PUFS – AN EXTENSIVE SURVEY

by

Yamini Ravishankar

A Thesis
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
The Requirements for the Degree
of
Master of Science
Computer Engineering

Committee:

_____	Dr. Jens-Peter Kaps, Thesis Director
_____	Dr. Kris Gaj, Committee Member
_____	Dr. Alok Berry, Committee Member
_____	Dr. Monson H. Hayes, Chairman, Department of Electrical and Computer Engineering
_____	Dr. Kenneth S. Ball, Dean, Volgenau School of Engineering

Date: _____ Summer Semester 2015
George Mason University
Fairfax, VA

PUFs – An Extensive Survey

A Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at George Mason University

by

Yamini Ravishankar
Bachelor of Technology
SASTRA University, 2012

Director: Jens-Peter Kaps, Associate Professor
Department of Computer Engineering

Summer Semester 2015
George Mason University
Fairfax, VA

DEDICATION

This is dedicated to my loving parents Shri. G.V. Ravisankar and Smt. S. Vijaya, beautiful sister Harini and my beloved fiancé Vasanth for their moral support and belief in me.

ACKNOWLEDGEMENTS

I would first like to thank my advisor Dr. Jens-Peter Kaps for giving me the opportunity to work on this thesis under him. Thank you for your valuable inputs and continuous guidance for the research and for your support during the schedule changes from my side.

I would also like to thank Dr. Kris Gaj for initially suggesting this research area for the course project in ECE646. Since then, the meetings with Dr. Kaps and Dr. Gaj have significantly improved my learning curve. The cryptography and hardware design courses helped me refine my analysis skills and thought process for approaching issues. Thank you all for molding me into the person that I am today.

I extend my sincere gratitude towards Dr. Alok Berry for being a mentor, and for his valuable advice at the personal, academic and professional levels.

I am really glad to have been part of the Cryptographic Engineering Research Group (CERG), and am thankful to all its members for the warm smiles and moral support to help get through the semesters. Thank you Bilal for your inputs and for helping me ramp up on PUFs initially.

A special thanks to Ms. Cynthia Ballentine for my first job as a Lab Assistant and being such a lovely person.

I am very grateful to my close friends, cousins and relatives for their words of hope and prayers and for always being there for me. I am also thankful to my laptop for putting up with me over the past six years during my under-graduate and graduate studies.

Finally, I extend my deepest gratitude towards God for guiding me like a polestar, through thick and thin and for keeping me grounded during success and failure.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF EQUATIONS

LIST OF ABBREVIATIONS

Advanced Encryption Standard ..... AES
Application Specific Integrated Circuit ..... ASIC
Arithmetic Logic Unit ..... ALU
Artificial Neural Networks ..... ANN
Butterfly PUF ..... BPUF
Built-In Self Test ..... BIST
Configurable Logic Blocks ..... CLB
Configurable RO-PUFs ..... CRO-PUFs
Differential Sequence Coding ..... DSC
Dynamic Random Access Memory based PUF ..... DRAM-PUF
Error Correcting Codes ..... ECC
Field Programmable Logic Arrays ..... FPGA
D-Flip-Flop based PUFs ..... DFF-PUF
Hamming Distance ..... HD
Hardware Intrinsic Security ..... HIS
Helper Data Algorithm ..... HDA
Hidden Markov Model ..... HMM
Integrated Circuit IC
Integrated Circuit Identification ..... ICID
Intellectual Property ..... IP
Kendall Syndrome Coding ..... KSC
Look-Up Table ..... LUT
Longest Increasing Subsequence-based Grouping Algorithm ..... LISA
Metal-Oxide Semiconductor Field-Effect Transistor ..... MOSFET
Non-Volatile Memory ..... NVM
Physical One-Way Function ..... POWF
Physical One-Way Hash Function ..... POWHF
Physical Unclonable Function ..... PUF
Public-Key ..... PK
Radio-Frequency Identification Device ..... RFID
Ring-Oscillator based PUFs ..... RO-PUFs
Sequential Pairing Algorithm ..... SPA
Static Random Access Memory based PUF ..... SRAM-PUF
Transient Effect RO-PUF ..... TERO-PUF
Very Large Scale Integrated Circuits ..... VLSI

ABSTRACT

PUFS – AN EXTENSIVE SURVEY

Yamini Ravishankar, M.S.

George Mason University, 2015

Thesis Director: Dr. Jens-Peter Kaps

Physical Unclonable Functions (PUFs) offer a promising solution to the issue of secure key generation on chips for cryptographic applications. For a given challenge, PUFs generate a response, unique to the device based on its inherent manufacturing variations, which is why PUFs are the biometrics of Integrated Circuits (ICs). Ring-Oscillator based PUFs (RO-PUFs) are a type of Silicon-based PUF that exploit the delay in interconnects and components of the design to generate unique keys. Configurable RO-PUFs (CRO-PUFs) reduce the number of ROs needed to generate a key of a given length compared to the RO-PUFs.

This thesis is an extensive survey of the history of PUFs – implementations and applications, and the evaluation, post-processing and attack methodologies. A CRO-PUF exploiting the delay of latches in the Configurable Logic Blocks (CLBs) of Spartan6 FPGAs was implemented on 20 Nexys3 boards. The statistical properties of the obtained responses indicated a Steadiness of 94.6% and a Uniformity of 46.7% respectively. A

novel proposal of using Hidden-Markov Models for post-processing of PUF responses for increased reliability is being made as a result of cross-disciplinary study of biometrics with hardware cryptography.

1. INTRODUCTION

The strength of any cryptographic implementation depends on the secrecy of the encrypting key or device identifier. Compromise on the secrecy of the key can result in the compromise of confidential information and breach of authentication protocol. Thus, the generation and storage of keys or identifiers is of prime importance to its security. Keys stored on non-volatile memory are vulnerable to attacks. Physical Unclonable Functions (PUFs) are the primitives which when implemented on Integrated Circuits (ICs) can generate unique and reliable keys without the need for secure storage on Non-Volatile Memories (NVM). Secure and low-cost key storage, unclonability, tamper resistance, randomness in responses are some advantages of using PUFs as security primitives.

1.1. Biometrics of Integrated Circuits

Biometric authentication is a means of identifying individuals based on their inherent characteristics like DNA, fingerprints, iris, retina, voice, ear, face, or signature. These characteristics are unique to every individual and hence nearly impossible to clone.

Similarly, silicon devices have unique inherent characteristics such as physical variations, frequency variations, etc. which can be exploited to uniquely identify them. A Physical Unclonable Function (PUF) is a challenge – response mechanism in which the mapping between a challenge (the stimulus) and the corresponding response (reaction of the PUF) is dependent on the complex and variable nature of the physical material. Unique Challenge-Response Pairs (CRPs) can be generated for the identification and

authentication of each IC, ie. the same challenge, when applied to different PUF instances, results in exclusive responses as shown in Fig.1. Thus, PUFs serve as the biometrics of Integrated Circuits.

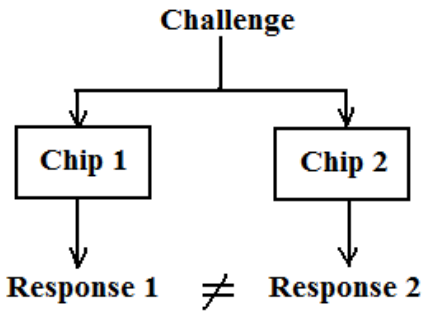

Figure 1. Uniqueness of CRPs from two different ICs

The three main qualities that make PUFs analogous to Biometrics are individualism, inherency and unclonability [Mae12].

1.2. Why Unclonable?

Any system is said to be truly unclonable if it exhibits the properties of physical and mathematical unclonability. PUFs have an unpredictable way of mapping the challenges to the responses based to the structural disorder of the IC and hence are Physically Unclonable. This complex-interaction of the challenge with the random components in ICs results in stochastic Challenge-Response Pairs (CRPs) which cannot be modeled, thus leading to Mathematical Unclonability. Thus, a PUF is truly unclonable.

1.3. Applications of PUFs

Since their formal introduction in the early 2000s, the applications of PUFs in the field of hardware cryptography have increased manifold based on the different PUF constructions. I start this thesis with the many applications of PUFs proposed in literature to emphasize their importance.

1.3.1. Key Generation and Storage

Key generation and storage are indispensable in a vast majority of cryptographic implementations. The requirements for secure key generation and storage as given by [Mae12] are that

a. Generated keys should be unique and unpredictable, and
b. The memory that stores the keys should be reliable and must shield the keys from unauthorized access.

PUFs satisfy both these conditions because the randomness is intrinsically present in the device and the need for a protected non-volatile memory for secure key storage is avoided since keys can be generated on-the-fly and depend on the device. Another advantage is that PUFs are capable of generating keys for both symmetric and asymmetric cryptographic operations [SD07]. Thus, cryptographic key generation is a significant application of PUFs. A number of PUF based key generation techniques [TS06, GKST08, GSTK$^+$09] have been proposed based on pattern matching [PD11], combination with fingerprints [HST10], recombination [YD10a].

1.3.2. Random Number Generators

Since the inherent nature of the PUF results in outputs that are random, PUFs could be used in random number generation. Some PUF based Random Number

Generators (RNG) have been implemented in literature [MNRS09, LSSTH12, AMSST10]. PUF-Pseudo-Random Functions (PUF-PRFs) were proposed in [AMSST10] for use as cryptographic primitives.

1.3.3. IP Protection

Intellectual Property (IP) protection is a major area of security research since any breach in the IPs of companies would lead to tremendous losses for the company. PUF protocols addressing the IP protection problem, with an emphasis on Public-Key cryptographic primitives have been proposed [GKST07a, GKST07b, GKST08]. Digital reconfigurable PUFs [ZP14] and PUF-Finite State Machine (FSM) based binding mechanisms [ZLLQ15] are also used to enforce IP protection.

1.3.4. Secure Microcontrollers and Processors

PUF implementations on ICs result in secure authentication and tamper-resistance. Secure microcontrollers and processors have been implemented to test their functionality and use in [SDSD05, BHP11, MS12, HSKV13].

1.3.5. Radio-Frequency Identification Device (RFID)

The RFID technology embeds a chip on a physical object to uniquely identify the object. These have proven to be indispensable in applications including travel cards, identification cards, tracking of animals, and so on. The use of PUFs as RFID tags has been proposed and tested in [TS06, DSPSZK08, KKLSSW11] with the advantage of unclonability.

1.3.6. Hardware Obfuscation of Logic

Hardware obfuscation of logic is used for IP protection wherein PUF based logic can be configured as arbitrary logic to thwart IC reverse engineering. Signal path

obfuscation and direct replacement of arbitrary logic using PUFs are proposed for hardware obfuscation of logic [WP14]. This is a relatively new application for PUFs.

1.3.7. Remote Attestation Schemes

Remote Attestation is an authentication method for hardware and software using a remote server. This enables a remote system to determine the level of integrity of another system. PUFatt is a new lightweight remote attestation scheme impersonation attacks because of the hardware-software binding in Arithmetic Logic Unit based PUFs

1.3.8. Vehicular Security

Vehicular security concerns with the IP protection in vehicles, modification of in-vehicle systems and its misuse with the normal vehicular operation in addition to the theft of the vehicle. [AGKT09] discusses in detail the application of PUFs for vehicular security, components identification and authentication.

1.3.9. Wireless Sensor Network Security

Wireless Sensor Networks (WSNs) provide a low cost solution to deploy large sensor arrays for military and civilian tasks. The storage and power limitations, unreliable communications and unattended operation pose security risks for the WSNs [LZLL14]. WSNs use Dynamic Random Access Memory (DRAM) as memory elements and hence [LZLL14] proposes the use of DRAM-PUFs for increasing security of WSNs.

PUFs can be used for licensing and certification applications and for building secure smart cards [GCDD02b], and also for remote services/features activation [GKST08].

Hence, the generation of a secure key/identifier from a PUF is a major concern since all applications make use of the intrinsic device variations. The security and

reliability of the generated key is of prime importance. Hence, a cross disciplinary study involving biometrics might lead to interesting methods of improving the statistical properties.

2. PHYSICAL-UNCLONABLE FUNCTIONS

The device mismatch between two ICs, based on the variations in the drain currents across an array of MOSFETs with common source and gate was proposed for IC Identification (ICID) [LDT00]. The basis for modern PUFs was laid by [Pap01] based on optically variable devices to derive unique and tamper-resistant identifiers at a very low cost. This work introduced the concept of physical one-way functions (POWFs) and physical one-way hash functions (POWHFs) as cryptographic primitives. It was later found that the intrinsically tamper-resistant microstructure of a medium's disordered structure can be converted to a fixed-length of binary digits for use as Physical One-Way Functions [PRTG02]. These led to the proposal for capitalizing on the inherent manufacturing variations of an Integrated Circuit as a Silicon Physical Unclonable Function (PUF) [LDT00, GCDD02b].

2.1. Basic Classification of PUFs

PUFs have been proposed on various technologies and materials. [Mae12] classifies the PUF constructions based on

1. Electronic nature of identifying features as
    a. Non-electronic PUFs – wherein the non-electronic nature of materials is the basis for identification. For example – optical PUFs,

b. Electronic PUFs – wherein the random variations in electronic characteristics like resistance and capacitance are used, For example, Silicon PUFs.

2. Construction property as
    a. Intrinsic PUFs – which are inherently present in the device due to manufacturing variations [GKST07a], and
    b. Non-intrinsic PUFs – wherein the PUF is externally evaluated or random features are explicitly introduced,
3. Security of challenge-response behavior as
    a. Strong PUFs – wherein the CRP set size grows exponentially with the PUF size and
    b. Weak PUFs – wherein the growth in the CRP set size is linear with the PUF size.

Intrinsic PUFs can be further classified based on their operating principles [Mae12] as

1. Delay-based PUFs – which measure the random variations on the delay of a digital circuit. This includes Arbiter-PUFs, Ring-Oscillator based PUFs and Glitch PUFs,
2. Memory-based silicon PUFs – which use random parameter variations called device mismatch. This includes Static Random Access Memory based PUFs (SRAM PUFs) and Dynamic Random Access Memory based PUFs (DRAM PUFs),

3. Mixed-signal circuits-based PUFs – which quantizes an analog signal to produce a digital response, for example, ICID – threshold voltage PUF and Inverter Gain PUF.

2.2. PUF Constructions

2.2.1. Silicon Based PUFs

Silicon PUFs form a major class of subclass of electronic PUFs. These exploit the manufacturing process variations in the logic and interconnects present in a chip to derive the CRPs. The first practical realization of Silicon PUF was done in [GCDD02b]. The main advantage of using Silicon-based PUFs for cryptographic implementations is that they can be readily deployed in digital circuits on chips. The various silicon PUF constructions proposed in literature have been summarized below in an alphabetical order, with emphasis on Ring-Oscillator based PUFs.

Anderson PUF

Anderson cells, as shown in Fig.2, form the primitives of the Anderson PUF [BBM15], a glitch based PUF. These cells produce logic-0 or logic-1 as output due to manufacturing variations only and do not require a challenge to generate a response. Thus, these can be used only for a single signature generation. The delay difference between the two pairs of shift-registers and multiplexers generates the glitch required for the operation of the Anderson PUF.

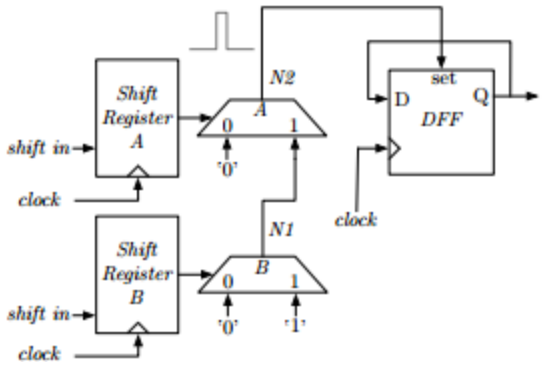

Figure 2. Logic schematic of Anderson PUF cell

Arithmetic Logic Unit Based PUF

Arithmetic Logic Unit based PUF (ALU-PUF) [KKPSW14] is a novel PUF design based on the delay difference caused by manufacturing variations in two ALUs or other logic components available in a processor as shown in Fig. 3. This can be designed with a very low overhead when the redundant components in a processor are made use of. The design and working of the ALU-PUF is similar to that of the Arbiter PUF.

