Printed Electronics-Based Physically Unclonable Functions for Lightweight Security in the Internet of Things

Zur Erlangung des akademischen Grades eines

DOKTOR-INGENIEURS (Dr.-Ing.)

von der KIT-Fakultät für Elektrotechnik und Informationstechnik des
Karlsruher Instituts für Technologie (KIT)

genehmigte

DISSERTATION

von

M.Sc. Lukas Zimmermann
geb. in Ettenheim

Tag der mündlichen Prüfung:	06.11.2020
Hauptreferent:	Prof. Dr. rer. nat. Ulrich Lemmer
1. Korreferent:	Prof. Dr.-Ing. Axel Sikora
2. Korreferentin:	Prof. Dr. rer. nat. Jasmin Aghassi-Hagmann

To my family for their continuous encouragement.

Lukas Zimmermann
77955 Ettenheim

Ich versichere wahrheitsgemäß, die Dissertation bis auf die dort angegebene Hilfe selbständig angefertigt, alle benutzten Hilfsmittel vollständig und genau angegeben und alles kenntlich gemacht zu haben, was aus Arbeiten anderer und eigenen Veröffentlichungen unverändert oder mit Änderungen entnommen wurde.

Karlsruhe, November 2020
Lukas Zimmermann

Acknowledgements

I would like to sincerely thank my advisers, Prof. Dr. rer. nat. Jasmin Aghassi-Hagmann and Prof. Dr.-Ing. Axel Sikora, who have continuously supported and encouraged me during my doctoral studies. I am grateful for the fruitful discussions we had throughout my research activities. I would also like to thank Prof. Dr. Mehdi Tahoori and Prof. Dr. rer. nat. Ulrich Lemmer for their help in improving my scientific work.

Also, I would like to thank all my colleagues in the Institute of Reliable Embedded Systems and Communication Electronics at the University of Applied Sciences Offenburg and in the MERAGEM Graduate School at the Karlsruhe Institute of Technology for their support. I especially thank Alexander Scholz for the numerous technical discussions, his contributions to my research work, as well as his invaluable personal assistance and support. I would like to thank him for being my best critic and for helping me to improve my work. I am very thankful to Andi Walz, Manuel Schappacher, Dr. Zubair Amjad, Saeed Abdolinezhad, and Mayukh Bhattacharyya for many technical discussions, their support, motivation, and inspiration.

Words cannot express my gratitude to my family and friends. Without their unconditional support and encouragement, this PhD thesis would not have been possible. I am deeply grateful to my beloved fiancée for her continuous support, understanding, and motivation.

Finally, I would like to thank the Ministry of Science, Research, and Arts of the state of Baden Württemberg, Germany for their financial support to my research activities in the form of the MERAGEM scholarship as well as the Institute of Reliable Embedded Systems and Communication Electronics (ivESK) for additional funding.

Abstract

Modern society is more than ever striving for digital connectivity – everywhere and at any time, giving rise to megatrends such as the Internet of Things (IoT). Already today, ’things’ communicate and interact autonomously with each other and are managed in networks. In the future, people, data, and things will be interlinked, which is also referred to as the Internet of Everything (IoE). Billions of devices will be ubiquitously present in our everyday environment and are being connected over the Internet. As an emerging technology, printed electronics (PE) is a key enabler for the IoE offering novel device types with free form factors, new materials, and a wide range of substrates that can be flexible, transparent, as well as biodegradable. Furthermore, PE enables new degrees of freedom in circuit customizability, cost-efficiency as well as large-area fabrication at the point of use. These unique features of PE complement conventional silicon-based technologies. Additive manufacturing processes enable the realization of many envisioned applications such as smart objects, flexible displays, wearables in health care, green electronics, to name but a few.

From the perspective of the IoE, interconnecting billions of heterogeneous devices and systems is one of the major challenges to be solved. Complex high-performance devices interact with highly specialized lightweight electronic devices, such as e.g. smartphones and smart sensors. Data is often measured, stored, and shared continuously with neighboring devices or in the cloud. Thereby, the abundance of data being collected and processed raises privacy and security concerns. Conventional cryptographic operations are typically based on deterministic algorithms requiring high circuit and system complexity, which makes them unsuitable for lightweight devices. Many applications do exist, where strong cryptographic operations are not required, such as e.g. in device identification and authentication. Thereby, the security level mainly depends on the quality of the entropy source and the trustworthiness of the derived keys. Statistical properties such as the uniqueness of the keys are of great importance to precisely distinguish between single entities.

