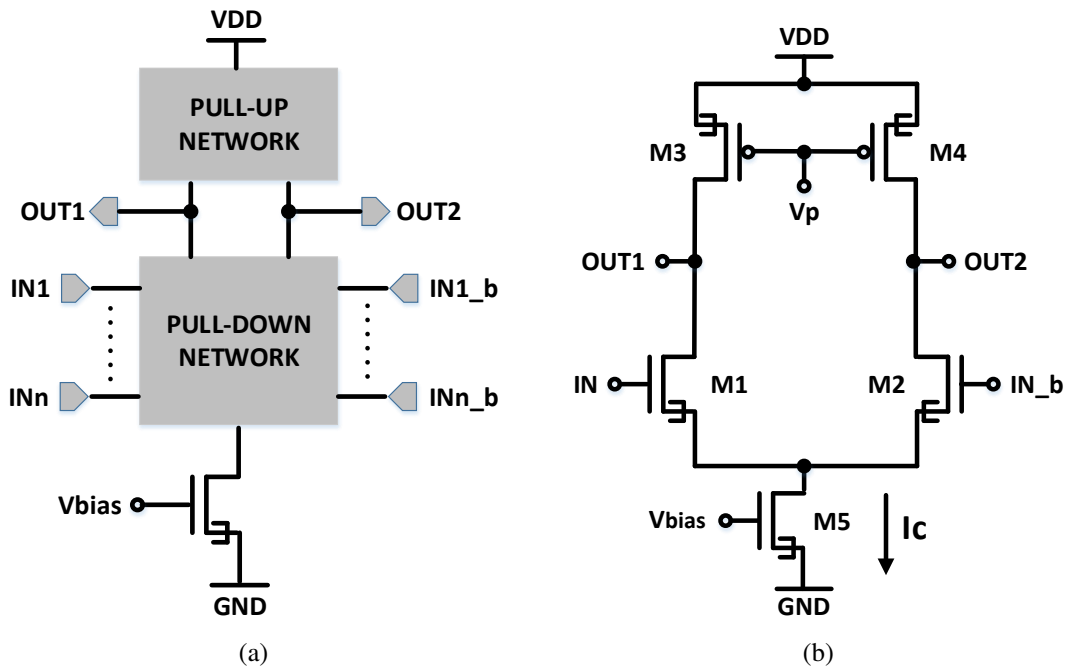


Figure 4.1: (a) The Universal Diagram of CML Circuits (b) Schematic of the TFET-based CML Inverter.

4.1.2 Design Optimization

In traditional CML design, the biggest challenge is the larger amount of power consumption than static logic, even though researchers have proposed different techniques to minimize the power consumption of CML [76, 77]. One common method is to decrease the supply voltage. However, because of scaling issues with CMOS technology, the voltage source must surpass the threshold value to turn on the transistor at a certain point (V_{th} is approximately 0.27 V for 20 nm technology). Also, the decreased supply voltage can dramatically increase the switching time of CMOS gates, and consequently increase the power-delay product (PDP).

As discussed in Chapter 2, TFETs are promising for low-power applications due to sub-60

mV/decade sub-threshold slopes. In [33], the authors considered the threshold of TFET as 0.15 V, thus the lowest possible supply voltage for TFET is 0.3 V. On the other hand (and again following an approach in [33]), to fairly compare TFETs with CMOS, as the corresponding current for a TFET at V_{GS} = 0.15 V is similar to CMOS at V_{GS} = 0.3 V, the minimum supply for CMOS is set to be 0.6 V. As a result, given the minimum requirement, the input/output voltage swing sits between 0.15 V and 0.3 V for TFET, while the voltage swing is between 0.3 V and 0.6 V for CMOS.

Figure 4.2 illustrates the delay and the power-delay product of the CML inverter with different supply voltages for TFETs when compared to a 20 nm FinFET equivalent assuming a VDD of 0.6 V. The voltage swing for all five cases is set as one half of the value of VDD. At the same supply voltage (VDD = 0.6 V), the power consumption of a TFET CML inverter is comparable to a CMOS CML inverter (426.9 nW for TFET vs. 434.3 nW for CMOS) – although the TFET CML inverter is slightly slower than the CMOS CML inverter (69 ps for TFET vs. 60 ps for CMOS). The driving current of the TFET CML inverter is 711.6 nA compared to CMOS CML inverter of 723.8 nA at $VDD = 0.6V$. When VDD is lowered to 0.3 V, although the switching time of the TFET CML inverter increases accordingly, the power consumption and power-delay product are dramatically reduced when compared to a CMOS CML inverter. This suggests that TFET-based CML gates could offer significant improvements over CMOS CML gates in ultra low power applications. Moreover, because other more complex logic gates (e.g., multiplexers) can be naturally implemented in differential mode style, TFET based CML gates should offer additional benefits compared to CMOS CML gates. For instance, a CML based multiplexer composed of nine transistors is more area efficient than a static multiplexer with fourteen transistors (three NANDs and one inverter). It is worth noting that the symmetry property can be better accomplished in CML based multiplexer compared to other CML based logic gates, such as AND/OR gates.

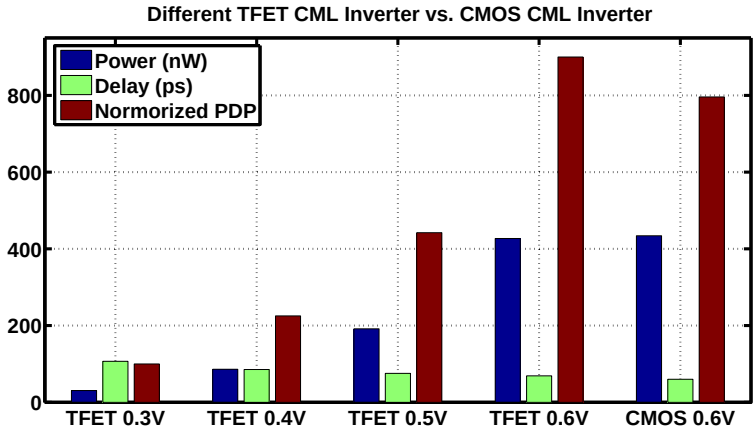


Figure 4.2: Different Configurations of TFET CML Inverter vs. CMOS CML Inverter.

4.1.3 TFET-based CML Standard Cells

The above analysis suggests that CML can perform various functions based on different configurations. In fact, three levels of CML implementations are introduced in [78]. By observing the stacked levels and different pairs, the delay of a gate with more than three-levels exceeds the delay of an equivalent three-level, static multiplexer. That is, the level of differential pairs is limited to three for the optimization in the CML implementation. Figure 4.3 depicts four two-input TFET-based CML functions with a two-level structure. Each of the gates has three differential pairs as inputs. A set of four functions (including AND, NAND, OR and NOR) can be derived from Figure 4.3a with different input/output configurations. The MUX, XOR/XNOR and D latch are also distinguished by wiring and the input/output selection shown in Figures 4.3b-d, respectively.

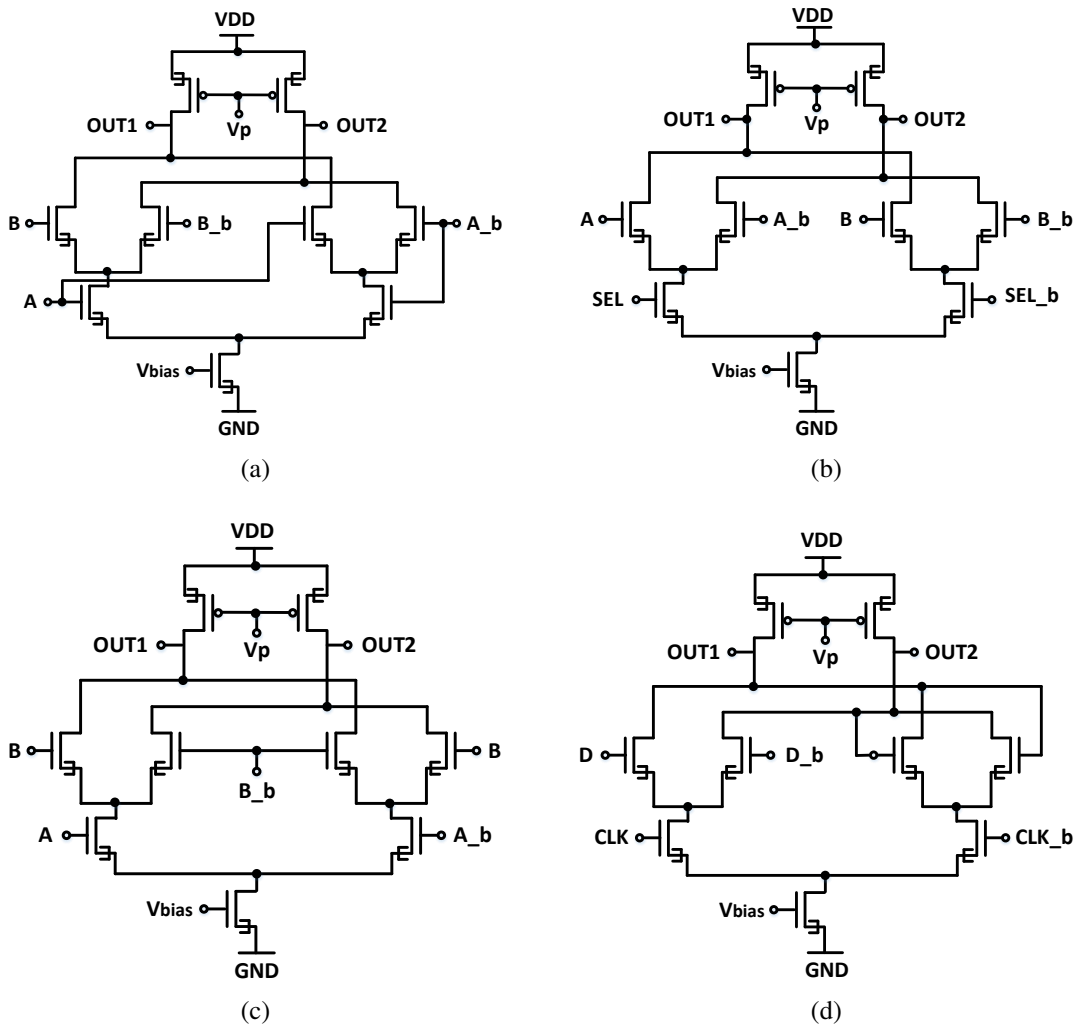
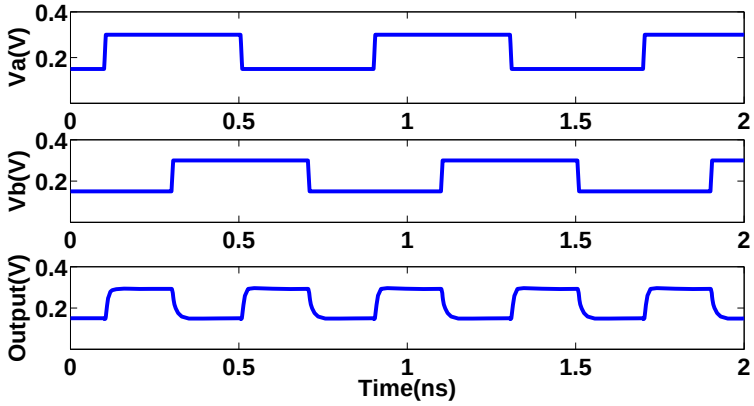


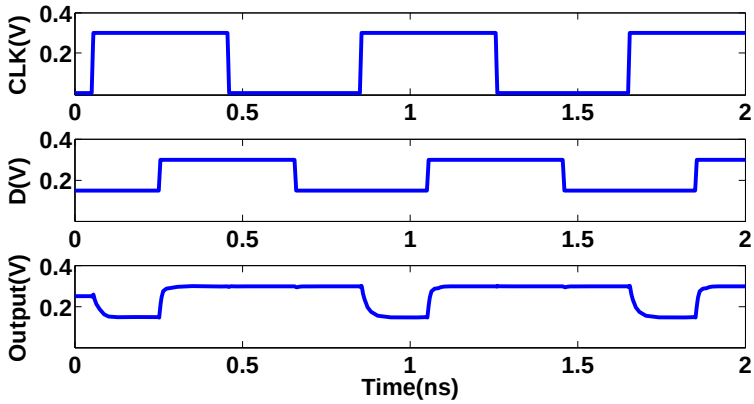
Figure 4.3: The Universal Schematics Structure of Four Different CML Circuits: (a) AND (b) Multiplexer (MUX) (c) Exclusive-OR (XOR) (d) D Latch.

As discussed in the previous section, we attempt to maintain the voltage swing of input and output between 0.15 V and 0.3 V for TFET CML gates. The configuration of the supply voltage and voltage swing sets the baseline for the other parameters, such as transistor size and biasing voltages. Here, we configure the TFET width to be the same size as the technology length to minimize the area. The 20 nm technology nodes are used for our evaluations. Consequently, it is

important to tune V_{bias} and V_p to achieve the necessary voltage swing for the entire standard logic cells. After voltage sweeping, the basic CML logic gates functions best when V_{bias} = 0.18 V and V_p = 0.14 V. Figure 4.4 presents the transient simulations for the exclusive-OR and D latch, where both the inputs and outputs are between 0.15 V and 0.3 V.



(a)



(b)

Figure 4.4: (a) XOR Simulation Results (b) D Latch Simulation results.

The other standard cells are also characterized and simulated under the same biasing condition. Table 4.1 shows the area, delay and power for the standard cells of TFET-based CML. Only ten cells are described, but more CML logic functions can be derived from the standard cells pro-

posed in Table 4.1. For instance, if we define OUT1 as the output pin, then a CML-based inversion function is possible per Figure 4.1a. However, if we choose OUT2 as the output pin, the CML schematic works as a buffer. Moreover, a standard cell library usually accounts for the different driving strengths of each individual function. In CML gates, a simple solution is to increase the constant current by the tail biasing transistor [75].

The area of CML and static TFET gates is also provided in Table 4.1. With the exception of a CML buffer and a four-input AND gate, all other CML standard cells consume less area compared to static counterparts. This feature may also be a major advantage for cryptographic systems, especially light-weight ciphers such as KATAN, where majority of the hardware is composed of D flip flops and multiplexers.

Table 4.1: Area, Delay and Power of the TFET-based CML Standard Cells

Cells	Transistor Counts	Area $[\mu m^2]$	Rising $[ps]$	Falling $[ps]$	Average $[ps]$	Power $[nW]$	PDP $[nW \times ps]$	CML area/ Static area
Buffer	5	0.0022	90	124	107	30.588	3272.916	1.833
OR2	9	0.0036	99	124	111.5	24.032	2679.568	1
AND2	9	0.0036	75	165	120	22.97	2756.52	0.818
AND4	27	0.011	476	644	560	70.828	39663.68	1.8
MUX2	9	0.0036	71	115	93	24.183	2249.019	0.5
XOR2	9	0.0039	99	105	102	25.848	2636.496	0.817
D-Latch	9	0.0037	102	168	135	23.122	3121.47	0.341
DFF	18	0.0074	100	200	150	45.500	6825	0.341
1-bit FA	45	0.0186	416	591	503.5	233.928	1.178×10^6	0.847
4-bit FA	180	0.744	654	591	622.5	939.150	5.846×10^6	0.847

4.1.4 Security Evaluation of TFET-based CML Gates

Before we consider implementations of lightweight ciphers with TFET CML gates, we first consider TFET CML in more detail from the hardware security perspective. It is well known that the key idea of differential power analysis is based on the power consumption during circuit transition.

In static CMOS logic, the major power consumption happens when the output of logic undergoes a 0→1 (or 1→0) transition. Because of this symbolic characteristic of static logic, the genuine cryptographic algorithm is vulnerable to the DPA attack. On the contrary, the CML structure is naturally resistant to a DPA attack considering the relatively constant power consumption for almost any transitions.