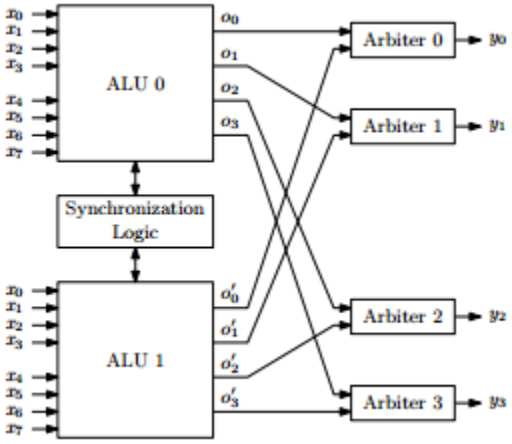

Figure 3. ALU PUF generating 4-bit responses

Arbiter PUF

Arbiter PUF is a delay-based silicon PUF in which the output bit is determined by an arbiter circuit which resolves a race between two symmetrical digital paths in a circuit. When the circuit is designed to be perfectly symmetrical, the output bit of the arbiter is stochastic in nature and depends only on the manufacturing variations. [LLGSDD04] proposed the first Arbiter-PUF design implementation based on the delay paths between two switch blocks as shown in Fig.4.

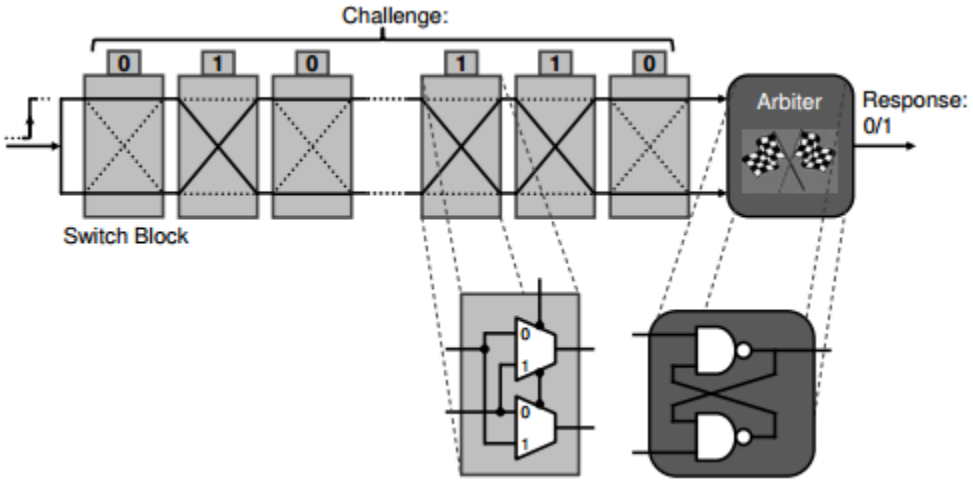

Figure 4. Basic arbiter PUF construction

The two conditions required for the optimal design of an Arbiter PUF are given by [Mae12] as

1. Delay lines should be perfectly symmetrical and
2. Arbiter circuit should be unbiased

An asymmetric routing of the delay lines will lead to the circuit being biased towards a particular output bit since the signal passing through the shorter delay line would reach the arbiter faster. An arbiter-based PUF exploiting Programmable Delay Lines (PDL) to cancel out delay skews due to asymmetries in routing was proposed [MDK10]. The basic SR-latch was proposed for use in Arbiter PUF [LHKSB10] due to its symmetric construction and unbiased nature.

Buskeeper PUF

A Buskeeper is a weak latch with no control signals as shown in Fig. 5. On-chip buses with multiple drivers lead to an increased power consumption when these buses are in a floating state. Buskeepers prevent this scenario by maintaining the last driven state of the bus, when added to the circuit. It is functionally equivalent to a D-latch when Vdd is connected to the enable signal.

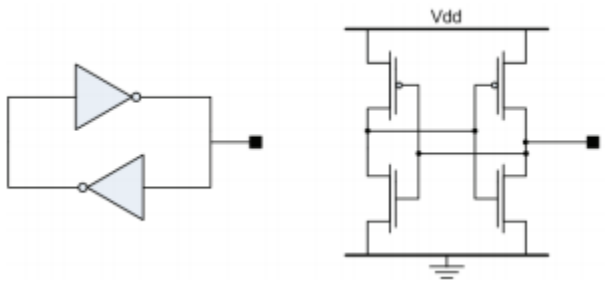

Figure 5. High-level Buskeeper cell (left) and transistor level (right)

Buskeeper PUF is a memory-based PUF construction using Buskeeper as primitives, similar to the D Flip-flop PUF (DFF-PUF) (described below). Experiments

[SSL12] prove that Buskeeper PUFs have a better reliability and uniqueness compared to DFF-PUFs and hence were proposed as their alternative.

Butterfly PUF

A cross-coupled circuit stores a bit value using a positive-feedback loop, and hence is widely used as building blocks of storage elements like latches, flip-flops and SRAM memories. The underlying concept of Butterfly PUF (BPUF) [KGMST08] is to design cross-coupled circuits in FPGAs which behave similar to SRAM cells. This was achieved by cross-coupling latches as shown in the Fig. 6

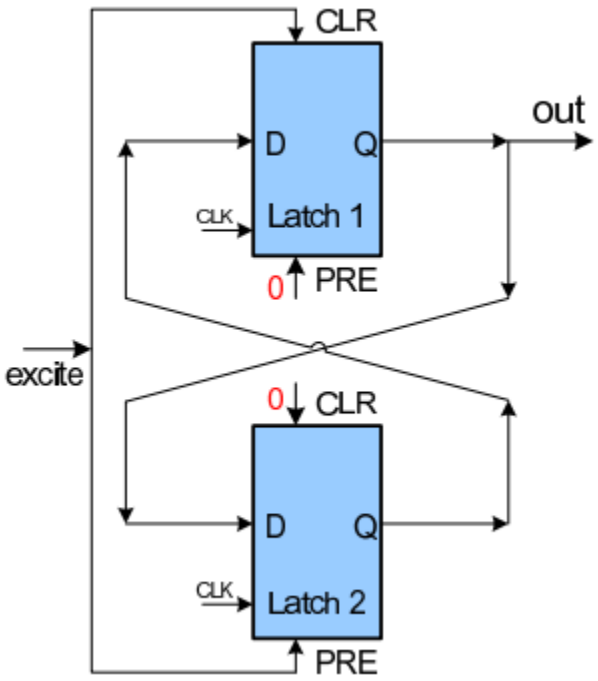

Figure 6. Buttefly PUF using cross-coupled latches

Composite PUF

A composite-PUF [SSM14], constructed with smaller PUFs as building blocks has a larger challenge-space and superior quality metrics than its constituents. For example, Fig. 7 shows six composite PUF designs composed of Arbiter PUFs and Ring Oscillator based PUFs with 64-bit challenges and 1-bit response each.

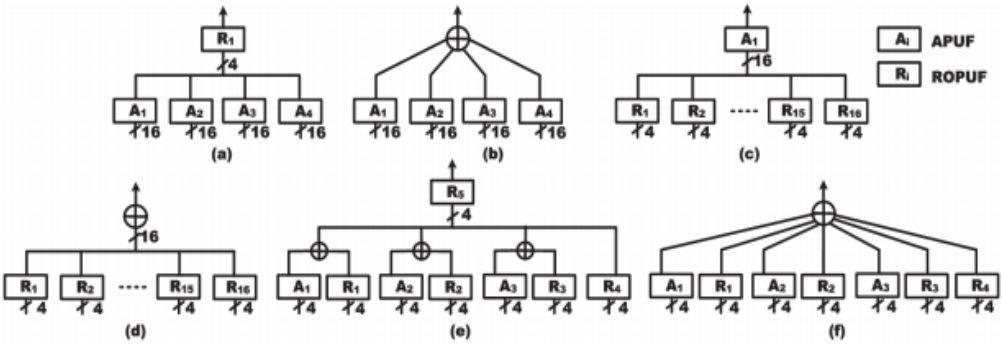

Figure 7. Examples of Composite PUF

DRAM PUF

Dynamic Random Access Memory (DRAM) is a type of volatile memory. The decay time for the different bit storage elements vary due to manufacturing effects and this concept is being exploited for its use as DRAM PUFs [LZLL14]. DRAM cells are a main constituent of the Wireless Sensor Networks (WSN) and hence the DRAM-PUFs are proposed to provide a solution to the security issue of WSNs.

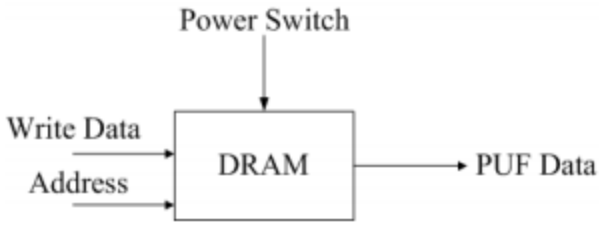

Figure 8. Schematic of DRAM PUF

Erasable PUF

The concept of Erasable-PUFs was proposed in [DR14a]. These are Strong PUFs wherein single responses can be erased from the PUF without affecting any of the other responses. A proof-of-concept implementation is pending for this type of PUF.

Flip-Flop Based PUF

The Flip-flop based PUF [MTV08] uses the powerup values of flip-flops of FPGAs similar to SRAM PUF. The main advantage of this type of PUF is that these can be implemented on FPGAs while SRAM PUF cannot because of the initial reset of SRAM-cells.

Logically Reconfigurable PUF

In a Logically Reconfigurable PUF (LR-PUF) [KKLSSW11], the challenge-response pairs depend both on the physical properties of the PUF and the logical state of a control logic. Dynamic reconfigurability is achieved by updating the state of the control logic.

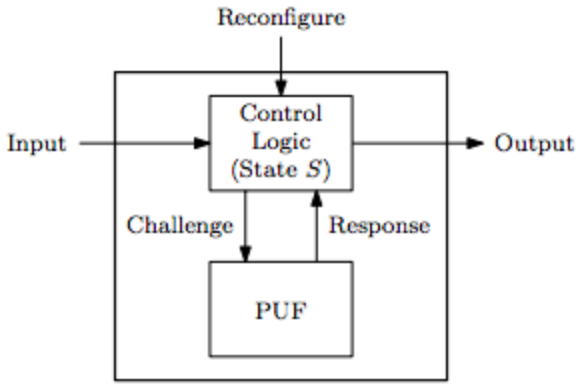

Figure 9. LR-PUF concept

Memristor PUF

The relationship between the flux and electric charge in memristors are similar to the relation between voltages and currents in fundamental circuit elements. The process variation dependent switching delays form the basis of Memristor-PUF demonstrated in [MRF15] as a single-bit Memristor-PUF.

MRAM PUF

MRAM is a nonvolatile magnetoresistive memory with a diverse range of applications. The unique energy-tilt resulting from the random geometric variations in the MRAM cells can be exploited as MRAM-based PUF with very high entropy [DSRBB15].

Quantum-Readout PUF

[Sko09] proposed a new type of security primitive – the Quantum Readout PUF (QR-PUF) which can be read out using quantum states, i.e. the challenge-response pairs are quantum states. It is based on the three physical assumptions namely – physical

unclonability, physical uniqueness and quantum-computational unclonability. [Sko13, SMP13] analyze the security of QR-PUF schemes. [SMP13] also focusses on challenge estimation attacks on QR-PUFs.

Reconfigurable PUF

The concept of PUF primitives capable of transforming themselves into completely new PUFs, with challenge-response pairs different from that of the original PUF is called Reconfigurable PUFs (rPUFs) [KSSST09].

Ring-Oscillator Based PUF

A basic ring-oscillator structure is shown in Fig. 10. The RO consists of an odd number of inverters connected in a loop which results in oscillations in the circuit. The frequencies of operation of two identical ROs vary due to process variations and are unique to each RO. This property of ROs is being exploited to implement the Ring-Oscillator based PUFs (RO-PUFs), proposed by [GCDD02b].

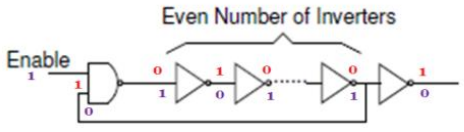

Figure 10. Basic Ring-Oscillator

The RO-based PUF structure is shown in Fig. 11. An array of identical Ring-Oscillators implemented on a chip will have frequency variations unique to each RO. The frequency difference between pairs of frequencies is used to characterize the device and

to generate the unique ID. The oscillations produced by one RO influence the oscillations of another RO if they operate at the same time. Thus, frequency measurements are to be made by turning off all ROs other than the one being measured. Multiplexers and counters are used to select a particular RO and measure its frequency (number of oscillations).

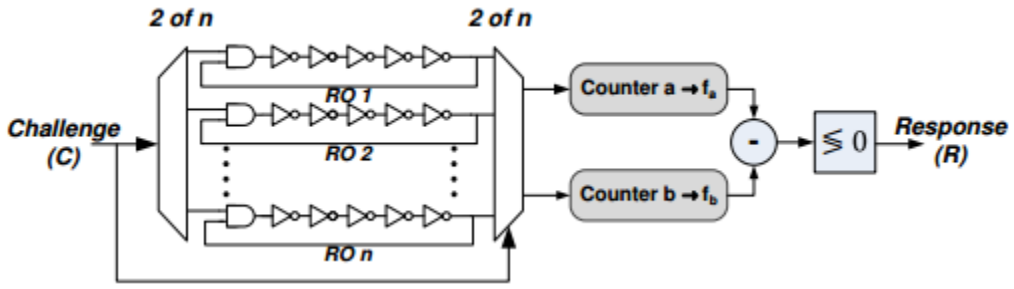

Figure 11. Ring-Oscillator PUF circuit

Configurable ROs [Mai12] have multiple loops in the same RO structure which result in multiple configurations for a single RO. This results in a redundancy of responses which help increase the reliability of the circuit because the configuration with the highest frequency difference can be selected for measuring oscillations.

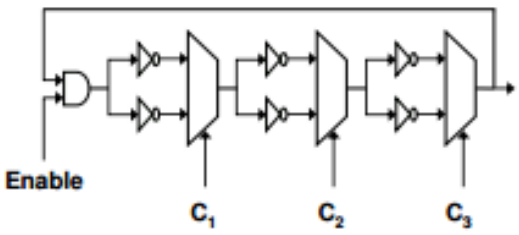

Figure 12. a. Configurable RO,

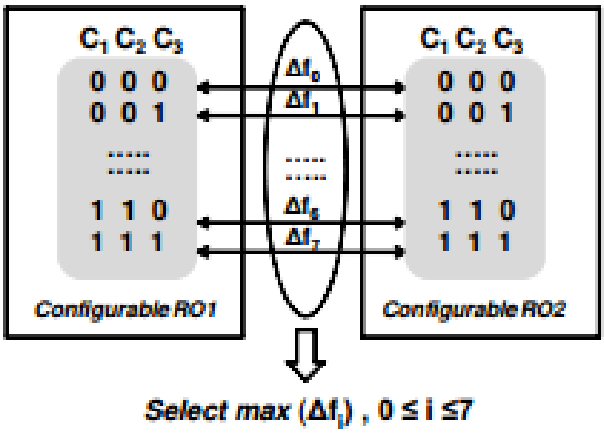

Figure 12. b. Selection of RO pair

Configurable RO-based PUF designs with chain-like mapping strategy [MS09b] for physical placement of oscillators offers a highly efficient solution for PUF reliability issue. An improvement over [MS09b] was proposed in [XKG11] which generates more IDs for the same area as used in the former. [MS11, MKS12] proposes compensation techniques (placement strategy and RO-pairs selection) to significantly improve the uniqueness and the CRPs of the RO-based PUFs. [HGK13] exploits the programmable delays of FPGA LUTs to generate additional bits of an identifier (ID) for a CRO-based PUF.

