2012

Secure and Energy Efficient Physical Unclonable Functions

Sudheendra Srivathsa
University of Massachusetts Amherst

SECURE AND ENERGY EFFICIENT PHYSICAL UNCLONABLE FUNCTIONS

A Thesis Presented

by

SUDHEENDRA K SRIVATHSA

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL AND COMPUTER ENGINEERING

February 2012

Department of Electrical and Computer Engineering

SECURE AND ENERGY EFFICIENT
PHYSICAL UNCLONABLE FUNCTIONS

A Thesis Presented

by

SUDHEENDRA K SRIVATHSA

Approved as to style and content by:

_____
Wayne P. Burleson, Chair

_____
Sandip Kundu, Member

_____ _____
Russell Tessier, Member

_____
C.V. Hollot, Department Head
Department of Electrical and Computer Engineering

ABSTRACT

**SECURE AND ENERGY EFFICIENT
PHYSICAL UNCLONABLE FUNCTIONS**

FEBRUARY 2012

SUDHEENDRA K SRIVATHSA

B.E, VISHVESHWARIAH TECHNOLOGICAL UNIVERSITY

M.S.E.C.E., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Wayne Burleson

Authentication of integrated circuits and hardware based secure cryptographic protocols play an important role in the field of hardware security. Smartcard applications, RFID tags and wireless sensor nodes are becoming widespread and secure communication among these devices is of paramount importance. Further, resource constrained applications impose tight constraints on the power consumption and area of the integrated circuit motivating the need for lightweight cryptographic protocols. An integral part of hardware cryptographic primitives are secret keys and unique IDs. Conventional methods rely on digital storage of secret keys in non volatile memory which is vulnerable to reverse engineering and side channel attacks.

Physical Unclonable Functions are a unique class of circuits that leverage the inherent variations in manufacturing process to create unique, unclonable IDs and secret keys. The distinguishing feature of PUFs is that even an untrusted foundry cannot create a copy of the circuit as it is impossible to control the manufacturing process variations. PUFs can operate reliably in presence of voltage and temperature variations. In this thesis, we explore the security offered by PUFs and tradeoffs between different metrics such as uniqueness, reliability and

energy consumption. Benefits of sub-threshold PUF operation and the use of delay based Arbiter PUFs and ring oscillator PUFs in low power applications is evaluated.

As we scale into lower technology nodes, there exists sufficient inter chip variation that enables each IC to be identified securely. The impact of scaling on the identification capabilities of a PUF and its reliability has been demonstrated in this work by analyzing the behavior of an Arbiter PUF in 45nm, 32nm and 22nm technology nodes. Further, the Arbiter PUF design has been implemented on a test-chip and fabricated using 45nm industry models and results from post silicon validation are presented.

Finally, we investigate a new class of PUF circuits in this work, that provide better security against machine learning based software modeling attacks. The strong identification capabilities and sufficiently high reliability offered by these PUF circuits make them promising candidates for future applications requiring secure hardware cryptographic primitives.

TABLE OF CONTENTS

ABSTRACT iv
LIST OF TABLES ix
LIST OF FIGURES ix
CHAPTER
1. INTRODUCTION 1
1.1 Challenges in Hardware Security 1
1.2 Physical Unclonable Functions 2
1.3 Applications of PUFs 4
1.3.1 Low Cost Authentication 4
1.3.2 Secret Key and Random Number Generation using PUFs 5
1.3.3 Controlled PUFs 6
1.4 Thesis outline 6
2. PHYSICAL UNCLONABLE FUNCTIONS 8
2.1 Silicon Physical Random Functions 8
2.2 Classification of PUFs 9
2.2.1 Strong PUFs 9
2.2.2 Weak PUFs 9
2.3 PUF Metrics 10
2.3.1 Uniqueness 10
2.3.2 Reliability 10
2.3.3 Security 10
2.4 PUF Circuits 11
2.4.1 Arbiter PUF 11
2.4.2 Feed Forward Arbiter PUFs and XOR Arbiter PUFs 12
2.4.3 Lightweight Secure PUFs 13
2.4.4 Ring Oscillator PUFs 14
2.4.5 SRAM PUFs 15
2.4.6 PUF based on passive device variations 16

3. ENERGY EFFICIENT DESIGN OF PUFS 17
3.1 Arbiter based PUF 17
3.2 Ring Oscillator PUF 19
3.3 Delay Line PUF 20
3.4 Experimental Setup 20
3.5 Uniqueness 21
3.6 Reliability 23
3.7 Discussion 25
4. TECHNOLOGY TRENDS IN UNIQUENESS AND RELIABILITY 27
4.1 Impact of scaling on PUF metrics 27
4.2 Arbiter-based PUF Circuit Design 27
4.3 Experimental Methodology 29
4.4 Uniqueness Analysis 29
4.4.1 Uniqueness Analysis with delay bias 32
4.5 Reliability Analysis 34
5. SILICON VALIDATION OF PUF TESTCHIP IN 45nm TECHNOLOGY 37
5.1 Circuit Schematic design 37
5.2 Functional and Timing Simulations 39
5.3 Layout Design 39
5.4 Physical Verification 41
5.5 Post silicon validation measurement setup 41
5.6 Measurement methodology 42
5.6 Uniqueness and reliability results 43
5.6.1 Uniqueness 43
5.6.2 Reliability 44
5.7 Discussion 44
6. SECURE PHYSICAL UNCLONABLE FUNCTIONS 46
6.1 Modeling attacks using Support Vector Machine classifiers 46
6.2 Logistic Regression Based Modeling Attacks 48
6.3 Secure PUF constructions 52
6.3.1 Secure PUF 1 53

6.3.2 Secure PUF with XORs 54
6.3.3 Secure PUF with LFSR 55
6.4 Uniqueness and reliability analysis 56
6.4.1 Uniqueness 56
6.4.2 Reliability 57
6.5 Other Approaches towards secure PUF implementation 59
6.5.1 Non-linearity 59
6.5.2 Controlled PUFs 59
6.5.3 Time bounded authentication 59
6.5.4 Multi bit response generation 60
6.6 Discussion 60
7. CONCLUSIONS 61
7.1 Scope for future work 62
APPENDIX: PUF SIMULATION METHODOLOGY 63
BIBLIOGRAPHY 67

LIST OF TABLES

Table Page

1. Uniqueness and Reliability 23

2. Power and energy consumption 25

3. Uniqueness in lower technology nodes..... 32

4. PUF Uniqueness with delay bias 33

5. ML attack on arbiter PUF [17] 49

6. ML attack on XOR Arbiter PUF [17]..... 50

7. ML attack on lightweight secure PUF [17] 50

8. ML attack on feed forward arbiter PUF [17] 51

9. Uniqueness..... 56

LIST OF FIGURES

Figure Page

1. Chip identification leveraging inter-die variations 3

2. Chip authentication scenario 4

3. Arbiter-based PUF circuit 11

4. Single delay stage 12

5. Feed-forward arbiter PUF 12

6. Lightweight secure PUF 13

7. Ring oscillator PUF 14

8. SRAM cell 15

9. Butterfly PUF cell 16

10. Arbiter PUF circuit 18

11. Delay stage in Arbiter PUF 18

12. Ring oscillator PUF 19

13. Delay line PUF 20

14. Arbiter PUF Uniqueness and Energy per CRP 22

15. RO PUF Uniqueness and Energy per CRP 22

16. Arbiter and RO PUF Reliability 24

17. Circuit diagram of arbiter-based PUF 28

18. Symmetric circuit design for a single PUF stage. 28

19. HD distribution of super threshold and sub threshold PUF in 45nm 30

20. HD distribution of super threshold and sub threshold PUF in 32nm 31

21. HD distribution of super threshold and sub threshold PUF in 22nm 31

22. Uniqueness improvement with technology scaling 33

23. PUF reliability with respect to supply voltage bias 35

24. PUF reliability with respect to temperature bias..... 35

25. PUF Circuit Schematic 38

26. PUF Design methodology..... 38

27. Arbiter PUF Layout with signal IOs..... 40

28. Snapshot of two PUF stages and arbiter 40

29. Post silicon validation lab setup..... 41

30. Super threshold and sub threshold response waveforms 42

31. Super threshold hamming distance distribution..... 43

32. Subthreshold hamming distance distribution..... 43

33. Single delay stage 46

34. SVM Attack on Arbiter PUF 47

35. Lightweight Secure PUF 50

36. Feed-forward arbiter PUF 51

37. Secure PUF 1 Schematic..... 53

38. Secure PUF 2 Schematic..... 54

39. Secure PUF with LFSR Schematic..... 55

40. Reliability under supply voltage bias..... 57

41. Reliability under temperature bias..... 58

42. HSPICE netlist creation flow..... 65

CHAPTER 1

INTRODUCTION

1.1 Challenges in Hardware Security

Integrated circuits have become an integral part of the world we live in. The era of ubiquitous computing is upon on us as we are surrounded by a host of electronic devices that facilitate different sectors such as banking, healthcare, supply chain and transportation. Smart card applications such as credit cards, transportation payment systems, RFID tags and wireless sensor networks are becoming increasingly widespread. The field of hardware security assumes greater significance in the context of these applications. Smart cards should be capable of performing reliable authentication, store sensitive data such as ATM passwords and perform secure communication between devices. These requirements motivate the need to have secure cryptographic primitives in hardware.

"Security engineers face the seemingly contradictory challenge of providing lightweight cryptographic algorithms for strong authentication, encryption and other cryptographic services that can perform on a speck of dust." [1].

The integrity of authentication schemes and encryption algorithms lies in a unique ID or a secret key. Hence it is imperative that these secret keys are generated and stored in a secure manner, protecting them from malicious attackers. Conventional approaches rely on storing the secret key in non volatile storage on chip, either in fuses or EEPROMs. However, these are susceptible to invasive attacks as the secret is stored permanently in digital form. Reverse engineering attacks using a combination of chemical and optical methods allow an attacker to

read out the entire digital content stored in memory. Preventing invasive attacks becomes an expensive proposition as it involves providing tamper resistant hardware [10].

Non invasive attacks such as side channel attacks pose a new threat to achieving secure hardware protocols. Side channel attacks prove to be very powerful as they bypass the theoretic and mathematical security of the cryptographic algorithms and extract the information presented due to implementation weaknesses. Side channel attacks leverage the fact that the electrical characteristics of a chip such as power and timing are data dependent. Successful attacks using differential power analysis and EM analysis has been carried out to leak the secret key used during encryption. Hence, any hardware mechanism aiming to be robust should be resistant to invasive and non invasive attacks.

In addition to these concerns, ultra low power applications such as wireless sensor networks and RFID tags impose additional constraints. Passive RFID tags are powered by RFID readers through inductive coupling, limiting the power that can be consumed by digital circuitry. The energy per operation becomes a concern in battery powered devices such as Active RFID tags. In the near future, wireless sensor nodes may depend on energy harvesting from ambient energy sources such as solar energy for their power requirements. This would impose tighter constraints on the power consumption of an integrated circuit. Further, smartcards are implemented with small form factors aimed at reducing the cost of each device. RFID tags limit the number of gates to be used by security primitives to 2000 [6]. Hence, a good cryptographic primitive should be lightweight, occupy little area on silicon and should have very low power consumption.

1.2 Physical Unclonable Functions

Physical Unclonable Functions prove to be an elegant solution as a lightweight cryptographic primitive. PUF circuits enable low cost authentication by supporting a challenge response protocol. In addition to authentication, PUFs can also act as a source of secret keys on chip, eliminating the need to store secret keys permanently in digital form in non volatile

memories. PUFs possess certain important properties which enable their use in security applications.

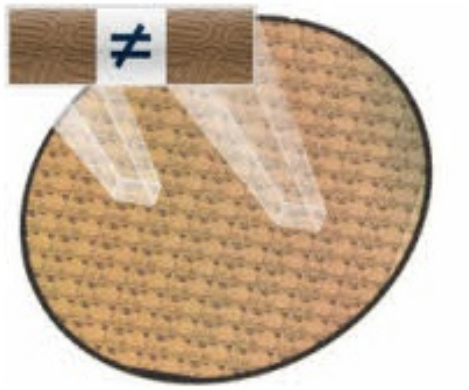

Figure 1. Chip identification leveraging inter-die variations [26]

The key notion in PUFs is that it is impossible to construct an exact replica of a PUF instance even with complete knowledge of the design. These circuits leverage the fact that there is enough inter chip variation to uniquely characterize each die.

The concept of a Physical Unclonable Function was originally proposed based on the variations in speckle patterns of optical materials [7]. The introduction of Silicon PUFs based on process variations led to several circuit implementations [8]. Arbiter based PUFs are implemented using long delay stages and an arbiter to classify the responses into 1s and 0s [9]. Ring oscillator based PUFs generate responses by comparing frequencies between multiple ring oscillators [10]. The initial state of an SRAM during bring up is random and these variations have been utilized to create unique chip IDs [11]. PUFs can also be constructed using variations in passive devices as demonstrated by the power distribution based PUF [12]. These PUF circuits enable a wide range of security applications that are discussed below.

1.3 Applications of PUFs

1.3.1 Low Cost Authentication

PUFs can be used to authenticate ICs with minimal hardware cost using a Challenge Response protocol.

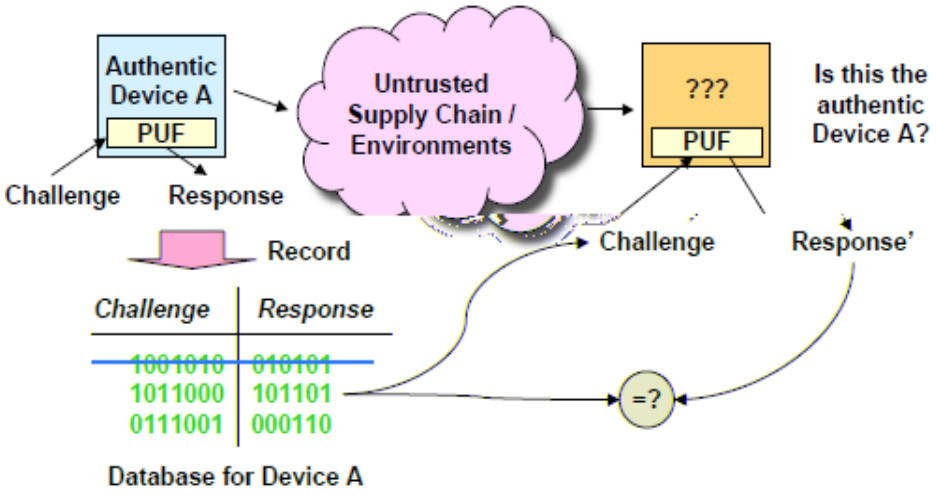

Figure 2. Chip authentication scenario [10]

In this process, a secure database stores a set of Challenge Response pairs from each PUF instance prior to the use of the IC. When the authenticity of the IC has to be queried, a set of CRPs are chosen randomly from this database and applied to the PUF circuit. The obtained response is compared with the responses stored in the database to authenticate the IC. It is important that challenges are never reused to prevent man-in-the-middle attacks [10]. Hence it is extremely useful to have a PUF that can support large number of CRPs. This feature has been demonstrated by implementing PUF based RFID tags in 0.18um technology [18]. Results have shown that with a 128bit response, the false positive and negative rates can be reduced to a few parts per billion. This can be improved further by using wider set of response bits. Hence PUFs are naturally suited for authentication and this been explored in several lightweight protocols [23][20]. Mutual authentication and ownership transfer protocols to identify both RFID readers

and tags by utilizing PUFs and LFSRs has also been proposed [21]. Existing hash functions require 8000 to 10,000 gates as compared to 784 gates used in this approach. It is also mentioned that an RFID tag can afford a maximum of 2000 gates for security features.

The use of PUFs has also been proposed for IC activation and prevention of piracy in integrated circuits [20]. Roy et al. have proposed the concept of Ending Piracy in Integrated Circuits (EPIC) which involves embedding a combinational locking mechanism on the IC [25]. A random IC key pair is generated during initial power-up and this is utilized to create a common key between the user and the IP provider. The IP provider transmits this common key to the user to unlock the IC. In resource constrained platforms, the use of PUFs has been proposed to generate the unique signature necessary for this application.

Bolotnyy et al. [22] have proposed the use of PUFs to implement privacy preserving tag identification and secure message authentication code. When a reader interrogates a tag, tag responds with its ID and updated its identifier to p(ID) (p(ID) - PUFs response to challenge, ID). The backend database will need to store p(ID), p^2(ID)… p^k(ID).A PUF based MAC protocol can use PUFs response to sign a message.

1.3.2 Secret Key and Random Number Generation using PUFs

Cryptographic primitives such as encryption and message authentication need the presence of a secret key. The use of PUFs for secret key generation was first proposed in [10]. In order to use PUF responses as a secret key, it has to be ensured that each bit of the response is a constant. However, PUFs cannot guarantee 100% reproducibility of responses under noise and environmental variations. This limitation can be overcome by adopting error correction. The error correction process involves two steps namely initialization and re-generation. During an initialization, an error syndrome is computed when the challenge is applied. This syndrome is used later during re-generation to correct any bit errors that might have occurred in the PUF response. The corrected PUF response is taken through a hash to generate the secret key. The use of PUF as a hardware random number generator has been explored by O'Donnell et al. [24].

The PUF output responses are taken through Von Neumann correction in which pairs of bits are XORed to increase the entropy. The NIST test results carried out indicate that a PUF can be used as a reasonably good hardware random number generator with low area overhead.

1.3.3 Controlled PUFs

The notion of controlled PUFs (CPUFs) was introduced by Gassend et al. [19]. Controlled PUFs are entities in which the PUF can be accessed only by an algorithm tied to the physical device. The use of CPUFs to generate a secret to be shared between a remote user and a physical device is mentioned in this work. In addition, introduction of a user, renewal of CRPs, and anonymity preserving protocols have been discussed. Applications such as certified execution and software licensing using CPUFs have been discussed. Certified execution involves producing a certificate verifying the authenticity of the IC. In distributed computing scenarios, this allows a remote user to know that his program ran on a certified chip without being tampered. Similarly, use of PUFs for software licensing will allow only authentic software to be run on a processor.