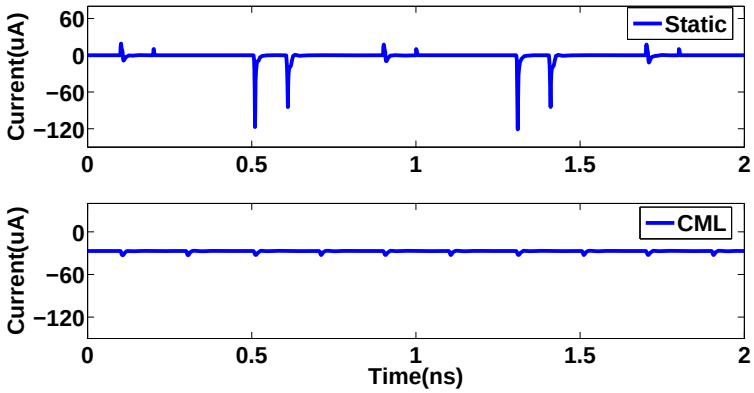


Figure 4.5: The Power Traces Between Static XOR and CML XOR.

Figure 4.5 depicts the power traces for the TFET static XOR gate and the TFET differential style XOR gate. Obviously, the TFET CML XOR gate dissipates almost constant power in contrast to the significant power overshoot of the static XOR gate. That is, the power profile of the TFET static XOR gate leaks more information for the attacker to identify the internal activity of the cryptographic system. However, the almost constant power consumption of a TFET CML XOR gate provides essentially no information about data transitions. Moreover, as we have discussed in previous section that the 0→1 transition is essentially mirrored to 1→0 transition in the CML gates, even though attackers may retrieve some information through the power glitches, it is very challenging for them to identify what the processing logic value is.

4.2 Implementation of Cryptographic System

Due to large area and high power consumption, using CML to implement cryptographic hardware is not common – especially in lightweight cryptographic systems. To protect cryptographic circuits against DPA attacks, researchers often employ other techniques [79, 80]. These solutions incur significant computation cost where the cryptography already involves massive computation and consumes relatively large power and area. As such, lower power, TFET-based CML could be especially valuable when considering devices for the IoT, WSN nodes, etc. Lacking an effective defense mechanism, hardware in these spaces can be substantially more vulnerable/susceptible to hardware attacks such as DPA.

To address these challenges, in the following sections, we consider the impact of TFET-based CML on a 32-bit KATAN cipher. More specifically, (a) the KATAN cipher is a hardware-oriented block cipher with a low GE – even among other lightweight ciphers, (b) applications that employ lightweight ciphers are typically power constrained – and thus could benefit from TFET technology, and (c) the limit for the application of CML on conventional block ciphers is the large power overhead, but power consumption in a lightweight cipher is typically much less. In subsequent sections, we will briefly discuss the working mechanism of the KATAN cipher. Implementations of the 32-bit KATAN cipher are provided in different circuit-level structures, where a table is presented to compare the TFET based implementation with the CMOS implementation. We will then present the correlation power analysis on KATAN32 with experimental results through design simulations.

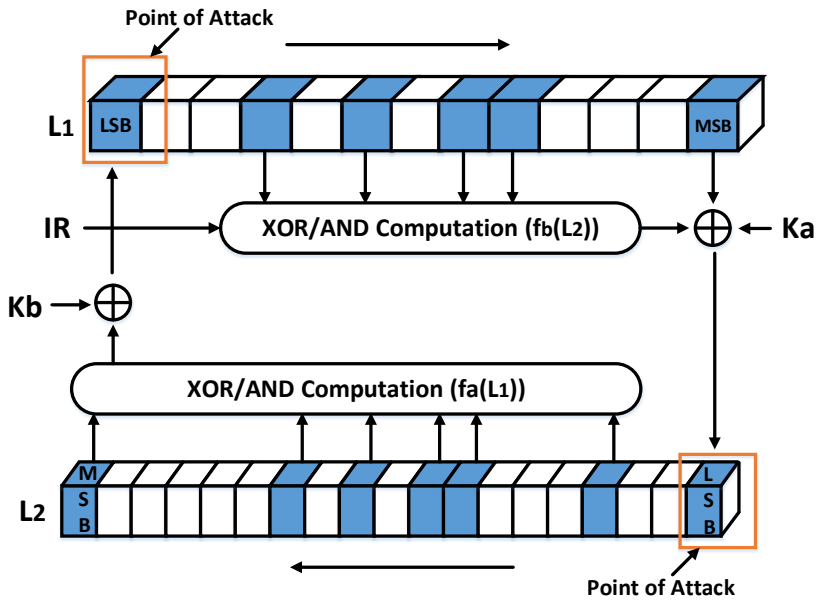


Figure 4.6: The Abstract Schematic of the KATAN Cipher.

4.2.1 Overview of the KATAN Cipher

The KATAN ciphers are a family of light-weight block ciphers, consisting of three variants with 32-bit, 48-bit and 64-bit blocks. All KATAN ciphers share the same key schedule with the key size of 80 bits as well as the 254-round iteration with the same non-linear function units [81]. Considering that different variants use the same hardware – except for a small difference in register count – we only focus on the smallest variant of KATAN with 32-bit blocks. As depicted in Figure 4.6, this 32-bit block is made of 32 registers divided into two parts – L_1 and L_2 – with corresponding sizes of 13 bits and 19 bits respectively. Both L_1 and L_2 are coded as a linear feedback shift register (LFSR), in which it shifts every clock cycle. The two registers are utilized by both plaintext and cipher text for the inputs and outputs. Meanwhile, all the computation of non-linear functions, namely f_a and f_b, can be identified as a combination of AND/XOR calculation in conjunction with different keys (k_a and k_b), and a non-linear irregular factor (IR).

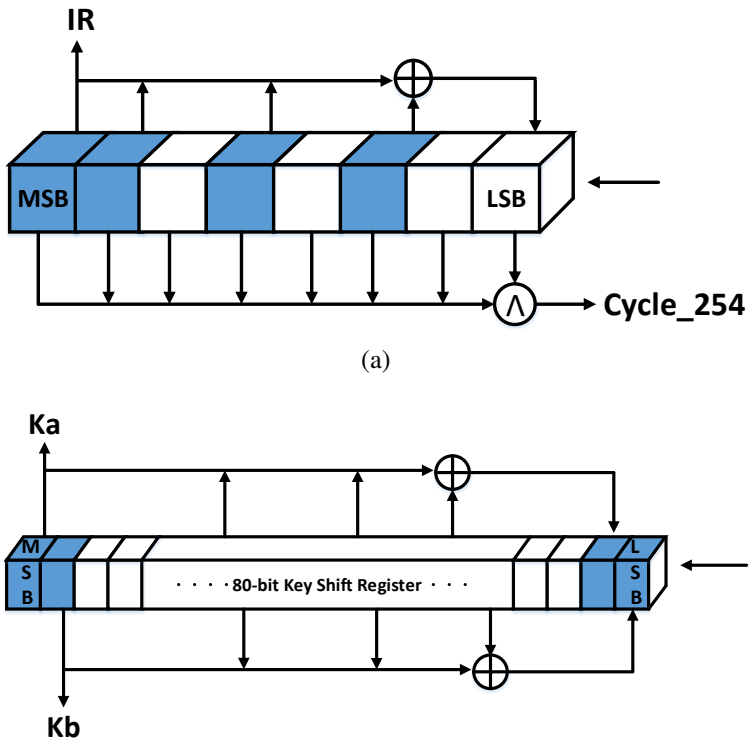


Figure 4.7: Two Additional Hardware Blocks: (a) IR (Counting Cycles) and (b) Key Schedule.

The encryption procedure is described as follows: the plaintext is loaded into two registers L_1 and L_2 such that the lower 19 bits of the plaintext are loaded into register L_2, while the higher 13 bits of the plaintext are loaded into register L_1. In Figure 4.6 the least significant bits (LSBs) and the most significant bits (MSBs) are specifically noted. Both L_1 and L_2 perform left-shift operations every clock cycle when the start signal is on. During each round, IR and two keys are also generated by two additional blocks. The IR block is shown in Figure 4.7a, where 8 registers compose an 8-bit LFSR. This block has two functions: first, it generates the irregular update value for the non-linear operations, and second, it counts down the 254 rounds (i.e., when the signal *cycle_254* is logic 1, KATAN has completed the entire encryption).

The key schedule block is illustrated in Figure 4.7b. Similar to the IR, the key schedule

block is an 80-bit LFSR. Before the encryption, the keys are stored in the registers. The LFSR shifts one bit to generate one roundkey. The two most significant bits are exported as k_a and k_b for KATAN every two clock cycles. The feedback polynomial with a minimal hamming weight of 5 is selected for the 80-bit shift register as derived in Equation (4.1). As a result, the subkey of round i can be defined in Equation (4.2), where the key is denoted as capital K.

$$f(x) = x^{80} + x^{61} + x^{50} + x^{13} + 1 \tag{4.1}$$

$$k_i = \begin{cases} K_i & i = 0...79 \\ k_{i-80} \oplus k_{i-61} \oplus k_{i-50} \oplus k_{i-13} & i > 79 \end{cases} \tag{4.2}$$

Two nonlinear functions f_a and f_b are defined in Equations (4.3) and (4.4), which represent the two abstract blocks (XOR/AND computation) in Figure 4.6. Here, considering that the 32-bit KATAN cipher is adopted, we have already located which bits of L_1 and L_2 are selected for the computation. For the other variants, the positions of bits can be different because of a different number of registers [81].

$$f_a(L_1) = L_1[12] + L_1[7] + (L_1[8] \cdot L_1[5]) + (L_1[3] \cdot IR) + k_a \tag{4.3}$$

$$f_b(L_2) = L_2[18] + L_2[7] + (L_2[12] \cdot L_2[10]) + (L_2[8] \cdot L_2[3]) + k_b \tag{4.4}$$

4.2.2 CML Implementation on KATAN

We now discuss how different transistor technologies could impact the power/performance of KATAN32 by using the Synopsys Design Compiler using 20 nm InAs Homojunction TFET [82] and the Predictive Technology Model (PTM) 20 nm FinFET technology [63]. In order to minimize the area consumption of KATAN32, the driving-strength-one library is employed for the synthesis. The synthesized transistor-level netlist is further converted into both the single-ended and differential modes. Synopsys Finesim is adopted for the gate-level simulation with less simulation time compared to the HSPICE simulator. The operating frequency of KATAN32 is set to 100 MHz to ensure its functional correctness.

Table 4.2: Power Consumption Comparison Among Different Implementations on KATAN32.

	Voltage Supply[V]	Gate Equivalent	Area [μm^2]	Average Current[μA]	Power [μW]	Area Change[%]	Power Change[%]
CMOS Static	0.6	1013	3.534	16.09	9.96	-	-
CMOS CML	0.6	393	1.415	283.65	170.19	-59.96%	+1608.7%
TFET Static	0.6	1013	3.536	3.14	1.89	+0.057%	-81.02%
TFET CML	0.3	393	1.441	32.53	9.76	-59.22%	-2.01%

Area and power data for four different implementations is summarized in Table 4.2. More specifically, we consider TFET and CMOS static implementations as well as CMOS CML with a 0.6 V supply, as well as TFET CML with a 0.3 V supply. A 2-input NAND gate is assumed when comparing equivalent gate numbers. It is worth noting that the number of the synthesized static GEs is more than what is reported in [81], mainly because we simplify our library for both TFET and CMOS by using our own driving-strength-one and two-input standard cells. Complex logic gates such as D flip flops and multiplexers, are not fully optimized and consume a relatively larger number of gates. (Future work will be performed to further optimize all TFET CML based logic gates.)

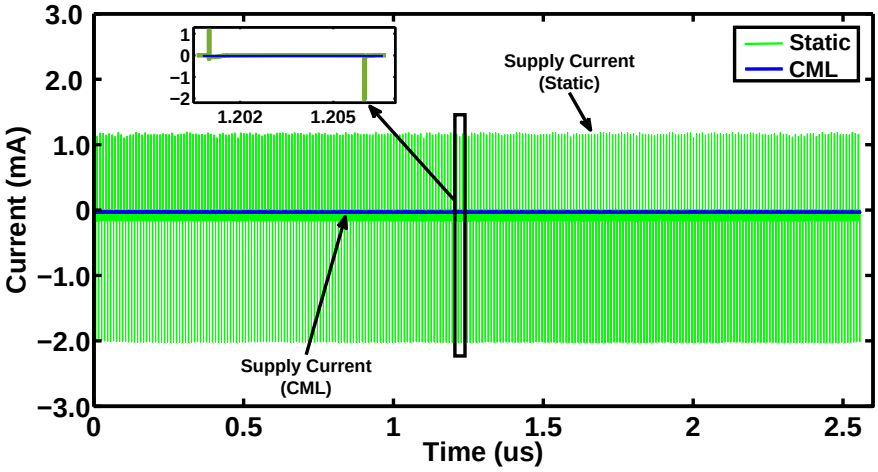


Figure 4.8: KATAN32 Power Measurements CML TFET vs. Static TFET.

Notably, it is not difficult to see that two CML implementations consume fewer gate equivalents and area compared to the two static counterparts given that KATAN32 is largely comprised of D flip flops, as we discussed in Section 4.1.3. The area of TFET CML KATAN32 is 1.441 μm^2, which is about 59% less than the static TFET KATAN32. Note that the area of TFET based static and CML KATAN32 is similar to their CMOS counterparts as comparable 20 nm technologies are used. The power consumption of *TFET CML* (9.76 μW) even outperforms *static CMOS* (9.96 μW) with slightly lower power consumptions. Figure 4.8 shows the power trace of the KATAN32 implementation for static and CML TFETs, respectively. The zoom-in subfigure displays the large current overshoot of TFET static KATAN32 compared to the constant current of TFET CML KATAN32.

4.2.3 Power Model and Attack Mechanism

When considering differential power analysis [12], we first need to identify the intermediate values that are a function of plaintext/ciphertext, and that are a portion of the keys. Given that when

launching a DPA attack, the round keys are part of complete keys, the complexity of DPA computation can be further reduced with the smaller size of round keys. Therefore, the portion of the keys must be as small as possible compared with the complete keys, thereby reducing the complexity of key analysis. The key-dependent intermediate values are further calculated by a group of hypothetical key guesses and are utilized as the inputs of the selection function. Subsequently, the selection function differentiates the power traces into two sets, where they are processed to show a peak for the right key hypothesis.

Correlation power analysis, on the other hand, is an extension of DPA where a model of the power consumption is created for use in the analysis phase of an attack. A power model is needed to approximate the power consumption of the target cryptographic device during an encryption operation. The resulting power predicted by the model will then be correlated to the actual measured power consumption using a key hypothesis. It employs the Hamming weight model (different from the Hamming distance model which is mostly adopted in DPA attack) to hypothesize the intermediate output result and evaluate the relation between the hypothesis values and power traces in a statistical way. Bard et al. proposed the security evaluation on the KATAN family, including algebraic and cube attacks [83]. They also pointed out the side channel analysis on KATAN but with only a high-level overview of possible vulnerabilities. To the best of our knowledge, there are not any detailed discussions in existing work about power analysis on the KATAN family. In this chapter, we will introduce the power analysis attack on KATAN, as well as the countermeasures – i.e., a TFET CML implementation of KATAN32.

By observing the KATAN algorithm, it is apparent that the two nonlinear functions f_a and f_b are able to connect the plaintext/ciphertext with partial keys (or more precisely, subkeys). We can then select the two bits each round generated by the nonlinear functions as our intermediate values or points of attack as highlighted in red in Figure 4.6. Besides those two arithmetic functions, the majority of KATAN32 hardware is made up of D flip flops such that the overall power consumption

mainly depends on the operation of shifting registers. As a result, it is important to come up with an attack mechanism that maximizes the power profile of two nonlinear operations.