SRAM PUF

Static Random Access Memory (SRAM) is a memory technology that uses bistable circuits and is built with six MOSFET transistors. The start-up values in SRAM-cells vary inherently and are exploited in the construction of SRAM-PUFs. These are the PUFs with commercially available applications because of their ease of implementation.

The drawback of using SRAM-PUFs is their vulnerability to physical attacks and high manufacturing cost. Various SRAM-based PUF constructions with varied applications have been proposed [GKST07a, GKST07b, GKST08]. describe different SRAM-PUF and Intrinsic PUF constructions respectively because of their presence in current FPGAs. [CDHS12] provides an analytical model for Start-Up Values (SUVs) of an SRAM PUF based on Static Noise Margin (SNM).

Sense-Amplifier PUF

Sense-Amplifiers (SA) are clocked circuits that amplify very small differential voltages into full swing digital values. Variations in device characteristics of a sense amplifier result in a bias. These variations are used to build the Sense-Amplifier PUF with very low Bit-Error Rates [BM14].

SuperPUF

The concept of a SuperPUF [WYM14] is to integrate the on-chip entropy components distributed across the chip. This significantly reduces the wiring in the design resulting in low area overhead.

2.2.2. Ring-Oscillator Based PUF Constructions

Inverter-Based RO-PUF

The RO-based PUF utilizes multiple inverters (odd in number) to generate the oscillations. The inverter-based PUF [GLQ14] is a novel configurable RO-PUF framework which utilizes a single inverter to produce the oscillations, significantly reducing the hardware cost.

Transient Effect RO-PUF

The Transient Effect Ring Oscillator (TERO) consists of an SR flip-flop with the S and R inputs connected to the same signal (here, ctrl signal), as shown in Fig. 13. Rising edge of the clock results in transitory oscillations in the TERO loop which stop after a short period of time due to intrinsic asymmetry. This phenomenon called oscillatory metastability is used for the construction of the TERO-PUF [BNCF13].

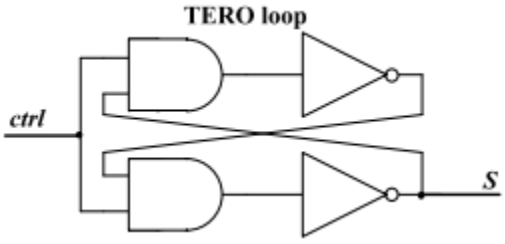

Figure 13. TERO loop

Ordering-Based RO-PUF

Sequential Pairing Algorithm (SPA) and Longest Increasing Subsequence-based Grouping Algorithm (LISA) are two effective secret extraction algorithms for RO-PUFs [YQ10]. PUFs in which the Grouping algorithms are used for error correction are called as Ordering-based PUFs. Ordering-based PUFs with the CRP enhancement schemes proposed in [KPD14] yield optimally robust and highly efficient PUF circuits with a large number of Challenge-Response Pairs [KPD15].

ARO-PUF

The aging-resistant RO-PUF [RFFT14] mitigates the effects of NBTI (Negative-bias temperature instability) and HCI (Hot-Carrier Injection) by deactivating the PUF when it is not in use. This significantly reduces the aging of the PUF.

2.2.3. ASIC-based PUF Constructions

Fewer PUF implementations have been proposed on Application Specific Integrated Circuits (ASICs) than on FPGAs due to the high cost involved. [YMSD11, YSSMD12] evaluate an integrated ASIC implementation of a PUF-based key storage with integrated error correction.

[MV10, RWPK14] provide an extensive analysis of the available PUF constructions and reveal interesting future directions. [BH12] is a systematic overview of PUFs including the theoretical background, different silicon PUF realizations and issues pertaining to the implementation of PUFs in ICs. [HYKD14, RH14] provides a systematic survey on the implementations, attacks, error correction techniques and applications as security primitives for strong-PUFs and weak-PUFs. [CLB12, MRVKSL12] offer a comparative analysis of SRAM PUFs and D Flip-Flop based PUFs (DFF-PUFs) in the 65nm. Six different PUF constructions, including SRAM-PUF and Bus-keeper PUFs were implemented and compared using the silicon characterization vehicle [MRVKSL12].

3. EVALUATION OF PUFS

3.1. Need for Metrics

Metrics are required to evaluate the performance of different types of PUFs and to standardize the security requirements expected from the PUFs.

3.2. Metrics Defined in Literature

[Mai12, HYKS10] have proposed various metrics based on the statistical properties of the responses because binary PUF responses are obtained from every PUF irrespective of the technique used. [Mai12] proposed three dimensions for the PUF measurements along three axes namely device, space and time as shown in Fig. 14. The device axis captures the inter-chip variations in the PUF responses while the other two capture the intra-chip variations.

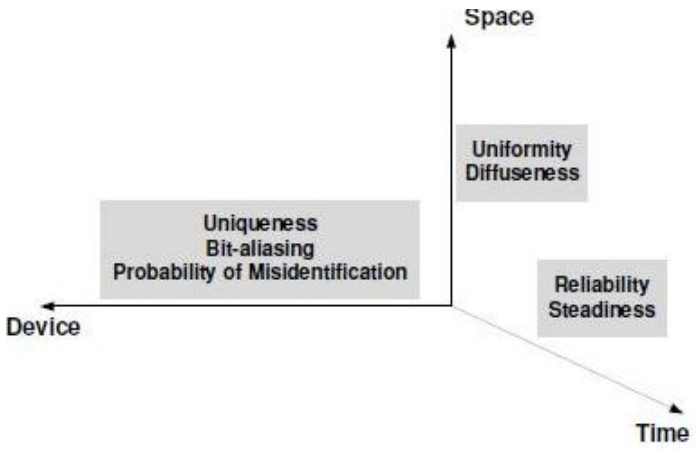

Figure 14. Dimensions for the metrics

The main metrics defined are

- Uniqueness
- Bit-Aliasing
- Uniformity
- Randomness
- Reliability
- Correctness
- Steadiness

3.3. Notations for the Metrics

Table 1. Notations

N	Total number of Chips analyzed
n	Index of a Chip (range 1 to N)
M	Total number of ROs
K	Total number of Identifiers (IDs) generated per Chip
k	Index of an ID in a Chip (range 1 to K)
T	Total number of Samples measured per ID
t	Index of a Sample (range 1 to T)
R	L-bit Response from the PUF
r	l^{th} bit of the Response R

Hamming Distance

Hamming Distance (HD) between two responses is the number of bits that are different between the two responses. For example, the HD of two vectors that have the same values, eg. “1010” and “1010” is 0, while the HD of “1010” and “0101” is 4.

3.4. Definition of the Metrics – Device Axis

3.4.1. Uniqueness

Uniqueness is the average inter-chip Hamming distance (HD) computed across a group of chips. It gives an estimate of the inter-chip variation in terms of the PUF responses. Both Maiti et al. [Mai12] and Hori et al. [HYKS10] have defined uniqueness and their expressions only differ by a scaling factor.

According to Maiti et al., the uniqueness is given by

Equation 1. Uniqueness [Mai12]

$$\text{Uniqueness} = \frac{1}{KL}\frac{2}{N(N-1)}\sum_{k=1}^{K}\sum_{l=1}^{L}\sum_{i=1}^{N-1}\sum_{j=i+1}^{N} r_{i,k,l} \oplus r_{j,k,l}$$

According to Hori et al., the uniqueness is given by

Equation 2. Uniqueness [HYKS10]

$$\text{Uniqueness} = \frac{1}{KL}\frac{4}{N^2}\sum_{k=1}^{K}\sum_{l=1}^{L}\sum_{i=1}^{N-1}\sum_{j=i+1}^{N} r_{i,k,l} \oplus r_{j,k,l}$$

The ideal value of uniqueness according to [Mai12] is 50%, which indicates that 50% of the bits between the PUF responses of any two different chips are different. The ideal value according to [HYKS10] is 100%. Discrete Cosine Transform (DCT) can be used in the post-processing of RO-PUFs [GI14] to de-correlate the RO outputs, to improve the uniqueness of the response and to increase the number of extracted bits.

3.4.2. Bit-Aliasing

Bit-aliasing [Mai12] estimates the bias of a particular response bit across several chips. It is defined as the Hamming-Weight of the l-th bit of the identifier across k-devices and is given by

Equation 3. Bit-Aliasing

$$(\text{Bit} - \text{Aliasing})_{k,l} = \frac{1}{N}\sum_{n=1}^{N-1} r_{n,k,l}$$

The ideal value is 50% which means that the bit is neither biased towards a logic-1 nor a logic-0.

3.5. Definition of the Metrics – Space Axis

3.5.1. Uniformity

For a response to appear random there should be an almost equal distribution of 1's and 0's in it. Thus, uniformity measures the proportion of 0's and 1's in the response bits of a PUF. Uniformity, as defined by [Mai12] is calculated as the percentage Hamming Weight of the n-bit response and is given by

Equation 4. Uniformity

$$\text{Uniformity} = \frac{1}{KL}\sum_{k=1}^{K}\sum_{l=1}^{L} r_{n,k,l}$$

Ideal value for Uniformity is 50%, that is, there should be an equal number of logic-0 and logic-1 in a response for it to appear random.

3.5.2. Randomness

Randomness [HYKS10] is very similar to the Uniformity metric. Randomness indicates the balance of 0's and 1's in the response bits of the PUF. It is given by

Equation 5. Randomness

$$\text{Randomness} = -\log_2 \max(p_n, 1-p_n)$$

$$\text{where } p_n = \frac{1}{KTL}\sum_{k=1}^{K}\sum_{l=1}^{T}\sum_{l=1}^{L} r_{n,k,t,l}$$

The difference between Correctness and Randomness is that the latter also considers the distribution of response bits over T samples. The ideal value is 100%. [MN14] proposed the Random Patch Mixer (RPM) scheme as a solution to the issue of computational cost as well as to improve the frequency distribution randomness.

3.6. Definition of the Metrics – Time Axis

3.6.1. Reliability

The reliability metric [Mai12] gives an estimate of how reliable the response bits are under varying operating conditions. It is the average value of the intra-chip Hamming Distance and is given by

Equation 6. Reliabililty

$$\text{Reliability} = 1 - \frac{1}{KTL}\sum_{k=1}^{K}\sum_{l=1}^{T}\sum_{l=1}^{L} r_{n,k,l} \oplus r_{n,k,t,l}$$

The ideal value for reliability is 100% which means that at any given time, the response bits should be constant. The reliability of the PUFs can be increased by

a. Filtering out the unstable challenge-response pairs based on a stable response signal during the enrollment phase [DB14b],
b. Offsetting the frequency values to be higher than a given threshold (Frequency-Offset algorithm - [TLZ14]).

3.6.2. Correctness

Correctness [HYKS10] is a metric similar to reliability. It is defined as the sum of the Hamming Distances normalized by T, K and L. It also gives an estimate of how correct the response will be under different conditions. It is given by

Equation 7. Correctness

$$\text{Correctness} = 1 - \frac{2}{KTL}\sum_{k=1}^{K}\sum_{l=1}^{T}\sum_{l=1}^{L} r_{n,k,l} \oplus r_{n,k,t,l}$$

Equation 8. Relation between Reliability and Correctness

$$\text{Correctness} = (2 \times \text{Reliability}) - 1$$

The ideal value is 100%.

3.6.3. Steadiness

Steadiness [Mai12] refers to the degree of bias of a response bit towards ‘0’ or ‘1’ over T samples. Steadiness is given by

Equation 9. Steadiness

$$\text{Steadiness}_n = 1 + \frac{1}{KL}\sum_{k=1}^{K}\sum_{l=1}^{L} \log_2 \max(p_n, 1-p_n) r_{n,k,t,l}$$

$$\text{where } p_{n,k,l} = \frac{1}{T}\sum_{l=1}^{T} r_{n,k,t,l}$$

Ideal value of steadiness is 100% which means that the probability of any specific bit towards either logic-0 or logic-1 should be 1.

3.7. Evaluation Methodologies in Literature

[MRVKSL12] presents a Silicon Characterization Vehicle for a comprehensive experimental evaluation. [MMS09] analyzes the delay-based PUF implementations on FPGA. [YHMV12] evaluates the Advanced Encryption Standard (AES) S-box based Glitch PUFs on FPGAs. [YMSD11, YSSMD12] evaluates an integrated key generator ASIC implementation for cryptographic key generation. Built-In Self-Test (BIST) PUF [HMK14] is an online evaluation methodology for evaluating the unpredictability and stability of PUF identifiers with a very low overhead.

3.7.1. Evaluation of Metrics

[SKAH+11] evaluates the physical phenomenon that the initial state of a 6T-SRAM cell is highly dependent on the process variations. [MS11] proposes compensation techniques (placement strategy and RO-pairs selection) to significantly improve the uniqueness of the RO-based PUFs. [CLB12] provides a test framework for measuring reliability and uniqueness of PUFs. [SL12] investigates the reliability and uniqueness of

SRAM-PUFs on different technology nodes. [KKRSVW12] presents an evaluation methodology for assessment of the PUF properties - robustness and unpredictability.

3.7.2. Evaluation of Bit-Error Probabilities

A precise estimation of the bit-error probabilities is obtained based on the distribution of frequency measurements [HSP13] rather than the bit-errors after frequency comparison.

3.7.3. Estimation of Entropy

[BSL13] proposes a new method for accurate estimation of the entropy of Binary PUFs. A cross-disciplinary approach for obtaining statistically optimal entropy has been proposed in [KMNSVZ10]. The entropy of optical PUFs was estimated by the context-tree weighting method (CTW), a lossless compression and prediction algorithm in [ISSTW06].

3.7.4. PUF System Model

Maiti, in his PhD. dissertation [Mai12] proposed an effective generic PUF system model [MGS12] to systematically optimize the quality factors as shown in Fig. 15. This divides the PUF into three components namely sample measurement, identity mapping and quantization. This is analogous to biometric identification as shown in Fig. 16. Sample measurement measures the process variation information from the individual chips. Identity mapping generates a unique identifier string for each chip. And quantization transforms the identifier into a binary string, which is the device identifier or key.

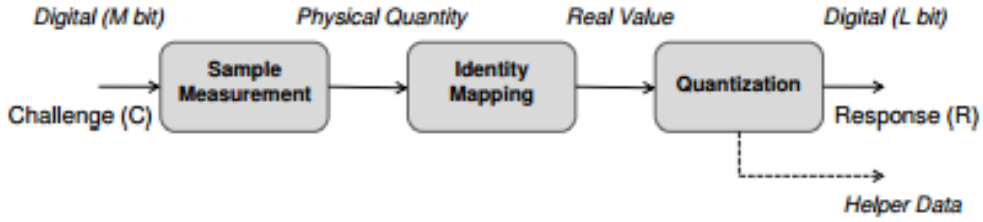

Figure 15. PUF system model

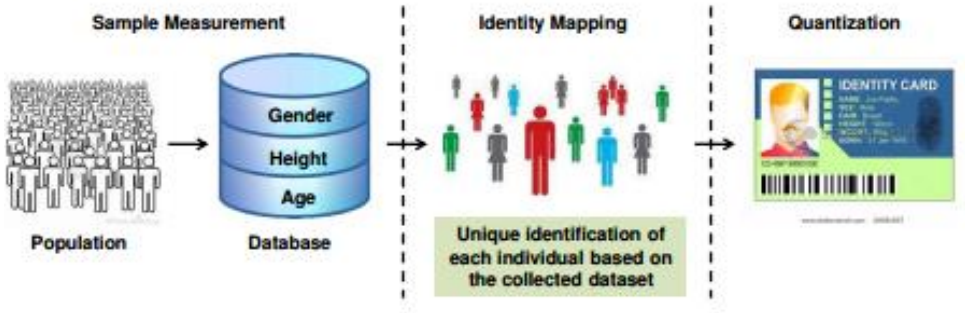

Figure 16. Analogy to biometric identification

Study of correlated process variations [MS09a], improvement of the existing RO-PUF design [MS09b, MMS09, MS11], PUF enhancement techniques [MKS12], characterization [MCHS10] of an RO-PUF over a large group of chips, study on the effect of aging on PUFs using accelerated aging [MDS11, MS13], PUF evaluation-characterization technique [MGS13] for formal performance evaluation of the PUF, and a microprocessor intrinsic PUF [MS12] are the main contributions of [Mai12].