PUF circuits are an ideal choice for security applications and they form a part of the security solutions offered in industry by Verayo and Intrinsic ID [26][27]. Verayo offers the PUF as an IP to be licensed for RFID, ASIC and FPGA applications. Intrinsic ID provides secure key storage to protect semiconductor products from cloning and reverse engineering.

1.4 Thesis outline

In this thesis, we begin with the advent of silicon physical unclonable functions, followed by classification of existing PUF circuits and their key properties. Chapter 3 explores the tradeoffs involved between security and energy consumption of an arbiter based PUF and ring oscillator PUF and presents a new energy efficient alternative. Chapter 4 presents the impact of technology scaling on PUF behavior. Design and implementation of the Arbiter PUF in a 45nm test-chip and post silicon validation results are presented in Chapter 5. Chapter 6 introduces a

new class of PUF circuits secure against modeling attacks, followed by conclusion and scope for future work in Chapter 7.

CHAPTER 2

PHYSICAL UNCLONABLE FUNCTIONS

2.1 Silicon Physical Random Functions

Silicon Physical Unclonable Functions came into being with the introduction of the notion of Physical Random Functions (PRFs) [8]. A Physical Random Function is defined to have the following properties

1) A physical random function is a function that maps challenges to responses, the challenge response pairs being characteristic of the physical device.

2) The challenge response pairs can be easily evaluated in a short amount of time.

3) The PRF is hard to characterize with the knowledge of a set of challenge response pairs. An attacker with a polynomial amount of resources should not be able to model the challenge response behavior of the PRF.

4) The PRF is manufacturer resistant or "physically unclonable" as it is impossible to produce 2 identical devices with the same physical properties

The above properties guide the design of Silicon PUF circuits. Physical Unclonability is a result of the inherent process variations in the CMOS manufacturing process, making it impossible to fabricate two ICs with the exact same physical properties. Process variations lead to differences in the electrical characteristics such as delay and power of ICs. These variations are undesirable during the design of high performance designs. However they form the foundation of Physical Unclonable Functions. Silicon PUF circuits leverage process variations to generate challenge response pairs enabling identification of each IC. Different mechanisms to generate challenge response pairs result in different PUF circuits that are discussed below.

2.2 Classification of PUFs

PUFs can be classified into Strong and Weak PUFs based on the number of challenge response pairs supported which subsequently determines the applications in which they are used [35]. The features of these two PUF categories are discussed below

2.2.1 Strong PUFs

Strong PUFs support a large number of CRPs and a complete measurement of all CRPs within a feasible time frame is impossible. Further, it should be difficult for an attacker to predict the response of the PUF for a random selected challenge, even with the prior knowledge of a limited number of CRPs. This implies that the PUF should not be susceptible to modeling attacks. Hence it is tough to mimic the behavior of a strong PUF and this class of PUFs is ideally suited for IC identification and secret key generation. Examples of strong silicon PUF constructions include Arbiter PUFs, feed forward arbiter PUFs, XOR arbiter PUFs and lightweight secure PUFs.

2.2.2 Weak PUFs

Weak PUFs support a limited number of CRPs, sometimes just a single challenge. This prevents their use in IC authentication applications as they will be susceptible to replay attacks. Responses derived from weak PUFs are used to generate a secret key necessary for embedded cryptosystems. Weak PUFs offer a better mechanism to generate secret keys as opposed to storing them in non volatile memory. The characteristics of a weak PUF will be harder to read out using invasive techniques compared to digital storage in memory. However the secret keys are still susceptible to side channel attacks just as in any physical cryptosystem. Typical examples of weak PUFs are SRAM PUFs and butterfly PUFs. The concept of a Physically Obfuscated Key (POK) is similar to the idea of a weak PUF where the responses are not given out and are used to generate a secret key internally.

2.3 PUF Metrics

The quality of a PUF is determined by three important metrics namely uniqueness, reliability and security. In addition to these metrics, the design cost of the PUF in terms of area and power consumption also plays a key role in choosing the PUF for different applications. The three main metrics of a PUF circuit are discussed below.

2.3.1 Uniqueness

Uniqueness is the most important property of a PUF as it indicates the ability to distinguish between different ICs. Uniqueness is measured by determining hamming distance between the responses obtained from different PUF instances. An ideal PUF circuit would achieve a relative hamming distance of 0.5. The identification capability of a PUF is directly related to the amount of process variation, specifically inter-chip variation present. Large process variation results in a larger value of uniqueness.

2.3.2 Reliability

A robust PUF circuit should be capable of reproducing CRPs in presence of noise and environmental variations. Supply voltage variations and temperature variations impact the delay and power consumption of a circuit and it may affect different parts of the circuit differently. This can result in different responses for the same challenge from a given PUF instance. Most PUF circuits use relative comparison to generate CRPs achieving a high degree of reliability. In spite of relative comparisons, some erroneous responses can occur. This is measured by looking at the total number of bit errors in responses obtained by subjecting the PUF to different voltage and temperature conditions

2.3.3 Security

The security metric in PUFs indicates a PUF's susceptibility to different types of modeling attacks. The key notion in PUFs is that it is impossible to construct an exact replica of a PUF instance even with complete knowledge of the design. This is an extremely useful property as it prevents untrusted foundries from producing counterfeit chips. However it is possible to mimic the challenge response behavior of a PUF through software modeling

techniques. In Linear PUFs, stages delays are additive in nature and this gives rise to modeling attacks through Support Vector Machines (SVM). High prediction accuracies greater than 90% can be achieved through SVM attacks on linear PUFs such as Arbiter PUFs. To counter these attacks, non linearities have been introduced to create feed forward and arbiter PUFs. However a recently proposed machine learning method is capable of breaking all current PUF constructions.

2.4 PUF Circuits

2.4.1 Arbiter PUF

Arbiter PUF was among the first set of Silicon PUF circuits to be proposed [9]. This PUF circuit leverages the delay variations across chips to generate unique challenge response pairs. The Arbiter PUF circuit consists of a set of delay stages followed by an Arbiter circuit as shown in Figure 3. Each delay stage consists of two multiplexers with the inputs connected as shown below in Figure 4. The challenge bits form the select inputs to the multiplexers that decide the path taken by the top and bottom signals. To evaluate the response bit for a particular challenge, an input rising edge is propagated through the delay stages. The response bit is determined to be a 1 or 0 based on the top and bottom signal arrival times. In this PUF circuit, a D latch is used as the arbiter to determine which signal arrived first.

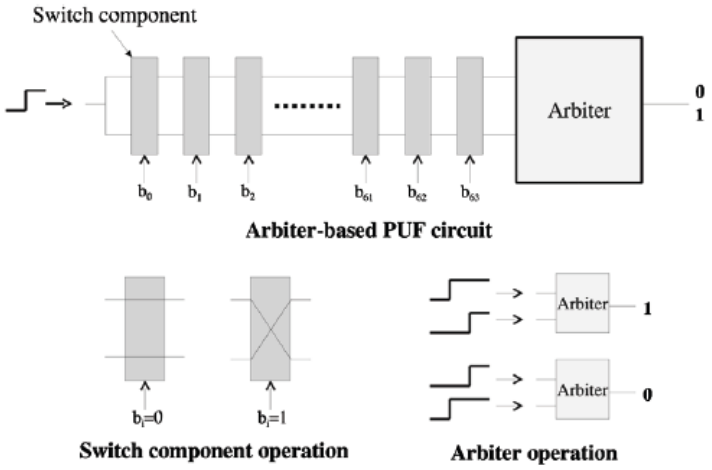

Figure 3. Arbiter-based PUF circuit [9]

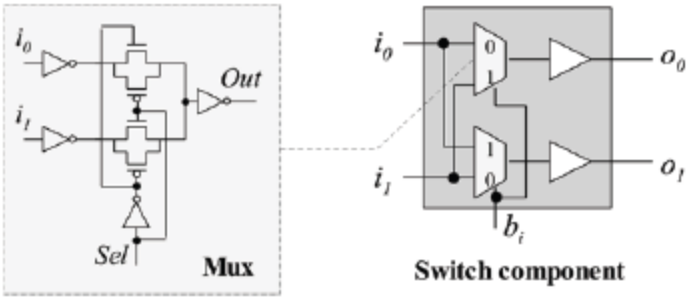

Figure 4. Single delay stage [9]

The arbiter PUF circuit implementation is a robust construction which supports exponential number of challenge response pairs. For instance, a 64 bit Arbiter PUF can support 2^64 CRPs. Another key property of this PUF circuit is that it relies on relative comparison to generate CRPs. This improves the reliability of the PUF circuit in presence of environmental variations significantly. The exponential number of delay paths available makes this circuit hard to model. However, the Arbiter PUF is a linear structure in which the cumulative path delay can be assumed to be a sum of the individual stage delays. By assuming an additive delay model, a software model can be created through Support Vector Machines (SVM). SVM uses a set of challenge response pairs as training samples to construct the model. This model can be used to predict other challenge response pairs with a high degree of accuracy. Prediction rates greater than 90% can be achieved through SVM attacks.

2.4.2 Feed Forward Arbiter PUFs and XOR Arbiter PUFs

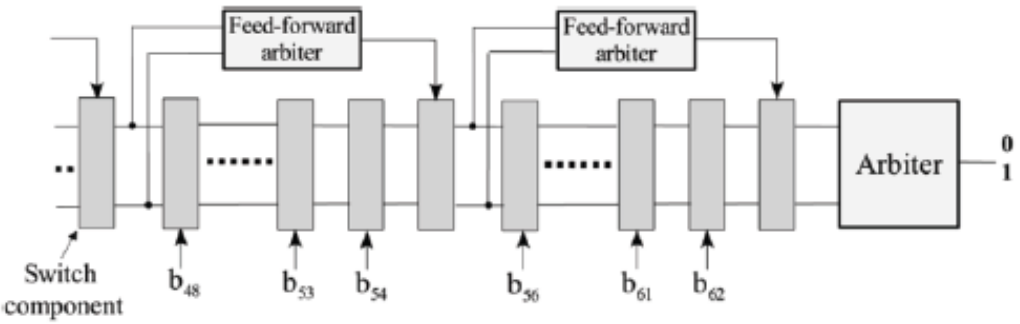

Figure 5. Feed-forward arbiter PUF [9]

The Arbiter PUF offers a strong PUF construction achieving high degree of uniqueness and reliability. However it is susceptible to software modeling attacks. In order to overcome this limitation, feed forward Arbiter PUFs were proposed [9]. In this PUF construction, some of the challenge bits are generated by intermediate signals along the PUF structure as shown above in Figure 5. This introduces non linearity in the design making it infeasible to build a software model based on linear additive delay assumptions.

Another approach to overcome software modeling attacks is to obfuscate the output response bits of the PUF. XOR Arbiter PUFs achieve this by XORing the output response bits of multiple PUFs [10]. An alternative approach would be to use the PUF response bits as challenge bits to a second PUF

2.4.3 Lightweight Secure PUFs

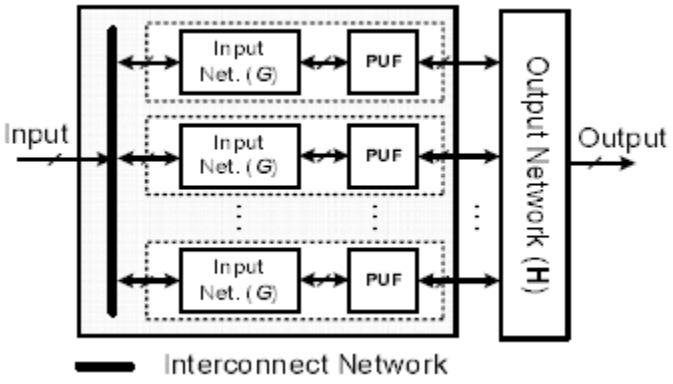

Figure 6. Lightweight secure PUF [33]

Lightweight Secure PUFs, shown in Figure 6 incorporate four building blocks namely an input logic network, output logic network, an interconnect network and parallel Arbiter PUFs to come up with a robust PUF circuit [33]. The three main features of this PUF are

1) Inclusion of multiple delay lines to generate response bits
2) Combination of input challenge bits using the input logic network
3) Combination of PUF outputs through output logic network.

The input network is constructed through XOR gates to create different combinations of challenge bits to each of the PUFs. The output logic network also consists of XORs to combine responses from different PUFs. The lightweight secure PUF circuit is resistant to reverse engineering and emulation attacks.

2.4.4 Ring Oscillator PUFs

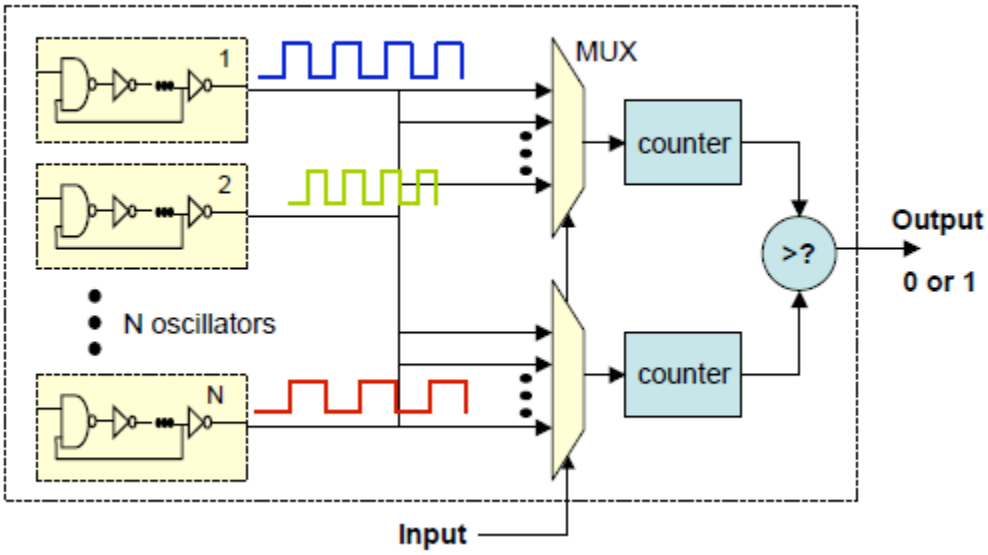

Figure 7. Ring oscillator PUF [10]

Ring oscillator PUFs generate challenge response pairs by comparing frequencies of different on chip ring oscillators [10]. Figure 7 shows a typical ring oscillator PUF consisting of two multiplexers to select ring oscillators for pairwise comparisons. The multiplexer outputs provide the clocks to the two counters. Comparison of the two counter values after a specific period of time yields the response bit. The response bit is determined to be a 1 if frequency of ring oscillator 1 is greater than that of ring oscillator 2. Ring oscillator PUFs offer a limited number of CRPs and hence their application is mainly restricted to secret key generation for ICs where the response bits are used internally. A RO PUF with N oscillators gives rise to ${}^{N}C_{2}$ challenge response pairs. However many of these pair wise comparisons are redundant and the

actual maximum entropy bearing challenges are equal to $\log_2 N$. RO PUFs can be expensive in terms of area and power.

2.4.5 SRAM PUFs

SRAM PUFs leverage the fact that the initial state of an SRAM after power-up is random to generate unique IDs for each IC [11]. SRAM cells are constructed with cross coupled inverters as shown in Figure 8 and the physical mismatch is kept as minimum as possible during design. However, manufacturing variations cause a random mismatch in each cell and the initial state of the SRAM cell might be biased towards a 0 or 1. This random mismatch varies across chips and the initial state of the SRAM can be treated as a fingerprint, unique to each IC.

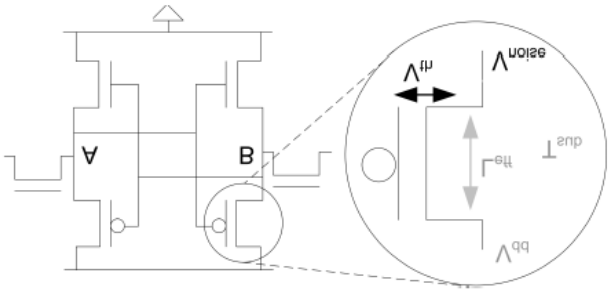

Figure 8. SRAM cell [11]

In most FPGAs, the initial state of the SRAM is hard reset to 0 and hence it is not possible to extract a unique ID during power-up. To counter this, Butterfly PUFs have been proposed that use two cross coupled transparent data latches to mimic an SRAM cell, shown in Figure 9. The latches are provided with preset and clear functionality which is used to introduce an unstable state. The butterfly PUF cell reaches a stable state based on the physical mismatch present similar to an SRAM cell [34]. Latch PUFs and flip flop PUFs work on the same principle.

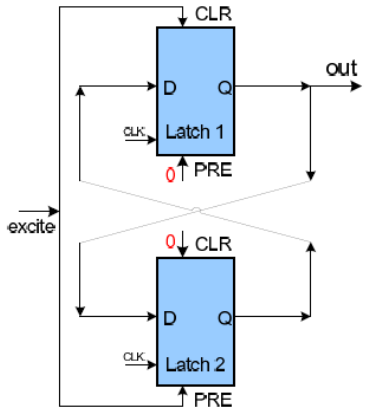

Figure 9. Butterfly PUF cell [34]

2.4.6 PUF based on passive device variations

Most of the PUF circuits proposed rely on the Vt variation of active devices as their primary source of randomness. A power distribution based PUF relies on resistance variations in the power grid [12]. In this circuit, the PUF signatures are generated by measuring the voltage drops or equivalent resistances at different locations in the power distribution network of an integrated circuit.