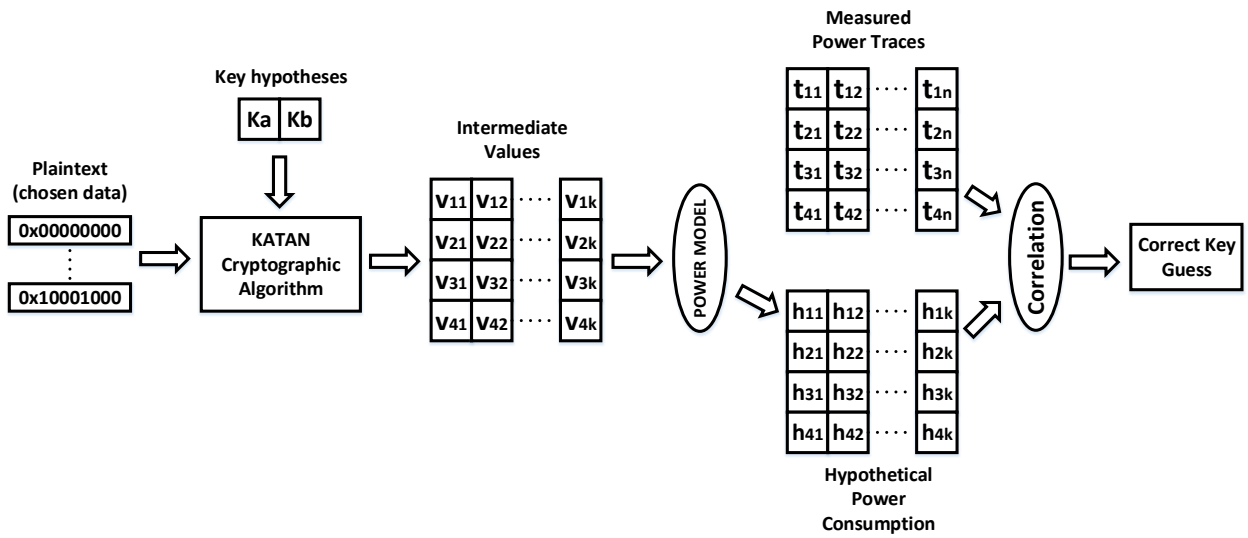


Figure 4.9: The Correlation Power Analysis Flow on KATAN Cipher.

In single-ended logic gates, power consumption only occurs during state transitions, either $0 \rightarrow 1$ or $1 \rightarrow 0$. If we configure the plaintext in a way that for certain clock cycles the power consumption of functions f_a and f_b contributes most, then the power information extracted from the supply current can be maximally related to the key information. More specifically, we can selectively configure the plaintext to be consecutive zeros or ones. Therefore, the power consumption of KATAN32 highly depends on functions f_a and f_b, because the power cost of the left-shift operation is negligible in each clock cycle.

4.2.4 Correlation Power Analysis on KATAN32

In this section, a case study of CPA on KATAN32 is described to disclose the two key values (K[79] and K[78]). Initially, four selected plaintexts are loaded into the two registers as given in Equation

(4.5) and the 80-bit keys are set to all zeros. Note that in real cases, the key is the attackers' target and is unknown to attackers.

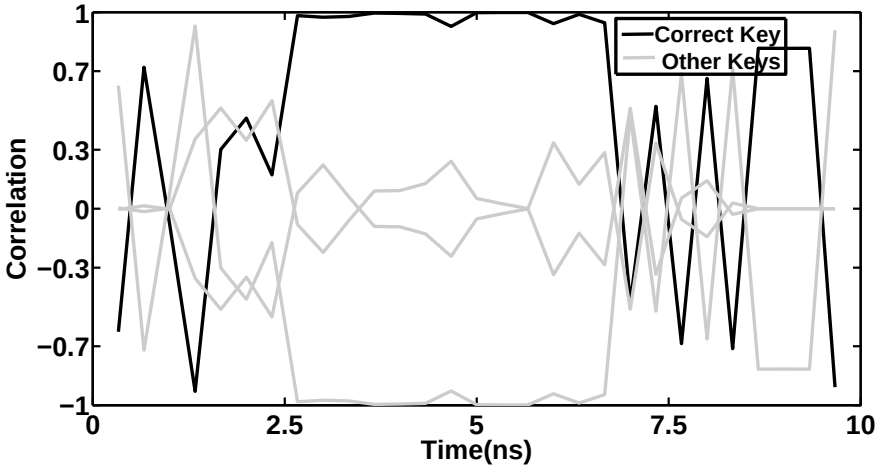
$$\begin{aligned} P1 &= \text{x00000000} \Rightarrow p[18] = 0, p[31] = 0 \\ P2 &= \text{x80000000} \Rightarrow p[18] = 0, p[31] = 1 \\ P3 &= \text{x00040000} \Rightarrow p[18] = 1, p[31] = 0 \\ P4 &= \text{x80040000} \Rightarrow p[18] = 1, p[31] = 1 \end{aligned} \tag{4.5}$$

However, the chosen input values are not constrained to Expression (4.5), as long as the plaintext interacts mostly with the subkeys. When the start signal is received, KATAN32 begins encryption. Figure 4.9 shows the proposed CPA attack flow on KATAN32. Each selected plaintext and the hypothetical subkeys K_a and K_b are calculated to achieve the intermediate values "v" matrix. Then, intermediate results are further calculated by the power model, which is defined as the Hamming weight model. The results from the Hamming weight model are defined as the hypothetical power consumption. Based on our chosen plaintexts, the matrix of hypothetical power consumption is given in Equation (4.6):

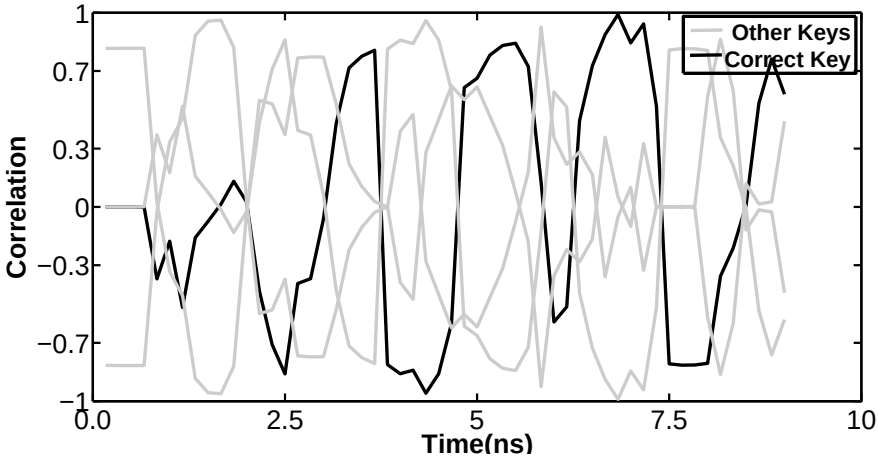
$$\text{hypothetical power consumption} = \begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{bmatrix} \tag{4.6}$$

$$\text{Corr. Coef.} = \frac{\sum_{i=1}^{4}(t_i - \overline{t}) \cdot (h_i - \overline{h})}{\sqrt{\sum_{i=1}^{4}(t_i - \overline{t})^2 \cdot \sum_{i=1}^{4}(h_i - \overline{h})^2}} \tag{4.7}$$

The predicted power consumption is then compared with the measured real power consumption by the correlation coefficient formula as given in Equation (4.7). The highest correlation coefficient result stands for the correctly guessed keys. In this case, the keys '00' reflect the largest correlation coefficient value. The next round follows the same mechanism, but with slightly different ciphertext, which is generated by the last round. Figure 4.10 shows the detailed correlation power analysis for the respective TFET static KATAN32 and TFET CML KATAN32 on one clock cycle. The black line describes the correct key value for subkeys K_a and K_b (='00'), which are the two most significant bits of the key. It is apparent that the correlation coefficient is largest for a static, TFET-based KATAN32 implementation when the correct keys are applied as shown in Figure 4.10a. By comparison, the correlation coefficient of TFET CML KATAN32 is more significant, and all four hypothetical keys are similarly distributed as shown in Figure 4.10b. Consequently, the TFET CML KATAN32 implementation is capable of successfully counteracting the correlation power analysis. Because the power consumption is mainly determined by AND/XOR logic gates of two nonlinear functions – and the effect of CPA is maximized – the correlation coefficients for KATAN32 are higher on average than other block ciphers, e.g., CPA on S-box [76].



(a)



(b)

Figure 4.10: CPA Attack on One Clock Cycle (a) TFET Static KATAN32 vs. (b) TFET CML KATAN32.

As the key schedule of KATAN32 suggests, the key generator block exports two subkeys and does a left-shift operation every clock cycle. Therefore, the 80-bit keys can be continuously output as subkeys in 80 clock cycles, which can be easily attacked by CPA using the chosen plaintexts. The pseudo code for Algorithm 1 describes the abstract CPA attack mechanism on the 80-bit keys of KATAN32. The criteria of choosing the plaintext is to ensure that power consumption is

highly dependent on the power cost of intermediate values in certain clock cycles. Moreover, the selected plaintext may be capable of discovering more than one key in different periods.

To launch the complete CPA on KATAN32, the attacker should first select plaintext values that are able to achieve a situation where $\text{Power}_{\text{KATAN32}} = \text{Power}_{\text{intermediate values}}$. Then, after 80 clock cycles, the attacker can calculate the correlation coefficients. If the correlation coefficients are significant at certain periods, the key can be discovered and Algorithm 1 can then be rerun for the next chosen plaintext. If there are not any significant correlation coefficients in the first 80 rounds, the selected plaintexts are not desired for the CPA attack on KATAN32. Because our goal is to leverage the TFET CML implementation on KATAN32 to counter the CPA attack, the completed 80-bit key evaluation will not be discussed in detail.

```
Data: plaintext and measured power
Result: correlation results (correct keys)
while uncovered keys ≤ 80 do
    select the plaintext;
    if Power(KATAN) ≃ Power(Intermediates) then
        while # of rounds ≤ 80 do
            run correlation coefficient;
            correct keys ++;
        end
    else
        unsuccessful plaintext ++ and go back to
        select the plaintext;
    end
end
```

Algorithm 1: CPA on recovering of 80-bit keys of KATAN.

4.3 Discussion

Here, we briefly discuss the next steps for this work. Potential circuit-level optimizations as well as algorithmic considerations are highlighted.

4.3.1 Circuit-Level Optimization

In this work, we use TFET based CML gates to realize lightweight ciphers with both high security and low power consumption. As an initial effort we have constructed generic current mode gates (without applying any circuit improvement techniques). However, this will be considered in our future work, and additional improvements with respect to power are expected. For example, the sleeping transistor in [76] can lead to additional energy improvements.

Considering the power advantage of TFET based CML gates, it is also promising that we continue to optimize our circuit specifications and develop the CML standard library. As we have mentioned, the good thing about building a current mode standard cell library is that the standard logic gates can be used to derive additional logic gates by following the pattern of the CML design template. Also, different driving strength designs of one logic gate can be accomplished through the modification of the tail current source.

Binary decision diagrams (BDD) have also proven to be a practical way to capture the behavior of CML [84]. The core of the differential cell is its pull down network, which manages the functionality of the CML gate. The PDN can be represented using BDDs where each node of the BDD is a differential pair. Each branch of the BDD is a connection between one drain and the source of another differential pair or an output.

4.3.2 Encryption Algorithm Consideration

Besides the optimization of the CML circuit, another goal is to extend the TFET-based CML for more complicated and popular block ciphers, such as AES. Given that a significant amount of work has been done in protecting conventional block ciphers, a concrete analysis is necessary to evaluate the amelioration using a TFET based CML implementation. Among the techniques, composite

field S-boxes are widely applied [85]. Polynomial, normal, and mixed basis composite fields will also be analyzed and one of three bases will be chosen for the TFET-based implementation to counter DPA attack. Although a DPA-based attack is mostly employed in attacking block ciphers, other emerging attacks are also worthy of being covered in the future work, such as fault analysis attacks [86–90]. Employing the existing techniques, we will study whether TFET-based CML designs are resistant to fault analysis based attacks.

Besides block ciphers, other encryption and authentication algorithms can also be protected using TFET CML. For example, Galois Counter Mode (GCM) is an authenticated encryption mode that simultaneously generates ciphertext and an authentication tag [91]. It can be implemented in hardware to achieve high speeds with low cost and low latency [92]. To incorporate the GCM into our TFET based block cipher implementation, two scenarios are taken into consideration: TFET static and TFET CML implementation. To our knowledge, no work has been done to implement GCM using CML style implementation. We will conduct a detailed theoretical analysis on how to incorporate GCM operation into CML-based cipher design.

4.4 Summery

In this chapter, we have demonstrated that the usage of emerging transistors, i.e. TFETs, can help improve circuit design resilience against CPA attacks while still preserving low power consumption compared to their CMOS counterparts. Additionally, besides the traditional criteria for emerging devices such as area, power, delay and non-volatility, security may serve as a new criterion to thoroughly judge the advantages and disadvantages of emerging devices. Using this new standard, we plan to revisit existing emerging transistors to have a full comparison between emerging technologies and CMOS technology. Meanwhile, we believe that more research outcomes are expected in this area where unique properties of emerging transistors can help enhance the security of circuit

designs.

CHAPTER 5: SPLIT MANUFACTRUING ON RF POWER AMPLIFIER

Both governmental agencies and industrial companies are looking for a balance between fabrication cost and design security to prevent foundries from learning the design details of submitted design layouts. Among existing approaches [54, 93, 94], design obfuscation and camouflaging are candidates, however both methods require the modification to the original circuits which may cause a performance overhead. Intelligence Advanced Research Projects Activity (IARPA) proposed a new methodology called split manufacturing which only adds trivial efforts to IC designers but is able to effectively prevent IC piracy [95]. In this chapter, we would like to present the proposed idea of applying split manufacturing on RF power amplifier design.

5.1 Motivation

The key idea of split manufacturing is to protect circuit/system designs by dividing the manufacturing chips into Front-End-of-Line (FEOL) consisting of transistor layers to be fabricated by off-shore foundries and Back-End-of-Line (BEOL) consisting of metallizations to be fabricated by trusted domestic facilities. Through this divided fabrication procedure, the design intention is not fully disclosed to the FEOL foundry. Even though the concept is straightforward, a successful implementation requires further research on various aspects, especially the balance between cost and security when the designer splits the layout into FEOL and BEOL. Analytical and experimental results have already been presented in digital circuits [96–103]. However, the analog/RF designs are rarely discussed when using split manufacturing even though analog/RF circuits are more likely to be IP piracy victims than their digital counterparts.

In fact, the fundamental difference between digital design flow and RF design process has

already raised concerns as to whether it is still applicable to apply split manufacturing in RF design. A deeper look into both design flows proves that it would be more suitable to apply split manufacturing in RF circuits than in digital circuits because of the unique functionality metal layers play in RF designs: 1) Metal layers are solely used as interconnections between gates and modules in digital circuits while in RF circuits, metal layers are also used to build functional blocks (e.g., inductors are often located on the top metal layer; capacitors are built in upper level metal layers); 2) While metal layers are abstracted as wire connections in digital designs, wire length and wire direction are both functional parameters in RF designs. Therefore, a foundry fabricating the FEOL part of digital circuits may face a mathematical problem with finite solutions in order to recover the whole functionality of the design[1]. On the other hand, the foundry of RF FEOL would need to explore an infinite solution space to recover the RF design.

Based on the above discussion, it becomes obvious that split manufacturing should be more effective to protect RF circuits from IP piracy. To assess our claim, analytical calculation and experimental demonstrations are performed in this chapter to solidify our findings and to push the territory of split manufacturing to cover all types of circuit designs.

5.2 RF Design Flow Basics

Thanks to the advanced EDA tools for RF circuit designs and the development of RF design kits, RF engineers have become more productive than ever before. Nevertheless, a typical RF design still involves heavy work of design fine-tuning and designers' experience plays a critical role here [104–106]. Figure 5.1 shows the steps of a modern RF design flow.

[1]Note that the possible solution space could be large given large amount of standard cells in digital circuits. In fact, this is the key criterion to evaluate the security level of split manufacturing method in digital circuits.