In the past decades, hardware-intrinsic security, particularly physically unclonable functions (PUFs), gained a lot of attraction to provide security features for IoT devices. PUFs use their inherent variations to derive device-specific unique identifiers, comparable to fingerprints in biometry. The potentials of this technology include the use of a true source of randomness, on demand key derivation, as well as inherent key storage.

Combining these potentials with the unique features of PE technology opens up new opportunities to bring security to lightweight electronic devices and systems. Although PE is still far from being matured and from being as reliable as silicon technology, in this thesis we show that PE-based PUFs are promising candidates to provide key derivation suitable for device identification in the IoE. Thereby, this thesis is primarily concerned with the development, investigation, and assessment of PE-based PUFs to provide security functionalities to resource constrained printed devices and systems.

As a first contribution of this thesis, we introduce the scalable PE-based Differential Circuit PUF (DiffC-PUF) design to provide secure keys to be used in security applications for resource constrained printed devices. The DiffC-PUF is designed as a hybrid system architecture incorporating silicon-based and inkjet-printed components. We develop an embedded PUF platform to enable large-scale characterization of silicon and printed PUF cores.

In the second contribution of this thesis, we fabricate silicon PUF cores based on discrete components and perform statistical tests under realistic operating conditions. A comprehensive experimental analysis on the PUF security metrics is carried out. The results show that the silicon-based DiffC-PUF exhibits nearly ideal values for the uniqueness and reliability metrics. Furthermore, the identification capabilities of the DiffC-PUF are investigated and it is shown that additional post-processing can further improve the quality of the identification system.

In the third contribution of this thesis, we firstly introduce an evaluation workflow to simulate PE-based DiffC-PUFs, also called hybrid PUFs. Hereof, we introduce a Python-based simulation environment to investigate the characteristics and variations of printed PUF cores based on Monte Carlo (MC) simulations. The simulation results show, that the security metrics to be expected from the fabricated devices are close to ideal at the best operating point. Secondly, we employ fabricated printed PUF cores for statistical tests under varying operating conditions including variations in ambient temperature, relative humidity, and supply voltage. The evaluations of the uniqueness, bit aliasing, and uniformity metrics are in good agreement with the simulation results. The experimentally determined mean reliability value is relatively low, which can be explained by the missing passivation and encapsulation of the printed transistors. The investigation of the identification capabilities based on the raw PUF responses shows that the pure hybrid PUF is not suitable for cryptographic applications, but qualifies for device identification tasks.

The final contribution is to switch to the perspective of an attacker. To judge on the security capabilities of the hybrid PUF, a comprehensive security analysis in the manner of a cryptanalysis is performed. The analysis of the entropy of the hybrid PUF shows that its vulnerability against model-based attacks mainly depends on the selected challenge building method. Furthermore, an attack methodology is introduced to assess the performances of different mathematical cloning attacks on the basis of eavesdropped challenge-response pairs (CRPs). To clone the hybrid PUF, a sorting algorithm is introduced and compared with commonly used supervised machine learning (ML) classifiers including logistic regression (LR), random forest (RF), as well as multi-layer perceptron (MLP). The results show that the hybrid PUF is vulnerable against model-based attacks. The sorting algorithm benefits from shorter training times compared to the ML algorithms. If the eavesdropped CRPs are erroneous, the ML algorithms outperform the sorting algorithm.