CHAPTER 3

ENERGY EFFICIENT DESIGN OF PUFS

Uniqueness and energy consumption are key metrics in the design of PUF circuits. These metrics indicate the efficiency of a PUF circuit in extracting entropy from random process variations on chip to create unique IDs. The minimum energy required to create a unique and reliable ID for each IC is an important lower bound to explore for future ultra low power applications. Further, lower energy consumption will help reduce the power signature of PUF circuits. This will make it harder for side channel attacks to extract the unique ID or secret key.

The energy consumed by a hardware cryptographic primitive is an important design goal for ultra low power applications. In this work, we look at the key metrics of uniqueness and reliability of different PUF circuits along with their energy consumption [30]. We choose the arbiter based PUF circuit which is representative of delay based PUFs such as feed-forward arbiter based PUFs and XOR arbiter PUFs. We also look at the RO PUF which provides easier implementation at the cost of increased area and energy. A delay line based PUF similar in structure to the RO PUF can achieve significant reduction in energy consumption by performing delay comparisons as opposed to frequency comparisons. The design of these PUF circuits is discussed below.

3.1 Arbiter based PUF

The arbiter based PUF is constructed from 64 delay stages and an SR Latch as an arbiter as shown in Figure 10. Each delay stage comprises of two multiplexers which the inputs connected as shown in Figure 11. SR Latch serves as a better arbiter as compared to an edge triggered D Flip Flop, due to a smaller bias [13]. The challenge bit selects the path through which the top and bottom signals are passed and the response bit is decided by the arbiter based

on the delay difference between the top and bottom signal arrival times at the final stage. The response bit is set to a 1 if the top signal arrives early and vice versa. The delay difference at the final stage is a function of the path chosen through the 64 stages determined by the challenge bits. A 64 bit Arbiter PUF offers 2^64 challenge response pairs making it a robust PUF circuit capable of preventing replay attacks that can occur due to limited number of CRPs

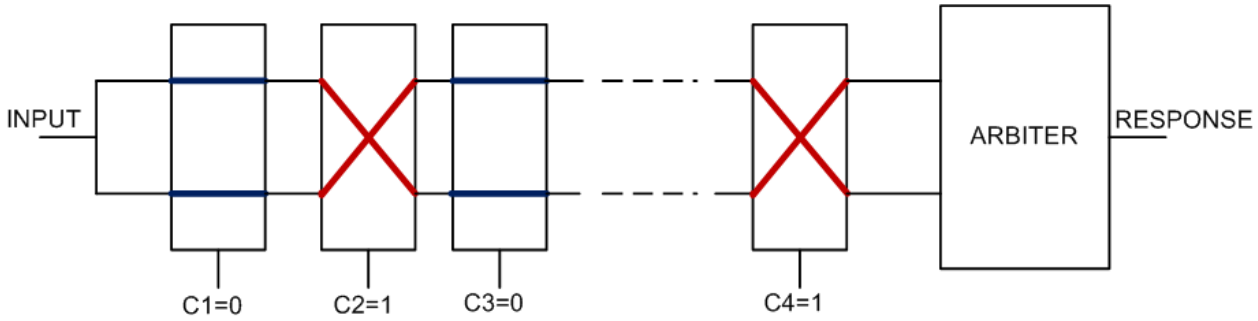

Figure 10. Arbiter PUF circuit

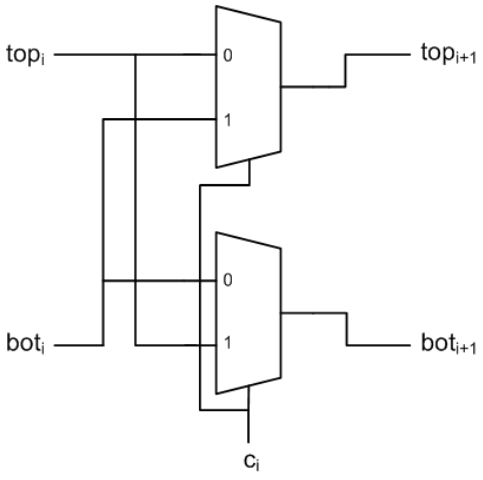

Figure 11. Delay stage in Arbiter PUF

3.2 Ring Oscillator PUF

The ring oscillator PUF comprises of 32 ring oscillators each ring oscillator having 41 stages, shown in Figure 12. Ring oscillators constructed with inverters results in lower power consumption as compared to a ring oscillator constructed with NAND gates with one of the inputs tied high. A NAND gate construction results in additional static power consumption due

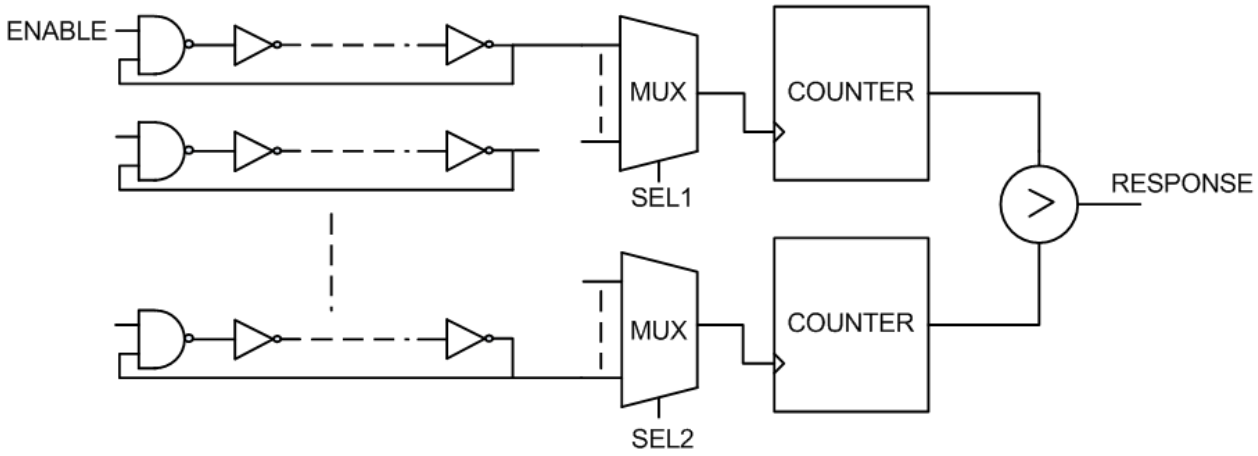

Figure 12. Ring oscillator PUF

to one of the inputs held high constantly. It can also be noted that the power consumed by a Ring oscillator is independent of the number of stages involved. In this PUF construction, a response bit is generated by comparing the frequencies of two ring oscillators. The multiplexer selects one of 32 ring oscillators which drive an 11 bit counter, the minimum counter width necessary to differentiate two RO frequencies. The two counter outputs are compared after a specific period of time and the response bit is set to a 1 if the frequency of RO 1 is greater than RO 2. The RO PUF offers a limited number of CRPs and for an N bit RO PUF, the total number of challenges supported is given N*(N-1)/2. Many of these pair-wise comparisons are redundant and the maximum entropy is given by $\log_2 N$ [10]. In case of a 32 bit RO PUF, the total number of CRPs is 496 with actual entropy bearing challenges being 117.

3.3 Delay Line PUF

The RO PUF generates response bits by comparing different RO frequencies. This can be expensive in terms of energy consumption due to the counting over thousands of cycles. Comparison of delays is much more efficient than frequency comparisons. In this work, we look at a new delay line based PUF structure similar to the RO PUF which offers a significant reduction in the energy consumed per CRP. The delay line PUF generates a response bit by comparing the delays of two lines. An input enable signal is propagated through the delay lines and fed to an SR Latch which acts as the Arbiter. The pair-wise selection of delay lines is controlled by the select lines to the multiplexer. The delay line PUF offers the same entropy as the RO PUF. This structure provides significant reduction in energy per CRP and achieves comparable uniqueness with no loss in reliability.

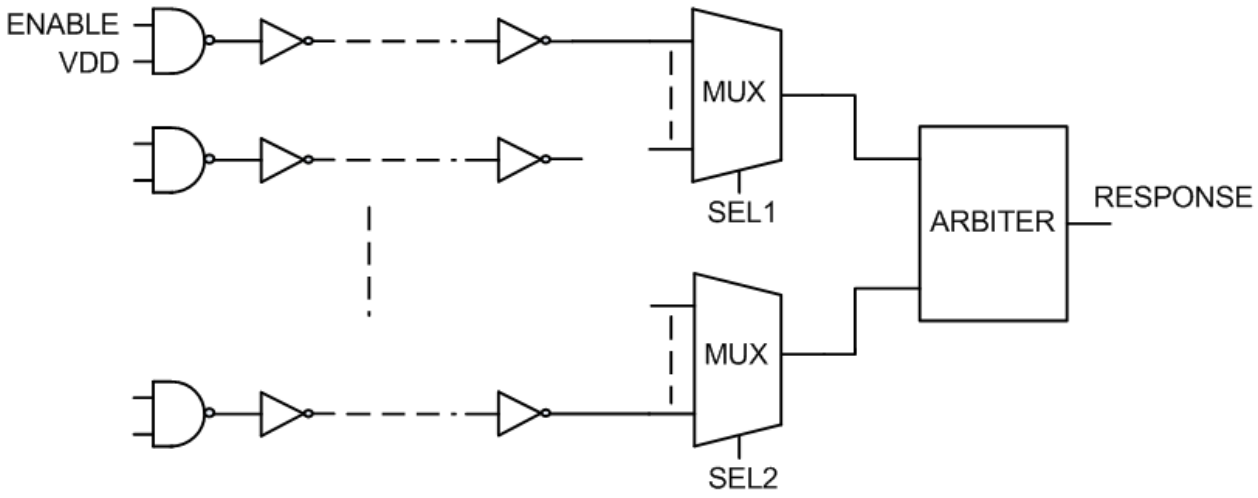

Figure 13. Delay line PUF

3.4 Experimental Setup

To determine the uniqueness and reliability metrics of the PUF circuits, we use 45nm Low power, High-K and strained Si PTM models [37]. The inter chip variation across different PUF instances is simulated by modeling threshold voltage variations through Monte Carlo simulations in Hspice. Vth variations impact circuit delays significantly as compared to variations in passive devices. Based on ITRS [15], a 3 sigma value of 0.16V and a Gaussian Vt

distribution is chosen for threshold voltage variation. The simulations are carried out for 40 different PUF instances to ensure high accuracy of Monte Carlo simulations. The impact of scaling supply voltage on uniqueness and reliability is observed by varying the supply voltage between 1.1V and 0.3V.

3.5 Uniqueness

The Uniqueness metric in PUF circuits indicate the identification capability achieved. For a set of challenges, we look at the hamming distance (HD) between the responses obtained from different PUF instances. An ideal PUF circuit would achieve a relative HD of 50%. In our work we look at 31 pair wise comparisons of the RO PUF and the delay line PUF to generate 31 response bits. Similarly we apply 31 challenges to the Arbiter PUF circuit. The relative HD is determined by calculating the mean HD across 40 PUF instances, which gives rise to ${}^{40}C_2$ comparisons. Further we determine the energy consumed by the PUF circuit to generate a single challenge response pair. Figs 14 and 15 show the uniqueness and energy per CRP for the Arbiter and RO PUF circuits at different supply voltages. Results clearly indicate that the Arbiter PUF offers better identification capability as compared to the RO PUF. Further, we see that operating the PUF at lower supply voltages results in an improvement in uniqueness. The optimal supply voltage for PUF operation is seen to be 0.4V. As we scale the supply voltage beyond 0.4V, the device delays increase significantly and the evaluation of each CRP is slower resulting in reduced energy efficiency.

The arbiter PUF achieves a relative HD of 49.5% at nominal voltage getting closer to the ideal value of 50% as we lower the supply voltage. The RO PUF gradually improves to 50% from 45% at the nominal voltage. This can be attributed to the fewer number of devices that are activated by a certain challenge in the RO PUF. Hence the number of devices contributing to variation is lesser and response bits are more likely to be same across different PUF instances. Further the energy per CRP consumed by an Arbiter PUF varies between 50–250 fJ. The RO PUF consumes 50–250 pJ which is 3 orders greater than that of the Arbiter PUF.

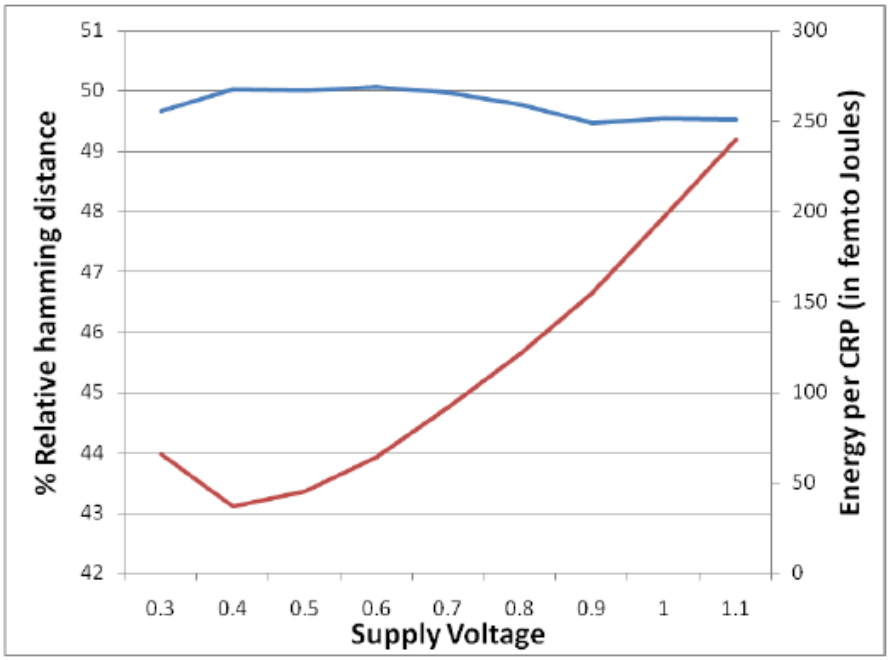

Figure 14. Arbiter PUF Uniqueness and Energy per CRP

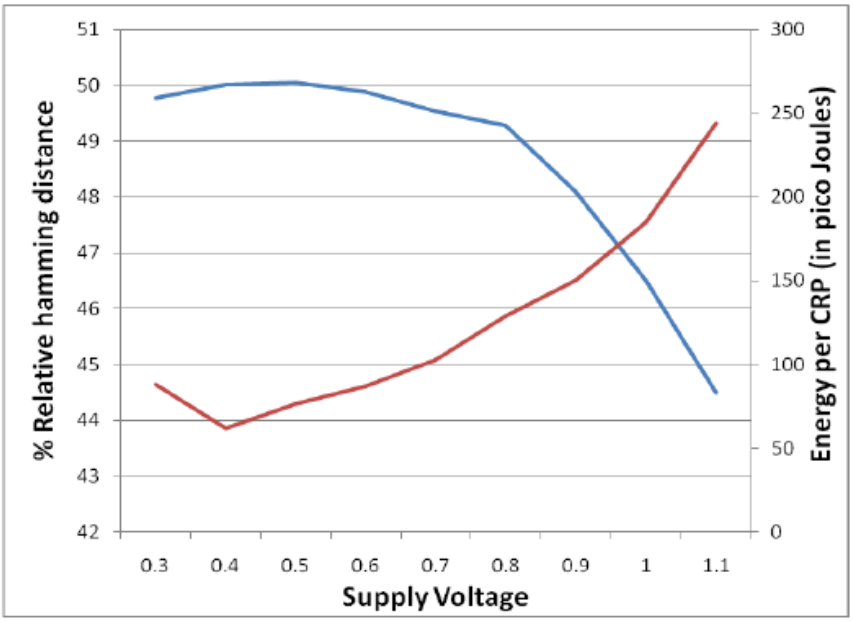

Figure 15. RO PUF Uniqueness and Energy per CRP

The delay line PUF structure can achieve comparable uniqueness at nominal voltage and a relative HD very close to 50% when operated in sub-threshold mode as shown in Table I. The

loss in uniqueness is due to the delay bias introduced by the multiplexers which is of the order of 20-40ps. This can be overcome through a careful symmetric design of the multiplexers. An increase in the number of CRPs can further improve the relative HD of these PUF circuits. However, it should be noted that a uniqueness of 40% and a reliability of 90% is still sufficient to authenticate a large number of chips with 31 CRPs [9].

Table 1. Uniqueness and Reliability

PUF Circuit	Uniqueness		Reliability	
	1.1V	0.4V	1.1V	0.4V
Arbiter PUF	49.51	50.02	95.56	95.76
RO PUF	44.5	50.01	97.17	98.18
Delay line PUF	40.1	50.34	96.57	92.54

3.6 Reliability

A robust PUF circuit should be able to perform authentication reliably in presence of noise and environmental variations. In applications where the PUF is used to generate a secret key, reliability has greater significance as each bit in the secret key needs to be constant under different conditions. The reliability of the PUF circuits is measured by obtaining the CRPs in presence of voltage and temperature variations and comparing it with the response obtained under nominal conditions. A change in the response obtained is treated as a bit error. We vary the supply voltage by +/- 10% and the temperature between -25^{o}C and 85^{o}C. Fig 16 shows the bit error rate percentage observed in Arbiter and RO PUF for different supply voltages. Table I shows a comparison of the reliability achieved by the 3 circuits at 1.1V and 0.4V. The results indicate that the reliability is not impacted significantly as we scale the supply voltage. Relative comparisons to generate the response bits results in high reliability in presence of temperature

and voltage variations. In RO and delay line PUFs, reliability errors are caused by changes in the path delays. Frequency comparisons performed through multiple cycles of counting does not provide any additional stability against path delay changes. However, the frequency comparison approach does protect output response bits from transient errors such as glitches. The reliability of the PUF circuits can be improved by eliminating some of the CRPs that are susceptible to environmental variation. In case of the RO and delay line PUFs, this process is relatively easier due to the limited number of CRPs.