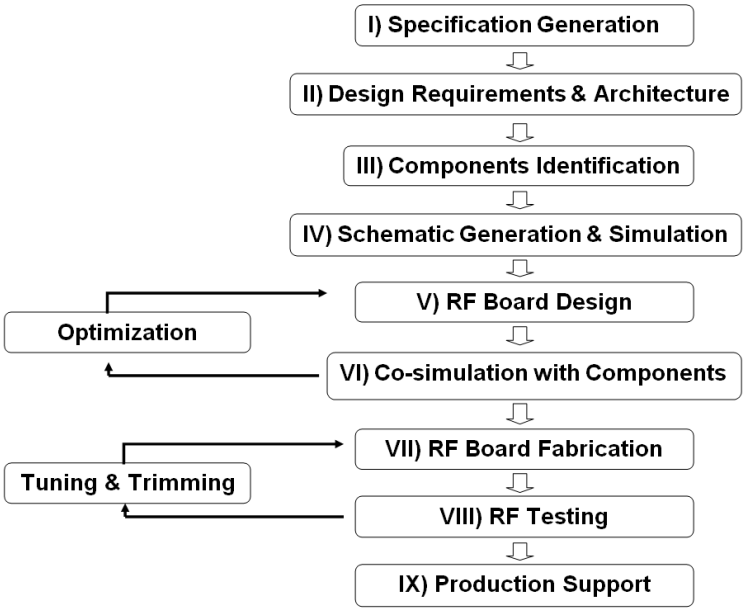


Figure 5.1: Standard RF Circuit Design Flow

5.2.1 RF Design Procedures

From Figure 5.1 we can see that steps I-III are the preparation of the RF circuit specification. Taking a power amplifier as an example, the defined specification will include design information such as the delivered output power, the amount of circuit stages, the operation class, etc. Different from digital designs where the specification is strictly followed, the specification for RF circuits only serves as a guideline as it often happens that the performance of the final design deviates from the original settings (experienced RF engineers may be able to narrow the performance gap which is why experienced RF designers are valued).

Guided by the specification, the circuit schematic will be designed, simulated and optimized. The optimized schematic will then guide the work of layout design and post-layout simulation. All physical-level parameters come into the map during the layout design and post-layout simulation such as parasitic capacitors, wire resistance, etc. For RF circuits, the parasitic components

can significantly affect the design performance and significantly deviate the circuit performance from the schematic level simulation. Therefore, the large portion of design time will be spent in layout optimization and circuit fine-tuning, even for experienced designers. If the circuit passes the post-layout simulation, it will be sent to the foundry for fabrication and for post-fabrication testing. Even though current foundries embrace advanced technology and delicate equipment, the parasitics introduced by the fabrication process remain a problem, i.e., unpredictable parasitic resistance and capacitance during the fabrication will affect both circuit functionality and performance. A fabricated RFIC circuit may not work properly which increases the demand for further tuning and trimming. To lower the fabrication cost and to increase the yield rate, techniques of post-fabrication calibration are used in modern RF designs, e.g., knob adjustments and Transverse Electro-Magnetic (TEM) cells.

5.2.2 Power Amplifier Modeling and Analysis

Power amplifiers are among the most widely used RF devices and are installed in almost every electronic device. For instance, power amplifiers serve as the very front end of transmitters in broadcasting systems and are used in audio systems to increase and decrease the volume. The basic functionality of a power amplifier can be described as an augmentation to the system power level. Therefore, being one of the most important tasks in RF design, researchers are dedicated to designing highly-efficient and robust power amplifiers. For example, the quality of a power amplifier design decides whether or not a wireless transmission signal can be well detected by wireless receivers or not. For this reason, we chose the power amplifier as the example in the rest of this chapter when we demonstrate how the split manufacturing can help improve design security and prevent IP piracy for RF circuits.

Besides the experimental design flow shown in Figure 5.1, analytical equations also play

critical roles to help designers derive the approximate range of the component sizes from the specification. Since most power amplifiers use N-type MOSFET, the drain current for N-type MOSFET in the saturation region is revisited in the following equations:

$$I_D = \frac{\mu_n C_{ox}}{2} \frac{W}{L} (V_{GS} - V_T)^2 (1 + \lambda V_{DS}) \tag{5.1}$$

$$V_T = V_{T0} + \gamma(\sqrt{\phi_B + V_{SB}} - \sqrt{\phi_B}) \tag{5.2}$$

where μ_n is the electron mobility, V_T is the threshold voltage, C_{OX} is the oxide capacitance per unit area, W is the channel width, L is the channel length, V_{GS} is the gate-source voltage of the MOSFET, and λ is the channel length modulation factor. Equation 5.2 presents the expression of threshold voltage, an important parameter in CMOS designs where γ is body effect constant, ϕ_B is the substrate Fermi potential and V_{SB} is source-to-body voltage. Since the inputs of power amplifiers are often nonlinear signals with DC biasing, particularly sinusoidal waves, the drain current in a power amplifier is showed in Equation 5.3 where I_m is the amplitude of the ac component of the drain current and ω is the resonant frequency.

$$i_D = I_{DC} + I_m \cos \omega t \tag{5.3}$$

Equations 5.1-5.3 determine the operation mode of the power amplifier because different DC biasing and operating frequency would cause different conduction angles. Note that the determination of operation mode guides the entire design flow. For instance, class-A power amplifiers need to constantly turn on the transistor all the time, which means drain current I_D should always be larger than zero. On the other hand, class-B power amplifiers require the operation on a 50% duty cycle,

where transistors are turned off for a half cycle. The typical characteristics of power amplifiers include the output power and the power-added efficiency whose calculations are listed below:

$$p_i = \frac{1}{2} real(v_{in} \times i_{in}^*) \tag{5.4}$$

$$p_o = \frac{1}{2} real(v_{out} \times i_{out}^*) \tag{5.5}$$

$$\eta_{add} = \frac{p_o - p_i}{P_{DC}} \tag{5.6}$$

In the above equations, i_{in}^* is the conjugate input current, i_{out}^* is the conjugate output current and P_{DC} is the DC power dissipation. Even though there are other reference parameters needed in power amplifiers, the output power and the power-added efficiency are the two key parameters for power amplifier evaluation. The attacker, who is assumed to be an experienced RF designer, should be aware of those equations as well and will apply them in RF circuit recovery from FEOL. However, it is noteworthy that unlike digital design, those equations can merely determine a reasonable range of design, the final results are derived after plenty of tuning and trimming work. In this chapter, we will evaluate the PA performance within these two parameters to demonstrate the application of split fabrication in RF circuits and evaluate the security level.

5.3 Split Manufacturing in RF Circuits

As we mentioned earlier, the removal of metal layers in RF circuits will not just hide the interconnections between circuit components but also eliminate the passive components which are built in

metal layers. Since a typical RF circuit only includes very few transistors and other passive components, the recovery of interconnections between these components will not be a difficult task. Rather, being able to derive the missing passive components and their sizes would be the main advantage of applying split manufacturing in RF designs. For the same reason, the difficulty level for attackers with the FEOL at hand to recover the passive components and to guess the sizes of these passive components will be the key criteria to assess the effectiveness of split manufacturing application in RF designs.

Compared to digital split fabrication [96] where the proximity attack dominates the security analysis, routing and mapping are no longer an issue for RF circuits. Furthermore, the recognition attack mechanism used in [100] cannot accurately explain the issue with RF split fabrication. To better guide the implementation of split manufacturing in RF circuits and to balance between the security level and design efforts, we propose three approaches/scenarios to perform the RF split fabrication:

- Scenario I: Remove only the top metal layer from the layers to generate FEOL. Since the inductors are often located in the top layer, the FEOL foundry does not have the information of interconnections through top metal layer as well as the inductor locations and sizes.
- Scenario II: Remove both the top and the second from the top metal layers. In this scenario, two upper metal layers are removed so that both inductors and capacitors are missing from the FEOL layout because the capacitors are often built through the top two metal layers.
- Scenario III: Design obfuscation. For RF designs, inductors are always located in metal rings and lower metal layers will be removed inside the rings for performance optimization (See example in Figure 5.12). Therefore, the rings themselves, which contain multiple metal layers, would indicate positions and approximate sizes of inductors. Similarly, the lower metal layers will not be used where capacitors are located. Therefore, attackers in both

scenarios I and II may learn the precise positions of the removed inductors/capacitors and may even further estimate their sizes. To further increase the security level but still avoid performance overhead, we propose an obfuscation technique during the design phase to insert non-functional rings and to create empty zones in the original design. Using this method, it becomes more difficult for attackers to pin down the location, the count, and the sizes of passive components.

For the demonstration purpose, the TSMC 0.18 μm technology supporting six metal layers is used. In both analytical and experimental demonstrations, scenario I indicates the removal of metal6 layers. Similarly, scenario II indicates the removal of the metal5 and metal6 layers. Scenario III follows the same rules that new rings and empty zones are removed from the metal layers metal1 to metal4. Note that the proposed three scenarios can be applied to any other process technology with the adjustment of available metal layers.

5.3.1 The First Example

To demonstrate all three application scenarios as well as their security levels, a single-stage single-transistor class-AB power amplifier is investigated as our first example where we assume that the inductor is using metal6 layer and the capacitors are using metal5 and metal6 layers [107]. A more sophisticated example with detailed layout information will be introduced in Section 5.4.

The class-AB power amplifier (see Figure 5.2 for detailed schematic) works at 5.8 GHz with a low supply voltage of 1.9 V. It is designed to deliver 19.8 dBm output power and 28.1% power-added efficiency.

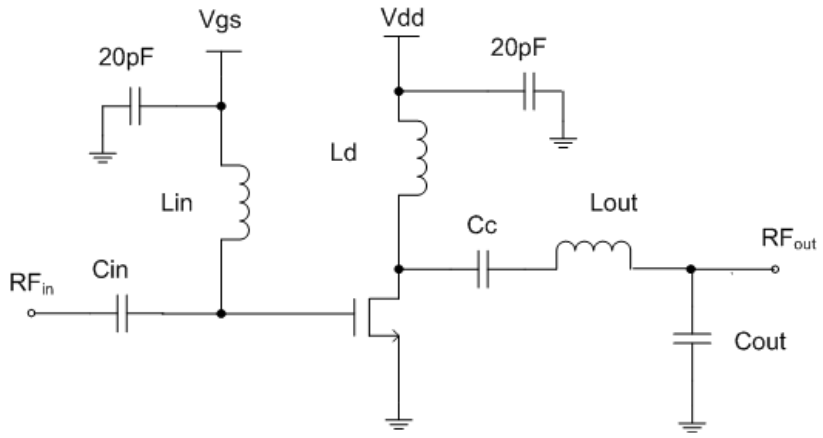


Figure 5.2: Schematic of A Class-AB Power Amplifier

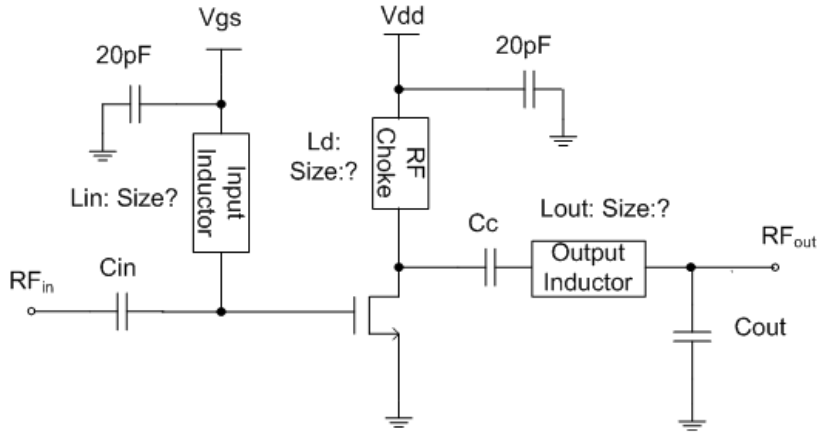


Figure 5.3: A Class-AB Power Amplifier With Metal6 Removed (Missing Inductors)

Scenario I: Removal of Metal6 Layers (Inductors)

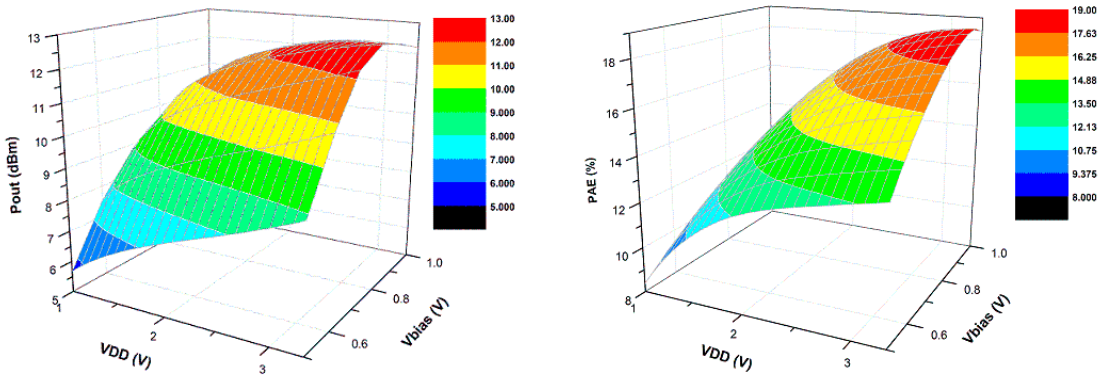
Since metal6 is removed from the FEOL, the schematic of the class-AB power amplifier, shown in Figure 5.3, is missing all inductor information. Although the attackers can easily recover the count and the locations of all inductors, they do not know the exact sizes and the values of the inductors. More specifically, the attackers can learn that 3 inductors are used in the design through the inductor rings. They can also extract the values for all other components. Therefore, the

attackers with the FEOL of the power amplifier at hand can easily guess the general functionality of the entire design. But a detailed specification including the the supply voltage and the operating frequency remains unknown. As a result, the task for attackers to recover the entire circuit is not as simple as sweeping all possible inductor values. As we emphasized earlier, we assume that the attackers are also experienced RF designers so they would also apply the analytical calculation based on Equations 5.1 - 5.6 and other parameters from the known components in order to derive the inductor values. The procedure to recover the whole circuit from the known FEOL by attackers is described in the following steps (Note that the IP piracy cost is directly related to the complexity of the these steps):

Step 1: In the first step, the attackers will try to find out the operating conditions such as bias voltage, supply voltage and operating frequency, which can significantly shift the power amplifier performance. Since the untrusted foundry is also the provider of the fabrication process (in our case, we are using the 0.18 μm technology), the attackers should be aware of the available supply voltage for this technology (from 1 to 3.3 V). The attackers should try at least 23 different supply voltages if a step size of 0.1 V is chosen[2]. In terms of gate biasing, the reasonable range for a power amplifier varies from 0.4 to 1 V, however it is not necessary that all designs follow this setting (e.g., an exception would be presented in the experimentation section). Hence, using 0.05 V as a voltage sweeping step, the gate biasing can have at least 13 different cases for attackers to choose. Meanwhile, the operating frequency still remains a puzzle to attackers, which acts as an imperative role in RF design. The attackers may narrow down the spectrum by assuming this example design works in the commercial communication protocol range, which basically ranges from 0.8 to 6 GHz. Again, the design may or may not take the communication frequency as its operating frequency, because the attackers are not aware if this layout works for some specific applications, either military or scientific confidentiality. Under this assumption, it comes to a group

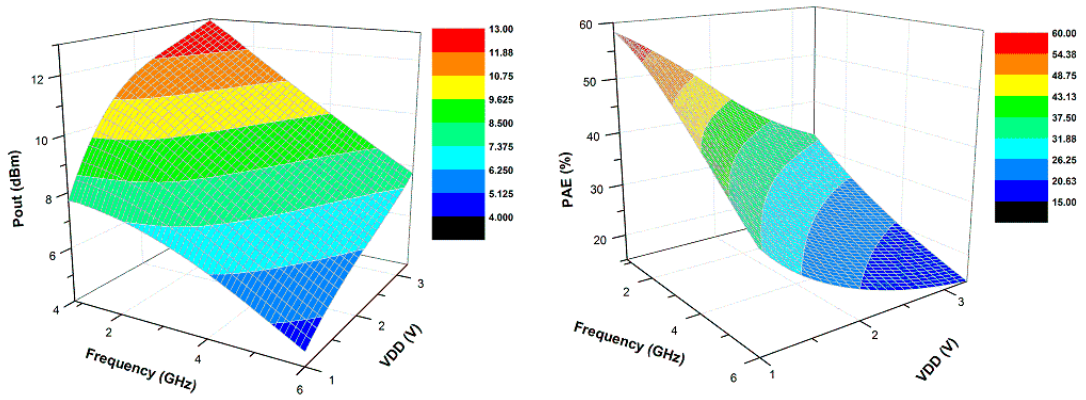
[2]They may try more supply voltages with smaller voltage step size in order to get more accurate simulation results.

of 53 possible values if a step of 0.1 GHz is selected.