Zusammenfassung

Die moderne Gesellschaft strebt mehr denn je nach digitaler Konnektivität – überall und zu jeder Zeit – was zu Megatrends wie dem Internet der Dinge (Internet of Things, IoT) führt. Bereits heute kommunizieren und interagieren „Dinge“ autonom miteinander und werden in Netzwerken verwaltet. In Zukunft werden Menschen, Daten und Dinge miteinander verbunden sein, was auch als Internet von Allem (Internet of Everything, IoE) bezeichnet wird. Milliarden von Geräten werden in unserer täglichen Umgebung allgegenwärtig sein und über das Internet in Verbindung stehen. Als aufstrebende Technologie ist die gedruckte Elektronik (Printed Electronics, PE) ein Schlüsselelement für das IoE, indem sie neuartige Gerätetypen mit freien Formfaktoren, neuen Materialien auf einer Vielzahl von Substraten mit sich bringt, die flexibel, transparent und biologisch abbaubar sein können. Darüber hinaus ermöglicht PE neue Freiheitsgrade bei der Anpassbarkeit von Schaltkreisen sowie die kostengünstige und großflächige Herstellung am Einsatzort. Diese einzigartigen Eigenschaften von PE ergänzen herkömmliche Technologien auf Siliziumbasis. Additive Fertigungsprozesse ermöglichen die Realisierung von vielen zukunftsträchtigen Anwendungen wie intelligente Objekte, flexible Displays, Wearables im Gesundheitswesen, umweltfreundliche Elektronik, um einige zu nennen.

Aus der Sicht des IoE ist die Integration und Verbindung von Milliarden heterogener Geräte und Systeme eine der größten zu lösenden Herausforderungen. Komplexe Hochleistungsgeräte interagieren mit hochspezialisierten, leichtgewichtigen elektronischen Geräten, wie z.B. Smartphones mit intelligenten Sensoren. Daten werden in der Regel kontinuierlich gemessen, gespeichert und mit benachbarten Geräten oder in der Cloud ausgetauscht. Dabei wirft die Fülle an gesammelten und verarbeiteten Daten Bedenken hinsichtlich des Datenschutzes und der Sicherheit auf. Herkömmliche kryptografische Operationen basieren typischerweise auf deterministischen Algorithmen, die eine hohe Schaltungs- und Systemkomplexität erfordern, was sie wiederum für viele leichtgewichtige Geräte ungeeignet macht. Es existieren viele Anwendungsbereiche, in denen keine komplexen kryptografischen Operationen erforderlich sind, wie z.B. bei der Geräteidentifikation und -authentifizierung. Dabei hängt das Sicherheitslevel hauptsächlich von der Qualität der Entropiequelle und der Vertrauenswürdigkeit der abgeleiteten Schlüssel ab. Statistische Eigenschaften wie die Einzigartigkeit (Uniqueness) der Schlüssel sind von großer Bedeutung, um einzelne Entitäten genau unterscheiden zu können.

In den letzten Jahrzehnten hat die Hardware-intrinsische Sicherheit, insbesondere Physically Unclonable Functions (PUFs), eine große Strahlkraft hinsichtlich der Bereitstellung von Sicherheitsfunktionen für IoT-Geräte erlangt. PUFs verwenden ihre inhärenten Variationen, um gerätespezifische eindeutige Kennungen abzuleiten, die mit Fingerabdrücken in der Biometrie vergleichbar sind. Zu den größten Potenzialen dieser Technologie gehören die Verwendung einer echten Zufallsquelle, die Ableitung von Sicherheitsschlüsseln nach Bedarf sowie die inhärente Schlüsselspeicherung.

In Kombination mit den einzigartigen Merkmalen der PE-Technologie werden neue Möglichkeiten eröffnet, um leichtgewichtige elektronische Geräte und Systeme abzusichern. Obwohl PE noch weit davon entfernt ist, so ausgereift und zuverlässig wie die Siliziumtechnologie zu sein, wird in dieser Arbeit gezeigt, dass PE-basierte PUFs vielversprechende Sicherheitsprimitiven für die Schlüsselgenerierung zur eindeutigen Geräteidentifikation im IoE sind. Dabei befasst sich diese Arbeit in erster Linie mit der Entwicklung, Untersuchung und Bewertung von PE-basierten PUFs, um Sicherheitsfunktionen für ressourcenbeschränkte gedruckte Geräte und Systeme bereitzustellen.

Im ersten Beitrag dieser Arbeit stellen wir das skalierbare, auf gedruckter Elektronik basierende Differential Circuit PUF (DiffC-PUF) Design vor, um sichere Schlüssel für Sicherheitsanwendungen für ressourcenbeschränkte Geräte bereitzustellen. Die DiffC-PUF ist als hybride Systemarchitektur konzipiert, die siliziumbasierte und gedruckte Komponenten enthält. Es wird eine eingebettete PUF-Plattform entwickelt, um die Charakterisierung von siliziumbasierten und gedruckten PUF-Cores in großem Maßstab zu ermöglichen.