4. POST-PROCESSING OF PUFS

4.1. Factors Affecting PUF Performance

The main factors that affect the quality of the PUF responses are systematic process variations, aging, noise and environmental perturbations. Systematic variations on the chip result in deterministic process variations based on the location of the PUF on the chip, reducing the uniqueness of the chip. For example, in a RO-based PUF implementation, certain sections of the chip will have an average frequency lesser than the average at other locations. This is due to on-chip spatial process variations. Comparison of two frequencies between ROs in such areas will lead to non-stochastic responses. Aging of the chip results in irreversible circuit variations altering the circuit behaviour over time. This eventually leads to false-positive and false-negative responses. Negative bias temperature instability (NBTI), temperature-dependent dielectric breakdown (TDDB), hot carrier injection (HCI), and electro-migration are some Very Large Scale Integrated Circuits (VLSI) phenomena which accelerate aging on chips. Noise and environmental changes like variations in the operating voltage and temperature results in unstable bits, bringing down the reliability of the circuit [Mai12]. The methods proposed in literature to counteract the effects of these factors are summarized below:

4.1.1. Counteracting the Effect of Systematic Process Variations

[Mai12, DB14a] respectively propose the use of frequency difference between adjacent pairs of ROs and the use of relative frequencies to reduce the effect of

systematic variations on PUF response. This was demonstrated to have a significant improvement on the uniqueness and uniformity of the PUF responses. Entropy distillation extracts the entropy from the PUF responses from noise and systematic variations. [YQ13b, YQ14] propose a polynomial-regression based Entropy Distiller which decouples the systematic variations from required random variations by building a model for systematic variation. A Random Patch Mixer (RPM) scheme was proposed in [MN14] to mitigate the effects of systematic variations in RO-PUFs, wherein random numbers generated from a Random Number Generator are normalized to the maximum value of the RO frequency difference from the average RO frequency on chip. These normalized numbers, called as the Patch are added to the RO frequency for ID generation.

4.1.2. Counteracting the Effects of Aging

The impact of aging on PUF characteristics have been examined in [MDS11, MRVKSL12, MS13] using accelerated aging tests. The aging-resistant RO-PUF [RFFT14] mitigates the effects of NBTI and HCI by deactivating the PUF when it is not in use. This significantly reduces the aging of the PUF circuitry.

4.1.3. Counteracting the Effects of Noise and Environmental Variations

Addition of two transistors to a regular inverter-based circuit causes the MOSFET transistors of the current-starved inverter circuit to operate in the subthreshold region. This results in a decreased delay of the inverter stage with increasing temperature. This positive temperature coefficient effect on current starved inverters was proposed for increased thermal stability to counteract the effect of negative temperature coefficient of

regular transistors [CZCC15]. Adapting the supply voltage ramp-up time to the ambient temperature reduces the noise on memory-based PUF responses [CHLMS13]. [BBM15] discusses the impact of voltage variation on the Anderson PUF implemented on Xilinx Spartan-3E. The temperature variation on PUF characteristics was studied in [MRVKSL12].

4.2. Need for Post-Processing of PUF Responses

The response bits obtained from a PUF cannot be used directly as a key, which demands high-entropy and reproducibility. Two main reasons for this are stated in [DV13a]:

1. The bits are not perfectly reproducible due to noise and environmental variations,
2. Statistical properties of some response bits might be undesirable, i.e. bias, correlations between responses or reduced entropy might exist.

Hence, to ensure the key generated from the PUF responses meets the requirements, post-processing is required.

4.3. Helper-Data Algorithms

The PUF responses are generally noisy random variables and can be referred to as the fuzzy secret. Helper Data Algorithms (HDAs), also called as Fuzzy Extractors or Shielding Functions are used to extract cryptographic keys from fuzzy secrets.

A detailed study of the currently existing Helper-Data Algorithms, threats due to their data leakage and manipulation and open problems was provided in [DGSV15]. Soft-decision information, wherein the bit reliabilities are used to determine the secret key from the noisy input, was proposed to improve the efficiency of Helper Data Algorithms

for SRAM-PUF responses in [MTV09a, MTV09b, SL12]. [GSTK+09] investigated the properties of Fuzzy Extractors and Helper Data algorithms to securely deploy secret keys to a low cost wireless node. [BGSST08] presents hardware-resource efficient Fuzzy Extractor implementations on FPGAs. Sequential Pairing Algorithm (SPA) and Longest Increasing Subsequence-based Grouping Algorithm (LISA) are two effective secret extraction schemes for RO-PUFs [YQ10]. Reverse fuzzy extractors [HKMP+12] are efficient for extremely lightweight implementations.

The three main components of a HDA are bit selection, error-correction and entropy compression.

4.3.1. Bit-Selection

The first step in HDAs is bit-selection, wherein the least reliable bits are discarded to reduce the complexity of the error-correction.

4.3.2. Entropy-Compression

Correlations and bias of the PUF responses and leakage of HDA information result in non-maximum entropy. Entropy compression or privacy amplification ensures the uniformity of key and preserves the entropy of the response by increasing the ratio of input to output bits. Hash functions are generally used for entropy compression.

4.3.3. Error-Correction

Error-correction schemes are used in HDAs to ensure that the generated keys are reproducible.

The different error-correction constructions in literature have been compiled in [DGSV15]. It includes

1. Temporal Majority Voting – which uses majority voting for reconstruction of the responses,
2. Exhaustive search – for searching error patterns, but is resource-intensive,
3. Secure-Sketch – commonly used in HDAs. Code-offset and Syndrome based constructions are the common Secure-sketch constructions,
4. Codes in parallel – non-overlapping sections of the response are processed independently to reduce the decoding complexity,
5. Concatenated codes – concatenation of two ECCs is capable of correcting many errors while maintaining entropy,
6. Soft-Decision decoding – depends on bit-reliabilities for decoding and has better error-correcting capabilities compared with Hard-decision decoding techniques,
7. Convolutional codes – have smaller code-words compared to block codes and are easier to implement, for example – Viterbi algorithm,
8. Substring matching – error patterns are detected by a substring search for errors in the response.

[YMDV13] provides an overview of the Syndrome Coding schemes proposed for post-processing of the PUF responses. The various error-coding schemes in implementations include Index-based Syndrome Coding [YD10b], Compressed Differential Sequence Coding [HS14], Bose-Chaudhuri and Hocquenghem (BCH) coding [KHKHI14a], Systematic Low Leakage Coding scheme (SSLC) [HYP15], Kendall Syndrome Coding (KSC) [KPD14, KPD15].

5. ATTACKS ON PUFS

5.1. Machine Learning Attacks

Machine learning attacks are implemented on PUFs by building models which determine the internal parameters of PUFs. Modeling attacks [RSSDDS10, RSSX^{+}13] are used to test the resilience of strong PUF designs. [HMV12] uses machine learning to introduce modeling attacks on 65 nm Arbiter PUFs. [RS14] is a detailed study on machine-learning based modeling attacks on strong PUFs and proposes suggestions for increasing the security of strong PUFs. Evolution Strategies (ES)-based machine learning techniques can successfully attack PUFs even if direct challenges and responses are not available [Beck15], thus increasing the vulnerability of highly obfuscated PUF responses. This has been demonstrated with successful attacks on reverse-fuzzy extractors. The Composite PUF is vulnerable to cryptanalysis and modeling attacks [SNMC15] when the independence of its components is exploited. Simulated results for a PUF design based on non-linear voltage transfer characteristics demonstrate improved machine-learning attack resistance in PUFs [VK15].

5.2. Attacks on PUF Interfaces

The assumption in most PUF designs in literature is that an adversary cannot modify or enhance a PUF interface in a "bad" way. Thus the vulnerability of PUF interfaces towards attacks and solutions are proposed in [DR14b].

5.3. Side-Channel Attacks

Side-channel attacks are a subset of physical attacks wherein the attacker gains information during the operation of the device and uses it for cryptanalysis. They are easy to implement and pose a serious threat to the security of cryptographic implementations. [Sch10] provided an extensive study on the side-channel analysis of PUFs. [XB14] proposed taxonomy of the different side-channel attacks on PUFs with a complete study on the challenges and countermeasures for the same. Arbiter-PUFs are prone to machine-learning modeling attacks when the challenge-response pairs are known to the attacker. Controlled PUFs overcome this issue because the direct challenge-response pairs are never revealed. However, a hybrid side-channel analysis along with machine-learning can enable an attacker to perform both active as well as passive side-channel attacks on controlled-PUFs [BK14]. A study on the physical vulnerabilities of PUFs [HBNTS14] shows that most SRAM-PUF implementations available in market as a replacement for non-volatile memory key-storage lack sufficient protection against physical attacks.

5.4. Helper-data Based Attacks

PUF-based pattern matching key generators are vulnerable against the manipulation of public helper data [DV13a]. [DV14b] exposes the vulnerability of sequential pairing algorithm, group-based RO-PUFs and entropy distiller constructions for key-recovery based on helper-data.

5.5. Repeatability Attacks

Environmental deviations induce faults in Arbiter and RO-based PUFs, resulting in repeatability attacks [DV13b]. The 65nm CMOS Arbiter PUFs can be modelled successfully by exploiting the response repeatability [DV13c]. Repeatablity attacks on

Arbiter-PUFs and RO-PUFs by increasing the fraction of unstable CRPs were studied in [DV14a].

5.6. Challenge-Based Attacks

Challenge estimation attacks are used for the analysis of the security of QR-PUFs [Sko13]. The increased number of CRPs in [MKS13] is prone to cryptanalytic attacks because the responses to different challenges are not independent, and along with the helper data, can be used to predict responses to unknown challenges with a high probability of success.

5.7. Scan-Chain Attacks

A generic procedure for testing Fuzzy Extractors was proposed [CRHN14] which also helps prevent scan-chain abuse for attacks.

5.8. Reverse-Engineering Attacks

Reverse engineering is the process of reproducing a circuit functionality based on the extracted knowledge. Hardware obfuscation of logic [WP14], covert indices and random subsets of the PUF response strings [RMKWD14] and gate- level characterization of the PUF in a sequential PUF architecture [WWNP14] exhibit resilience to functional reverse-engineering of the PUF.

5.9. Invasive Attacks

Invasive attacks are the attacks on PUFs which causes irreversible changes in the circuitry. Controlled PUFs (CPUFs) [GCDD02a], Reconfigurable PUFs (rPUFs) [WWNP14] and PUF-PRFs [AMSST10] exhibit resilience against invasive physical attacks.

.

6. RING-OSCILLATOR BASED PUFS

6.1. Need for Ring-Oscillator Based PUFs

The start-up values of memory cells are used for the generation of key in some memory-based PUFs, for example SRAM-PUF. Modeling attacks on these memory-based PUFs are possible if the memory-cell values are compromised. The delay-based PUFs generate keys on-the-fly and do not require the key to be stored in a non-volatile memory and hence offer more security than memory-based PUFs. The Arbiter PUF, a delay-based PUF described in Chapter 3, requires that the design be highly symmetrical to ensure that the output is dependent on the process variations and also to ensure unbiased results. A highly symmetric design for an Arbiter PUF requires rigorous placement and routing and is nearly impossible on an FPGA. In contrast, for the Ring-Oscillator based PUF design, the basic Ring-Oscillators which have to be identical can be easily implemented on FPGAs and are thus preferred over Arbiter-based PUFs.

6.2. Spartan6 FPGAs

Field Programmable Gate Arrays (FPGAs) are re-programmable semiconductor devices which can be programmed according to the design requirements. They consist of a matrix of Configurable Logic Blocks (CLBs) connected through programmable interconnects. The major manufacturers of FPGAs are Xilinx, Altera and Actel.

The CLBs are the logic resources in an FPGA wherein the design is implemented. In Xilinx Spartan6 FPGAs, each CLB consists of two slices – SLICEX and

SLICEM/SLICEL as shown in Fig. 17. The slices in the bottom-left corner of CLBs consist of alternating SLICEM and SLICEL while the ones on the top-right corner are the SLICEX. Each CLB is connected to a Switch Matrix and the slices in a CLB do not have direct connections with each other.

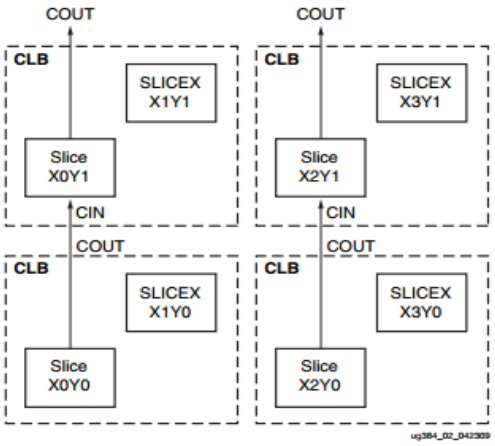

Figure 17. Four CLBs of Spartan6 showing the slices and carry chain

Every slice consists of eight storage elements and four look-up tables. SLICEX (Fig. 18) is the basic slice of the three. SLICELs (Fig. 19) contain an arithmetic carry structure in addition to the basic components along with wide-function multiplexers. SLICEMs (Fig. 20) have the additional capability of using the LUTs as distributed RAM and variable-length shift registers.