(a) (b)

Figure 5.4: (a) Supply Voltage and Gate Biasing versus Output Power (b) Supply Voltage and Gate Biasing versus Power-added Efficiency

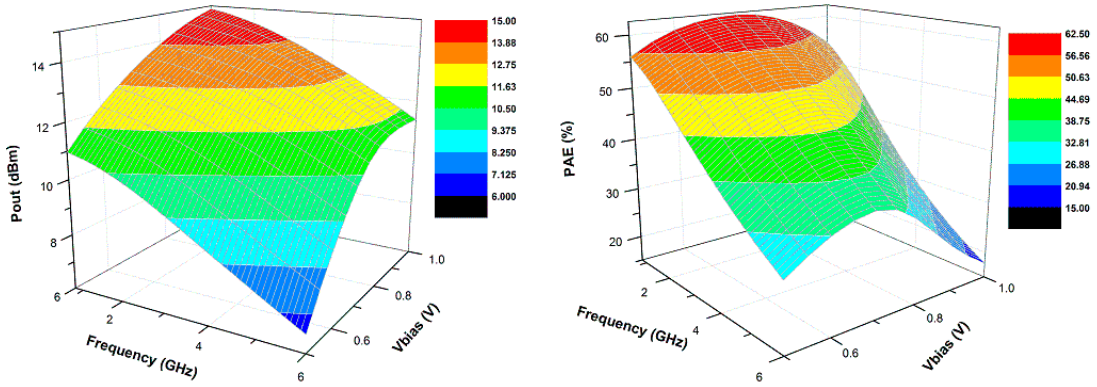


(a) (b)

Figure 5.5: (a) Supply Voltage and Frequency versus Output Power (b) Supply Voltage and Frequency versus Power-added Efficiency

With all of these possible cases available, the attackers will then run simulations to recover the original design by choosing the result with the best output power and power-added efficiency.

For example, Figures 5.4 (a) and (b) show the case that the actual supply voltage and gate bias, namely 1.9 and 1 V, do not deliver the best output yields. Similarly, Figures 5.5 (a) and (b) show that the maximum output power is not coincident with the maximum power-added efficiency. Since this power amplifier is designed for low-power applications, the specification defines the operating frequency to be 5.8 GHz; however, Figure 5.5 shows that the defined operating frequency is located in the middle level of the overall performance. Clearly attackers cannot recover the original design if the optimized parameter settings are chosen. Figures 5.6 (a) and (b) reflects the relationship of circuit performance versus frequency and gate bias. As shown in the figure, the actual values for frequency and gate bias, 5.8 GHz and 1 V, are located in the low performance area. Therefore, if the attackers follow the recovery process through Figures 5.4, 5.5 and 5.6, they cannot find the correct settings. Note that this sample testing process only represents a small fraction of the overall testing space meaning that it will take significant amount of time for attackers to fully simulate the design and collect the original design parameters, even for a simple RF circuit.

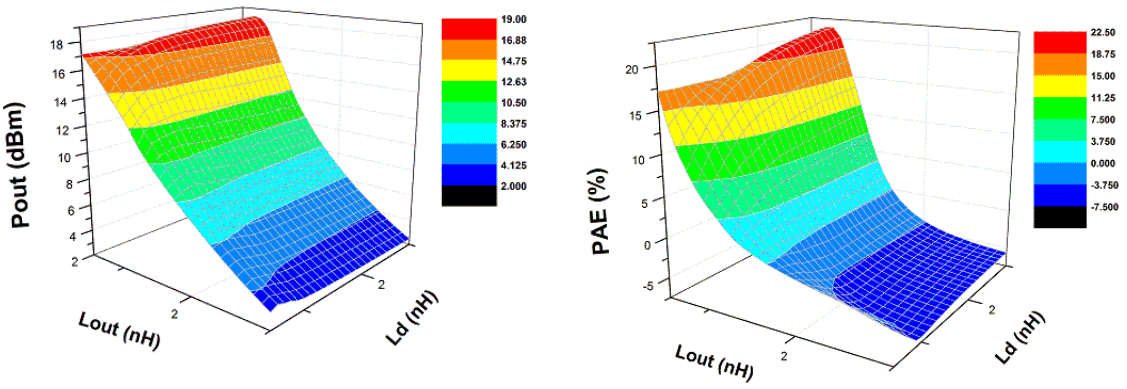


(a) (b)

Figure 5.6: (a) Gate Biasing and Frequency versus Output Power (b) Gate Biasing and Frequency versus Power-added Efficiency

Step 2: In the second step, we assume that the attackers have chosen the correct operating

conditions for the power amplifier, next they need to set the biasing conditions to precisely recover the inductor values. Following a general RF design methodology, the experienced attackers will sweep the RF choke L_d and the input inductor L_{in} by a reasonable range, which is from 0.5 to 3 nH in the 0.18 μm technology, to check the input reflection coefficient S11 and to further guess the frequency range, rather than a random sweeping on different frequencies. Based on the simulation results, the attackers will probably learn the circuit working frequency between 4 and 7 GHz. The derived frequency range helps to narrow the possible range of the input inductor, however the attackers need to select the inductor value for 4 to 7 GHz design operation. The attackers will then sweep the RF choke L_d and the output inductor L_{out} to optimize the output performance and the matching network. The simulation results will be meaningless if a wrong input inductor value is chosen.



(a) (b)

Figure 5.7: (a) Output Inductor and RF Choke versus Output Power (b) Output Inductor and RF Choke versus Power-added Efficiency

Figure 5.7 illustrates the output results that vary with respect to the RF choke and the output inductor. The actual values for the RF choke and the output inductor are 963 and 670 pH,

respectively. However, from Figure 5.7 we can see that both values produce good but not the best performance. It is possible that the attackers only aim for the best performance so they may choose inductor values from the wrong range.

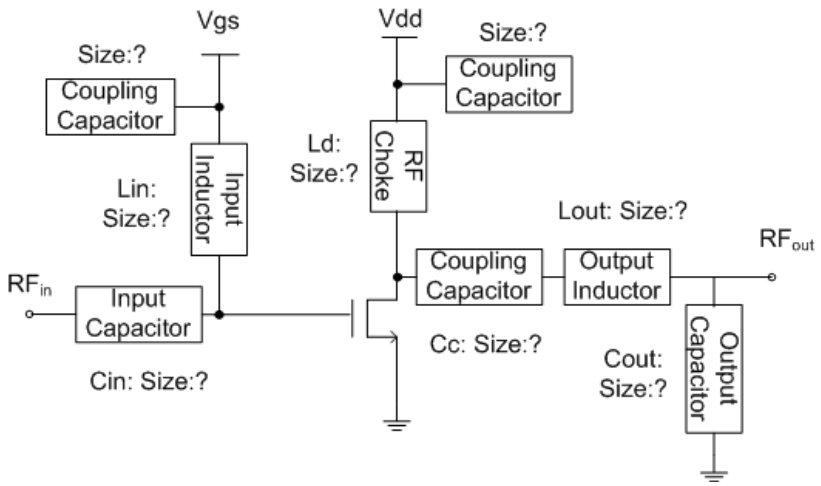
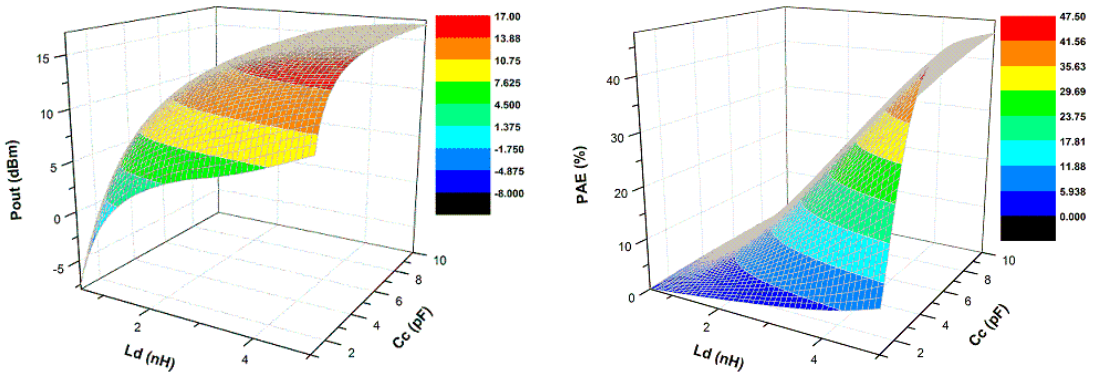


Figure 5.8: Schematic of Class-AB Power Amplifier Without Top Two Metal Layers (Missing Inductors and Capacitors)

Scenario II: Removal of Metal5 and Metal6 Layers (Capacitors and Inductors)

In this case, both inductors and capacitors are not available to the untrusted foundry because of the removal of the metal5 and metal6 layers from the FEOL. The missing capacitors add additional uncertainty, which makes it difficult for attackers to recover the whole design. That is, the unknown capacitors add more freedom in the simulation though parameter sweepings and will produce large amounts of combinations of inductors and capacitors. In this case, it is much easier for an experienced attacker to follow the typical power amplifier design procedure to retrieve the missing components.

Step 1: The first step of circuit testing is exactly the same as that in Scenario I.



(a) (b)

Figure 5.9: (a) RF Choke and Output Coupling versus Output Power (b) RF Choke and Output Coupling versus Power-added Efficiency

Step 2: After selecting the operating point, the attacker needs to figure out the RF choke inductor and output coupling capacitor. The 0.18 μm technology indicates that the reasonable ranges for inductor and capacitor are 0.5 to 5 nH and 1 to 10 pF, respectively. Using a sweeping step of 0.1 nH and 0.1 pF for inductors and capacitors, respectively, the attackers will come up with a total of 45 possible values for inductors and 90 possible values for capacitors[3]. Figure 5.9 shows the overall circuit performance when the values of the choke inductor and the output capacitor are changing. The figure helps attackers to recover the correct values of both components.

Step 3: After selecting the RF choke and coupling capacitor from various combinations, the attackers need to perform output matching to achieve a matched 50 Ω output. RF designers often perform output matching through load pull simulation, which provides the designers a bunch of matching combinations to choose from. Advanced EDA tools can help synthesize the maximum output power and power-added efficiency as well as further reflect the impedance of the optimal

[3]Note that the range of inductor shifts from 0.5 to 5 nH rather than from 0.5 to 3 nH due to the fact that capacitor values are unknown in Scenario II.

points. After choosing the impedance, the designers can use the Smith chart to recover the output matching network. Due to the simple structure of the single transistor power amplifier, the output matching network only includes one inductor and one capacitor. Relying on the load pull simulation, the attackers can retrieve four possible matching networks as showed in Figure 5.10.

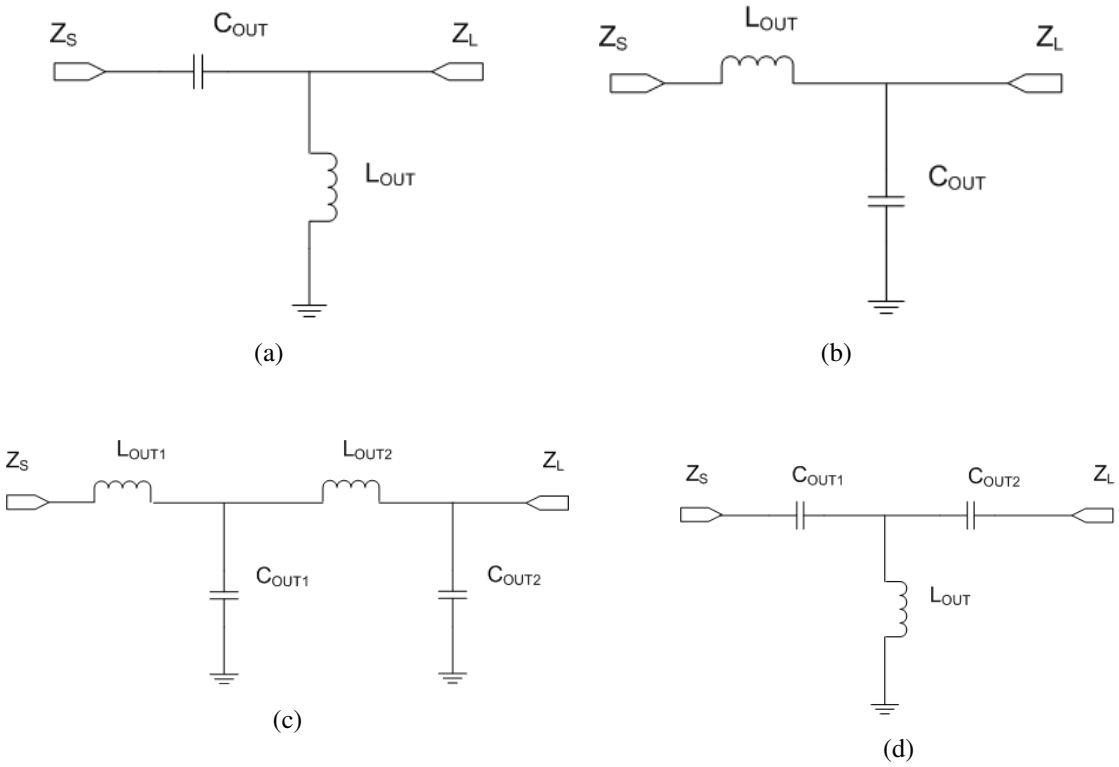


Figure 5.10: Four Possible Output Matching Network for the Class-AB Power Amplifier

The possible topologies cover L-type (Figures 5.10(a) and (b)), Π-type (Figure 5.10(c)) and T-type (Figure 5.10(d)), which are all basic network topology in RF design. All component values for each topology are located in reasonable design ranges; however, only the first two networks are possible given the number of passive components.

Step 4: After the load pull simulation, the attackers need to use the source pull simulation to

recover the input matching network, which follows a similar procedure to the load pull simulation.

Step 5: The final tuning is necessary for attackers to adjust the performance before all circuit parameters are recovered.

Scenario III: Obfuscation Techniques

Although various obfuscation techniques can be applied that increase the difficulty for attackers to recover the original circuit, in order to balance the performance impact and lower the design cost only two obfuscation methods are demonstrated in this chapter. Those two methods add 1) extra block space where the capacitors/inductors are located and 2) dummy cells to mislead the attackers into incorrect simulations.

To avoid high frequency signals interfering with each other, the lower level metals are not used where the inductors/capactors are located. The existence of these empty areas may reveal the approximate sizes of the inductors/capacitors which can lead to the recovery of the original design. To address this issue and to further increase the difficulty of RF IP piracy, we propose an obfuscation technique to deliberately increase passive component area. This will have the effect of lowering the correlation between the area of each inductor/capacitor and their value.

A second method will also be applied which includes unused empty blocks in the original design so that the attackers are unable to find the correct circuit structure. Those extra blocks can be located either in the input or the output side. For example, the attackers will only select L-types output matching networks from Figures 5.10(a) and (b), but they will also consider other topologies if two empty blocks are inserted.