Im zweiten Beitrag dieser Arbeit werden siliziumbasierte PUF-Cores auf Basis diskreter Komponenten hergestellt und statistische Tests unter realistischen Betriebsbedingungen durchgeführt. Eine umfassende experimentelle Analyse der PUF-Sicherheitsmetriken wird vorgestellt. Die Ergebnisse zeigen, dass die DiffC-PUF auf Siliziumbasis nahezu ideale Werte für die Uniqueness- und Reliability-Metriken aufweist. Darüber hinaus werden die Identifikationsfähigkeiten der DiffC-PUF untersucht, und es stellte sich heraus, dass zusätzliches Post-Processing die Identifizierbarkeit des Identifikationssystems weiter verbessern kann.

Im dritten Beitrag dieser Arbeit wird zunächst ein Evaluierungsworkflow zur Simulation von DiffC-PUFs basierend auf gedruckter Elektronik vorgestellt, welche auch als Hybrid-PUFs bezeichnet werden. Hierbei wird eine Python-basierte Simulationsumgebung vorgestellt, welche es ermöglicht, die Eigenschaften und Variationen gedruckter PUF-Cores basierend auf Monte Carlo (MC) Simulationen zu untersuchen. Die Simulationsergebnisse zeigen, dass die Sicherheitsmetriken im besten Betriebspunkt nahezu ideal sind. Des Weiteren werden angefertigte PE-basierte PUF-Cores für statistische Tests unter verschiedenen Betriebsbedingungen, einschließlich Schwankungen der Umgebungstemperatur, der relativen Luftfeuchtigkeit und der Versorgungsspannung betrieben. Die experimentell bestimmten Resultate der Uniqueness-, Bit-Aliasing- und Uniformity-Metriken stimmen gut mit den Simulationsergebnissen überein. Der experimentell ermittelte durchschnittliche Reliability-Wert ist relativ niedrig, was durch die fehlende Passivierung und Einkapselung der gedruckten Transistoren erklärt werden kann. Die Untersuchung der Identifikationsfähigkeiten basierend auf den PUF-Responses zeigt, dass die Hybrid-PUF ohne zusätzliches Post-Processing nicht für kryptografische Anwendungen geeignet ist. Die Ergebnisse zeigen aber auch, dass sich die Hybrid-PUF zur Geräteidentifikation eignet.

Der letzte Beitrag besteht darin, in die Perspektive eines Angreifers zu wechseln. Um die Sicherheitsfähigkeiten der Hybrid-PUF beurteilen zu können, wird eine umfassende Sicherheitsanalyse nach Art einer Kryptoanalyse durchgeführt. Die Analyse der Entropie der Hybrid-PUF zeigt, dass seine Anfälligkeit für Angriffe auf Modellbasis hauptsächlich von der eingesetzten Methode zur Generierung der PUF-Challenges abhängt. Darüber hinaus wird ein Angriffsmodell eingeführt, um die Leistung verschiedener mathematischer Klonangriffe auf der Grundlage von abgehörten Challenge-Response Pairs (CRPs) zu bewerten. Um die Hybrid-PUF zu klonen, wird ein Sortieralgorithmus eingeführt und mit häufig verwendeten Classifiers für überwachtes maschinelles Lernen (ML) verglichen, einschließlich logistischer Regression (LR), Random Forest

(RF) sowie Multi-Layer Perceptron (MLP). Die Ergebnisse zeigen, dass die Hybrid-PUF anfällig für modellbasierte Angriffe ist. Der Sortieralgorithmus profitiert von kürzeren Trainingszeiten im Vergleich zu den ML-Algorithmen. Im Falle von fehlerhaft abgehörten CRPs übertreffen die ML-Algorithmen den Sortieralgorithmus.