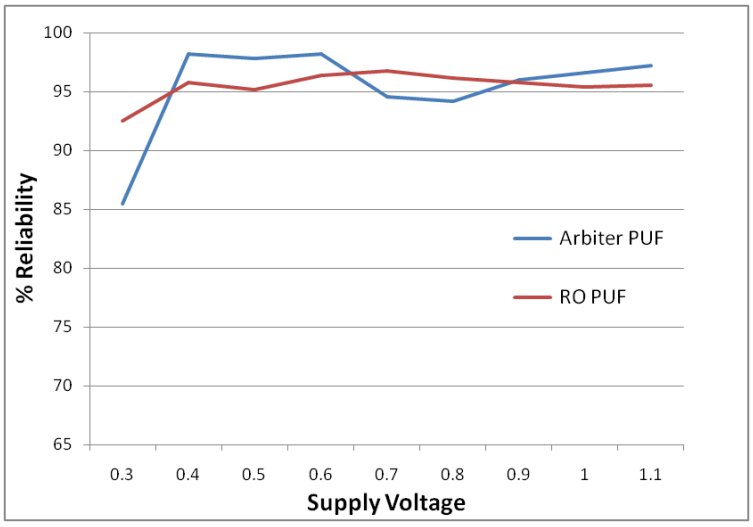

Figure 16. Arbiter and RO PUF Reliability

The gate count, power consumption, the time required and energy per CRP of the three PUF circuits is shown in Table II. The dynamic power consumed by RO PUF is 3-8 times that of the Arbiter and delay line PUF. However the significant difference in energy per CRP is due to the slow operation of the RO PUF, which requires 1000s of cycles to generate a response bit. It can be seen that the delay line PUF offers the lowest energy per CRP.

Table 2. Power and energy consumption

PUF Circuit	Gate count	Dynamic power (in uW)	Time per CRP (in ns)	Energy per CRP (in pJ)
Arbiter PUF	450	47.9	5	0.239
RO PUF	1159	148.0	1650	244.2
Delay line PUF	795	16.7	4	0.066

3.7 Discussion

The most important feature of a PUF circuit is its unclonable nature making it impossible even for the manufacturer to create a duplicate. Arbiter based PUFs support exponential number of CRPs and consists of numerous timing arcs making it harder to model. However it has been shown that by assuming an additive delay model, a software model can be created through SVM attacks [16]. RO PUFs and the delay line PUF support a limited number of CRPs, making them easier to model and hence it should be made sure that challenges and responses are obfuscated. Recently it has been shown that all current PUF constructions including Arbiter PUFs and RO PUFs are susceptible to modeling attacks [17]. The uniqueness and reliability results clearly indicate that the Arbiter PUF performs reliable authentication with low energy consumption. Hence Arbiter PUFs are ideal choices for ultra low power applications. The delay line PUF can achieve significant reduction in the energy per CRP as compared to the RO PUF. Further, we see that PUF operation at low supply voltages improves uniqueness with no impact on reliability, along with the benefit of low energy consumption [30].

Energy consumption of hardware security primitives is a key design goal in ultra low power applications. In this work, we present the energy and uniqueness benefits achieved through PUF operation at low supply voltages [30]. We also note that an Arbiter PUF is the natural choice for low power applications and the delay line PUF provides an energy efficient alternative.

CHAPTER 4

TECHNOLOGY TRENDS IN UNIQUENESS AND RELIABILITY

4.1 Impact of scaling on PUF metrics

Moore's law has driven CMOS scaling technology over the years leading to increased complexities in designs. Deep sub-wavelength lithography used in lower technology nodes brings greater challenges in the manufacturing process. The amount of process variation seen follows an increasing trend with technology and is becoming increasingly significant. As a result, designs aiming for high performance will find it exceedingly difficult to meet the requirements in presence of these variations. However, an increase in process variation benefits the identification capability that can be achieved by PUFs. PUF uniqueness is directly related to the amount of inter-chip variation seen and with technology scaling, we expect PUF uniqueness to increase. However an increase in process variations may impact the reliability across different environmental conditions. We explore this hypothesis by observing PUF behavior in 45nm, 32nm and 22nm technologies. In this work, the metrics for an arbiter-based PUF are evaluated across different technologies along with supply voltage scaling [32].

4.2 Arbiter-based PUF Circuit Design

The arbiter based PUF is implemented using n delay stages and an SR Latch as arbiter as shown in Figure. 17, where n is 64 for this analysis. Each delay stage comprises of two CMOS multiplexers with their inputs connected as shown in Figure 18. The devices in the delay stage have equal sizes to ensure that the delays are equal in all paths. The delay element consists of four timing arcs which are selected based on the challenge applied for that particular stage. From Figure 18, it can be observed that p and q are always chosen together and hence they are assigned to the same gate input in the 2nd level NAND gates. The SR latch used as an arbiter

provides a response bit depending on the top and bottom signal arrival times. The fundamental principle of PUF operation is based on the fact that, process variations introduce different amounts of delay on each of the selected paths. Hence for a given challenge, the overall response bit will be a function of a particular path selected across the 64 stages.

The arbiter evaluates whether the top or bottom signal arrives first and correspondingly the response bit is set to either a 1 or 0. A fair arbiter will correctly evaluate the response based on positive or negative delay differences irrespective of their magnitude. Hence the selection of arbiter is a critical step in the PUF circuit design which can have a significant impact on the uniqueness and reliability of the PUF.

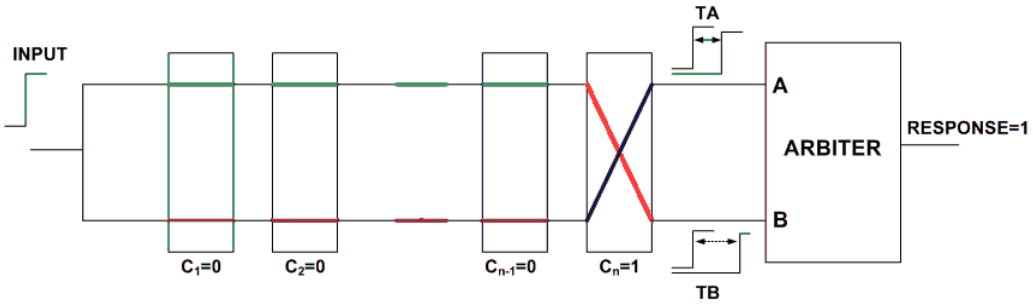

Figure 17. Circuit diagram of arbiter-based PUF

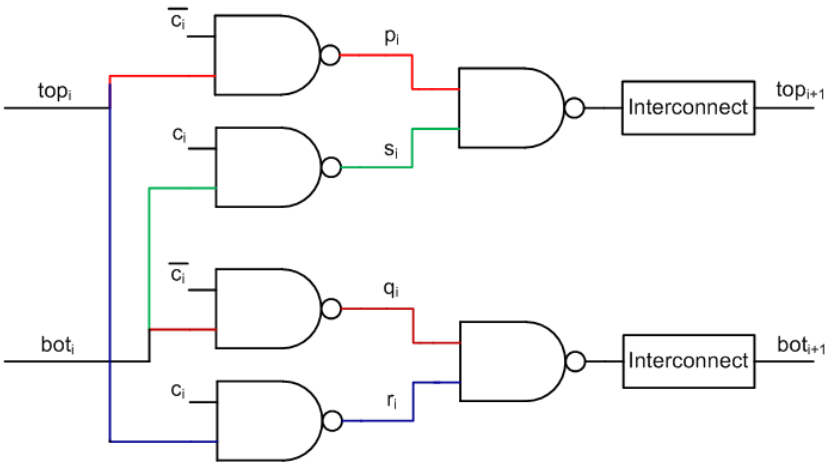

Figure 18. Symmetric circuit design for a single PUF stage.

It has been demonstrated that edge triggered flip flops are not necessarily fair arbiters [13]. A large bias of up to 20-30 ps can be seen by using D Flip-Flops. On the contrary, SR latch has a significantly smaller bias of less than 2ps. SR latch is a symmetric circuit made up of cross coupled NAND gates which leads to a smaller bias making it a suitable choice for the arbiter.

4.3 Experimental Methodology

PUF circuit analysis was carried out in Hspice using high performance, high-k and strained silicon PTM device models [28][37]. The analysis was carried out across 45nm, 32nm and 22nm technology nodes. The nominal voltages were 1.0V, 0.9V and 0.8V respectively. The nominal threshold voltage values for 45nm NMOS and PMOS are 0.46 and -0.49 respectively. The corresponding values are 0.49 and -0.49 for 32nm and 0.5 and -0.46 for 22nm. 3σ threshold voltage variations of 42% which corresponds to 120mV for 45nm PUF evaluation are used. The 3σ threshold voltage variation for 32nm and 22nm technology nodes is projected to be higher. Based on [29], the PUF design has been evaluated with a 3σ of 160mV for 32nm design and 210mV for 22nm design. Sub-threshold circuits are sensitive to supply voltage and temperature variations, causing unreliable responses. According to [13], the PDP is lowest when operated at 0.43V. In this work, the sub-threshold PUF analysis was carried out with a supply voltage of 0.4V across all technologies considered.

4.4 Uniqueness Analysis

With an increase in process variations, the probability of responses being same in two different PUF instances decreases. Smaller device dimensions such as gate length and width cause the device to be more sensitive to process variations. As per ITRS projections [15], percentage of process variations is set to increase further and this can only result in improved uniqueness getting us closer to a hamming distance of 0.5. Hence we can conclude that in deep

submicron technologies there exists sufficient inter-chip and intra-chip variations, which enable use of PUFs as authentication circuits.

In PUF circuits, process variation in the delay elements is leveraged to create unique challenge-response pairs. To validate the PUF uniqueness, 40 different PUF instances were evaluated using 500 challenges for each PUF instance. To study the technology scaling trend, uniqueness has been evaluated across different technology nodes (45nm, 32nm and 22nm) using the PTM models [37]. Sub-threshold circuits are more sensitive to Vth variation with an exponential dependence [29]. Hence, the uniqueness analysis was also carried out in sub-threshold region for all the 3 technology nodes. The detailed results obtained for both regions of operation are provided below.

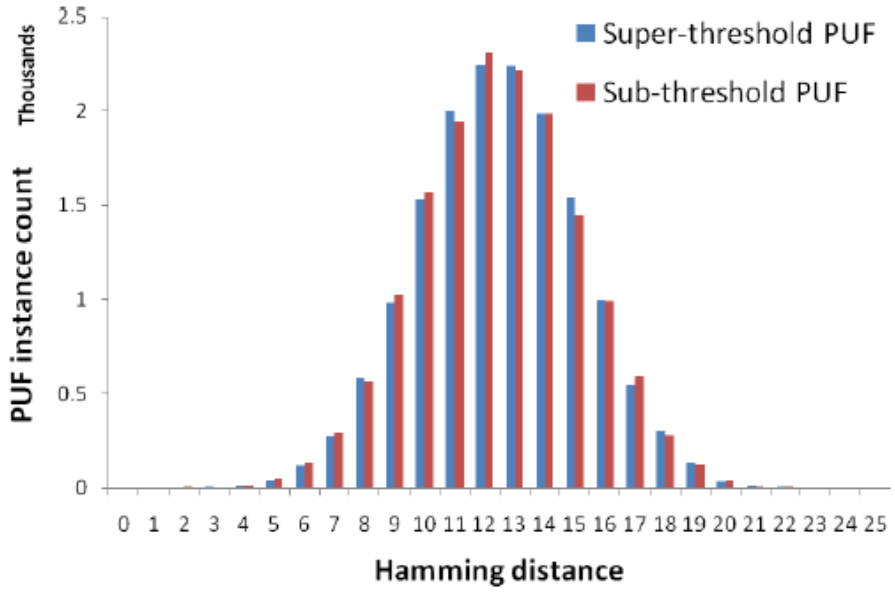

Figure 19. HD distribution of super threshold and sub threshold PUF in 45nm

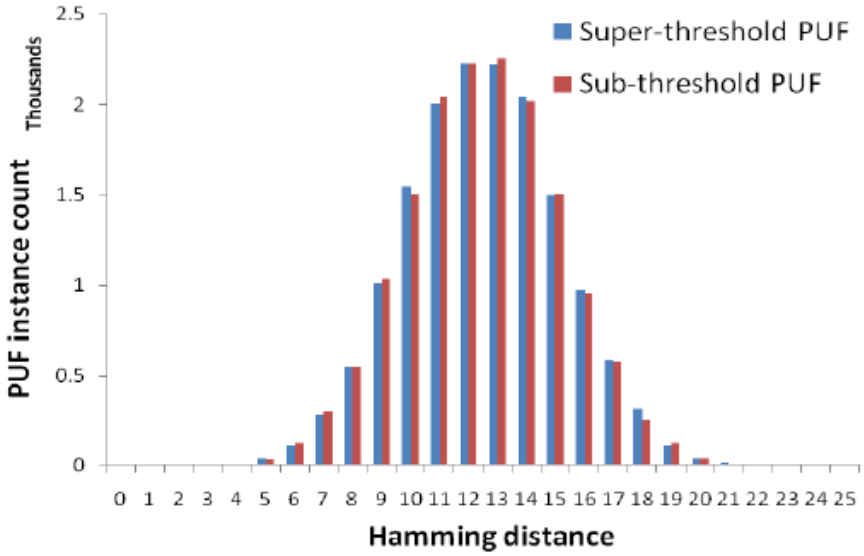

Figure 20. HD distribution of super threshold and sub threshold PUF in 32nm

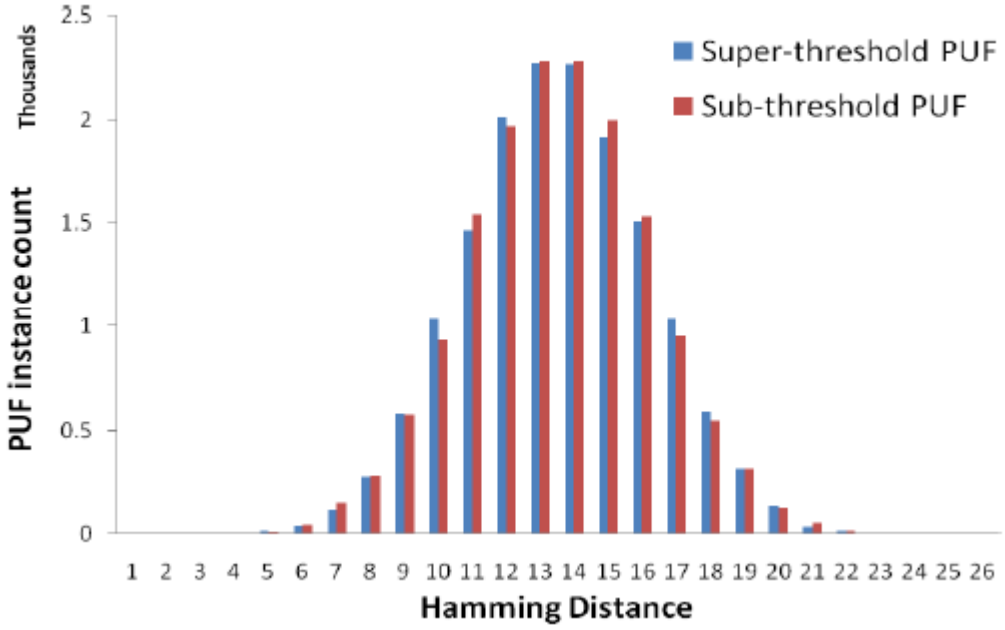

Figure 21. HD distribution of super threshold and sub threshold PUF in 22nm

500 challenges generate 500 1-bit responses and the Hamming Distance is calculated for 20 sets of 25 bits each. The HD distribution plots of PUF design in 45nm, 32nm and 22nm are shown in Figures 19-21. In each figure, the distribution of super-threshold PUF and sub-threshold PUF are overlapped for fine comparisons.

Table 3. Uniqueness in lower technology nodes

Technology	Mean HD	Relative HD
45nm	12.46	49.84
32nm	12.48	49.92
22nm	12.51	50.04

It is clearly observed that, uniqueness values converge to the ideal value of 50% for 45nm super-threshold PUF. This means that there are sufficient variations in 45nm designs that enable each chip to be identified uniquely. As expected, with increased process variations uniqueness is not hampered and remains close to the ideal value of 50% when we scale down to lower technology nodes such as 32nm and 22nm. This is also true for sub-threshold PUFs, though with a smaller uniqueness improvement than super-threshold PUFs.

4.4.1 Uniqueness Analysis with delay bias

A PUF circuit layout should exhibit perfect symmetry to minimize delay bias between the top and bottom signals. However, variations in the interconnects and parasitics during the manufacturing process can give rise to a delay bias. This would cause the PUF circuit to favor either a 0 or 1 response resulting in reduced uniqueness. In order to analyze the impact of delay bias, the PUF circuit is simulated in super threshold mode by introducing a delay bias of 10ps between the top and bottom stages. The relative hamming distances obtained across different technologies is shown in Figure 22 and Table IV.