Different from the IP protection scenarios I and II, the obfuscation technique in scenario III requires modifying the original layout. The RF design performance will be affected due to the sen-

sitivity of layout modifications. To address this issue, we suggest a new RF design methodology, called security co-design, which considers security at the early stage of the RF designs by altering some design rules to integrate the obfuscation technique in the design flow.

5.4 Experimentation

Through a simple class-AB power amplifier, we demonstrate that the split fabrication method is applicable to RF circuit protection and provide a robust, low-cost, and highly secure approach to prevent RF IC piracy. Encouraged by the results from the simple RF circuit, we applied the split manufacturing method and the same security analysis procedure to a class-E power amplifier which we recently designed, calibrated, and fabricated [108]. This class-E power amplifier works at a frequency of 5.2 GHz under 0.18 μm technology and delivers 12.5 dBm output power and 25% power-added efficiency. The circuit consists of five inductors and six capacitors and the detailed schematic is shown in Figure 5.11. The layout and the fabricated chip are shown in Figure 5.12.

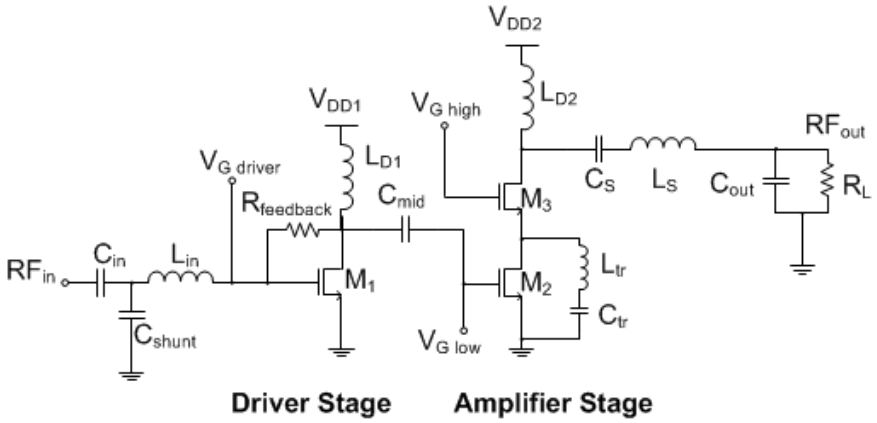
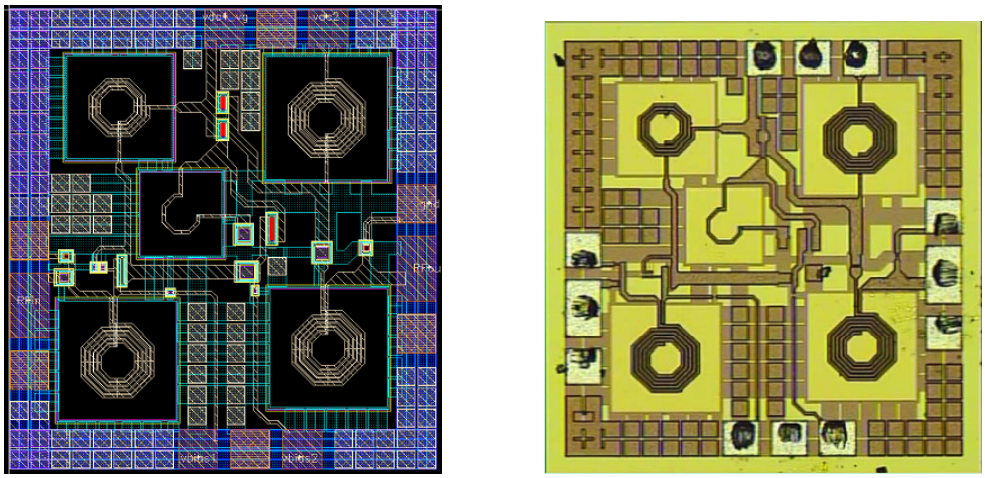


Figure 5.11: Schematic of A Cascode Class-E Power Amplifier

The gate bias of each transistor is not the same, nor is the supply voltage to each stage; this significantly increases the effort for attackers with the FEOL to recover the whole circuit, as we

will demonstrate shortly. The gate biases for the three transistors are 0.1, 0.7 and 1 V, while the DC supplies are 1 and 2.4 V for the two stages.



(a) (b)

Figure 5.12: (a) Layout of Class-E Power Amplifier (b) Microchip View of the Fabricated Class-E Power Amplifier

5.4.1 Scenario I: Removal of Metal6 Layers (Inductors)

Figures 5.13 and 5.14 show the FEOL part of the power amplifier schematic and its layout after the removal of metal6 layer. It is clear that the inductors occupy the majority of the RF circuit, which leads the attackers to easily identify that the missing components are inductors. Furthermore, the sample circuit caters to a boost technique of power-added efficiency (see the loop of M_2, L_{tr}, and C_{tr} [108]); therefore, even though only a few interconnections are missing, the attackers may still be unable to recover the circuit topology.

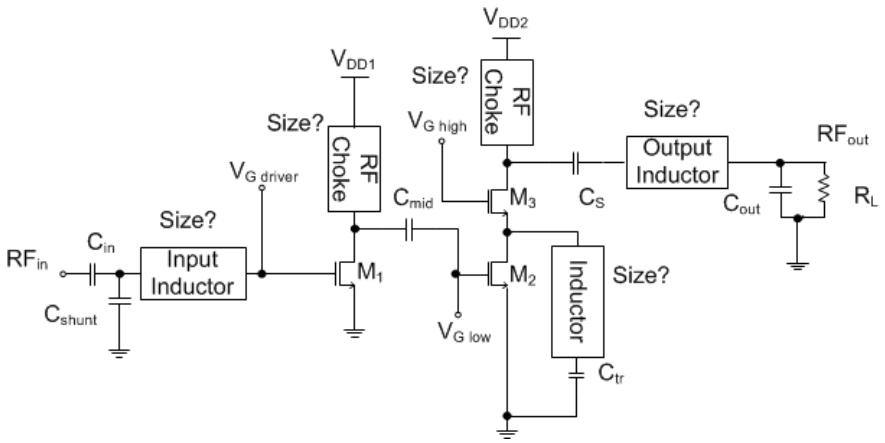


Figure 5.13: Schematic of the Class-E Power Amplifier Without Metal6

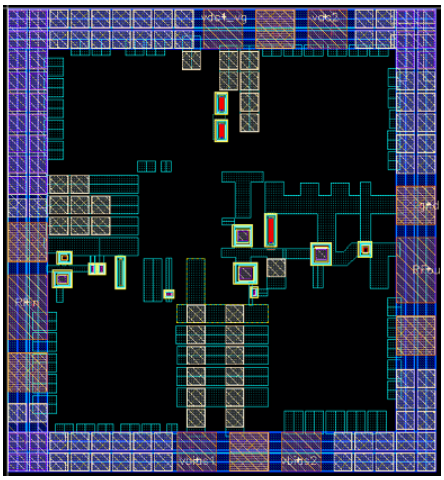


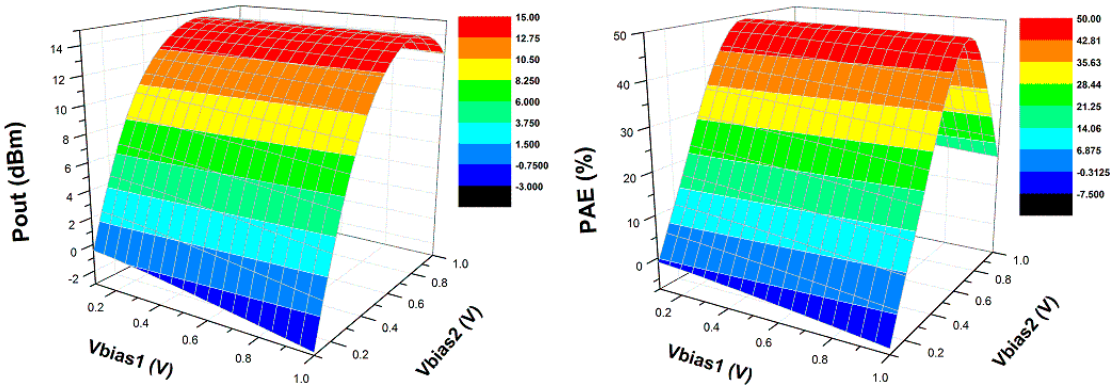
Figure 5.14: Layout of the Class-E Power Amplifier Without Metal6

In the first stage of the design, there are two inductors, L_{in} and L_{d1}. In the second stage, there are also two inductors, L_{d2} and L_s. We assume the attacker knows how the inductors are connected. The first task for attackers is to set up the DC biasing and operating frequency. As we can see from the schematic, the DC biasing (gate biasing and supply voltage) is more complicated than that in the one transistor case. The class-E power amplifier has three different gate biases

and two different supply voltages. The partial topology may suggest that it is a class-E power amplifier and that the first stage works as a driver (so that a low gate biasing will be used). It can also be interpreted as other types of power amplifiers as well, such as multi-stage class-A or class-AB power amplifiers, where the much larger gate biasing values are used. So the attacker needs to sweep the gate biasing by a large range, probably from 0.1 to 1 V, in order to decide the gate biasing in the first stage. The original design sets the first gate biasing at 0.1 V to make it work as a switch to the power amplifier. For supply voltage, a reasonable range can be from 1 to 3.3 V in terms of the 0.18 μm technology.

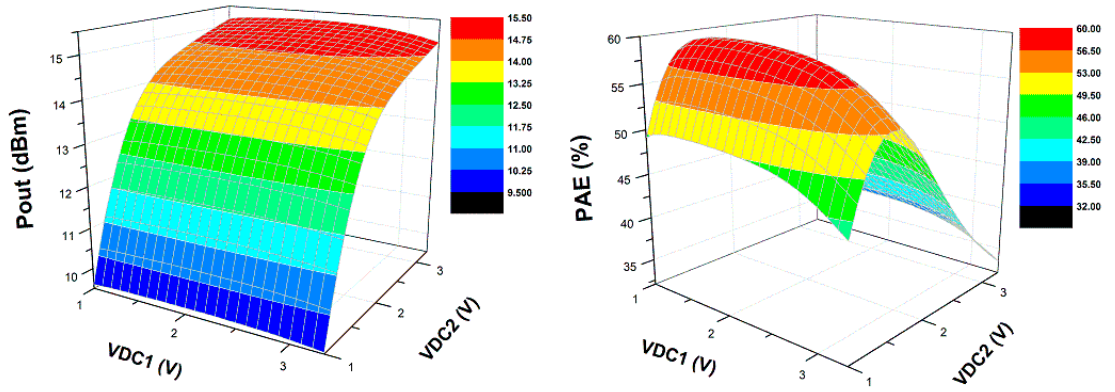
To demonstrate the impact of circuit performance with respect to gate biasing and supply voltage, we add back the correct inductor values and sweep the gate biasing and the supply voltage for both the first and the second stages. The simulation results are showed in Figures 5.15 and 5.16. From both figures, we can easily conclude that the overall performance is rather sensitive to the change of the gate biasing and the supply voltage, which makes the selection of operation conditions very important[4].

[4]In real case that the attackers do not know the inductor values, the task will be further complicated for them to derive the correct operation conditions.



(a) (b)

Figure 5.15: First-stage and Second-stage Gate Biases versus (a) Output Power (b) Power-added Efficiency.



(a) (b)

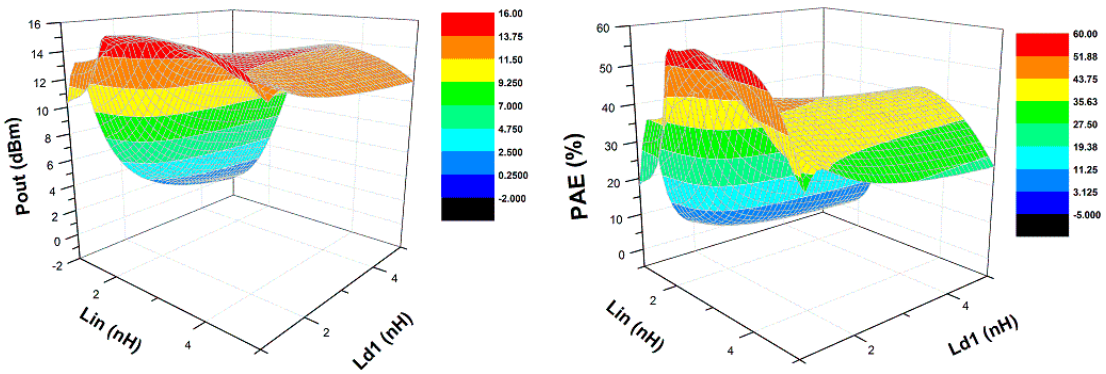
Figure 5.16: First-stage and Second-stage Supply Voltages versus (a) Output Power (b) Power-added Efficiency.

Normally, a higher supply voltage leads to a better output power but, a high supply voltage will also increase power consumption and decrease power-added efficiency. For this reason foundries often provide the reference for supply voltage to balance overall performance, i.e., 1.8

to 3.3 V for the 0.18 μm technology. For example, from Figure 5.16(a), we learn that the output does not change when V_{DC1} varies from 1.8 to 3.3 V; however, the maximum output power occurs when V_{DC2} is equal to its highest allowable value. In terms of efficiency shown in Figure 5.16(b), a high power-added efficiency can be achieved when V_{DC1} is below 3 V and V_{DC2} is around 2 V. With a voltage step of 0.1 V the attackers have 37 options for V_{DC1} selection and 19 options for V_{DC2} selection[5].

The next step is to derive the inductor values (operating frequency). We assume the attacker picks the correct DC bias, the gate biases and supply voltages for both stages. The attackers will then sweep the input stage inductor values to test and guess the operating frequency. They may conclude that the operating frequency ranges from 3 to 7 GHz, indicating that 41 choices are available for a 0.1 GHz step (the actual operating frequency is 5.2 GHz for this design). Once the attackers select the right frequency they will sweep the inductor values again to check the performance. Although multi-parameter sweeping is applied for all five inductors, to graphically show the simulation procedure, we group the testing cases into 3 cases. Within each case only one or two inductors change their values but, the rest of the values are fixed. In the first case only the input inductor L_{in} and first stage RF choke L_{d1} vary (see Figure 5.17); in the second case, the output inductor L_s and the second stage RF choke L_{d2} vary (see Figure 5.18); in the third case, only L_{tr} varies (see Figure 5.19).

[5]Note that the simulation results are derived from the situation that correct inductors are chosen for demonstrative purpose.

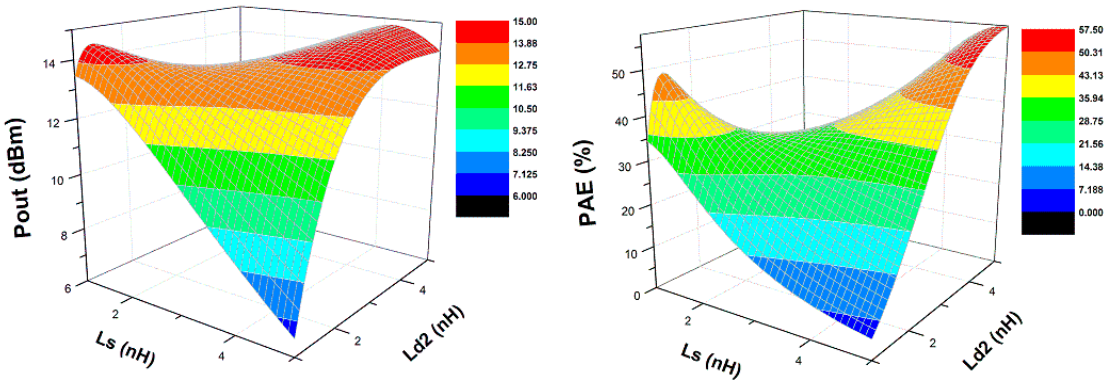


(a) (b)

Figure 5.17: (a) Output Power versus L_{in} and L_{d1} (b) Power-added Efficiency versus L_{in} and L_{d1}

The correct sizes of the input inductor L_{in} and the first-stage RF choke L_{d1} are 3.61 nH and 1.47 nH, respectively. However, from Figure 5.17, more than one parameter combination is available to achieve the best performance (note that other inductors values are correctly selected in the simulation). The attackers will have to guess the values of L_{in} from 2 to 4 nH and L_{d1} from 1 to 2 nH purely based on the performance comparison. We want to emphasize that the purpose of applying split manufacturing is to prevent the attackers from learning the exact circuit design which will later be used in critical infrastructures. Through the simulation, attackers may be able to derive an even better performance class-E power amplifier. However, a better design does not mean that it would be fitted into the overall system design or some application-specific design. For example, the required power amplifier is supposed to have 15 dBm amplification at operating frequency of 900 MHz. Meanwhile, the attackers retrieve a better amplification of 20 dBm at 2 GHz. In this case, our power amplifier is secured even though attackers come up with a better design. In our class-E power amplifier, the chances that the attacker can derive exactly the same power amplifier are relatively low (4.76% for L_{in} and 9.09% for L_{d1} given the rest three inductors

are correctly selected). To fully elaborate the results, the sweeping range for L_{in} is from 2 to 4 nH and for L_{d1} is from 1 to 2 nH. The sweeping step for both L_{in} and L_{d1} is 0.1 nH. Thus, the probability to guess L_{in} right is one out of twenty-one (= 4.76%) and to guess L_{d1} right is one out of eleven (= 9.09%).