List of Publications

Journals

- **L. Zimmermann**, A. Scholz, U. Gengenbach, L. Koker, Z. Chen, H. Hahn, A. Sikora, M.B. Tahoori, and J. Aghassi-Hagmann, “Hybrid Low-Voltage Physical Unclonable Function Based on Inkjet-Printed Metal-Oxide Transistors“, *Nature Communications*, vol. 11, no. 1, pp. 1-11, 2020.
- A. Scholz, D. Gerig, **L. Zimmermann**, M. Seiberlich, N. Strobel, G. Hernandez-Sosa, and J. Aghassi-Hagmann, “A Hybrid Optoelectronic Sensor Platform with an Integrated Solution-Processed Organic Photodiode“, *Advanced Materials Technologies*, p. 2000172, 2020.
- **L. Zimmermann**, A. Scholz, A. Sikora, M.B. Tahoori, and J. Aghassi-Hagmann, “Embedded Analog Physical Unclonable Function System to Extract Reliable and Unique Security Keys“, *Applied Sciences*, vol. 10, no. 3, p. 759, 2020.
- **L. Zimmermann**, A. Scholz, M.B. Tahoori., J. Aghassi-Hagmann, and A. Sikora, “Design and Evaluation of a Printed Analog-Based Differential Physical Unclonable Function“, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 11, pp. 2498-2510, 2019.

Conferences

- **L. Zimmermann**, A. Scholz, M.B. Tahoori, A. Sikora, and J. Aghassi-Hagmann, “Hardware-Intrinsic Security with Printed Electronics for Identification of IoE Devices“, *In 2020 European Conference on Circuit Theory and Design (ECCTD)*, IEEE, pp. 1-4, 2020.
- Z. Ahmad, **L. Zimmermann**, K.-U. Müller, and A. Sikora, “Modeling of Random Variations in a Switched Capacitor Circuit Based Physical Unclonable Function“, *8th International Conference on Information Technology (ICIT) 2020*, (accepted).
- A. Sikora, A. Walz, and **L. Zimmermann**, “Research Aspects for a Secure Industrial Internet of Things“, *In 2020 International Conference on Dependable Systems, Services and Technologies (DESSERT)*, IEEE, pp. 1-6, 2020.
- **L. Zimmermann**, A. Scholz, A. Sikora, and J. Aghassi-Hagmann, “A Hybrid System Architecture for the Readout of a Printed Physical Unclonable Function“, *In 2018 International Conference on Electronics Technology (ICET)*, IEEE, pp. 11-14, 2018.

Hardware Demonstrator

- A. Scholz, **L. Zimmermann**, A. Sikora, M.B. Tahoori, and J. Aghassi-Hagmann, “Demonstration of Differential Circuit (DiffC)-PUF Addressing and Readout Platform“, *IEEE International Symposium on Hardware Oriented Security and Trust*, EasyChair Preprint no. 1571, EasyChair, 2019.

Contents

List of Figures

List of Tables

Abbreviations

ADC	Analog-to-digital converter
AES	Advanced Encryption Standard
AI	Artificial intelligence
ANN	Artificial neural network
AOWF	Algorithmic one-way function
AUROC	Area under receiver operating characteristics
BCH	Bose-Chaudhuri-Hocquenghem
BER	Bit error rate
BIMUX	Bidirectional multiplexer
BR	Binary relation
CN	Carbon nanotube
COMP	Comparator
CRP	Challenge-response pair
CSPE	Composite solid polymer electrolyte
D2D	Die-to-die
DAC	Digital-to-analog converter
DEMUX	Demultiplexer
DES	Data Encryption Standard
DiffC	Differential Circuit
DSS	Digital Signature Standard
ECC	Error correcting code
EGT	Electrolyte-gated field-effect transistor
EM	Electromagnetic
EEPROM	Erasable programmable read-only memory

EER	Equal-error-rate
FAR	False-acceptance-rate
FET	Field-effect transistor
FHD	Fractional hamming distance
FN	False negative
FP	False positive
FPGA	Field programmable gate array
FPR	False-positive-rate
FRR	False-rejection-rate
GND	Ground
HD	Hamming distance
I/O	Input/output
IC	Integrated circuit
ICID	Integrated circuit identification
IEC	International Electrotechnical Commission
IoE	Internet of Everything
IoT	Internet of Things
IP	Intelectual property
ITO	Indium tin oxide
KIT	Karlsruher Institut für Technologie
L-BFGS	Limited-memory Broyden-Fletcher-Goldfarb-Shanno
LCD	Liquid Crystal Display
LR	Logistic regression
M-PUF	Memristor physical unclonable function
MC	Monte Carlo
ML	Machine learning
MLP	Multi-layer perceptron
MOSFET	Metal-oxide-semiconductor field-effect transistor
MUX	Multiplexer