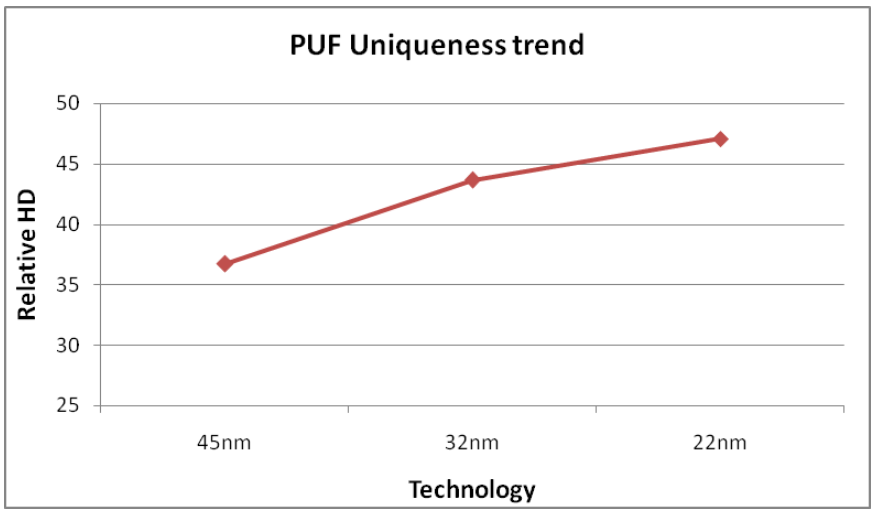

Figure 22. Uniqueness improvement with technology scaling

Table 4. PUF Uniqueness with delay bias

Technology	Super threshold		Sub threshold	
	Mean HD	Relative HD	Mean HD	Relative HD
45nm	183.72	36.74	250.41	50.08
32nm	218.18	43.63	249.68	49.93
22nm	235.41	47.08	247.35	49.47

As seen from the figure, there is a clearly discernible trend in PUF uniqueness with technology scaling. A 10 ps delay bias in 45nm technology can reduce the PUF uniqueness from 49.7 to 36.74. However, as we scale to lower technologies, the increase in process variations counters any delay mismatch between the stages and we obtain an improvement in uniqueness. A similar analysis was carried out in sub-threshold mode by introducing a delay bias of 1 ns between the top and bottom paths. It can be observed that even in presence of delay bias, subthreshold operation results in high uniqueness across technologies.

The uniqueness of delay based arbiter PUFs mainly depends upon the number of delay stages, number of CRPs used, and the amount of process variations in the given technology node [16]. It is seen that, as we increase the number of delay stages and CRPs, uniqueness converges to the ideal value of 50%. However, there may be several trade-offs in terms of power consumption, time required for authentication, complexity of the server side database etc. Lim et al. claimed that for 180nm technology, 300 CRPs were sufficient to uniquely identify more than a billion PUFs [16]. In 45nm technology and beyond, 100 CRPs is sufficient to achieve obtain high relative hamming distances between responses ensuring unique identification [32].

4.5 Reliability Analysis

To evaluate the reliability of the PUF, challenge response pairs are evaluated for a single PUF instance across a range of supply voltages and operating temperatures individually. The supply voltage variation is taken to be ±10% and temperature is varied between -25 and 85 degree Celsius. Reliability is measured by observing the bit error rate in responses for 1000 challenges. This experiment was repeated across all technologies considered in this work. Reliability analysis was also performed in sub-threshold mode of operation across all 3 technology nodes with the same percentage variations for temperature and voltage as in super-threshold analysis. The delay in sub-threshold operation has an exponential relationship with temperature [29] which makes the circuit more vulnerable for bit errors due to temperature instability.

Figure 23 summarizes the Vdd reliability results for both super-threshold and sub-threshold PUFs across all three technology nodes. A general trend can be found that technology scaling degrades the reliability slightly within 2%, especially for sub-threshold PUFs. The

reliability of sub-threshold PUFs tends to be better than that of super-threshold PUFs, except for a sudden degradation with a large supply voltage bias in 22nm technology.

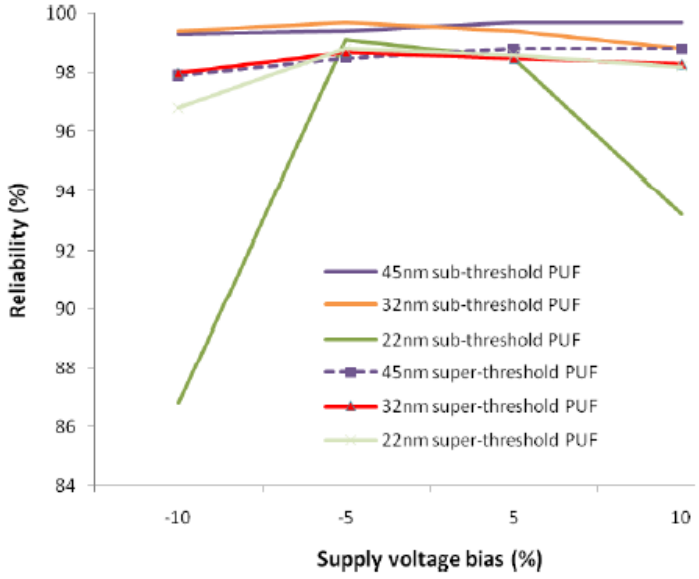

Figure 23. PUF reliability with respect to supply voltage bias

In a similar way, Figure 24 summarizes the temperature reliability results for both super-threshold and sub-threshold PUFs across all three technology nodes.

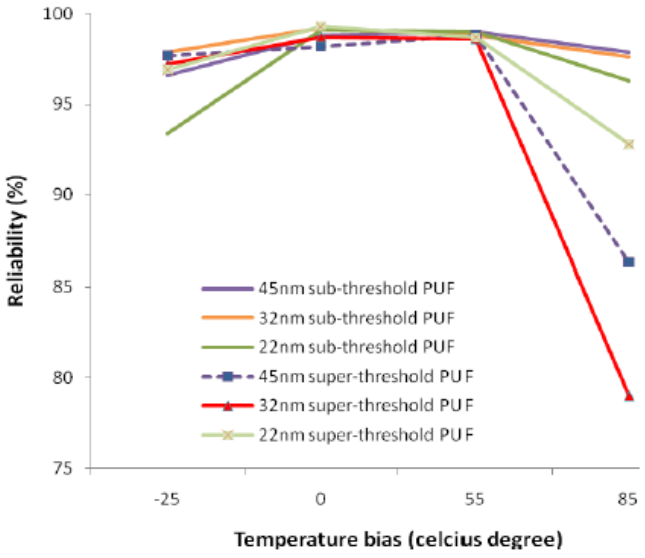

Figure 24. PUF reliability with respect to temperature bias

From the results, we can observe that extreme temperature bias has more impact on PUF reliability than supply voltage bias [32]. Maximum bit error rates were observed for high temperature and low Vdd values, when there is an increase in circuit delays. The worst case reliability seen for the Arbiter PUF is 78%. In applications where PUFs are used for authentication, reduced reliability at extreme operating conditions is not prohibitive and the authentication process can use more CRPs to identify a chip. However, in applications where the PUF is used to generate a secret key, reliability needs to be very high close to 100%. Even a single secret key bit flipped would impact the encryption or decryption process adversely.

As we scale to lower technology nodes, the identification capability of a PUF improves due to increased process variations. However, reliability under changing operating conditions suffers which would necessitate better PUF circuit design practices.

CHAPTER 5

SILICON VALIDATION OF PUF TESTCHIP IN 45nm TECHNOLOGY

As we scale into lower technology nodes, process variation has become increasingly significant and can impact design performance considerably. These process variations can be accounted for in the design stage by running extensive simulations to validate the functional and timing behavior of the circuit. However simulations cannot capture all variations affecting circuit behavior in silicon. Design validation in real hardware can provide valuable insights into the effectiveness of the circuit in presence of process variations, environmental variations and noise. To validate our previous PUF simulation results on silicon, we fabricate the 64-stage PUF circuit using 45nm SOI libraries. Two instances of PUFs are included on one die to analyze intra-chip variation impacts on PUF. 40 dies are fabricated to analyze the inter-chip variation impacts on PUF. Through post silicon validation, PUF metrics in super-threshold and sub-threshold modes of operation are evaluated [31][32].

The different steps involved in the design of the PUF testchip, shown in Figure 25, are described below

5.1 Circuit Schematic design

The Arbiter PUF has been designed with 64 delay stages and an SR latch as Arbiter. To minimize the number of signal IOs on this PUF test chip, a 64 bit Pseudo Random Number Generator (PRNG) is implemented to generate the challenge vectors. The 64 bit PRNG has been implemented using a maximal length LFSR so that it can generate all possible challenges. The

PRNG circuit is provided with a reset signal and a fixed initial seed so that it can be reset to a known state when necessary.

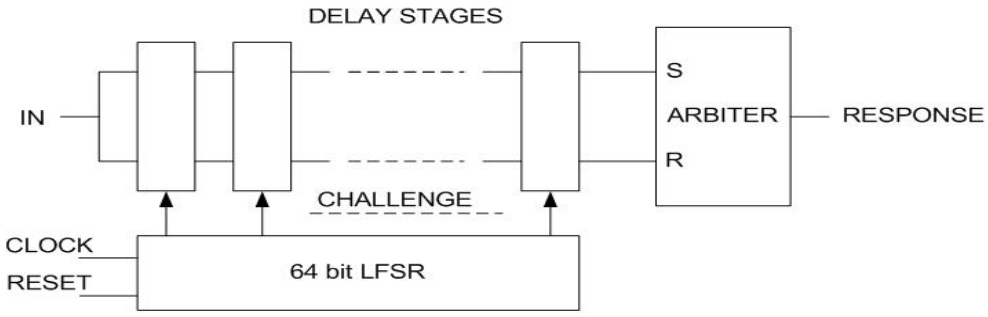

Figure 25. PUF Circuit Schematic

Since devices sizes can affect the delay stage's sensitivity to process variations, minimum device sizes are used in the delay stage to facilitate threshold voltage variations during manufacturing process. The schematic design is performed in Cadence Virtuoso.

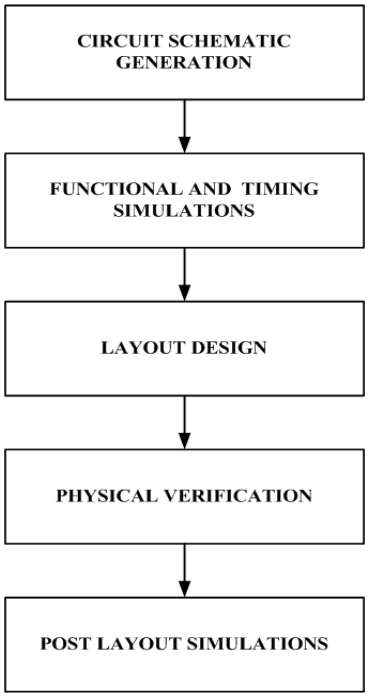

Figure 26. PUF Design methodology

5.2 Functional and Timing Simulations

The functional and timing behavior of the circuit is simulated in Hspice. 45nm SOI models have been used for simulation at a nominal voltage of 1.0V. A hierarchical design methodology is followed wherein the standard cells and delay stages are designed. Each circuit is tested for functionality and the timing delays are measured. The linear feedback shift register functionality is also tested by applying the reset signal and ensuring that the outputs start from an initial seed and cycle through the expected sequence as per the polynomial. The LFSR polynomial chosen would generate the maximal length sequence.

$$F = 1 + x^3 + x^{63} + x^{64}$$

After the 64 bit PUF schematic is built, the PRNG is activated to apply different challenges to the PUF delay stages and the Arbiter response is captured.

5.3 Layout Design

Layout design has to allow sufficient process variations for randomness and to minimize unwanted variations due to delay path imbalance. To ensure sufficient random variations, the devices in the delay stage are sized to have minimum width rendering them sensitive to threshold voltage variations. Since a delay bias of the top and bottom delay paths will compromise the uniqueness of PUF CRPs, the PUF stage layout is carefully balanced to avoid inducing any unintended bias on either path. A single delay stage and one bit of the PRNG are grouped together to form a tile. The tile layout is performed carefully and replicated 64 times to build the complete Arbiter PUF layout. This ensures symmetry in the layout along with ease of implementation. However, a perfectly balanced layout is hard to achieve since manufacturing

process will still result in some unintended imbalance. The layout design is carried out in Cadence Virtuoso. Figure 27 shows a snapshot of the complete Arbiter PUF layout along with power and signal IOs.

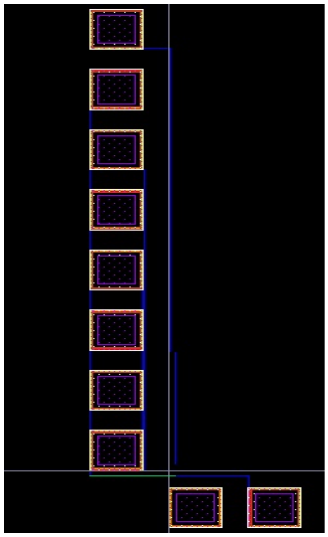

Figure 27. Arbiter PUF Layout with signal IOs

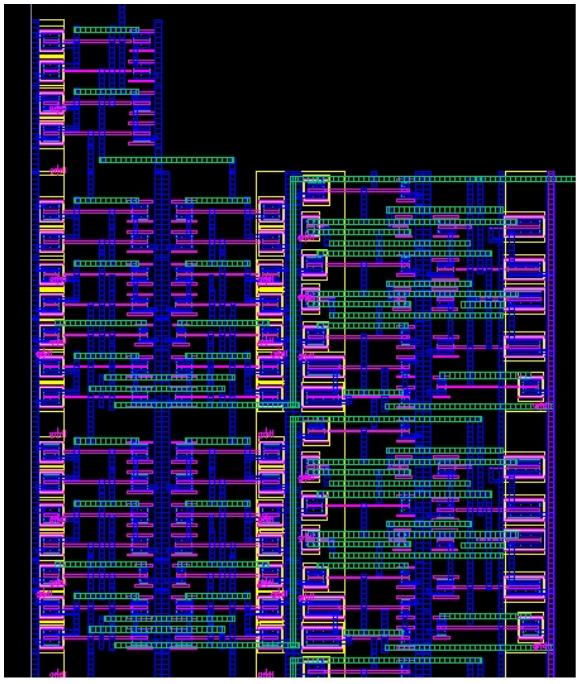

Figure 28. Snapshot of two PUF stages and arbiter

5.4 Physical Verification

After the PUF layout design, physical verification is performed to ensure design rule compliance and layout versus schematic equivalence. Calibre DRC and LVS checks are carried out using the 45nm SOI library rule decks.

5.5 Post silicon validation measurement setup

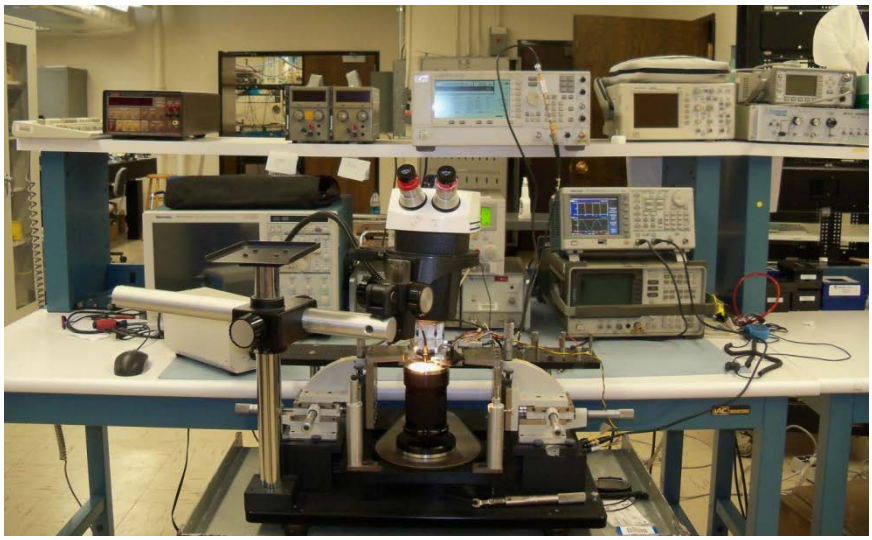

Figure 29. Post silicon validation lab setup

To measure PUF CRPs from the fabricated dies, a post-silicon validation platform was setup by our team [31][32]. An adjustable DC power supply is used to supply chip power. Tektronix AFG3000 and Agilent 8251A signal generators are used to generate the PRNG clock and set signals, and an input signal to the Arbiter PUF. The clock signal results in the PRNG outputs changing every cycle, which form the challenge bits to the Arbiter PUF. The input signal to the Arbiter PUF is setup to have the same period as the clock signal but with a 30% phase lag. This is to ensure that the challenge bits are stable before the input signal is applied. We use a microscope and probe station to mount a 2-pin DC probe and an 8-pin AC probe on the die. The 2 pin DC probe is used to supply Vdd to the chip. The 8-pin AC probe which consists of 4 signal

pins interspersed with 4 ground pins is used to provide the 3 inputs signal namely PRNG clock, set and the Arbiter input and capture the PUF output response. The Picoscope 5000 with 1GS/s sampling rate is used to capture the response bits. The set signal applied to the PRNG also acts as the trigger signal and is provided to the oscilloscope and the test chip simultaneously by a power splitter and BNC cables.

5.6 Measurement methodology

With the above mentioned post silicon validation platform, members of our team recorded CRP measurements by subjecting the PUF to different supply voltages [31][32]. The PRNG set signal was setup to have a period equal to 10,000 clock cycles and an active period of 10 cycles. With the rising edge of the set signal, the PRNG is reset to a known state which sets all the PRNG output bits to 1. The rising edge of the set signal also acts as the trigger signal to the oscilloscope which proceeds to capture the output response signal. Each measurement captured approximately 10,000 response bits and for each PUF circuit tested, 5 measurements were recorded.