(a) (b)

Figure 5.18: (a) Output Power versus L_s and L_{d2} (b) Power-added Efficiency versus L_s and L_{d2}

The correct size of the output inductor is L_s = 3.61 nH and the second-stage RF choke is L_{d2} = 4.56 nH. These sizes are within the best performance region as shown in Figure 5.18. If the attackers are guided by the performance, they may choose L_s from 3.6 to 5 nH and L_{d2} from 4 to 5 nH. Therefore, the probabilities of a correct recovery for the output inductor L_s is 6.25% and for the second-stage RF choke L_{d2} is 9.09%.

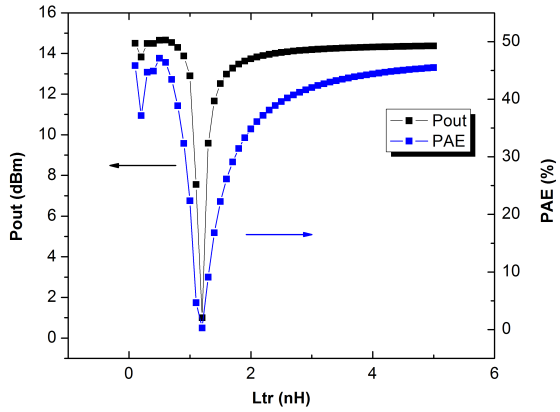


Figure 5.19: Overall Performance versus L_{tr}

The correct size of the inductor L_{tr} is 0.27 nH. This inductor is located in parallel with the transistor M2 and is used for improving the power-added efficiency; however, the inductor is located in the middle of the entire layout which may be mis-interpreted as an intermedium matching network between the first and the second stage. In that case, the attackers have no way to recover the circuit structure; otherwise, as shown in Figure 5.19, the attackers may select its value from 0.1 to 0.8 nH with respect to its physical size and the overall circuit performance.

5.5 Discussion

The main focus of our chapter is the split manufacturing on radio-frequency design. We have presented a small portion of obfuscation technique. However, we believe that the concrete study of obfuscation technique can further improve the security of split manufacturing. For instance, the original design could deliberately include many sub-optimal components along with many optimally designed components. Then the attacker is faced with a dilemma whether any given local

component is intended to be realized with the optimal parameters or not. Deliberately creating this dilemma for each component could perhaps make the overall design even harder to retrieve.

5.6 Summery

Split manufacturing has presented a new solution against reverse engineering and IP piracy as the IC design flow becomes more globalized. Different from all previous work to apply the split manufacturing in digital circuits, we introduced the first attempt to implement a similar method in RF designs. Quantitative analysis was presented to assess the security protection level for RF designs in the event that untrusted foundries would like to recover the circuit designs based on part of the circuit layout. To further guide the application of split manufacturing in RF circuits, three different FEOL and BEOL separation and obfuscation methods were introduced. All of these methods were demonstrated on two RF circuits: a simple class-AB power amplifier and a more sophisticated class-E power amplifier. The experimental results confirmed that the unknown passive components, either inductors or capacitors, along with the missing DC biasing conditions, can raise a significant amount of uncertainty for the attacker to recover the RF circuits. In conclusion, split manufacturing is more effective in RF IC trust than in digital circuit security. We hope to pursue a real silicon-level implementation in our future work.

CHAPTER 6: CONCLUSION

Today's integrated circuit (IC) development demands a large capital investment. Many third-parties are involved in IC design and manufacturing process, in order to reduce costs. Therefore, the semiconductor supply chain becomes more vulnerable to a wide range of attacks than ever before. To improve security and trustworthiness of ICs, we presented a series of design and test methodologies to deal with four challenging hardware security problems. The major contributions of the thesis will be presented in this chapter.

6.1 Enhanced Hardware Security Primitives beyond PUFs

Considering the large amount of emerging device models including graphene transistors, atomic switches, memristors, MOTT FET, spin FET, nanomagnetic and all-spin logic, spin wave devices, OST-RAM, magnetoresistive random-access memory (MRAM), spintronic devices, etc. [109], two fundamental questions have recently been raised related to their applications in the hardware security domain: 1) *Can emerging technology provide a more efficient hardware infrastructure than CMOS technology in countering hardware Trojans and IP piracy*? 2) *What properties should the emerging technology-based hardware infrastructure provide so that software-level protection schemes can be better supported*?

Chapter 3 presents two emerging devices, SiNW FETs and graphene SymFETs, for demonstration. Five different security applications were designed and verified, ranging from IP protection to efficient cryptographic computation. The first question has been answered by providing preliminary experimental results and hardware infrastructure designs. Experimental schematics and layouts as well as their testing results are also provided to uphold our claim that some emerging

technologies outperform CMOS in many hardware security applications.

6.2 DPA-resilient Block Cipher Design

Conventional circuit level protection schemes such as current mode logic (CML) trade power efficiency for security. To tackle this problem, chapter 4 presents a new methodology that leverages new transistor technology for the cryptographic applications. The usage of emerging tunnel FET is demonstrated to help improve cryptographic circuit design resilience against CPA attacks while still preserving low power consumption compared to their CMOS counterparts. Compared to the CMOS-based CML designs, the TFET CML circuit consumes 15 times less power while achieving a similar level of DPA resistance.

6.3 Split Manufacturing on RF Power Amplifier

Chapter 5 presents a innovative security application, which applies the split fabrication method into RF circuit protection. Three different scenarios of split fabrication are proposed and analyzed. A single-stage class-AB power amplifier is adopted as first example for demontration of effectiveness of proposed technique. A more accurate class-E power amplifier, which we recently designed, calibrated and fabricated, is used for thorough security analysis. The experimental results confirm that the unknown passive components, either inductors or capacitors, along with the missing DC biasing conditions, can raise a significant amount of uncertainty for the attacker to recover the RF circuits. Consequently, we demontrate that split manufacturing in RF IC can be more effective compared to digital circuit counterparts.

LIST OF REFERENCES

[1] B. Sedighi, X. Hu, H. Liu, J. Nahas, and M. Niemier, "Analog circuit design using tunnel-fets," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 62, no. 1, pp. 39–48, Jan 2015.

[2] D. Hisamoto, W.-C. Lee, J. Kedzierski, H. Takeuchi, K. Asano, C. Kuo, E. Anderson, T.-J. King, J. Bokor, and C. Hu, "Finfet-a self-aligned double-gate mosfet scalable to 20 nm," *Electron Devices, IEEE Transactions on*, vol. 47, no. 12, pp. 2320–2325, Dec 2000.

[3] V. Saripalli, G. Sun, A. Mishra, Y. Xie, S. Datta, and V. Narayanan, "Exploiting heterogeneity for energy efficiency in chip multiprocessors," *Emerging and Selected Topics in Circuits and Systems, IEEE Journal on*, vol. 1, no. 2, pp. 109–119, June 2011.

[4] M. De Marchi, D. Sacchetto, S. Frache, J. Zhang, P.-E. Gaillardon, Y. Leblebici, and G. De Micheli, "Polarity control in double-gate, gate-all-around vertically stacked silicon nanowire fets," in *Electron Devices Meeting (IEDM), 2012 IEEE International*, Dec 2012, pp. 8.4.1–8.4.4.

[5] P.-E. Gaillardon, L. G. Amarù, S. Bobba, M. De Marchi, D. Sacchetto, and G. De Micheli, "Nanowire systems: technology and design," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 372, no. 2012, 2014.

[6] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13, 2013, pp. 709–720.

[7] P.-E. Gaillardon, S. Bobba, M. D. Marchi, D. Sacchetto, and G. D. Micheli, "Nanowire systems: Technology and design," *Philosophical Transactions of the Royal Society of London A*, vol. 372, no. 2012, 2014.

[8] U. Avci, R. Rios, K. Kuhn, and I. Young, "Comparison of performance, switching energy and process variations for the tfet and mosfet in logic," in *VLSI Technology (VLSIT), 2011 Symposium on*, June 2011, pp. 124–125.

[9] I. Verbauwhede and P. Schaumont, "Design methods for security and trust," in *Design, Automation and Test in Europe Conference and Exhibition, 2007. DATE '07*, 2007, pp. 1–6.

[10] I. Inc., "Secure cryptographic coprocessor. (http://www.research.ibm.com/ssd_scop)."

[11] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *Computers, IEEE Transactions on*, vol. 51, no. 5, pp. 541–552, 2002.

[12] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO '99, 1999, pp. 388–397.

[13] C. Herder, M. D. 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.

[14] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "Puf modeling attacks on simulated and silicon data," 2013.

[15] C. Helfmeier, C. Boit, D. Nedospasov, and J. P. Seifert, "Cloning physically unclonable functions," in *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*, June 2013, pp. 1–6.

[16] Chipworks, "Intel's 22-nm tri-gate transistors exposed," 2012. [Online]. Available: http://www.chipworks.com/blog/technologyblog/2012/04/23/intels-22-nmtri-gate-transistors-exposed/.

[17] R. Torrance and D. James, "The state-of-the-art in semiconductor reverse engineering," in *Design Automation Conference (DAC), 2011 48th ACM/EDAC/IEEE*, June 2011, pp. 333–338.

[18] D. A. R. P. Agency, "Trust in integrated circuits (TIC)," 2007. [Online]. Available: https://www.fbo.gov/spg/ODA/DARPA/CMO/BAA07-24/listing.html

[19] Chipworks, "Reverse engineering software," 2014. [Online]. Available: http://www.chipworks.com/en/technical-competitive-analysis/resources/reverse-engineering-software.

[20] P. Rohatgi, *Cryptographic Engineering*. Springer US, 2009, ch. Improved Techniques for Side-Channel Analysis, pp. 381–406.

[21] P. C., P. J., and B. Preneel, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer-Verlag, 2010.

[22] P. Rohatgi, *Cryptographic Engineering*. Boston, MA: Springer US, 2009, ch. Electromagnetic Attacks and Countermeasures, pp. 407–430.

[23] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert, *Cryptographic Hardware and Embedded Systems – CHES 2012: 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*. Springer Berlin Heidelberg, 2012, ch. Simple Photonic Emission Analysis of AES, pp. 41–57.

[24] D. Genkin, A. Shamir, and E. Tromer, *Advances in Cryptology – CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I.* Springer Berlin Heidelberg, 2014, ch. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis, pp. 444–461.

[25] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The sorcerer's apprentice guide to fault attacks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 370–382, Feb 2006.

[26] A. Iyengar, K. Ramclam, and S. Ghosh, "Dwm-puf: A low-overhead, memory-based security primitive," in *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*, 2014, pp. 154–159.

[27] B. Sedighi, X. S. Hu, J. J. Nahas, and M. Niemier, "Boolean circuit design using emerging tunneling devices," *International Conference on Computer Design (ICCD)*, pp. 355–360, 2014.

[28] A. C. Seabaugh and Q. Zhang, "Low-voltage tunnel transistors for beyond cmos logic," *Proceedings of the IEEE*, vol. 98, no. 12, pp. 2095–2110, Dec 2010.

[29] H. Lu and A. Seabaugh, "Tunnel field-effect transistors: State-of-the-art," *Electron Devices Society, IEEE Journal of the*, vol. 2, no. 4, pp. 44–49, July 2014.

[30] G. Zhou, R. Li, T. Vasen, M. Qi, S. Chae, Y. Lu, Q. Zhang, H. Zhu, J.-M. Kuo, T. Kosel, M. Wistey, P. Fay, A. Seabaugh, and H. Xing, "Novel gate-recessed vertical inas/gasb tfets with record high ion of 180 $\mu a/\mu m$ at vds=0.5 v," in *Electron Devices Meeting (IEDM), 2012 IEEE International*, Dec 2012, pp. 32.6.1–32.6.4.

[31] H. Lu, J. W. Kim, D. Esseni, and A. Seabaugh, "Continuous semiempirical model for the current-voltage characteristics of tunnel fets," in *Ultimate Integration on Silicon (ULIS), 2014 15th International Conference on*, 2014, pp. 25–28.

[32] H. Lu, D. Esseni, and A. Seabaugh, "Universal analytic model for tunnel {FET} circuit simulation," *Solid-State Electronics*, vol. 108, pp. 110 – 117, 2015.

[33] W.-Y. Tsai, H. Liu, X. Li, and V. Narayanan, "Low-power high-speed current mode logic using tunnel-fets," in *Very Large Scale Integration (VLSI-SoC), 2014 22nd International Conference on*, Oct 2014, pp. 1–6.

[34] A. Colli, S. Pisana, A. Fasoli, J. Robertson, and A. C. Ferrari, "Electronic transport in ambipolar silicon nanowires," *physica status solidi (b)*, vol. 244, no. 11, pp. 4161–4164, 2007.

[35] R. Martel, V. Derycke, C. Lavoie, J. Appenzeller, K. K. Chan, J. Tersoff, and P. Avouris, "Ambipolar electrical transport in semiconducting single-wall carbon nanotubes," *Phys. Rev. Lett.*, vol. 87, 2001.

[36] A. K. Geim and K. S. Novoselov, "The rise of graphene," *Nature Materials*, vol. 6, pp. 183–191, 2007.

[37] Y.-M. Lin, J. Appenzeller, J. Knoch, and P. Avouris, "High-performance carbon nanotube field-effect transistor with tunable polarities," *Nanotechnology, IEEE Transactions on*, vol. 4, no. 5, pp. 481–489, 2005.

[38] N. Harada, K. Yagi, S. Sato, and N. Yokoyama, "A polarity-controllable graphene inverter," *Applied Physics Letters*, vol. 96, no. 1, 2010.

[39] J. Appenzeller, J. Knoch, E. Tutuc, M. Reuter, and S. Guha, "Dual-gate silicon nanowire transistors with nickel silicide contacts," in *Electron Devices Meeting, 2006. IEDM '06. International*, 2006, pp. 1–4.

[40] A. Heinzig, S. Slesazeck, F. Kreupl, T. Mikolajick, and W. M. Weber, "Reconfigurable silicon nanowire transistors," *Nano Letters*, vol. 12, no. 1, pp. 119–124, 2012.

[41] C. H. Jan, U. Bhattacharya, R. Brain, S. J. Choi, G. Curello, G. Gupta, W. Hafez, M. Jang, M. Kang, K. Komeyli, T. Leo, N. Nidhi, L. Pan, J. Park, K. Phoa, A. Rahman, C. Staus, H. Tashiro, C. Tsai, P. Vandervoorn, L. Yang, J. Y. Yeh, and P. Bai, "A 22nm soc platform technology featuring 3-d tri-gate and high-k/metal gate, optimized for ultra low power, high performance and high density soc applications," in *Electron Devices Meeting (IEDM), 2012 IEEE International*, Dec 2012, pp. 3.1.1–3.1.4.