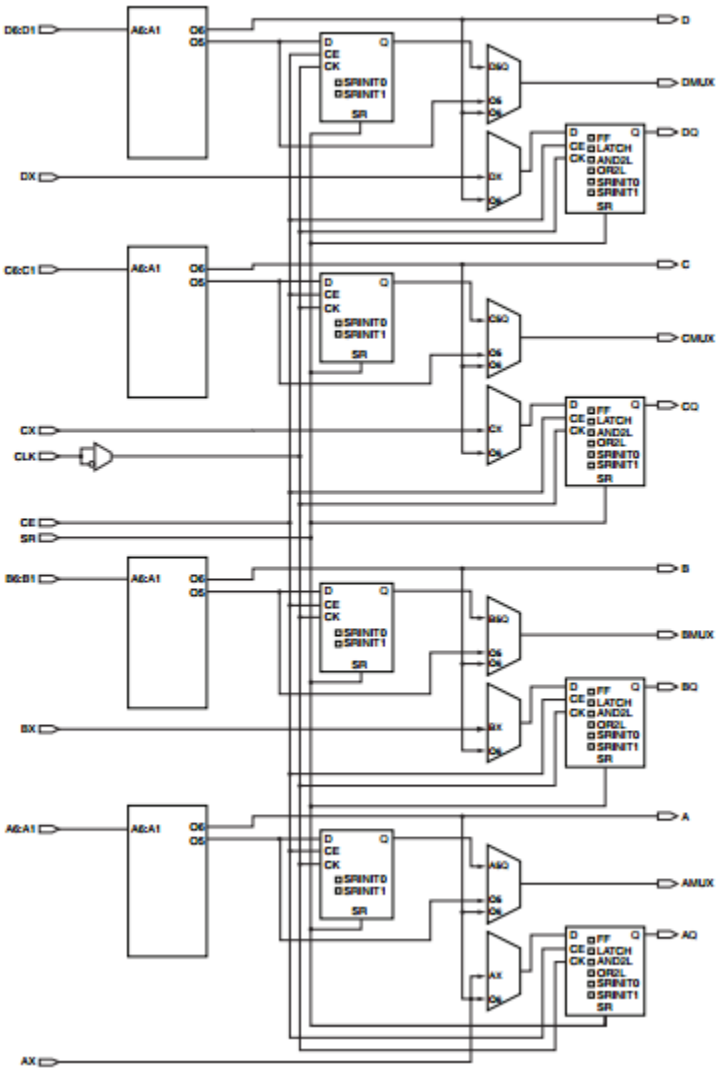

Figure 18. SLICEX internal structure

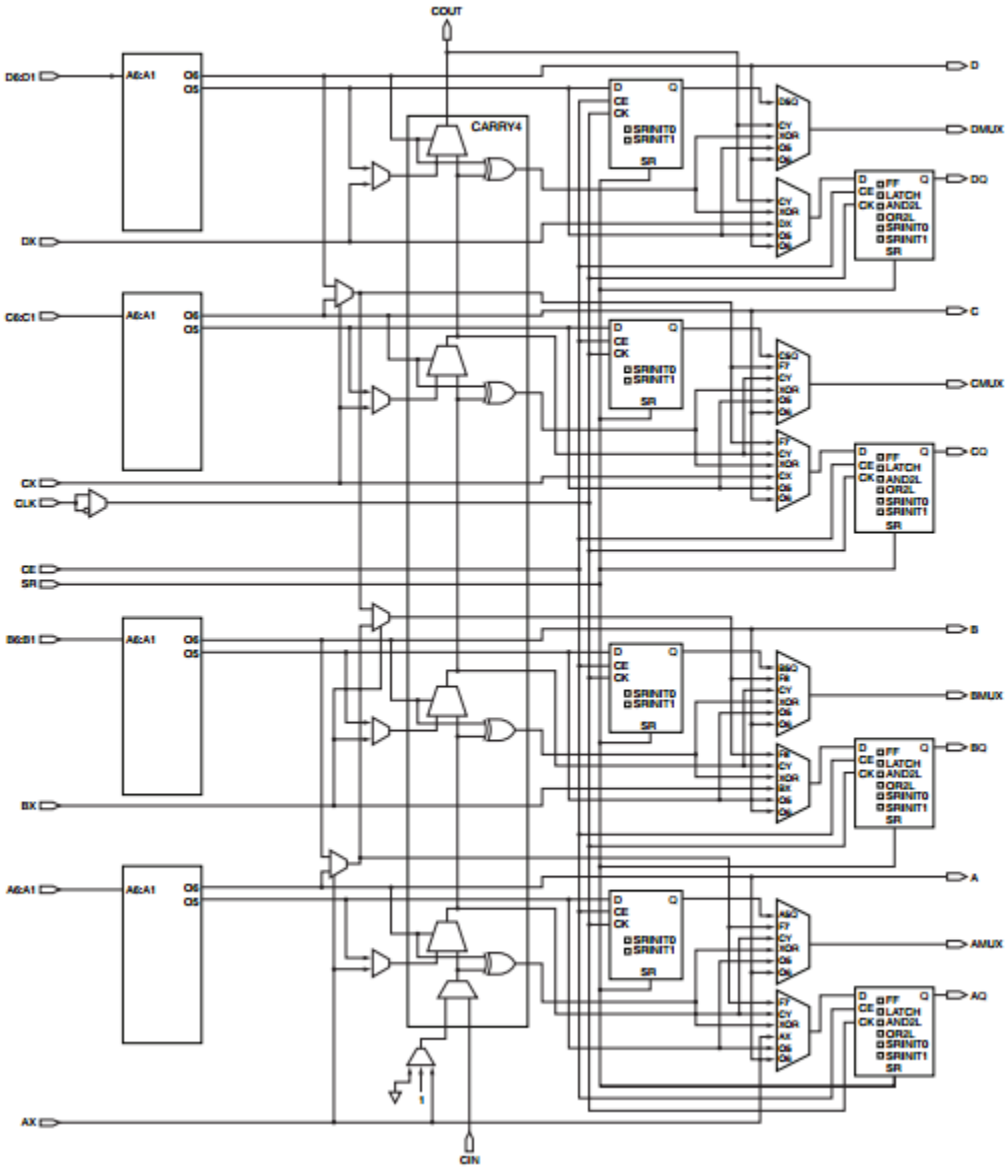

Figure 19. SLICEL internal structure

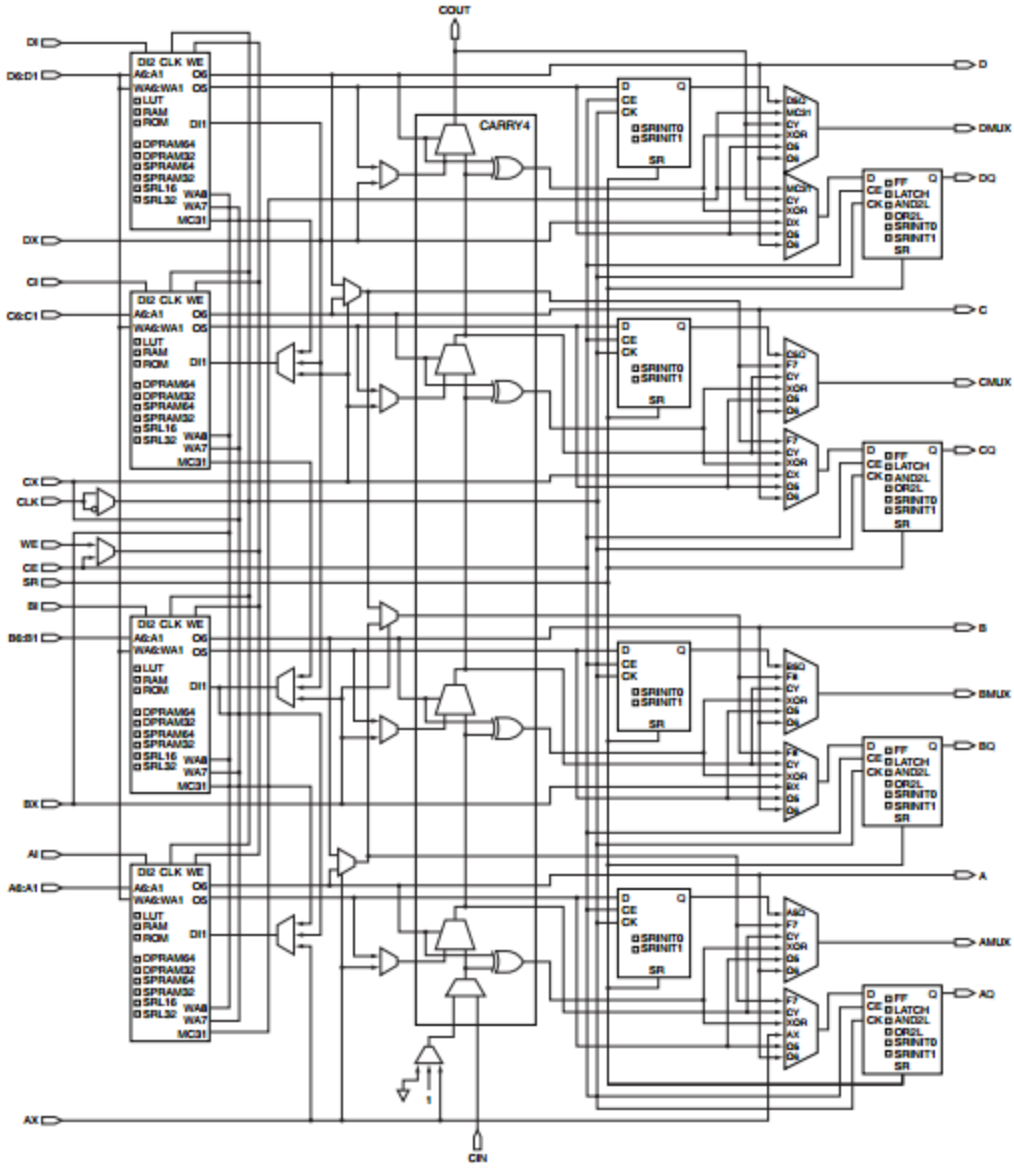

Figure 20. SLICEM internal structure

6.3. Configurable Ring-Oscillator Based PUF

Multiple configurations for a single RO is the essence of CRO-PUFs, as described in Chapter 3. The different configurations could be used to generate higher number of bits per RO. The highly reliable configurations could be used for applications by masking the configurations with unsteady bits. For calculating the frequency difference of two ROs, care should be taken to ensure that both the RO are operating in the same configuration. This is important because different configurations have different wire-lengths and would lead to biased outputs.

6.4. CRO-PUF by Maiti et al.

The Configurable Ring-Oscillator proposed in [Mai12] fits into a single Configurable Logic Block as shown in the Fig. 21. The main advantage of restricting a design to a single CLB is that it can be defined as a macro and duplicated with identical routing leaving the frequency variation only to the physical variations.

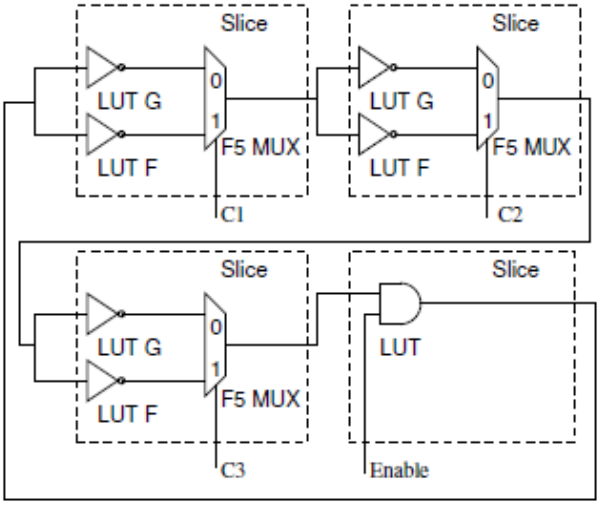

Figure 21. Configurable Ring Oscillator proposed by Maiti et al.

A single RO makes use of three slices with two Look-Up Tables each to function as inverters and the fourth slice is used as an enable switch for the RO. The internal MUXes in the CLB Slices are used to select either LUTG or LUTF with select signals C1-C3. Thus the design has eight different configurations. When the select signals are used as challenges, we get eight CRPs from a single RO compared to one CRP in a basic RO. When a value of “000” or “111” is given to the select signals, they represent the basic ring-oscillator.

6.5. CRO-PUF by Xin et al.

The CRO-PUF model proposed in [XKG11] is based on [Mai12]. This design has a higher number of configurations compared to [Mai12] and utilizes the latches available in the FPGA CLBs to add delays on the RO as shown in Fig. 22. Each RO was implemented on a single CLB of Spartan3 FPGAs which consists of 4 slices each.

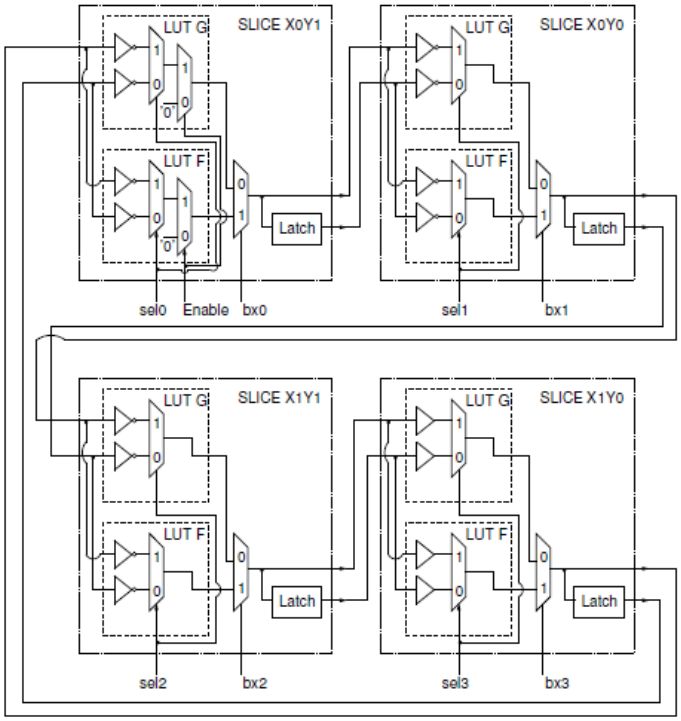

Figure 22. Configurable RO-PUF by Xin et al.

This design has 256 possible configurations for each configurable RO and still fits into a single CLB block. The select signal *bx* selects which LUT should be used in the ring while the *selx* signals decide whether the latch of the previous slice is included in the ring. This model results in a lower frequency compared to the [Mai12] because of the inclusion of the latches.

6.6. FPGA-PUF based on Programmable LUT delays by Bilal et al.

The CRO by Bilal et al. [HGK13] was designed on Spartan3E devices. Each RO consists of three inverters and an AND gate as shown in Fig. 23, and fit in a single CLB of the FPGA. The inverters are configured in the LUTs of the CLB. 130 ROs were implemented on each chip with 8 configurations each. Hence the number of response bits generated is 1032 bits. The difference of this design with the previous two is that in this, the path outside the LUTs remains constant, minimizing the impact of routing and wire delays on oscillator frequency. This exploits the inherent randomness in the LUTs to derive the ID.

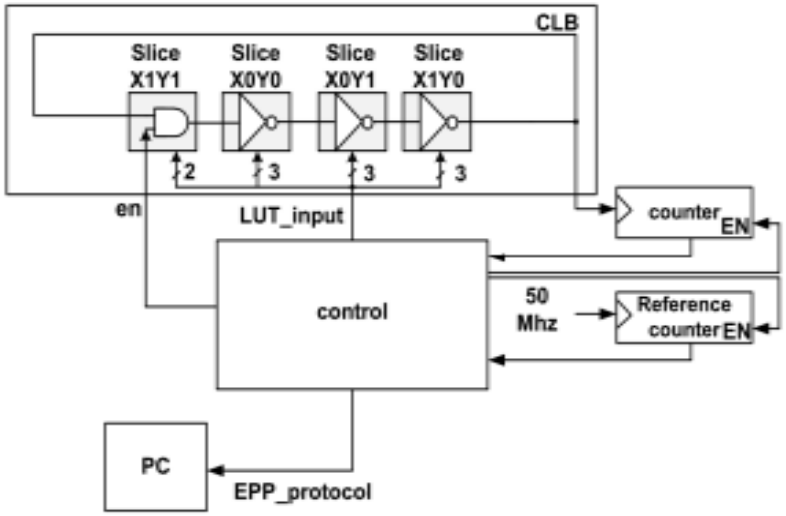

Figure 23. FPGA-PUF based on Programmable LUT delays

7. PROPOSED CONFIGURABLE RO-PUF DESIGN

7.1. Proposed Design

The proposed Configurable RO-PUF model (Fig. 24) is an adaptation of Xin's design [XKG11] on Spartan6 FPGAs and consists of 256 configurations. Each individual RO is implemented on a single CLB utilizing a total of 8 LUTs of SLICEX and SLICEL or SLICEM. The first SLICEX is implemented with buffer such that the total number of inverters in the design is odd. The *en* signal is used to enable the Ring-Oscillator. The MUXes external to the LUTs select the path through a particular LUT while the internal MUXes in LUTs select whether the delay due to the latches are taken into consideration. This inclusion of latch in the RO differentiates Maiti's work from Xin's design and this proposed design with increased number of configurations. The main difference between this design and Xin's implementation is that this was implemented on 2 slices with 4 LUTs each while Xin's design was implemented on 4 slices with 2 LUTs each.

7.2. Implementation

The PUF design was implemented on Spartan6 FPGAs present in the Nexys3 boards with 64 ring oscillators. The design was tested on 20 boards and the frequency data was collected.