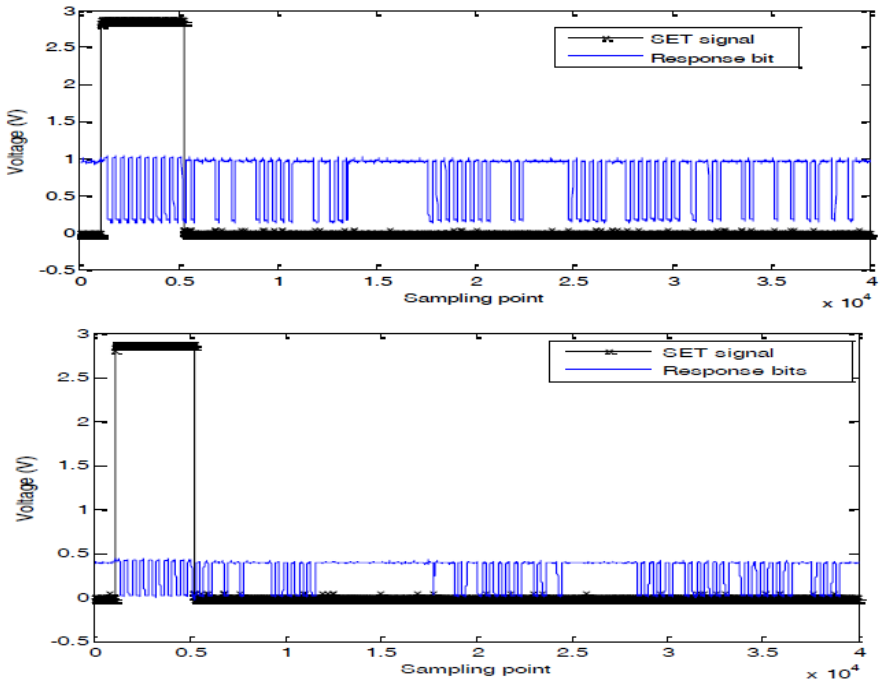

Figure 30. Super threshold and sub threshold response waveforms

A majority of the 5 measurements were recorded as the response during post processing of data and this prevented recording of erroneous data due to occurrence of any glitches in the output signal. This procedure was repeated for 2 PUF instances on each die and for each of the 40 dies respectively. Each PUF circuit was tested under nominal supply voltage condition at Vdd of 1V and also in the sub threshold region by applying a Vdd of 0.4V. Response waveforms captured in super threshold and sub threshold mode are shown below in Figure 30.

5.6 Uniqueness and reliability results

5.6.1 Uniqueness

Based on the 10,000 response bits extracted from each PUF instance, hamming distances between each PUF pair are computed [31][32]. The hamming distance distributions in super threshold and subthreshold operation are as shown in Figure 31 and 32.

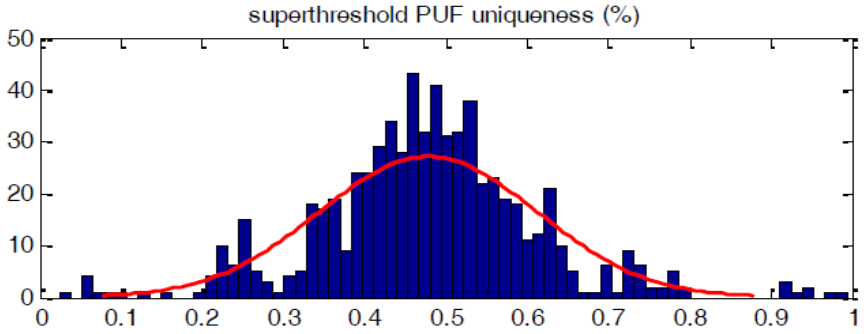

Figure 31. Super threshold hamming distance distribution

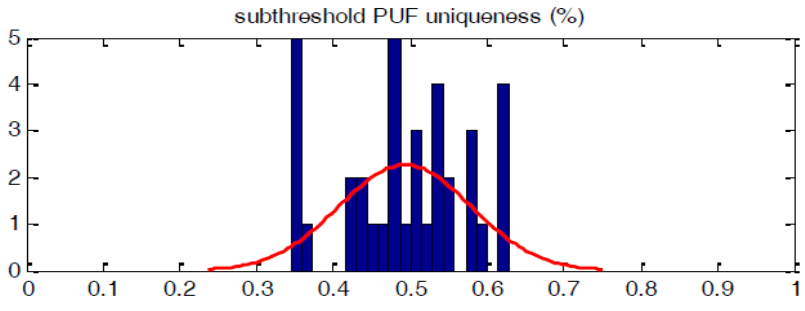

Figure 32. Subthreshold hamming distance distribution

The relative hamming distance in super threshold mode is calculated to be 38%. The relative hamming distance in sub threshold mode is calculated to be 44%, but with a much smaller sample set. During post silicon measurements, fewer dies produced output responses with acceptable voltage swings in sub threshold operation. One of the possible reasons for this reduced yield is the lower noise margins seen in sub threshold region. This is also exacerbated by the systematic noise seen from the DC power supply used in our lab setup and the coupling between input signals.

5.6.2 Reliability

To evaluate reliability of PUF circuits in silicon, a ±5% supply voltage bias is applied and the temperature is increased up to 75%. Under supply voltage bias or +25°C temperature bias, the average reliability of four tested chips is around 99%. For extremely high temperature of +75°C, the reliability can quickly degrade with an ever-increasing number of noisy CRPs [31][32].

5.7 Discussion

From the post silicon validation measurements, we can observe that the Arbiter PUF circuit was able to successfully generate different challenge response pairs across dies. Our team also carried out Support Vector Machine attacks on the challenge response pairs obtained from some PUF instances. The SVM attacks were successful and achieved a high prediction rate on the challenge response set for a few PUFs. A successful SVM attack verifies the additive delay model behavior of the Arbiter PUF, proving the validity of the fabricated PUF circuit. However, SVM attacks were not successful on all PUF instances, which could indicate the presence of noisy or erroneous CRPs in the data set.

We can also observe that the relative hamming distance seen during subthreshold operation was higher than that of super threshold operation, albeit on a handful of instances. In order to improve the yield of subthreshold PUFs, a more comprehensive subthreshold simulation methodology needs to be explored. Lower noise margins seen in subthreshold operation can be

affected due to supply voltage noise, power grid IR drop or crosstalk. Analyzing the impact of these effects on PUF functionality would provide valuable insight into the design of robust subthreshold PUFs.

CHAPTER 6

SECURE PHYSICAL UNCLONABLE FUNCTIONS

PUF circuits demonstrate strong identification capabilities and can perform reliable authentication over a range of environmental variations. These features are determined by the uniqueness and reliability metrics of a PUF circuit. However, the security offered by a PUF circuit also depends on its resistance to different modeling attacks. As we know, the most important feature of a PUF circuit is its un-clonability which makes it impossible even for the manufacturer to create a duplicate. However, PUFs have been shown to be susceptible to software modeling attacks. These modeling attacks create a software model of the PUF circuit using the knowledge of a limited number of CRPs. The resultant model is capable of predicting responses generated by the PUF circuit to randomly generated challenges, with a high degree of accuracy. Here we look at the current modeling attacks that have been successful in breaking the PUF construction and look at new directions toward creating a robust PUF circuit.

6.1 Modeling attacks using Support Vector Machine classifiers

Delay based PUFs constitute a major portion of the Strong PUF category, with the foremost being the Arbiter PUF. The Arbiter PUF circuit has been shown to be susceptible to software modeling attacks that assume an additive delay model [16]. In this model, the top and bottom path delays at the final stage are taken to be a sum of the stage delays. Each delay stage comprises of 4 timing arcs and hence an n-stage PUF consists of 4n timing arcs.

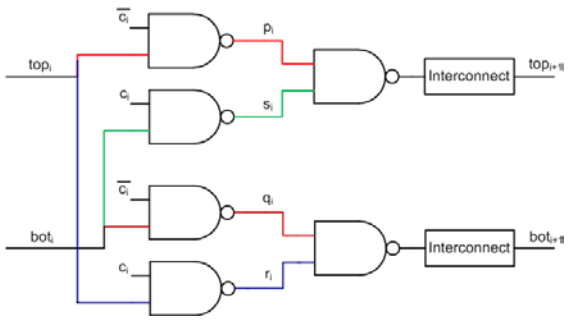

Figure 33. Single delay stage

If the delays of these 4n timing arcs can be estimated, it is possible to calculate the delay difference at the final stage and hence predict the response. Challenge bits of 0 and 1 are denoted as (-1,1) for modeling reasons. The top and bottom delays at the (i+1)th stage and the delay difference at an arbitrary nth stage are given by the equations below.

$$\delta_{top}(i+1)=(1+C_{i+1})/2(p_{i+1} + \delta_{top}(i)) + (1 - C_{i+1})/2(s_{i+1} + \delta_{bottom}(i)) \quad \dots (1)$$

$$\delta_{bottom}(i+1)=(1+C_{i+1})/2(q_{i+1} + \delta_{bottom}(i)) + (1 - C_{i+1})/2(r_{i+1} + \delta_{top}(i)) \quad \dots (2)$$

$$\Delta=\delta_{top}(n)- \delta_{bottom}(n) \quad \dots (3)$$

If we assume that we are provided with m number of CRPs for a 64 stage PUF, we can construct a matrix B of size *mx256* that indicates which segments are activated by a certain challenge. The weights of each of the 256 timing arcs are given by a column vector w. Then the delay difference matrix Δ for each of the m challenges can be expressed as

$$Bw = \Delta \quad \dots (4)$$

While performing modeling attacks, it is not possible to obtain the delay difference for each CRP. We can only obtain the sign of the delay difference through the response bit. This translates to a linear constraint such as $b_j w < 0$ or $b_j w > 0$ for each CRP. Linear programming techniques can be adopted to solve these constraints.

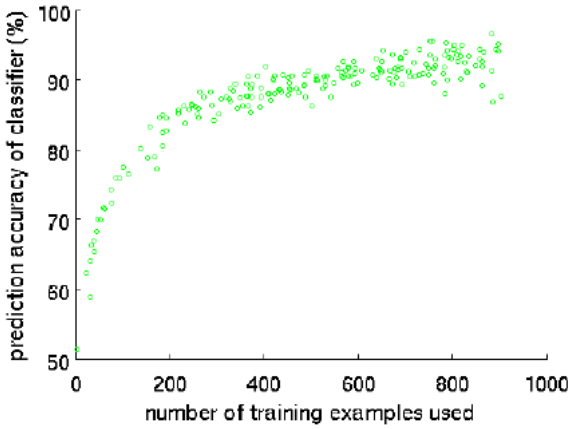

Figure 34. SVM Attack on Arbiter PUF [13]

In previous work, Support Vector Machine classifiers have been used instead of linear programming. SVM classifiers find a maximum-margin hyper plane that separates the 0 and 1 responses. A training sample consisting of a limited number of CRPs is used to build the model. This model is used to predict future responses on a randomly selected set of challenges. As shown above, SVM attacks can achieve high prediction accuracy greater than 90% with a training sample set of approximately 300 CRPs.

While analyzing security, a very important aspect that needs to be considered is the relation between security and reliability. In order to compromise the security of a PUF, the prediction accuracy achieved through modeling attacks has to be at least higher than the reliability achieved by the PUF. Even though SVM attacks can achieve prediction rates of 90%, it may still prove insufficient to impersonate a PUF instance. To elaborate further, the authentication process of a PUF circuit with reliability of 95% will expect at least 94 responses out of 100 to be correct. Hence a prediction rate of 90% is not sufficient since a software PUF model which gets only 90 out of 100 CRPs correct would be rejected by the authentication process. Adding non linearity to PUF circuits can break this linear additive delay model and thwart SVM attacks. Feed forward arbiter PUFs, XOR arbiter PUFs and light weight secure PUFs have been proposed to resist such modeling attacks.

6.2 Logistic Regression Based Modeling Attacks

Recently, it has been demonstrated that machine learning based modeling attacks using logistic regression methods can break all current PUF constructions [17]. Using a polynomial amount of resources and CRPs, it is possible to break the security of these PUF circuits.

The authors present an attack model for different classification of PUF circuits namely strong PUFs, controlled PUFs and weak PUFs. In all machine learning attacks, it is imperative to have access to a set of challenge response pairs that form the training samples. In case of strong PUFs, access to CRPs is unrestricted and an attacker can obtain CRPs either through eavesdropping or by direct access of the PUF circuit. Most delay based PUFs such as Arbiter

PUFs, Feed forward Arbiter PUFs, XOR Arbiter PUFs, and Lightweight Secure PUFs and even Ring oscillator PUFs are considered to be strong PUFs. Controlled PUFs employ a strong PUF and obfuscate the challenge inputs and responses generated though one way hash functions. In this scenario, an attacker cannot obtain the CRPs directly. However it is possible to probe the inputs and outputs of the strong PUF through reverse engineering methods to obtain digital CRP information. This process is very expensive and cumbersome. Given that CRPs are obtained in this manner, the Controlled PUF protocol can be broken if the underlying strong PUF can be successfully modeled. Weak PUFs typically offer few CRPs that are not let out to the external world. These are susceptible to reverse engineering and side channel attacks. Some weak PUFs are constructed by integrating strong PUFs and these implementations again prove to be susceptible to machine learning attacks.

In recent work, machine learning techniques namely logistic regression and evolution strategies have been used to break different strong PUF circuits [17]. It is interesting to note that the underlying models need not be strictly linear and need to be differentiable for machine learning attacks to be successful.

Table 5. ML attack on arbiter PUF[17]

ML Method	No. of Stages	Prediction Rate	CRPs	Training Time
LR	64	95%	640	0.01 sec
		99%	2,555	0.13 sec
		99.9%	18,050	0.60 sec
LR	128	95%	1,350	0.06 sec
		99%	5,570	0.51 sec
		99.9%	39,200	2.10 sec

It can be seen from the results shown above that Arbiter PUFs can be broken relatively easily with a small number of CRPs in very short durations. The logistic regression based attacks achieve a high prediction rate of 99% in a very short training time with the knowledge of only 2,555 CRPs.

Table 6. ML attack on XOR Arbiter PUF [17]

ML Method	No. of Stages	Pred. Rate	No. of XORs	CRPs	Training Time
LR	64	99%	4 5 6	12,000 80,000 200,000	3:42 min 2:08 hrs 31:01 hrs
LR	128	99%	4 5 6	24,000 500,000 —	2:52 hrs 16:36 hrs —

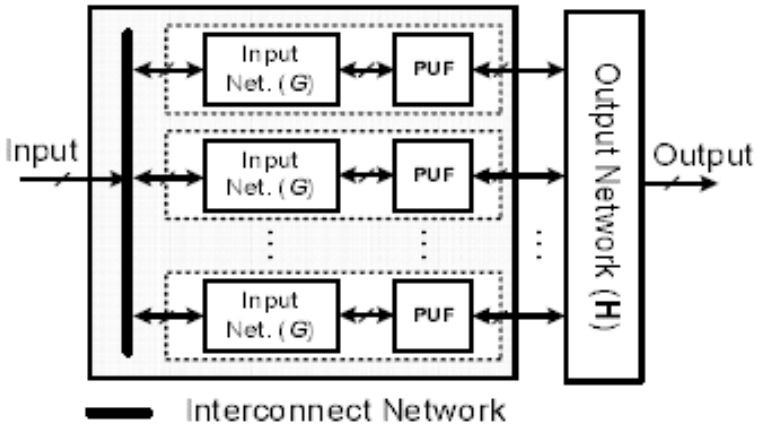

Figure 35. Lightweight Secure PUF [33]

Table 7. ML attack on lightweight secure PUF [17]

No. of Stages	Pred. Rate	No. of XORs	CRPs	Training Time
64	99%	3 4 5	6,000 12,000 300,000	8.9 sec 1:28 hrs 13:06 hrs
128	99%	3 4 5	15,000 500,000 10^6	40 sec 59:42 min 267 days

XOR Arbiter PUFs generate output responses by XORing response bits from 4-6 identical Arbiter PUF circuits. Lightweight Secure PUFs use input networks comprising of XORs that generate different deterministic combinations of challenge inputs. These circuits also use a output network of XORs to generate the final response bit. The proposed attacks are

successful in breaking these 2 categories of circuits. The models constructed for these two PUF circuits are similar with the lightweight secure PUF adopting additional hashing of challenge bits resulting in longer computation time for prediction. It can be noted that the number of CRPs and the training time required have increased owing to circuit complexity.

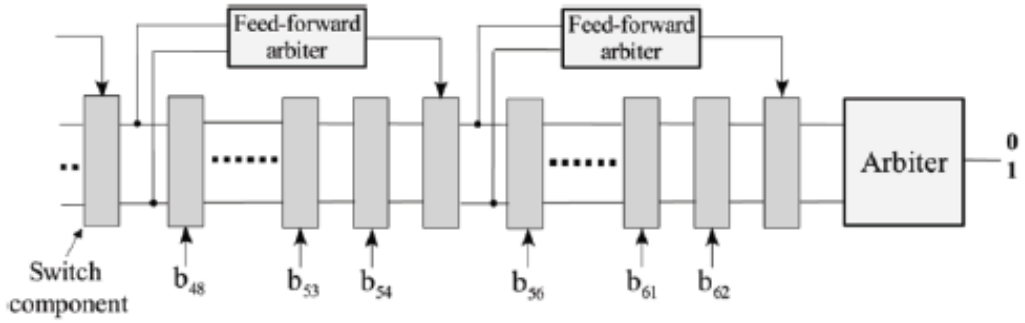

Figure 36. Feed-forward arbiter PUF [9]

Table 8. ML attack on feed forward arbiter PUF [17]

No. of Stages	FF-loops	Pred. Rate Best Run	CRPs	Training Time
64	6	97.72%	50,000	07:51 min
	7	99.38%	50,000	47:07 min
	8	99.50%	50,000	47:07 min
	9	98.86%	50,000	47:07 min
	10	97.86%	50,000	47:07 min
128	6	99.11%	50,000	3:15 hrs
	7	97.43%	50,000	3:15 hrs
	8	98.97%	50,000	3:15 hrs
	9	98.78%	50,000	3:15 hrs
	10	97.31%	50,000	3:15 hrs

Feed forward Arbiters, shown in Figure 36 prove to be the most challenging class of circuits to model owing to the non linearity introduced through feed forward loops. The ML modeling attacks can still achieve prediction rates of 99% albeit with a large number of CRPs.

Some of the interesting observations that can be made based on this paper are listed below

- ML attacks achieve prediction rates greater than the PUF circuit's reliability.