[42] A. C. Seabaugh and Q. Zhang, "Low-voltage tunnel transistors for beyond cmos logic," *Proceedings of the IEEE*, vol. 98, no. 12, pp. 2095–2110, Dec 2010.

[43] P. Zhao, R. Feenstra, G. Gu, and D. Jena, "Symfet: A proposed symmetric graphene tunneling field-effect transistor," *Electron Devices, IEEE Transactions on*, vol. 60, no. 3, pp. 951–957, March 2013.

[44] L. Britnell, R. V. Gorbachev, A. K. Geim, L. A. Ponomarenko, A. Mishchenko, M. T. Greenaway, T. M. Fromhold, K. S. Novoselov, and L. Eaves, "Resonant tunnelling and negative differential conductance in graphene transistors," *Nat Commun*, vol. 4, p. 1794, 04 2013.

[45] B. Sedighi, X. S. Hu, J. Nahas, and M. Niemier, "Nontraditional computation using beyond-cmos tunneling devices," *Journal of Emerging and Selected Topics in Circuits and Systems*, vol. 4, no. 4, pp. 438–449, 2014.

[46] M. Stiles and A. Zangwill, "Anatomy of spin-transfer torque," *Physical Review B*, vol. 66, no. 1, p. 014407, 2002.

[47] H. Yoda, E. Kitagawa, N. Shimomura, S. Fujita, and M. Amano, "The progresses of mram as a memory to save energy consumption and its potential for further reduction," in *VLSI Circuits (VLSI Circuits), 2015 Symposium on*. IEEE, 2015, pp. T104–T105.

[48] S. Ikeda, K. Miura, H. Yamamoto, K. Mizunuma, H. Gan, M. Endo, S. Kanai, J. Hayakawa, F. Matsukura, and H. Ohno, "A perpendicular-anisotropy cofeb–mgo magnetic tunnel junction," *Nature materials*, vol. 9, no. 9, pp. 721–724, 2010.

[49] J. Gibbons and W. Beadle, "Switching properties of thin nio films," *Solid-State Electronics*, vol. 7, no. 11, pp. 785–790, 1964.

[50] H.-S. P. Wong, H.-Y. Lee, S. Yu, Y.-S. Chen, Y. Wu, P.-S. Chen, B. Lee, F. T. Chen, and M.-J. Tsai, "Metal–oxide rram," *Proceedings of the IEEE*, vol. 100, no. 6, pp. 1951–1970, 2012.

[51] H. Akinaga and H. Shima, "Resistive random access memory (reram) based on metal oxides," *Proceedings of the IEEE*, vol. 98, no. 12, pp. 2237–2251, 2010.

[52] D. J. Wouters, R. Waser, and M. Wuttig, "Phase-change and redox-based resistive switching memories," *Proceedings of the IEEE*, vol. 103, no. 8, 2015.

[53] H. Lee, P. Che, T. Wu, Y. Che, C. Wan, P. Tzen, C. Lin, F. Chen, C. Lien, and M. Tsai, "Low power and high speed bipolar switching with a thin reactive ti buffer layer in robust hfo2 based rram," in *Electron Devices Meeting, 2008. IEDM 2008. IEEE International*. IEEE, 2008, pp. 1–4.

[54] Y. Bi, P.-E. Gaillardon, X. Hu, M. Niemier, J.-S. Yuan, and Y. Jin, "Leveraging emerging technology for hardware security - case study on silicon nanowire FETs and graphene Symfets," in *Test Symposium (ATS), 2014 IEEE 23rd Asian*, Nov 2014, pp. 342–347.

[55] Y. Bi, K. Shamsi, J.-S. Yuan, P.-E. Gaillardon, G. D. Micheli, X. Yin, X. S. Hu, M. Niemier, and Y. Jin, "Emerging technology-based design of primitives for hardware security," *J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 1, pp. 3:1–3:19, Apr. 2016.

[56] L.-W. Chow, J. Baukus, and W. C. U. Patent, "Integrated circuits protected against reverse engineering and method for fabricating the same using an apparent metal contact line terminating on field oxide," U.S. Patent US Patent 7,294,935, 2002. [Online]. Available: http://www.google.com/patents/US7294935

[57] P. Ronald, P. James, and J. Bryan, "building block for a secure cmos logic cell library," U.S. Patent 8 111 089, 2012.

[58] L. W. Chow, J. P. Baukus, B. J. Wang, and R. P. C. U. Patent, "Camouflaging a standard cell based integrated circuit," U.S. Patent US Patent 8,151,235, 2012. [Online]. Available: http://www.google.com/patents/US8151235

[59] A. Stoica, R. Zebulum, D. Keymeulen, M. Ferguson, and V. Duong, "Taking evolutionary circuit design from experimentation to implementation: some useful techniques and a silicon demonstration," *IEE Proceedings-Computers and Digital Techniques*, vol. 151, no. 4, pp. 295–300, 2004.

[60] R. Ruzicka, "New polymorphic nand/xor gate," in *Proceedings of 7th WSEAS International Conference on Applied Computer Science*, vol. 2007. Citeseer, 2007, pp. 192–196.

[61] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Logic encryption: A fault analysis perspective," in *Proceedings of the Conference on Design, Automation and Test in Europe*. EDA Consortium, 2012, pp. 953–958.

[62] A. Stoica, R. Zebulum, and D. Keymeulen, *Polymorphic Electronics*. Springer, 2001.

[63] Arizona State University, "PTM model," 2014. [Online]. Available: http://ptm.asu.edu/

[64] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing ic piracy using reconfigurable logic barriers," *Design Test of Computers, IEEE*, vol. 27, no. 1, pp. 66–75, Jan 2010.

[65] A. Barenghi, G. Bertoni, L. Breveglieri, M. Pellicioli, and G. Pelosi, "Fault attack on aes with single-bit induced faults," in *Information Assurance and Security (IAS), 2010 Sixth International Conference on*, 2010, pp. 167–172.

[66] J. Guo and K. N. Leung, "A 6-μw chip-area-efficient output-capacitorless ldo in 90-nm cmos technology," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 9, pp. 1896–1905, Sept 2010.

[67] K. Shamsi, Y. Bi, Y. Jin, P. E. Gaillardon, M. Niemier, and X. S. Hu, "Reliable and high performance stt-mram architectures based on controllable-polarity devices," in *Computer Design (ICCD), 2015 33rd IEEE International Conference on*, Oct 2015, pp. 343–350.

[68] Y. Bi, X. S. Hu, Y. Jin, M. Niemier, K. Shamsi, and X. Yin, "Enhancing hardware security with emerging transistor technologies," in *Proceedings of the 26th Edition on Great Lakes Symposium on VLSI*, ser. GLSVLSI '16, 2016, pp. 305–310.

[69] X. Li, W.-Y. Tsai, V. Narayanan, H. Liu, and S. Datta, "A low-voltage low-power lc oscillator using the diode-connected symfet," in *VLSI (ISVLSI), 2014 IEEE Computer Society Annual Symposium on*, July 2014, pp. 302–307.

[70] K. Gomina, J.-B. Rigaud, P. Gendrier, P. Candelier, and A. Tria, "Power supply glitch attacks: Design and evaluation of detection circuits," in *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*, May 2014, pp. 136–141.

[71] P.-E. Gaillardon, L. Amaru, J. Zhang, and G. De Micheli, "Advanced system on a chip design based on controllable-polarity fets," in *Proceedings of the Conference on Design, Automation & Test in Europe*, ser. DATE '14, 2014.

[72] Y. Bi, K. Shamsi, J. S. Yuan, F. X. Standaert, and Y. Jin, "Leverage emerging technologies for dpa-resilient block cipher design," in *2016 Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2016, pp. 1538–1543.

[73] Y. Bi, K. Shamsi, J. S. Yuan, Y. Jin, M. Niemier, and X. S. Hu, "Tunnel fet current mode logic for dpa-resilient circuit designs," *IEEE Transactions on Emerging Topics in Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[74] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *VLSI Design, 2007. Held jointly with 6th International Conference on Embedded Systems., 20th International Conference on*, Jan 2007, pp. 854–862.

[75] S. Badel, E. Guleyupoglu, O. Inac, A. Martinez, P. Vietti, F. Gurkaynak, and Y. Leblebici, "A generic standard cell design methodology for differential circuit styles," in *Design, Automation and Test in Europe, 2008. DATE '08*, March 2008, pp. 843–848.

[76] A. Cevrero, F. Regazzoni, M. Schwander, S. Badel, P. Ienne, and Y. Leblebici, "Power-gated mos current mode logic (pg-mcml): A power aware dpa-resistant standard cell library," in *Design Automation Conference (DAC), 2011 48th ACM/EDAC/IEEE*, June 2011, pp. 1014–1019.

[77] M. Elmasry and M. Allam, "Dynamic current mode logic family," Feb. 22 2000, uS Patent 6,028,454.

[78] S. Badel, I. Hatirnaz, and Y. Leblebici, "Semi-automated design of a mos current mode logic standard cell library from generic components," in *Research in Microelectronics and Electronics, 2005 PhD*, vol. 2, July 2005, pp. 155–158.

[79] N. Debande, Y. Souissi, M. A. E. Aabid, S. Guilley, and J.-L. Danger, "Wavelet transform based pre-processing for side channel analysis," in *Proceedings of the 2012 45th Annual IEEE/ACM International Symposium on Microarchitecture Workshops*, 2012, pp. 32–38.

[80] J. G. J. van Woudenberg, M. F. Witteman, and B. Bakker, "Improving differential power analysis by elastic alignment," in *Proceedings of the 11th International Conference on Topics in Cryptology: CT-RSA 2011*, ser. CT-RSA'11, 2011, pp. 104–119.

[81] C. Cannière, O. Dunkelman, and M. Knežević, "Katan and ktantan – a family of small and efficient hardware-oriented block ciphers," in *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, ser. CHES '09. Springer-Verlag, 2009, pp. 272–288.

[82] H. Liu, V. Saripalli, V. Narayanan, and S. Datta, "III-V tunnel FET model," Apr 2015.

[83] G. V. Bard, N. Courtois, J. N. Jr., P. Sepehrdad, and B. Zhang, "Algebraic, aida/cube and side channel analysis of KATAN family of block ciphers," in *Progress in Cryptology - INDOCRYPT 2010 - 11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings*, 2010, pp. 176–196.

[84] F. Macé, F.-X. Standaert, J.-J. Quisquater, and J.-D. Legat, "A design methodology for secured ics using dynamic current mode logic," in *Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation*, 2005, vol. 3728, pp. 550–560.

[85] Y. Nogami, K. Nekado, T. Toyota, N. Hongo, and Y. Morikawa, "Mixed bases for efficient inversion in f((22)2)2 and conversion matrices of subbytes of aes," in *Proceedings of the 12th International Conference on Cryptographic Hardware and Embedded Systems*, ser. CHES'10, 2010, pp. 234–247.

[86] X. Guo, D. Mukhopadhyay, C. Jin, and R. Karri, "Security analysis of concurrent error detection against differential fault analysis," *Journal of Cryptographic Engineering*, vol. 5, no. 3, pp. 153–169, 2015.

[87] ——, "Nrepo: Normal basis recomputing with permuted operands," in *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*, May 2014, pp. 118–123.

[88] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A lightweight high-performance fault detection scheme for the advanced encryption standard using composite fields," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 19, no. 1, pp. 85–91, Jan. 2011.

[89] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error analysis and detection procedures for a hardware implementation of the advanced encryption standard," *Computers, IEEE Transactions on*, vol. 52, no. 4, pp. 492–505, April 2003.

[90] S. Bayat-Sarmadi, M. Mozaffari-Kermani, and A. Reyhani-Masoleh, "Efficient and concurrent reliable realization of the secure cryptographic sha-3 algorithm," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 33, no. 7, pp. 1105–1109, July 2014.

[91] D. McGrew and J. Viega, "The galois counter mode of operation," *NIST*, May 2005. [Online]. Available: http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-revised-spec.pdf

[92] A. Satoh, T. Sugawara, and T. Aoki, "High-performance hardware architectures for galois counter mode," *Computers, IEEE Transactions on*, vol. 58, no. 7, pp. 917–930, July 2009.

[93] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *Design Test of Computers, IEEE*, vol. 27, pp. 10–25, 2010.

[94] Y. Jin, B. Yang, and Y. Makris, "Cycle-accurate information assurance by proof-carrying based signal sensitivity tracing," in *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 99–106.

[95] I. A. R. P. Activity, "Trusted integrated chips (TIC) program," 2011. [Online]. Available: https://www.fbo.gov/notices/36a5148742778693073399 9edc40f321

[96] J. Rajendran, O. Sinanoglu, and R. Karri, "Is split manufacturing secure?" in *Design, Automation Test in Europe Conference Exhibition (DATE), 2013*, 2013, pp. 1259–1264.

[97] F. Imeson, A. Emtenan, S. Garg, and M. Tripunitara, "Securing computer hardware using 3d integrated circuit (ic) technology and split manufacturing for obfuscation," in *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*. Washington, D.C.: USENIX, 2013, pp. 495–510. [Online]. Available: https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/imeson

[98] B. Hill, R. Karmazin, C. Otero, J. Tse, and R. Manohar, "A split-foundry asynchronous fpga," in *Custom Integrated Circuits Conference (CICC), 2013 IEEE*, 2013, pp. 1–4.

[99] K. Vaidyanathan, B. P. Das, E. Sumbul, R. Liu, and L. Pileggi, "Building trusted ics using split fabrication," in *Hardware-Oriented Security and Trust (HOST), 2014*, 2014.

[100] K. Vaidyanathan, R. Liu, E. Sumbul, Q. Zhu, F. Franchetti, and L. Pileggi, "Efficient and secure intellectual property (ip) design with split fabrication," in *Hardware-Oriented Security and Trust (HOST), 2014*, 2014.

[101] M. Jagasivamani, P. Gadfort, M. Sika, M. Bajura, and M. Fritze, "Split-fabrication obfuscation: Metrics and techniques," in *Hardware-Oriented Security and Trust (HOST), 2014*, 2014.

[102] K. Vaidyanathan, B. P. Das, and L. Pileggi, "Detecting reliability attacks during split fabrication using test-only beol stack," in *Proceedings of the The 51st Annual Design Automation Conference on Design Automation Conference*, ser. DAC '14, 2014, pp. 156:1–156:6.

[103] Y. Bi, J. S. Yuan, and Y. Jin, "Split manufacturing in radio-frequency designs," in *The International Conference on Security and Management*, ser. SAM '15, 2015, pp. 204–210.

[104] ——, "Beyond the interconnections: Split manufacturing in rf designs," *Electronics*, vol. 4, no. 3, p. 541, 2015.

[105] J. Yuan, Y. Xu, S. Yen, Y. Bi, and G. Hwang, "Hot carrier injection stress effect on a 65 nm lna at 70 ghz." *IEEE Transactions on Device and Materials Reliability*, vol. 14, pp. 931–934, 2014.

[106] J. Yuan and Y. Bi, "Process and temperature robust voltage multiplier design for rf energy harvesting." *Microelectronics Reliability*, vol. 55, pp. 107–113, 2015.

[107] J. Carls, R. Eickhoff, P. Sakalas, S. von der Mark, and S. Wehrli, "Design of a c-band cmos class ab power amplifier for an ultra low supply voltage of 1.9 v," in *Microwave and Optoelectronics Conference, 2007. IMOC 2007. SBMO/IEEE MTT-S International*, 2007, pp. 786–789.

[108] J.-S. Yuan, H.-D. Yen, S. Chen, R.-L. Wang, G.-W. Huang, Y. Z. Juang, C.-H. Tu, W.-K. Yeh, and J. Ma, "Experimental verification of rf stress effect on cascode class-e pa performance and reliability," *Device and Materials Reliability, IEEE Transactions on*, vol. 12, no. 2, pp. 369–375, 2012.

[109] "International technology roadmap for semiconductors," 2013, 2013 EDITION. EMERGING RESEARCH DEVICES.