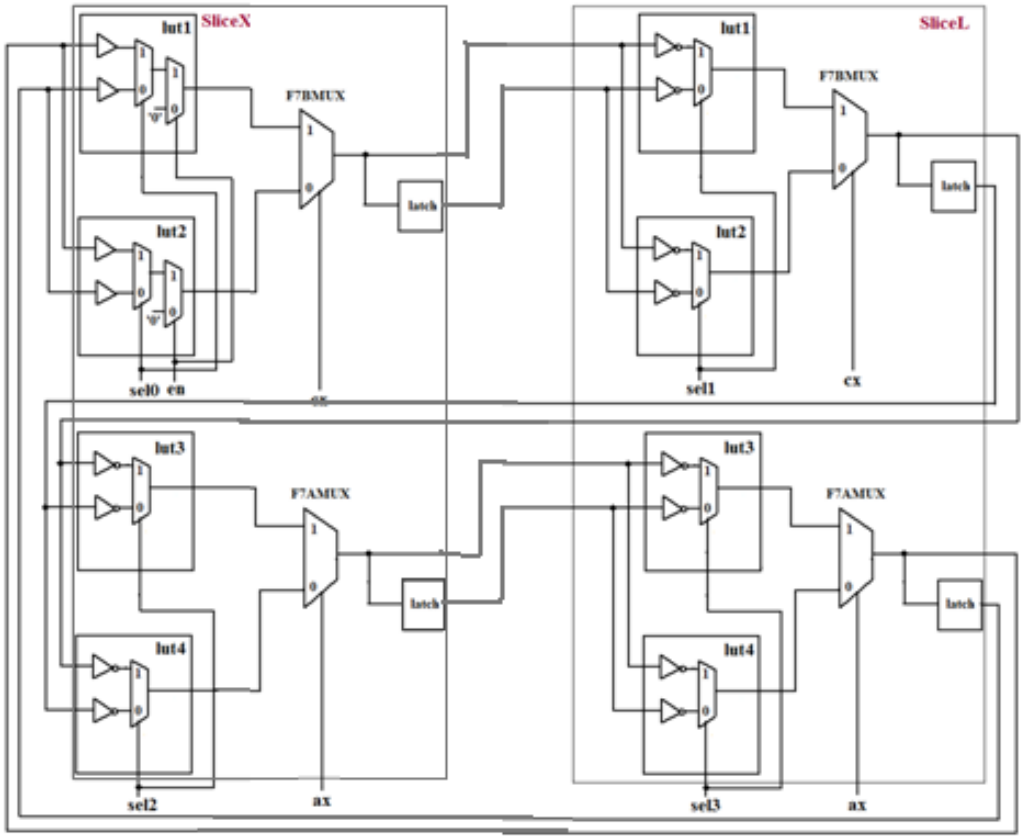

Figure 24. Proposed Configurable RO-PUF

7.3. Frequency Measurement

The frequency of the selected RO is obtained by using two counters – one for counting the rising edges of the RO and the other driven by a crystal of 50 MHz. The RO-counter value is read by a MicroBlaze processor when the std_counter reaches the maximum value. This process is repeated for subsequent ROs in the same configuration and frequencies are found. Adjacent ROs must be used for pairwise comparisons to eliminate the effects of systematic variations and also because the covariance is too small

[WHP14]. A Configurable RO consisting of N-ROs will produce a response of (N-1) bits. Thus the design produces 256 IDs – one for each configuration with 63 bits each.

7.4. Advantages of the Proposed Design

- Increased number of configurations leads to increased number of CRPs,
- Increase in robustness,
- CRPs with higher number of unstable bits can be discarded to ensure high value of steadiness and reliability.

Due to the large number of CRPs, the design can also be used as a one-time pad for authentication and preventing repeatability attacks.

7.5. Results and Analysis

7.5.1. Data Collection

The proposed PUF design was implemented on Spartan6 FPGAs (Nexys3 boards) with 64 ring-oscillators. The design was tested on 20 boards and the frequency data was collected for 10 samples each. The differences between adjacent frequencies were taken to calculate the identifier from the PUF response.

7.5.2. Datasets

The characteristics of the datasets analyzed are given in Table 2.

Table 2. Datasets analyzed

Parameters/Dataset	**Maiti et. al**	**Xin et al.**	**Bilal et al.**	**Proposed CRO**
N (number of chips)	193	NA	32	20
M (number of ROs)	512 ROs	64 CROs	130 CROs	64 CROs
K (number of identifiers)	1	2	1	1
L (length of response)	511	63	1032	63
T (number of samples)	100	NA	20	10

7.5.3. Evaluation of Metrics

The datasets for the PUF implementations were evaluated using Python scripts based on the definitions provided in [MS11]. The metrics obtained for the three PUF implementations are tabulated in Table 3 to enable easy comparison.

Table 3. Comparison of Metrics of predecessor designs with proposed design

Metric	Ideal value (%)	Calculated Values (in %)			
		[Mai12]	Bilal - horizontal	Bilal – Vertical	Proposed design
Uniqueness – Maiti et al.	50	47.236	48.3	47.67	45.372
Uniqueness – Hori et al.	100	93.983	-	-	91.598
Bit – Aliasing	50	50.56	51.8	50.75	46.711
Uniformity	50	50.56	50.13	50.75	46.711
Randomness	100	94.948	-	-	91.320
Reliability	100	99.13	97.88	98.1	99.123
Correctness	100	98.26	-	-	98.450
Steadiness	100	98.503	99.5	99.5	94.602

Thus, the implemented RO-PUF design has a higher uniqueness value compared to [HGK13] and is comparable to that of [Mai12]. Also, the number of CRPs obtained by this method is higher compared to [Mai12], thus more reliable IDs can be generated for the same area consumed.

8. A NOVEL PROPOSAL FOR POST-PROCESSING OF PUF RESPONSES

8.1. Biometrics

A biometric feature is described as a physiological or behavioral characteristic that can be measured to confirm the identity of an individual [DCGM07]. Biometrics are classified as

a. Physical Biometric – if the physical characteristics of an individual like fingerprint, iris, facial features are used for identification or
b. Behavioral Biometric – wherein the behavioral characteristics like voice, handwriting, gait, etc. form the basis of identification.

8.2. Artificial Neural Networks

Artificial Neural Networks (ANN) emulate the functioning of biological neural networks. This, in biological terms would be 'to learn' based on conditions and experiences. An ANN is an adaptive non-linear system that learns to perform a function based on data. The training phase enables the tuning of the input parameters based on the system conditions. The learning rule is to optimize the performance criterion by a systematic procedure. The testing phase deploys the problem at hand to be solved based on the parameters that are 'learnt' during the training phase.

8.3. Hidden Markov Models

Hidden Markov Models are mainly used for statistical pattern recognition. Their effective self-organizing learning capabilities and time-warping capabilities have led

them to be used in the state-of-the-art behavioral recognition systems like speech recognition, handwriting recognition [Dol98]. A Hidden Markov Model (HMM) [RJ86] is a stochastic model used for modelling the structure of an observation sequence with a high level of flexibility. Each observation is paired with a (hidden) state (probability density function) and this enables easy recovery of the (hidden) structure of a sequence of observations.

The Markov property states that the transition at each step depends only on the previous transition. A HMM follows the Markov property with hidden states and visible outcomes. The inputs to a HMM are a sequence of observations, and for each outcome, the computation consists of determining a path of state transitions which is the most probable among all paths to produce the given observations.

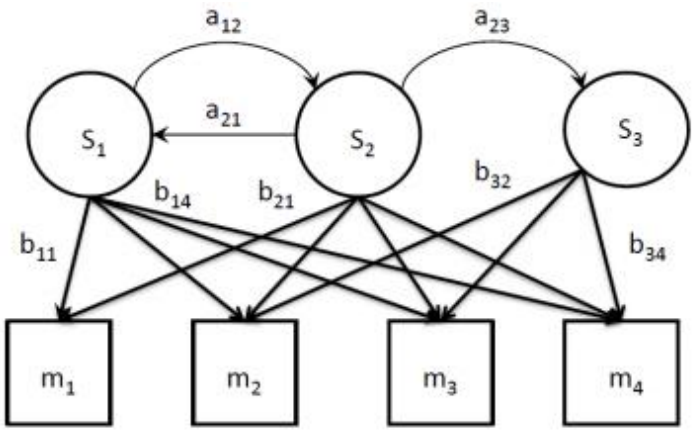

Figure 25. Hidden Markov Model

A HMM [AB13], as shown in Fig. 25 consists of

a. N states – denoted by S

b. M possible outcomes – denoted by m

c. Initial state probability distribution vector (pi)

d. State transition probability matrix (N x N) – cells denoted by aij

e. Output probability matrix (N x M) – cells denoted by bij

The Forward Algorithm, Viterbi Algorithm and Expected Maximum (EM) Algorithms are used for dynamic programming of HMM computation to compute the most likely path based on the observations.

8.4. Proposal for Post-Processing

Hidden Markov Models use pattern recognition to determine the correct outcome based on hidden states. This principle can be exploited for use in the post-processing of PUFs. The HMM should be initially trained with the sample measurements in the enrollment phase. The observation sequences of the responses form a path of state transitions in the HMM. During the testing phase, when PUF measurements are fed to the HMM, it finds the most likely path of state transitions based on the input and generates the outcome which is highly reliable. HMMs could thus be used to generate secure and highly reliable keys from PUF circuits.

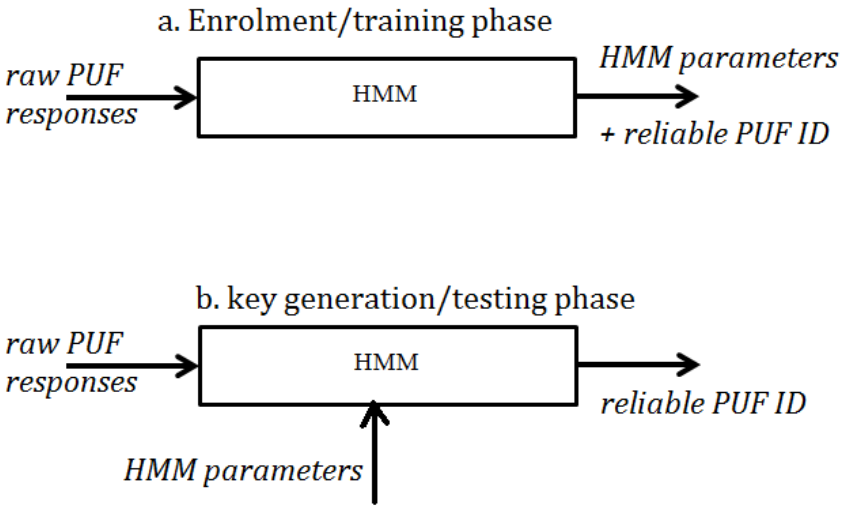

Figure 26. Proposed methodology using HMMs

8.4.1. Advantages of this Method

a. Noisy, unstable bits may be completely removed from the PUF key based on the training sequence

b. Reliability of the circuit becomes very high

c. Because of its use in speech and voice recognition, the error tolerance would be high

8.4.2. Concerns of this Method

a. Ease of implementation

b. Area overhead for implementation

9. CONCLUSION

9.1. Open Questions and Future Research Directions

Some of the open problems in the area of PUFs are:

1. How to construct a truly strong PUF?

The PUF circuits that are proposed to be truly strong attain the required level of authentication by compromising on other security parameters like Confidentiality. Thus research on how to achieve high levels of confidentiality and authentication without compromising on one another would be important.

2. How to construct a physically reconfigurable PUF?

Reconfigurable PUFs seem to be a very interesting direction for PUFs, so focus on their implementations would bring up new ideas leading to stronger and efficient PUFs.

3. More techniques for investigation of PUFs.

Only statistical metrics proposed by Maiti et al. [MS11, MS13] are being used for the evaluation of PUFs. Non-statistical parameters like Power consumption, Area for implementation, etc. might also shed light upon developing efficient PUFs.

4. PUFs as formal primitives to deploy in security systems.

PUFs primitives would enable designers who are non-familiar with PUFs to use them in their designs.

5. Cross-disciplinary studies to explore innovative design methodologies for PUFs.

9.2. Future Research Direction

Post-processing of PUF responses using the novel post-processing technique and its performance evaluation will be done in the future. This will require knowledge of artificial neural networks but will definitely be an interesting research area for PUFs post-processing.

9.3. Conclusion

An extensive up-to-date survey on the various PUF constructions, evaluation methodologies, post-processing, attacks and applications of PUFs was done. A configurable Ring-Oscillator based PUF similar to a previous work was implemented on Spartan6 FPGA boards with each RO confined to a single CLB of the FPGA. A total of 64 ROs were implemented, with 256 configurations each, capable of yielding 256 IDs with 63 bits each. On evaluation the implemented PUF was found to have statistical metrics comparable to the ideal values with higher number of CRPs. The number of configurations can be further increased by incorporating more inverters in the design since 6- input LUTs are available in Spartan6 in contrast to the 4-input LUTs available in Spartan3. A post-processing methodology using Hidden Markov Models was proposed as a cross-disciplinary study between biometrics and PUFs which will be capable of improving the reliability of the generated ID.

REFERENCES

[AB13] A. Aliasgari and M. Blanton, “Secure computation of Hidden Markov Models”, *SECRYPT,* pp. 242-253, 2013.

[AGKT09] M. Asim, J. Guajardo, S. S. Kumar and P. Tuyls, “Physical Unclonable Functions and their applications to vehicle system security”, *Vehicular Technology Conference (VTC),* pp. 1-5, 2009, IEEE.

[AMSST10] F. Armknecht, R. Maes, A.-R. Sadeghi, B. Sunar and P. Tuyls, “Memory Leakage-Resilient Encryption Based on Physically Unclonable Functions”, *Towards Hardware-Intrinsic Security,* pp. 135-164, 2010, Springer Berlin Heidelberg.

[BBM15] M. Barbareschi, P. Bagnasco and A. Mazzeo, "Supply Voltage Variation Impact on Anderson PUF Quality", *Design & Technology of Integrated Systems in Nanoscale Era (DTIS), 10th International Conference on,* pp. 1-6, 2015.

[BDKOS05] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky and A. Smith, "Secure Remote Authentication Using Biometric Data", *Eurocrypt (LNCS), Proceedings of,* 3494, pp. 147-163, 2005.

[Beck15] G. T. Becker, "On the Pitfalls of using Arbiter-PUFs as Building Blocks", *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on,* PP(99), pp. 1-1, 2015.

[Ber12] R. van den Berg, “Entropy Analysis of PUFs”, PhD. Dissertation, EUT, Netherlands, 2012.

[BGSST08] C. Bösch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi and P. Tuyls, “Efficient helper data key extractor on FPGAs”, *Cryptographic Hardware and Embedded Systems (CHES),* pp. 181-197, 2008, Springer Berlin Heidelberg.

[BH12] C. Böhm and M. Hofer, “*Physical unclonable functions in theory and practice”,* 2012, Springer

[BHP11] C. Böhm, M. Hofer and W. Pribyl, "A microcontroller SRAM-PUF", *Network and System Security (NSS), 2011 5th International Conference on*, pp. 269-273, 2011, IEEE.

[BK14] G. T. Becker and R. Kumar, "Active and passive side-channel attacks on delay based puf designs", *IACR Cryptology ePrint Archive*, pp. 287, 2014.

[BM14] M. Bhargava and K. Mai, "An efficient reliable PUF-based cryptographic key generator in 65nm CMOS," in *Proc. Design Autom. Test Europe (DATE)*, pp. 1–6, 2014.

[BNCF14] L. Bossuet, X.T. Ngo , Z. Cherif and V. Fischer, "A PUF based on transient effect ring oscillator and insensitive to locking phenomenon", *Emerging Topics in Computing, IEEE Transactions on*, 2(1), pp. 30-36, 2014.

[BR14a] R. Bernardini and R. Rinaldo, "Helper-less physically unclonable functions and chip authentication,", *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, pp. 8193-8197, 2014.

[BSL13] R. van den Berg, B. Skoric and V. van der Leest, "Bias-based modeling and entropy analysis of PUFs", *Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices*, pp. 13-20, 2013, ACM.

[CDHS12] M. Cortez, A. Dargar, S. Hamdioui and G. J. Schrijen, "Modeling SRAM start-up behavior for Physical Unclonable Functions", *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium on*, pp. 1-6, 2012, IEEE.

[CHLMS13] M. Cortez, S. Hamdioui, V. van der Leest, R. Maes and G. J. Schrijen, "Adapting voltage ramp-up time for temperature noise reduction on memory-based PUFs", *Hardware-Oriented Security and Trust (HOST)*, pp. 35-40, 2013.

[CLB12] M. Claes, V. van der Leest, A. Braeken, "Comparison of SRAM and FF PUF in 65nm Technology", *Information Security Technology for Applications*, pp. 47-64, 2012, Springer Berlin Heidelberg.