- Number of CRPs required by ML attacks grows linearly or log linearly with number of stages, XORs or feed forward loops.
- Training times are generally low degree polynomial. However, they can be quite long with increase in complexity of feed forward Arbiter PUFs.
- ML attacks can break all current strong PUFs but they sometimes require up to 50,000 CRPs. In a real scenario, this is possible only through physical access to the device and not through eavesdropping.
- Increasing the bit length of XOR PUFs or number of PUF instances in Lightweight secure PUFs prove to be resistant to current ML attacks.
- Addition of non linearity or exploiting analog behavior of PUFs can result in secure PUF implementations in the future.

6.3 Secure PUF constructions

As discussed above, current PUF implementations are susceptible to machine learning based modeling attacks. This motivates us to look at new ways of constructing PUF circuits that can overcome these limitations.

Here we explore a new class of PUF circuits whose central theme is the use of challenge inputs derived from a secondary PUF structure. In these circuits, in addition to the output response, input challenge bits to the main PUF structure are also dependent on process variations. This would force a software attack model to learn features (stage delays) of the secondary PUF circuit, in addition to that of the primary PUF circuit. Based on this theme, a new architecture for implementation of Secure PUF circuits is studied. We look at the security benefits offered by 3 PUF circuit designs and evaluate their identification capabilities and reliability.

6.3.1 Secure PUF 1

Figure below shows the schematic of a proposed secure PUF structure.

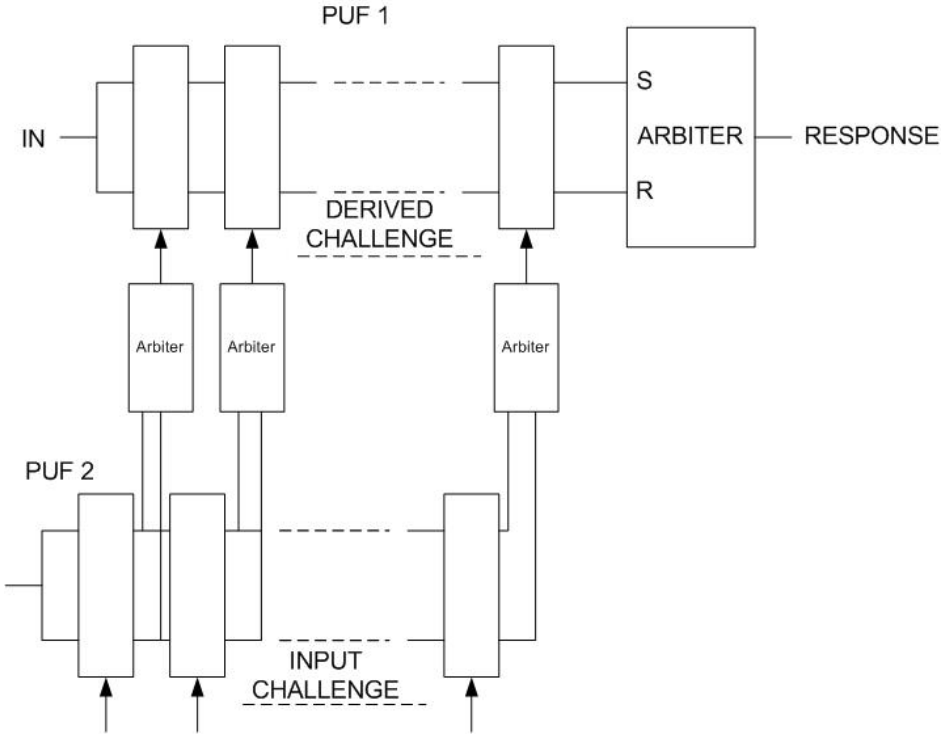

Figure 37. Secure PUF 1 Schematic

In this circuit, the input challenges are applied to a secondary Arbiter PUF circuit. Based on the delay differences at each stage, Arbiters generate n-bit length derived challenge bits. These derived challenge bits are fed as challenge inputs to the primary Arbiter PUF circuit and the final response bit is generated.

For a standard arbiter PUF, we can represent the response bit as a function

$$\text{Response} = f(\text{input\_challenge}, \text{stage\_delays}) \quad \ldots. (4)$$

Since the attacker would know the challenge bits, his objective with machine learning attacks would be to essentially try and learn the transistor/stage delays. In these proposed structures, the attacker would need to estimate the stage delays of the secondary PUF structure as well. So the final response can be represented as

Response = f(derived_challenge, primary_PUF_stage_delays) …. (5)

Derived challenge = f(input_challenge , secondary_PUF_stage_delays) …. (6)

It would be a complex function of the form,

Response = f(f(input_challenge, secondary_PUF_stage_delays), primary_PUF_stage_delays)

…. (7)

Hence it would be tougher to create a model for this PUF circuit which could be solved with machine learning attacks. Further, even if a model is created, the order of computation or the training time required to create a model will not be linear or low degree polynomial.

6.3.2 Secure PUF with XORs

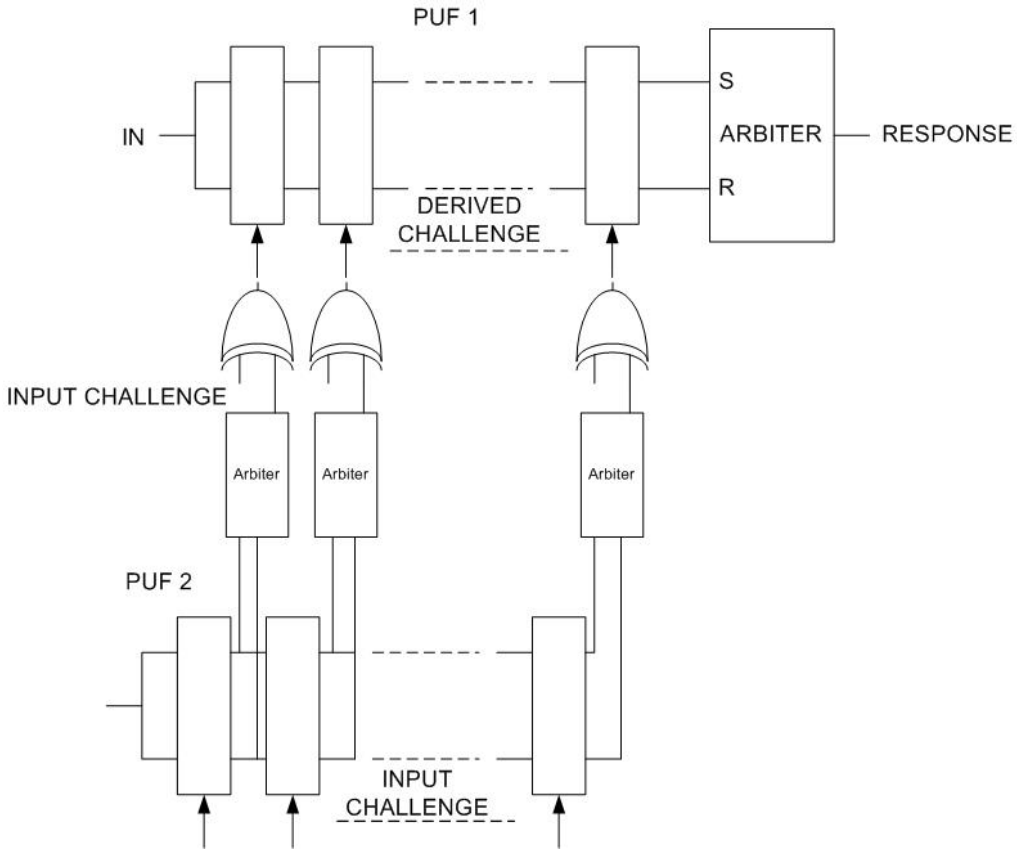

Figure 38. Secure PUF 2 Schematic

In the first PUF structure seen, most of the derived challenge bits may be same because delay differences at consecutive stages in the secondary PUF are correlated. For any given die, it is possible that some stage delays dominate over the other stages. Further, variations in the interconnects can cause imbalances. In such a scenario, a large number of derived challenge bits being same will result in reduced uniqueness. This can easily be fixed by XORing the derived challenge bits with the input challenge bits.

6.3.3 Secure PUF with LFSR

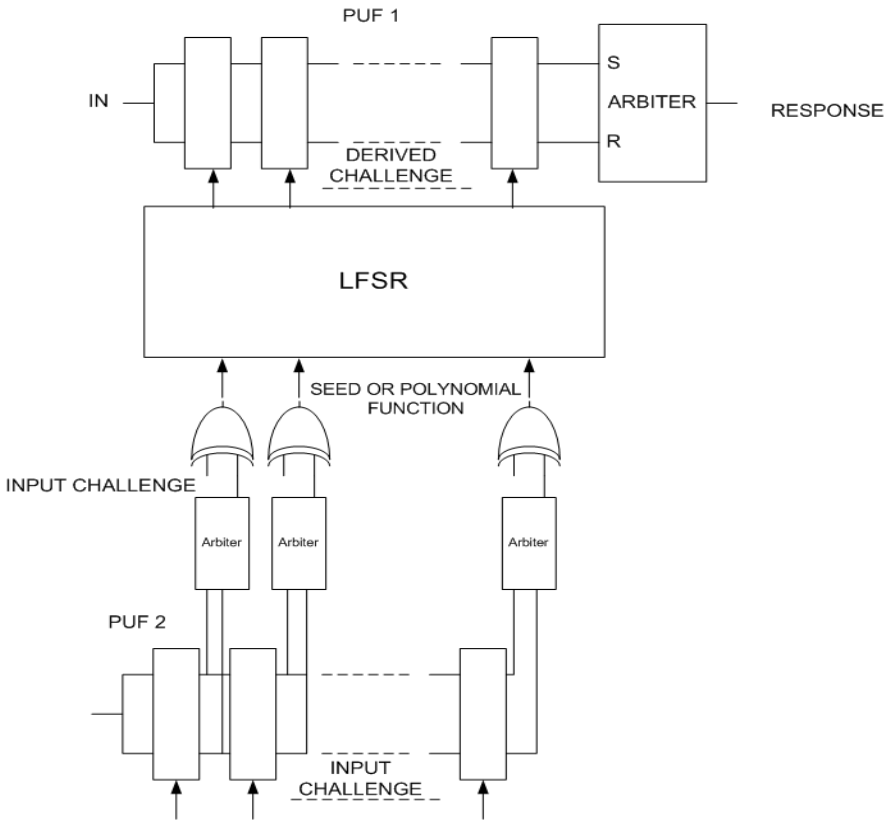

Figure 39. Secure PUF with LFSR Schematic

A stronger PUF circuit can be constructed by incorporating an LFSR circuit. In this circuit, the intermediate arbiter outputs are fed as a seed to the LFSR. The LFSR output forms the derived challenge bits driving the primary PUF circuit. The addition of an LFSR would effectively isolate the primary and secondary PUF challenge bits and it would be virtually impossible to guess the seed input to the LFSR and subsequently the derived challenge bits.

6.4 Uniqueness and reliability analysis

Having identified a PUF architecture that would prove secure against machine learning attacks, the next step is to determine the uniqueness and reliability metrics that can be achieved with this new class of circuits. The PUF circuits are implemented using Cadence Virtuoso and Perl scripts. Basic gates such as inverters, XORs, Arbiters and the PUF delay stage are implemented in Cadence Virtuoso. Since PUF circuits are comprised of a series of repetitive delay stages, Perl scripts are used to generate the complete circuit consisting of 64 stages. The use of D Flip Flops and SR latch as arbiters is also evaluated.

6.4.1 Uniqueness

Simulating uniqueness involves modeling the behavior of different silicon dies and extracting responses from each die for a given set of challenges. The PUF circuits are simulated using 45nm high performance PTM models [37]. Inter-chip variations are modeled by varying the transistor threshold voltages using Monte Carlo simulations in Hspice. A Gaussian distribution is used for the Vt distribution and the 3 σ value for the distribution is chosen based on the ITRS roadmap [15]. 40 Monte Carlo iterations are carried out to simulate the behavior of 40 different dies and responses are extracted from each die for a set of 100 challenges. Hamming distances between responses are calculated for each PUF pair. Finally the mean and relative hamming distance for the different circuits is computed, shown below in Table IX.

Table 9. Uniqueness

PUF TYPE	Arbiter Type	Relative Hamming Distance
Secure PUF 1	D Flip Flop	49.7
Secure PUF 1	SR Latch	49.83
Secure PUF with XORs	D Flip Flop	49.95
Secure PUF with XORs	SR Latch	50.11

As seen from the results, all PUF circuits achieve a high uniqueness value close to 50%. This can be attributed to the high percentage of process variation seen in 45nm technology.

6.4.2 Reliability

Reliability of PUF circuits is a measure of its robustness in presence of operating condition fluctuations. This is determined by subjecting the PUF to a +/- 10% supply voltage bias and by varying the operating temperature between -25C to 75C. For a set of 1000 challenges, responses are extracted at each operating condition. For each challenge, a change in the response bit when compared to response observed under nominal conditions is treated as a bit error.

The reliability evaluated from different circuits is shown below in Figures 40 and 41.

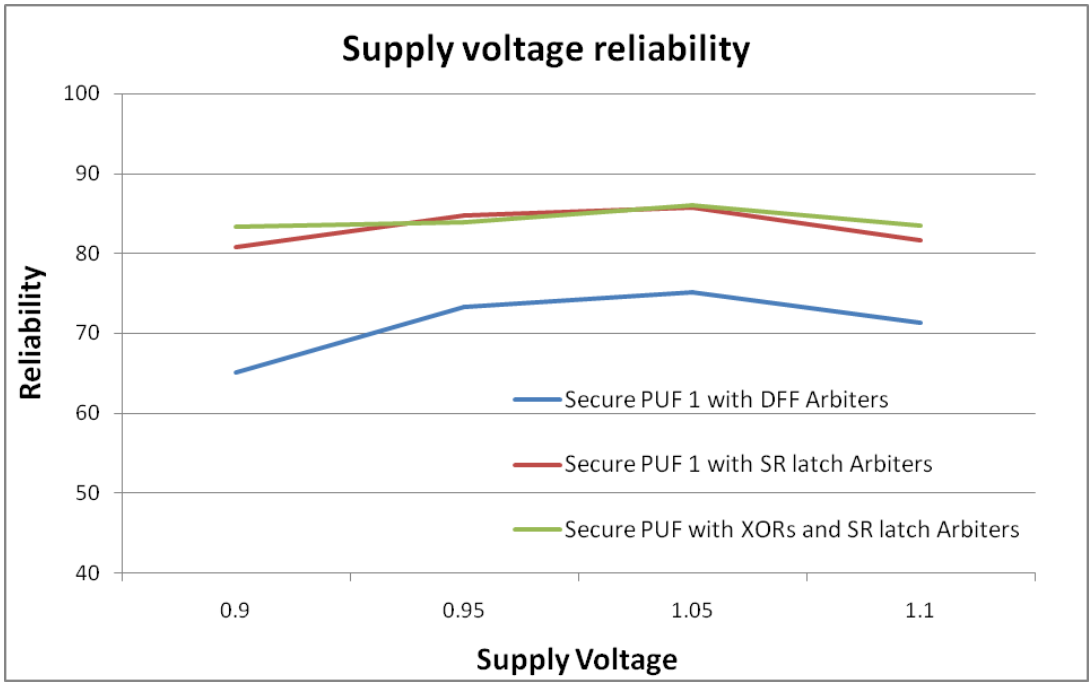

Figure 40. Reliability under supply voltage bias

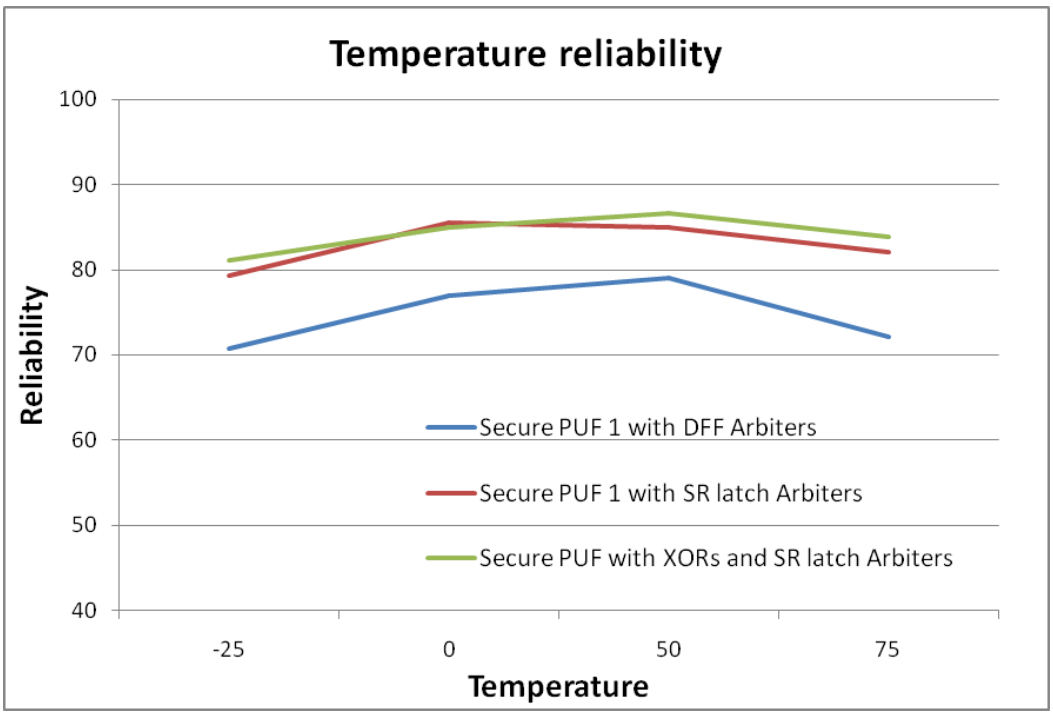

Figure 41. Reliability under temperature bias

The worst case reliability seen is as follows

- Secure PUF 1 with DFFs as Arbiters – 65.1 %
- Secure PUF 1 with SR Latch as Arbiters – 80.8 %
- Secure PUF with XORs and SR Latch as Arbiters – 83.3 %

It is quite clear that the use of D flip flops is not advisable as it impacts reliability significantly. A D flip flop arbiter has a setup time in the order of 10-15 ps and any delay difference within this window is not resolved reliably. It can also be observed that the worst case reliability with SR latch as Arbiter is 80.8%. This is lower than the reliability achieved with a standard Arbiter PUF which is typically around 90%. The reason for the dip in reliability is due to the use of a secondary PUF structure for the generation of challenges. In this class of circuits, 2 factors lead to reliability errors. Any changes in delay differences in the primary structure can

flip the response bit. In addition, changes in delay differences in the secondary PUF structure alters the input challenge bits to the primary PUF thereby impacting the response bit.