[CRHN14] M. Cortez, G. Roelofs, S. Hamdioui, and G. Di Natale, "Testing PUF-based secure key storage circuits", *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, pp. 1–6, 2014.

[CZCC15] Y. Cao, L. Zhang, C-H. Chang and S. Chen, “A Low-Power Hybrid RO PUF With Improved Thermal Stability for Lightweight Applications”, *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on,* 34(7), pp. 1143-1147.

[DB14a] C. Du and G. Bai, “A Novel Relative Frequency Based Ring Oscillator Physical Unclonable Function”, *Computational Science and Engineering (CSE), 2014 IEEE 17th International Conference on*, pp. 569-575, 2014.

[DB14b] C. Du and G. Bai, “A Novel Technique for Ring Oscillator Based PUFs to Enroll Stable Challenge Response Pairs”, *Computer and Information Technology (CIT), 2014 IEEE International Conference on*, pp. 270-275, 2014.

[DCGM07] D. Daleno, L. Cariello, M. Giannini and G. Mastronardi, “Pseudo 2D Hidden Markov Model and Neural Network Coefficients in Face Recognition”, *Automatic Identification Advanced Technologies, 2007 IEEE Workshop on,* pp. 107-111, 2007.

[DGSV15] J. Delvaux, D. Gu, D. Schellekens, and I. Verbauwhede, “Helper data algorithms for puf-based key generation: Overview and analysis”, *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on,* PP(99), pp. 1–1, 2014.

[Dol98] J. G. A. Dolfing, “Handwriting Recognition and Verification – A Hidden Markov Approach”, Ph.D. Dissertation, Philips Nat. Lab, 1998.

[DR14a] M. van Djik and U. Ruhrmair, “Protocol Attacks on Advanced PUF Protocols and Countermeasures”, *Design, Automation and Test in Europe Conference and Exhibition (DATE),* pp. 1-6, 2014.

[DR14b] M. van Djik and U. Ruhrmair, “PUF Interfaces and their Security”, VLSI (ISVLSI), 2014 IEEE Computer Society Annual Symposium on, pp. 25-28, 2014.

[DSPSZK08] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola and V. Khandelwal, "Design and implementation of ‘unclonable’ RFID ICs for anti-counterfeiting and security applications”, *RFID, IEEE International Conference on*, pp. 58-64, 2008.

[DSRBB15] J. Das, K. Scott, S. Rajaram, D. Burgett and S. Bhanja, “MRAM PUF: A Novel Geometry Based Magnetic PUF With Integrated CMOS”, *Nanotechnology, IEEE Transactions on,* 14(3), pp. 436-443, 2015.

[DV13a] J. Delvaux and I. Verbauwhede, “Attacking PUF-based pattern matching key generators via helper data manipulation”, *Cryptology ePrint Archive,* 566, 2013.

[DV13b] J. Delvaux and I. Verbauwhede, “Fault injection modeling attacks on 65nm Arbiter and RO Sum PUFs via Environmental Changes”, *Cryptology ePrint Archive,* 619, 2013.

[DV13c] J. Delvaux and I. Verbauwhede, “Side channel modeling attacks on 65nm arbiter PUFs exploiting CMOS device noise”, *Hardware-Oriented Security and Trust (HOST),* pp. 137-142, 2013.

[DV14a] J. Delvaux and I. Verbauwhede, “Fault injection modeling attacks on 65nm arbiter and RO sum PUFs via environmental changes,” *Circuits and Systems I, IEEE Transactions on,* 61(6), pp. 1701–1713, 2014.

[DV14b] J. Delvaux and I. Verbauwhede, “Key-recovery attacks on various RO PUF constructions via helper data manipulation,” *Design, Automation and Test in Europe Conference and Exhibition (DATE),* pp. 1-6, 2014.

[GCDD02a] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Controlled Physical Random Functions", *Proceedings of the 18th Annual Computer Security Applications Conference,* pp. 149-160, 2002, IEEE.

[GCDD02b] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon Physical Random Functions", *Proceedings of the 9th Computer and Communications Security Conference,* pp. 148-160, 2002, ACM.

[GCDTTD08] B. Gassend, D. Clarke, M. van Dijk, E. Torlak, P. Tuyls, and S. Devadas, "Controlled physical random functions and applications”, *ACM Transactions on Information and System Security (TISSEC),* 10(4), 3, 2008.

[GI14] O. Gunlu and O. Iscan, “ DCT based ring oscillator Physical Unclonable Functions”, *Acoustics, Speech and Signal Processing (ICASSP), IEEE International Conference on,* pp. 8198-8201, 2014.

[GKST07a] J. Guajardo, S. S. Kumar, G. J. Schrijen and P. Tuyls, “FPGA Intrinsic PUFs and Their Use for IP Protection”, *Cryptographic Hardware and Embedded Systems (CHES),* pp. 63-80, 2007, Springer.

[GKST07b] J. Guajardo, S. S. Kumar, G. J. Schrijen and P. Tuyls, “Physical Unclonable Functions, FPGAs and Public-Key Crypto for IP Protection”, *Field Programmable Logic and Applications (FPL), International Conference on,* pp. 189-195, 2007, IEEE.

[GKST08] J. Guajardo, S. S. Kumar, G. J. Schrijen and P. Tuyls, "Brand and IP protection with physical unclonable functions", *Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on,* pp. 3186-3189, 2008.

[GLQ14] M. Gao, K. Lai and G. Qu, "A highly flexible ring oscillator PUF", *51st ACM/IEEE Design, Automation Conference, Proceedings of the,* pp. 1-6, 2014.

[GSTK+09] J. Guajardo, B. Skoric, P. Tuyls, S. S. Kumar, T. Bel, A. H. M. Blom, G. J. Schrijen, "Anti-counterfeiting, key distribution, and key storage in an ambient world via Physical Unclonable Functions", *Information Systems Frontiers*, 11(1), pp. 19-41, 2009.

[Gua11] J. Guajardo, "Physical Unclonable Functions (PUFs)", *Encyclopedia of Cryptography and Security*, pp. 929-934, 2011.

[HB10] M. Hofer and, C. Böhm, "An alternative to error correction for SRAM-like PUFs", *Cryptographic Hardware and Embedded Systems (CHES2010),* pp. 335-350, 2010, Springer Berlin Heidelberg.

[HBNTS14] C. Helfmeier, C. Boit, D. Nedospasov, S. Tajik and J.-P, Seifert, "Physical vulnerabilities of Physically Unclonable Functions", *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, pp. 1-4, 2014.

[HGK13] B. Habib, K. Gaj, and J.-P. Kaps, "FPGA PUF based on programmable LUT delays", *Digital System Design (DSD), 2013 Euromicro Conference on*, pp. 697-704, 2013, IEEE.

[HKMP+12] A. van Herrewege, S. Katzenbeisser, R. Maes, R. Peeters, A.-R. Sadeghi, I. Verbauwhede and C. Wachsmann, "Reverse Fuzzy Extractors: Enabling Lightweight Mutual Authentication for PUF-Enabled RFIDs", *Financial Cryptography and Data Security*, pp. 374-389, 2012, Springer Berlin Heidelberg.

[HMK14] S. U. Hussain, S. Yellapantula, M. Majzoobi and F. Koushanfar, "BIST-PUF: Online, Hardware-based Evaluation of Physically Unclonable Circuit Identifiers", *Computer-Aided Design (ICCAD), 2014 IEEE/ACM International Conference on,* pp. 162-169, 2014.

[HMV12] G. Hospodar, R. Maes and I. Verbauwhede, "Machine learning attacks on 65nm Arbiter PUFs: Accurate modeling poses strict bounds on usability", *WIFS,* pp. 37-42, 2012.

[HS14] M. Hiller and G. Sigl, “Increasing the efficiency of syndrome coding for PUFs with helper data compression”, *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, pp. 1–6, 2014.

[HSKV13] A. van Herrewege, A. Schaller, S. Katzenbeisser and I. Verbauwhede, “Inherent PUFs and secure PRNGs on commercial off-the-shelf microcontrollers”, *Proceedings of the 2013 ACM SIGSAC conference on Computer and Communications Security,* pp. 1333-1336, 2013.

[HSP13] M. Hiller, G. Sigl, and M. Pehl, “A new model for estimating bit error probabilities of ring-oscillator PUFs”, *Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), 8th International Workshop on*, pp. 1-8, 2013, IEEE.

[HST10] H. Handschuh, G. J. Schrijen and P. Tuyls, “Hardware Intrinsic Security from Physically Unclonable Functions”, *Towards Hardware-Intrinsic Security*, pp. 39-53, 2010, Springer Berlin Heidelberg.

[HYKD14] C. Herder, M. D. Yu, F. Koushanfar and S. Devadas, “Physical unclonable functions and applications: A tutorial”, *Proceedings of the IEEE*, 102(8), pp. 1126–1141, 2014.

[HYKS10] Y. Hori, T. Yoshida, T. Katashita and A. Satoh, “Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs”, *Reconfigurable Computing and FPGAs (ReConFig), 2010 International Conference on*, pp. 298-303, 2010.

[HYP15] M. Hiller, M. Yu und M. Pehl, “Systematic Low Leakage Coding for Physical Unclonable Functions”, *Information, Computer and Communications Security, Proceedings of the 10th ACM Symposium on*, pp. 155-166, 2015.

[ISSTW06] T. Ignatenko, G.-J. Schrijen, B. Skoric, P. Tuyls and F. Willems, “Estimating the Secrecy-Rate of Physical Unclonable Functions with the Context-Tree Weighting Method”, *Information Theory, 2006 IEEE International Symposium on*, pp. 499-503, 2006.

[KGMST08] S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen and P. Tuyls, “The Butterfly PUF : Protecting IP on every FPGA”, *Hardware-Oriented Security and Trust (HOST), IEEE International Workshop on,* pp. 67-70, 2008.

[KHCW14] S. T. C. Konigsmark, L. K. Hwang, D. Chen, M. D. F. Wong, “System-of-PUFs: Multilevel Security for Embedded Systems”, *Hardware/Software Codesign and System Synthesis (CODES+ISSS), 2014 International Conference on,* pp. 1-10, 2014.

[KHKHI14a] H. Kang, Y. Hori, T. Katashita, M. Hagiwara and K. Iwamura, “Cryptographic key generation from PUF data using efficient fuzzy extractors”, *Advanced Communication Technology (ICACT), 2014 16th International Conference on,* pp. 23-26, 2014.

[KHKHI14b] H. Kang, Y. Hori, T. Katashita, M. Hagiwara and K. Iwamura, “Performance Analysis for PUF Data Using Fuzzy Extractor”,*Ubiquitous Information Technologies and Applications, Lecture Notes in Electrical Engineering,* pp. 277-284, 2014.

[KKLSSW11] S. Katzenbeisser, U. Koçabas, V. van der Leest, A.-R. Sadeghi, G. J. Schrijen, C. Wachsmann, “Recyclable PUFs : Logically reconfigurable PUFs”, *Journal of Cryptographic Engineering*, 1(3), pp. 177-186, 2011, Springer.

[KKPSW14] J. Kong, F. Koushanfar, P. K. Pendyala, A.-R. Sadeghi and C. Wachsmann, “PUFatt: Embedded platform attestation based on novel processor-based PUFs”, *Design Automation Conference (DAC), 2014 51st ACM/EDAC/IEEE,* pp. 1-6, 2014.

[KKRSVW12] S. Katzenbeisser, Ü. Koçabas, V. Rozic, A.-R. Sadeghi, I. Verbauwhede and C. Wachsmann, “PUFs: myth, fact or busted? A security evaluation of Physically Unclonable Functions (PUFs) cast in Silicon (Extended Version)”, *IACR Cryptology ePrint Archive 2012*, pp. 557, 2012.

[KMNSVZ10] I. Kim, A. Maiti, L. Nazhandali, P. Schaumont, V. Vivekraja and H. Zhang, "From statistics to circuits : Foundations for future Physical Unclonable Functions”, *Towards Hardware Intrinsic Security*, Eds. A. Sadeghi, pp. 55-78, 2010, Springer Berlin Heidelberg.

[KPD14] G. Komurcu, A. E. Pusane and G. Dundar, “Robust RO-PUFs with Enhanced Challenge-Response Set”, *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2014 11th International Conference on*, pp. 1-6, 2014.

[KPD15] G. Komurcu, A. E. Pusane and G. Dundar, “Enhanced challenge-response set and secure usage scenarios for ordering-based ring oscillator-physical unclonable functions”, *Circuits, Devices & Systems, IET,* 9(2), pp. 87-95, 2015.

[KSSST09] K. Kursawe, A.-R. Sadeghi, D. Schellekens, B. Skoric and P. Tuyls, “Reconfigurable Physical Unclonable Functions - Enabling technology for tamper-resistant storage”, *Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on,* pp. 22-29, 2009.

[LDT00] K. Lofstrom, W. Daasch, and D. Taylor, “IC identification circuit using device mismatch”, *Solid-State Circuits Conference, Digest of Technical Papers*, pp. 372–373, 2000.

[LHKSB10] L. Lin, D. Holcomb, D. K. Krishnappa, P. Shabadi and W. Burleson, “Low-Power Sub-Threshold Design of Secure Physical Unclonable Functions”, *Low power Electronics and Design, ACM/IEEE International Symposium on*, pp.43–48, 2010.

[LLGSDD04] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. V. Dijk and S. Devadas, “A technique to build a secret key in integrated circuits with identification and authentication applications”, *VLSI Circuits Symposium, IEEE Proceedings of the*, pp. 176–179, 2004.

[LSSTH12] V. van der Leest, E. Sluis, G.-J. Schrijen, P. Tuyls, and H. Handschuh, "Efficient implementation of true random number generator based on SRAM PUFs”, *Cryptography and Security: From Theory to Applications*, Ed. D. Naccache, pp. 300-318, 2012, Springer Berlin Heidelberg.

[LT13] V. van der Leest and P. Tuyls, “Anti-counterfeiting with hardware intrinsic security”, *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1137-1142, 2013, IEEE.

[LZLL14] W. Liu, Z. Zhang, M. Li and Z. Liu, “A Trustworthy Key Generation Prototype Based on DDR3 PUF forWireless Sensor Networks”, *Computer, Consumer and Control (IS3C), 2014 International Symposium on*, pp. 706-709, 2014.

[Mai12] A. Maiti, "A Systematic Approach to Design an Efficient Physical Unclonable Function", PhD. Dissertation, Virginia Tech, 2012.

[MCHS10] A. Maiti, J. Casarona, L. McHale and P. Schaumont, "A large scale characterization of RO-PUF", *Hardware-Oriented Security and Trust (HOST),2010 IEEE International Symposium on,* pp. 94-99, June 2010.

[MDK10] M. Majzoobi, S. Devadas and F. Koushanfar, "FPGA PUF Using Programmable Delay Lines", *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on,* pp. 1-6, December 2010.

[MDS11] A. Maiti, L. McDougall and P. Schaumont, "The impact of aging on an FPGA-based Physical Unclonable Function", *Field Programmable Logic and Applications (FPL), 21st International Conference on*, pp. 151-156, September 2011, IEEE.

[MGS13] A. Maiti, V. Gunreddy and P. Schaumont, "A systematic method to evaluate and compare the performance of Physical Unclonable Functions", *Embedded System Design with FPGAs*, Eds. P. Athanas, D. Pnevmatikatos and N. Sklavos, pp. 245-267, 2013, Springer.

[MHV12] R. Maes, A. van Herrewege and I. Verbauwhede, "PUFKY: A fully functional PUF-based cryptographic key generator", *Cryptographic Hardware and Embedded Systems (CHES 2012)*, pp. 302-319, 2012, Springer Berlin Heidelberg.

[MKS12] A. Maiti, I. Kim and P. Schaumont, "A robust Physical Unclonable Function with enhanced challenge-response set", *Information Forensics and Security, IEEE Transactions on*, 7(1), pp. 333-345, February 2012.