6.5 Other Approaches towards secure PUF implementation

Some of the other potential solutions are discussed below

6.5.1 Non-linearity

Addition of non linearity can be achieved by designing delay stages differently through the use of AND, OR gates which can perform MAX or MIN functions [16] or through the use of pass transistors to construct multiplexers. Non-linearity can cause the circuit to be slower increasing the time required to generate a single CRP. However, time required for authentication is typically not a concern and this might even act as an advantage as it reduces the number of CRPs that can be collected by an attacker in a given period of time. Non-linearity can also potentially impact the reliability of the PUF circuit.

6.5.2 Controlled PUFs

Controlled PUFs offer strong features of security as they restrict direct access to actual CRPs generated by the strong PUF [19]. Controlled PUFs make it exceedingly difficult to access CRPs and an attacker can obtain CRPs only through invasive methods. However, this comes at the cost of implementing expensive hash functions in hardware which might be prohibitive for some applications.

6.5.3 Time bounded authentication

Another technique to provide a secure PUF implementation is to limit the time taken by the PUF to generate a response once the challenge is applied. All current attacks construct software models that mimic the CRP behavior of a PUF circuit. However, a software model cannot generate CRPs in time periods comparable to that of the hardware PUF implementation. This concept has been demonstrated for PUF circuits in FPGA applications [36].

6.5.4 Multi bit response generation

Current PUF circuits generate a single bit response to each challenge and hence any machine learning attack has to perform binary classification to predict the PUF CRP behavior. We can explore the idea of generating a multi bit response for each challenge which can make it harder for ML methods to classify the responses. One such method would be to digitize the delay difference obtained at the final stage of an arbiter PUF circuit.

Apart from the methods mentioned here, analog techniques to leverage process variations can prove to be effective in achieving a robust PUF construction.

6.6 Discussion

From the uniqueness results seen above, we can observe that the proposed Secure PUF circuits achieve a high identification capability. Due to the use of secondary PUF structures, the reliability of these circuits is lower than that of standard delay based PUFs. A reliability of 80% would still allow these circuits to be used for authentication applications, but would prove prohibitive for secret key generation applications. In this work, Arbiter PUFs were used to build a Secure PUF structure that would resist machine learning attacks. This architecture can prove to be much tougher to model than current PUF constructions. The concept of using derived challenges could be easily extended to build PUF circuits with different building blocks such as ring oscillators. Use of more reliable stage elements would be a step towards building secure and reliable PUF circuits.

CHAPTER 7

CONCLUSIONS

This thesis looks at the design of Secure Physical Unclonable Functions, lightweight cryptographic primitives that enable reliable authentication of integrated circuits. In the era of ubiquitous computing, hardware security assumes great significance and PUFs prove to be an elegant solution. In this work, we study the design of PUF circuits, their applications and some of the key features that drive PUF design such as uniqueness, reliability, security and energy consumption.

The energy required to generate a challenge response pair is a key design goal for low power applications. In this work, we explore the uniqueness and energy tradeoffs in Arbiter and RO PUF circuits and provide an energy efficient PUF circuit alternative. Arbiter and delay line PUFs offer a significant reduction in the energy per CRP. Further, we look at the benefits of sub-threshold operation and demonstrate the asymptotic improvement in uniqueness as we scale the supply voltage.

In deep submicron technologies, increase in process variations will greatly impact design performance. However, the identification capabilities of PUF circuits will be enhanced with increased process variations. A technology perspective on PUF circuit design is provided in this work by studying the impact of scaling on PUF. Improving trends in uniqueness are shown by analyzing PUF behavior in 45nm, 32nm and 22nm technologies.

In order to validate PUF behavior in silicon, a 64 bit Arbiter PUF circuit with an on chip linear feedback shift register has been implemented on a test-chip and fabricated in 45nm technology. Post silicon validation measurements have successfully demonstrated PUF functionality and the identification capabilities of PUFs in super threshold and sub threshold

modes have been evaluated. The uniqueness improvements indicate the promise of subthreshold operation. However, robust design practices are necessary to tackle lower noise margins and improve subthreshold PUF yield.

Finally, we study the threat of machine learning based software modeling attacks to PUF security. A new class of PUF circuits is proposed whose central theme is the use of challenge inputs derived from a secondary PUF structure. Uniqueness and reliability analysis on these circuits demonstrates strong identification capabilities and sufficiently high reliability. The proposed new architecture can be used with different PUF elements such as ring oscillators. These features make them promising candidates for future applications requiring secure hardware cryptographic primitives.

7.1 Scope for future work

This thesis has explored improvements in uniqueness, energy consumption and a new PUF architecture resilient to machine learning attacks. Better uniqueness or identification can be achieved in PUF circuits through good design practices. Ensuring that there are enough number of devices to leverage process variations, supporting large number of challenge response pairs and symmetric layout design practices improve uniqueness. Subthreshold operation results in further improvements in uniqueness and also provides significantly lower energy consumption. Reliability of PUFs is a main concern especially for secret key generation applications. Future work can look into new directions to analyze the source of reliability errors and achieve 100% reliability in both super threshold and subthreshold operation. As machine learning techniques evolve, there is a continuous need to look at newer PUF architectures that can resist software modeling attacks with minimal area and power overhead.

APPENDIX

PUF SIMULATION METHODOLOGY

Modeling inter-chip variation:

Physical Unclonable Functions leverage inter-chip process variations to create challenge response pairs. Hence it is essential to model these variations to study PUF behavior. Hspice offers the capability to run Monte Carlo simulations on circuits that help us to capture the effects of process variations. Variations in active or passive devices are characterized through distributions, which are typically found to be Gaussian in nature for semiconductor process variations. In each Monte Carlo iteration, random values are assigned to the device parameters adhering to the Gaussian distribution. Vth variations impact circuit delays significantly as compared to variations in passive devices. In this work, inter-chip variation has been captured by modeling Vth variations. This is performed by using the AGAUSS function and the DELVTO parameter. The DELVTO parameter is a numerical delta value added to the nominal threshold voltage of the device. The AGAUSS function generates a Gaussian distribution with a user specified 3 sigma value, which is subsequently used in Monte Carlo simulations to assign random Vth values to devices. The simulations are carried out for 40 different PUF instances to ensure high accuracy of Monte Carlo Simulations. Modeling inter-chip variation allows us to calculate the uniqueness achieved by PUF circuits.

Reliability achieved by the PUF circuit under different environmental conditions is a key metric. In order to evaluate reliability, PUF behavior has to be analyzed for different voltage and temperature conditions. This is accomplished in Hspice by varying the nominal voltage by +/- 10% and operating temperature between -25^{o}C and 85^{o}C.

Post processing data - Extraction of responses, uniqueness and reliability evaluation:

Monte Carlo simulations are expensive in terms of runtime and hence it is essential to run these iterative simulations effectively. This is accomplished through an automated Perl based simulation setup. Running Hspice simulations through Perl scripts helps us change different parameters such as supply voltage and temperature. It also helps in managing the data volume efficiently.

From the simulation data generated by Hspice, extraction of responses, calculation of mean hamming distance and relative hamming distance across PUF instances to determine uniqueness is carried out through Perl scripts. Extraction of responses is carried out by sampling the response signal voltages periodically and determining whether the signal is a 0 or 1. Sampling both the response signal and its complement and checking whether they are of opposite polarities, ensures that our sampling time is correct. Based on the responses extracted from all PUF instances, a Perl script is used to estimate mean, relative hamming distances and standard deviation of the distribution. The number of PUFs to be used for evaluation and number of challenges can be passed as parameters to the script. This helps us analyze the dependence of uniqueness on these parameters.

Similarly to evaluate reliability, bit errors in responses across different operating conditions are determined through Perl scripts. The response bit extracted for each challenge under a given operating condition is compared with the response obtained under nominal case. If they differ, a bit error is recorded.

Flat Hspice netlist creation:

One of the requirements to run Monte Carlo simulations is that the input Hspice netlist should be flat consisting only of device instantiations rather than .SUBCKT instantiations. This is to ensure that each device in the design gets a different value of Vt. However constructing transistor level schematics in Cadence Virtuoso can be quite cumbersome. Further, building bigger PUF circuits such as the RO PUF consisting of large bit width counters and comparators

can be time consuming. The methodology shown below in Figure 40 helps to build PUF circuits faster and create flat Hspice netlists necessary for Monte Carlo simulations.

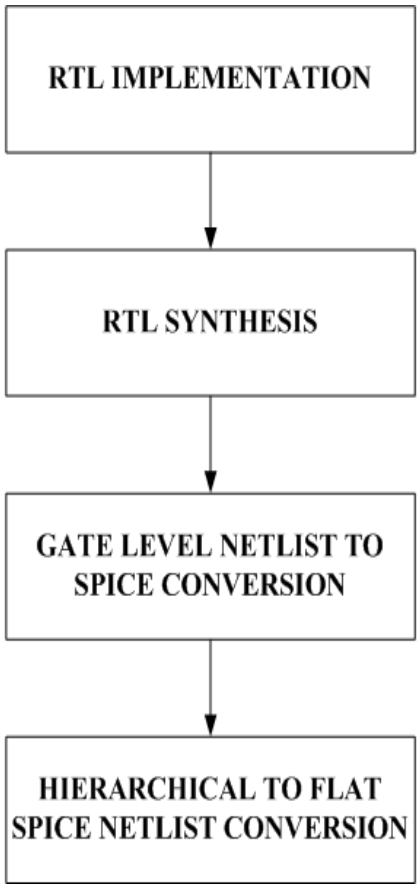

Figure 42. HSPICE netlist creation flow

The PUF circuit is initially implemented in Verilog. The Verilog netlist is taken through RTL synthesis in Synopsys DesignCompiler to obtain a gate level netlist. The gate level netlist is converted to a spice netlist using the netlist translation utility. This process requires us to have standard cell CDL (Circuit Description Language) models available. The resulting Hspice netlist is hierarchical and it is converted to a flat spice netlist using a Perl script. The Perl script replaces the hierarchical instantiations by transistor equivalents. The above mentioned methodology saves considerable amount of time in creating flat Hspice netlists for large PUF circuits.

PUF Circuit Schematic generation:

PUF circuits are typically constructed by cascading N identical stages followed by an arbiter or other response generation circuitry. Since PUF simulation methodology requires flat Hspice netlists, a flat transistor level schematic can be built in Cadence Virtuoso. However this approach is cumbersome and prone to manual errors. An alternative way would be to design the schematic of a basic building block such as the delay stage in Cadence Virtuoso. The N bit PUF schematic can be generated through a Perl script that replicates the single PUF stage N times, creates the appropriate interconnections. Finally, the generated hierarchical or .SUBCKT level netlist can be converted to a flat netlist through scripts. This approach offers several advantages such as ease of implementation and increased flexibility to build different circuits with varying lengths. In this work, Perl scripts were used to create different Secure PUF circuit schematics.

BIBLIOGRAPHY

[1] J.P. Kaps, G. Gaubatz and B. Sunar, "Cryptography on a speck of dust", in Computer, 40(2):38–44, 2007.

[2] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels and T. O'Hare, "Vulnerabilities in First-Generation RFID-enabled Credit Cards", in Financial Cryptography, 2007.

[3] K. Nohl and D. Evans," Reverse-engineering a cryptographic RFID tag", in USENIX Security Symposium, pages 185-193, 2008.

[4] Y. Oren and A. Shamir, "Remote password extraction from RFID tags", in IEEE Transactions on Computers, 56(9):1292-1296, 2007.

[5] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and W. H. Maisel, " Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses", in Proceedings of Symposium on Security and Privacy, pages 129-142, 2008.

[6] A. Juels and S. A. Weis, "Authenticating pervasive devices with human protocols", in Lecture notes in computer science, 3621:293, 2005.

[7] R. S. Pappu, B. Recht, J. Taylor and N. Gershenfeld, " Physical one-way functions", in Science, 297(6):2026-2030, 2002.

[8] B. Gassend, D. Clarke, M. Van Dijk and S. Devadas, " Silicon physical random functions", in Proceedings of the 9th ACM conference on computer and communications security, pages 148-160, 2002.

[9] J.W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, " A technique to build a secret key in integrated circuits with identification and authentication applications", in Proceedings of the VLSI Circuits Symposium, June 2004.

[10] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation", in ACM/IEEE Design Automation Conference, pages 9-14, 2007.

[11] D. E. Holcomb, W. P. Burleson, and K. Fu, " Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers", in IEEE Transactions on Computers, 58(9):1198-1210, 2009.

[12] R. Helinski, D. Acharyya and J. Plusquellic, "A physical unclonable function defined using power distribution system equivalent resistance variations", in ACM Design Automation Conference (DAC), pp. 676-681, 2009.

[13] L. Lin, D. E. Holcomb, D. Krishnappa, P. Shabadi and W. Burleson, “Low power sub-threshold design of secure physical unclonable functions.”, in IEEE International Symposium on Low-Power Design (ISLPED), pp.43-48, 2010.

[14] V. Vivekraja and L. Nazhandali, “Circuit-Level Techniques for Reliable Physically Uncloneable Functions.”, in IEEE International Workshop on Hardware-Oriented Security and Trust, HOST, pages 30-35, 2009.

[15] International Technology Roadmap for Semiconductors, 2006 ITRS report, http://www.itrs.net/Links/2006Update/2006UpdateFinal.htm

[16] D. Lim, “Extracting secret keys from integrated circuits,” M.S. thesis Cambridge, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., May 2004.

[17] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas and J. Schmidhuber, “Modeling attacks on physical unclonable functions”, in ACM Conference on Computer and Communications Security (CCS), pp.237-249, 2010.

[18] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola and V. Khandelwal, ”Design and Implementation of PUF-Based Unclonable RFID ICs for Anti-Counterfeiting and Security Applications”, in IEEE International Conference on RFID, 2008.

[19] B. Gassend, D. Clarke, M.V. Dijk and S. Devadas, “Controlled Physical Random Functions”, in Proceedings of the 18th Annual Computer Security Applications Conference, 2002.

[20] J. Huang and J. Lach, ”IC Activation and User Authentication for Security-Sensitive Systems,” in IEEE International Workshop on Hardware-Oriented Security and Trust, HOST 2008.

[21] L. Kulseng, Z. Yu, Y. Wei and Y. Guan, “Lightweight Mutual Authentication and Ownership Transfer for RFID Systems”, in IEEE INFOCOMM 2010.

[22] L. Bolotnyy and G. Robins, “Physically Unclonable Function -Based Security and Privacy in RFID Systems”, in PerCom 2007.

[23] P.F. Cortese, F. Gemmiti, B. Palazzi, M. Pizzonia and M. Rimondini, “Efficient and Practical Authentication of PUF-Based RFID Tags in Supply Chains”, in IEEE International Conference on RFID-Technology and Applications, June 2010.

[24] C.W. O’Donnell, G.E. Suh and S. Devadas, “PUF-Based Random Number Generation”, in MIT CSAIL CSG Technical Memo 481.

[25] J.A. Roy, F. Koushanfar and I.L. Markov, “EPIC: Ending Piracy of Integrated Circuits”, in Design, Automation and Test in Europe, 2008.

[26] http://www.verayo.com.

[27] http://www.intrinsic-id.com.

[28] W. Zhao and Y. Cao, “New generation of Predictive Technology Model for sub-45nm early design exploration”, in IEEE Transactions on Electron Devices, vol. 53, no. 11, pp. 2816-2823, 2006.

[29] B. Calhoun, S. Khanna, R. Mann and J. Wang, “Sub-threshold circuit design with shrinking CMOS devices”, in IEEE International Symposium on Circuits and Systems (ISCAS), pp. 2541-2544, 2009.

[30] S. Srivathsa and W. Burleson, “Subthreshold design of Physical Unclonable Functions”, in IEEE Subthreshold Microelectronics Conference 2011.

[31] L. Lin, S. Srivathsa, C. Paar and W. Burleson, “45nm Arbiter-Based Physical Unclonable Function Design”, in SRC TECHCON 2011.

[32] L. Lin, S. Srivathsa, D. K. Krishnappa, P. Shabadi and W. Burleson, “Design and Validation of Arbiter-Based PUFs for Sub-45nm Low-Power Security Applications”, submitted to IEEE Transactions on Information Forensics and Security.

[33] M. Majzoobi, F. Koushanfar and M. Potkonjak, “Lightweight Secure PUFs”, in IEEE International Conference on Computer-Aided Design, 2008

[34] S. S. Kumar, J. Guajardo, R. Maes, Geert-Jan Schrijen and P. Tuyls, “Extended Abstract: The Butterfly PUF Protecting IP on every FPGA”, in IEEE International Workshop on Hardware-Oriented Security and Trust, HOST 2008.

[35] Ahmad-Reza Sadeghi and D. Naccache, ”Towards Hardware-Intrinsic Security”, Springer, 1st Edition, 2010.

[36] M. Majzoobi and F. Koushanfar, ”Time-Bounded Authentication of FPGAs”, in IEEE Transactions on Information Forensics and Security, 2011.

[37] Predictive Technology Model (PTM), Arizona State University (ASU), http://www.eas.asu.edu/~ptm/