[MMS09] S. Morozov, A. Maiti and P. Schaumont, "A comparative analysis of delay based PUF implementations on FPGA", *IACR Cryptology ePrint Archive*, 2009.

[MN14] M. Mustapa and M. Niamat, "Novel RPM Technique to Dismiss Systematic Variation for RO-PUF on FPGA", *Aerospace and Electronics Conference, NAECON 2014-IEEE National*, pp. 368-373, 2014.

[MNRS09] A. Maiti, R. Nagesh, A. Reddy and P. Schaumont, "Physical Unclonable Function and True Random Number Generator, "a compact and scalable implementation", *Very Large Scale Integrated circuits (GLSVLSI), Proceedings of the 19th Great Lakes Symposium on*, pp. 425-428, May 2009, ACM.

[MRF15] A. Mazady, M. T. Rahman, D. Forte and M. Anwar, "Memristor PUF—A Security Primitive: Theory and Experiment", *Emerging and Selected Topics in Circuits and Systems, IEEE Journal on*, 5(2), pp. 222-229, 2015.

[MRKWD12] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach and S. Devadas, "Slender PUF protocol : A lightweight, robust, and secure authentication by substring matching", *IEEE Symposium on Security and Privacy Workshops*, pp. 33-44, 2012.

[MRVKSL12] R. Maes, V. Rozic, I. Verbauwhede, P. Koeberl, E. van der Sluis and V. van der Leest, "Experimental evaluation of Physically Unclonable Functions in 65 nm CMOS", *ESSCIRC, 2012 Proceedings of the*, pp. 486-489, 2012, IEEE.

[MS09a] A. Maiti and P. Schaumont, "Impact and compensation of correlated process variations on Ring Oscillator based PUF", *Field Programmable Gate Arrays (FPGA), Proceedings of the 17th International Symposium on*, pp. 285-285, February 2009, ACM.

[MS09b] A. Maiti and P. Schaumont, "Improving the quality of a Physical Unclonable Function using configurable ring oscillators", *Field Programmable Logic and Applications (FPL), 19th International Conference on*, pp. 703-707, September 2009, IEEE.

[MS11] A. Maiti and P. Schaumont, "Improved ring oscillator PUF, "An FPGA friendly secure primitive", *Journal of Cryptology*, 24(2), pp. 375-397, April 2011, Springer.

[MS12] A. Maiti and P. Schaumont, "A novel microprocessor-intrinsic Physical Unclonable Function", *Field Programmable Logic and Applications (FPL), 2012 Intl. Conf. on*, pp. 29-31, August 2012.

[MS13] A. Maiti and P. Schaumont, "The impact of aging on a Physical Unclonable Function", *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, preprint, 2013.

[MT09] R. Maes and P. Tuyls, "Process variations for security : PUFs", *Secure Integrated Circuits and Systems*, pp. 125-141, 2010, Springer.

[MTV08] R. Maes, P. Tuyls and I. Verbauwhede, "Intrinsic PUFs from Flip-flops on reconfigurable devices", *3rd Benelux Workshop on Information and System Security*, 2008.

[MTV09a] R. Maes, P. Tuyls and I. Verbauwhede, "Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs", *Cryptographic Hardware and Embedded Systems (CHES)*, pp. 332-347, 2009.

[MTV09b] R. Maes, P. Tuyls and I. Verbauwhede, "A soft decision helper data algorithm for SRAM PUFs", *Information Theory (ISIT), IEEE International Symposium on*, pp. 2101-2105, 2009.

[MV10] R. Maes and I. Verbauwhede, “Physically Unclonable Functions: A study on the state of the art and future research directions”, *Towards Hardware-Intrinsic Security*, pp. 3-37, 2010, Springer Berlin Heidelberg.

[NSCM15] P. H. Nguyen, D. P. Sahoo, R. S. Chakraborty and D. Mukhopadhyay, “Efficient attacks on robust ring oscillator PUF with enhanced challenge-response set”, *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 641-646, 2015.

[Osw13] D. Oswald, “Implementation attacks: From theory to practice”, Dissertation, Ruhr-Universität Bochum, 2013.

[Pap01] R. Pappu, "Physical One-Way Functions", PhD. Dissertation, MIT, 2001.

[PD11] Z. Paral and S. Devadas, "Reliable and efficient PUF-based key generation using pattern matching", *Hardware-Oriented Security and Trust (HOST), IEEE International Symposium on*, pp. 128-133, June 2011.

[PRTG02] R. Pappu, B. Recht, J. Taylor and N. Gershenfeld, “Physical One-Way functions”, *Science*, 297(5589), pp. 2026–2030, 2002.

[RFFT14] M. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, “ARO-PUF: An aging-resistant ring oscillator PUF design”, *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, pp. 1–6, 2014.

[RH14] U. Ruhrmair and D. E. Holcomb, “PUFs at a glance”, *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, pp. 347, 2014.

[RJ86] L. R. Rabiner and B. H. Juang, “An introduction to Hidden Markov Models”, *IEEE ASSP Magazine*, 3(1), pp. 4-16, 1986..

[RMKWD14] M. Rostami, M. Majzoobi, F. Koushanfar, D. Wallach and S. Devadas, “Robust and Reverse-Engineering Resilient PUF Authentication and Key-Exchange by Substring Matching”, *Emerging Topics in Computing, IEEE Transactions on*, PP(99), pp. 1–1, 2014.

[RS14] U. Ruhrmair and J. Solter, “PUF modeling attacks: An introduction and overview”, *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, pp. 1-6, 2014.

[RSSDDS10] U. Ruhrmair, F. Sehnke, J. Soelter, G. Dror, S. Devadas and J. Schmidhuber, "Modeling Attacks on Physical Unclonable Functions", *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 237-249, October 2010.

[RSSX+13] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, S. Devadas, "*PUF Modeling Attacks on Simulated and Silicon Data*", IEEE Transactions on Information Forensics and Security, 8(11), pp. 1876-1891, 2013.

[RWPK14] M. Rostami, J. B. Wendt, M. Potkonjak and F. Koushanfar, "Quo vadis, PUF? Trends and challenges of emerging physical-disorder based security", *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, pp. 1-6, 2014.

[SD07] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Key Generation", *Proceedings of the 44th Design Automation Conference*, pp. 9-14, 2007.

[SDSD05] G. E. Suh, C. W. O'Donnell, I. Sachdev, and S. Devadas, "Design and Implementation of the AEGIS Secure Processor Using Physical Random Functions", *Proceedings of the International Symposium on Computer Architecture*, 33(2), 2005, IEEE Computer Society.

[SKAH+11] G. N. Selimis, M. Konijnenburg, M. Ashouei, J. Huisken, H. de Groot, V. van der Leest, G. J. Schrijen, M. van Hulst and P. Tuyls, "Evaluation of 90nm 6T-SRAM as Physical Unclonable Function for secure key generation in wireless sensor nodes", *Circuits and Systems (ISCAS), 2011 IEEE International Symposium on*, pp. 567-570, 2011.

[Sko09] B. Skoric, "Quantum readout of Physical Unclonable Functions: Remote authentication without trusted readers and authenticated Quantum Key Exchange without initial shared secrets", *Cryptology ePrint Archive*, 369, 2009.

[Sko10] B. Skoric, "Quantum Readout of Physical Unclonable Functions", *Progress in Cryptology – AFRICACRYPT*, pp. 369-386, 2010, Springer Berlin Heidelberg.

[Sko13] B. Skoric, "Security analysis of Quantum-Readout PUFs in the case of generic challenge-estimation attacks", *Cryptology ePrint Archive*, 479, 2013.

[SL12] G. J. Schrijen and V. van der Leest, "Comparative analysis of SRAM memories used as PUF primitives", *Proceedings of the Conference on Design, Automation and Test in Europe*, pp. 1319-1324, 2012.

[SM10] B. Skoric and M. X. Makkes, “Flowchart description of security primitives for controlled physical unclonable functions”, *International Journal of Information Security*, 9(5), pp. 327-335, 2010.

[SMP13] B. Skoric, A. P. Mosk and P. W. H. Pinkse, “Security of Quantum-Readout PUFs against quadrature based challenge estimation attacks”, *Cryptology ePrint Archive,* 84, 2013.

[SNMC15] D. Sahoo, P. Nguyen, D. Mukhopadhyay and R. Chakraborty, “A Case of Lightweight PUF Constructions: Cryptanalysis and Machine Learning Attacks”, *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on,* PP(99), pp. 1-1, 2015.

[SSL12] P. Simons, E. van der Sluis, V. van der Leest, “Buskeeper PUFs, a promising alternative to D Flip-Flop PUFs”, *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on,* pp. 7-12, 2012.

[SSM14] D. P. Sahoo, S. Saha, D. Mukhopadhyay, R. S. Chakraborty, and H. Kapoor, “Composite PUF: A New Design Paradigm for Physically Unclonable Functions on FPGA”, *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on,* pp. 50-55, 2014.

[STO05] B. Skoric, P. Tuyls and W. Ophey, “Robust Key Extraction from Physical Uncloneable Functions”, *Applied Cryptography and Network Security*, pp.407-422, 2005.

[TLZ14] B. Tang, Y. Lin and J. Zhang, “Improving the reliability of RO PUF using frequency offset”, *Field-Programmable Technology (FPT), 2014 International Conference on,* pp. 338-341, 2014.

[TS06] P. Tuyls and B. Skoric, “Physical Unclonable Functions for enhanced security of tokens and tags”, *ISSE 2006—Securing Electronic Business Processes,* pp. 30-37, 2006, Vieweg.

[TSSAO05] P. Tuyls, B. Skoric, S. Stallinga, A. H. M. Akkermans and W. Ophey, “Information-Theoretic Security Analysis of Physical Uncloneable Functions”, *Financial Cryptography and Data Security,* pp. 141-155, 2005, Springer.

[Tuy06] P. Tuyls, “Grey-Box Cryptography : Physical Unclonable Functions”, *Security and Privacy in Ad-Hoc and Sensor Networks,* pp. 3-5, 2006, Springer Berlin Heidelberg.

[Tuy10] P. Tuyls, “Hardware Intrinsic Security”, *Radio Frequency Identification: Security and Privacy Issues,* pp. 123-123, 2010, Springer Berlin Heidelberg.

[Ver12] I. Verbauwhede, “Efficient and secure hardware”, *Datenschutz und Datensicherheit - DuD,* 36(12), pp. 872-875, 2012

[VK15] A. Vijayakumar and S. Kundu, “A novel modeling attack resistant PUF design based on non-linear voltage transfer characteristics”, *Design, Automation & Test in Europe Conference & Exhibition (DATE),* pp. 653-658, 2015.

[VM11] I. Verbauwhede and R. Maes, “Physically unclonable functions: manufacturing variability as an unclonable device identifier”, *Proceedings of the 21st edition of the great lakes symposium on Great lakes symposium on VLSI,* pp. 455-460, 2011, ACM.

[WP14] J.B. Wendt and M. Potkonjak, “Hardware Obfuscation using PUF-based Logic”, *Computer-Aided Design (ICCAD), 2014 IEEE/ACM International Conference on,* pp. 270-271, 2014.

[WHP14] Wilde, F.; Hiller, M.; Pehl, M. “Statistic-Based Security Analysis of Ring Oscillator PUFs”, *Integrated Circuits (ISIC), 2014 14th International Symposium on,* pp. 148-151, 2014.

[WWNP14] S. Wei, J. B. Wendt, A. Nahapetiany and M. Potkonjak, “Reverse Engineering and Prevention Techniques for Physical Unclonable Functions Using Side Channels”, *Design Automation Conference (DAC), 2014 51st ACM/EDAC/IEEE*, pp. 1-6, 2014.

[WYM14] M. Wang, A. Yates and I. L. Markov, “SuperPUF: Integrating Heterogeneous Physically Unclonable Functions”, *Computer-Aided Design (ICCAD), 2014 IEEE/ACM International Conference on*, pp. 454-461, 2014.

[XB14] X. Xiaolin and W. Burleson, “Hybrid Side-Channel/Machine-Learning Attacks on PUFs: A New Threat?”, *Design, Automation and Test in Europe Conference and Exhibition (DATE),* pp. 1-6, 2014.

[XKG11] X. Xin, J.-P. Kaps, and K. Gaj, “A configurable ring-oscillator-based PUF for Xilinx FPGAs”, *Digital System Design (DSD), 2011 Euromicro Conference on*, pp. 651-657, 2011, IEEE.

[YD10a] M. Yu and S. Devadas, "Recombination of Physical Unclonable Functions", *GOMACTech Conference*, March 2010.

[YD10b] M. Yu and S. Devadas, "Secure and Robust Error Correction for Physical Unclonable Functions", *IEEE Design and Test Computing*, 27(1), pp. 67-70, 2010.

[YHMV12] D. Yamamoto, G. Hospodar, R. Maes and I. Verbauwhede, "Performance and security evaluation of AES S-box-based glitch PUFs on FPGAs", *Security, Privacy, and Applied Cryptography Engineering (SPACE)*, pp. 45-62, 2012, Springer Berlin Heidelberg.

[YMDV13] M. Yu, D. M'raihi, S. Devadas, and I. Verbauwhede, "Security and reliability properties of syndrome coding techniques used in PUF key generation", *GOMACTech Conference*, pp. 1-4, 2013.

[YMSD11] M. Yu, D. M'Raihi, R. Sowell and S. Devadas, "Lightweight and secure PUF key storage using limits of machine learning", *Cryptographic Hardware and Embedded Systems (CHES 2011)*, pp. 358-373, September 2011, Springer Berlin Heidelberg.

[YQ10] C.-E. D. Yin and G. Qu, "LISA- Maximizing RO PUF's secret extraction", *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*, pp. 100-105, 2010.

[YQ13a] C. E. Yin, G. Qu and Q. Zhou, "Design and Implementation of a Group-based RO PUF", *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, pp. 416-421, 2013.

[YQ13b] C. Yin and G. Qu, "Improving PUF Security with Regression-based Distiller", *50th Annual Design Automation Conference, Proceedings of the*, pp.1-6, 2013

[YQ14] C. Yin and G. Qu, "Obtaining Statistically Random Information From Silicon Physical Unclonable Functions" *Emerging Topics in Computing, IEEE Transactions on*, 2(2), pp. 96-106, 2014.

[YSSMD12] M. Yu, A. Singh, R. Sowell, D. M'raihi and S. Devadas, "Performance Metrics and Empirical Results of a PUF Cryptographic Key Generation ASIC", *Hardware-Oriented Security and Trust (HOST), IEEE International Symposium on*, pp. 108-115, June 2012.

[ZLLQ15] J. Zhang, Y. Lin, Y. Lyu and G. Qu, "A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-Per-Device Licensing", *Information Forensics and Security, IEEE Transactions on*, 10(6), pp. 1137-1150, 2015.

[ZP14] J. X. Zheng and M. Potkonjak, "A Digital PUF-based IP Protection Architecture for Network Embedded Systems", *Architectures for networking and communication systems, IEEE symposium on*, pp. 255-256, 2014.

[ZWLZ13] J. Zhang, Q. Wu, Y. Lyu, Q. Zhou, Y. Cai, Y. Lin and G. Qu, "Design and Implementation of a Delay-based PUF for FPGA IP Protection", *Computer-Aided Design and Computer Graphics (CAD/Graphics), IEEE International Conference on*, pp. 107-114, 2013.

[Misc10] "Spartan-6 FPGA Configurable Logic Block", *User Guide, Xilinx*, 2010. http://www.xilinx.com/support/documentation/user_guides/ug384.pdf

BIOGRAPHY

Yamini Ravishankar graduated from Sri Sowdeswari Vidyala, Coimbatore, India, in 2008. She received her Bachelor of Technology (Hons.) from SASTRA University in 2012 with the Best Outgoing Student award for the class of 2012. She received the Graduate Teaching Assistantship during her graduate study with the Department of Electrical and Computer Engineering, Volgenau School of Engineering. She graduated with a Master of Science degree in Computer Engineering from George Mason University in 2015. She was awarded the Outstanding Achievement Award for the year 2015 from the Department of Electrical and Computer Engineering.