NIST	National Institute of Standards and Technology
NIST-STS	National Institute of Standards and Technology Statistical Test Suite
NL	Noice level
NLVTC	Non-linear voltage transfer characteristics
NVM	Non-volatile memory
OWF	One-way function
PC	Personal computer
PCB	Printed circuit board
PCM	Phase change memory
PE	Printed electronics
PEDOT:PSS	Poly(3,4ethylenedioxythiophene):poly(styrenesulfonate)
PSA	Platform Security Architecture
POK	Physical obfuscated key
POWF	Phyiscal one-way function
PRF	Physical random function
PUF	Physically unclonable function
rPUF	Reconfigurable physically unclonable function
RF	Random forest
RNG	Random number generator
ROC	Receiver operating characteristics
RO	Ring oscillator
RoT	Root of trust
RSA	Rivest-Shamir-Adleman
RTL	Resistor-transistor-logic
SCPI	Standard Commands for Programmable Instruments
SEM	Scanning electron microscopy
SHA	Secure hash algorithm
SLP	Single-layer perceptron
SMD	Surface-mounted device

SoC	System on a chip
STD	Standard deviation
TN	True negative
TP	True positive
TPM	Trusted Platform Module
TPR	True-positive-rate
TRNG	True random number generator
TV-PUF	Threshold voltage physically unclonable function
USA	United States of America
USB	Universal Serial Bus
W2W	Wafer-to-wafer
WID	Within-die

1 Introduction

1.1 Motivation

In the past years, computing devices have become ubiquitous in our everyday life and the modern society is more than ever striving for digital connectivity. Megatrends such as the Internet of Things (IoT), where devices communicate and interact autonomously with each other, have become real and gain more and more popularity all over the world. Recently, the IoT is evolving to the so-called Internet of Everything (IoE) describing the interconnection of people, data, and things (objects) through processes. Billions of devices are being connected over the Internet [1]. The application areas are numerous reaching from home automation [2, 3], energy management [4, 5], transportation [6, 7], industry [8, 9] up to health care [10, 11] and wearables [12, 13]. Information can be gathered and processed continuously to provide real-time services to humans and machines anytime and anywhere. Thereby, data is often not retraceable to the originator, be it a human being or a machine. This rises privacy and security concerns, since personalized information can fall into wrong hands without knowledge and consent of the consumer.

In this regard, platform architectures have been introduced to attain security and trust in network-based ecosystems. Examples include the widely used Trusted Platform Module (TPM) architecture [14], design guidelines (e.g. NIST 800-160 [15]), and standards (e.g. IEC 62443 [16]) for security in information systems. Cryptography provides the tools to secure communication channels and to prevent data abuse. The most commonly used cryptographic algorithms include Rivest-Shamir-Adleman (RSA) [17], Blowfish [18], Advanced Encryption Standard (AES) [19] to name but a few. In this context, random number generators (RNGs) are often used to generate random binary sequences. On that basis, cryptographic keys for data encryption and decryption can be generated and stored in the device's non-volatile memory (NVM). As a consequence, the security level of the system depends on the trustworthiness of the stored secrets, which is also referred to as the root of trust (RoT). This rises security threats particularly concerning devices operated in untrusted environments by making them prone to physical attacks. Making NVMs secure against physical attacks requires costly anti-tamper measures [20]. This is conflicting to the concept of the IoE, where heterogeneous devices and systems of different complexities are interconnected and exchange information. As a result, conventional cryptographic security solutions may not be suitable for lightweight electronic systems [21].

One promising solution to tackle the aforementioned challenges is hardware-intrinsic security, in particular physically unclonable functions (PUFs). PUFs are specifically designed for lightweight identification, authentication, and cryptographic key generation. PUFs make use of their inherent variations to produce random signatures in the form of a device-specific fingerprint. The internal physical characteristics of the PUF are uncontrollably induced during the fabrication process. Since the device-specific signature is permanently present in the PUF, security keys can be generated on demand and no additional NVM is required.

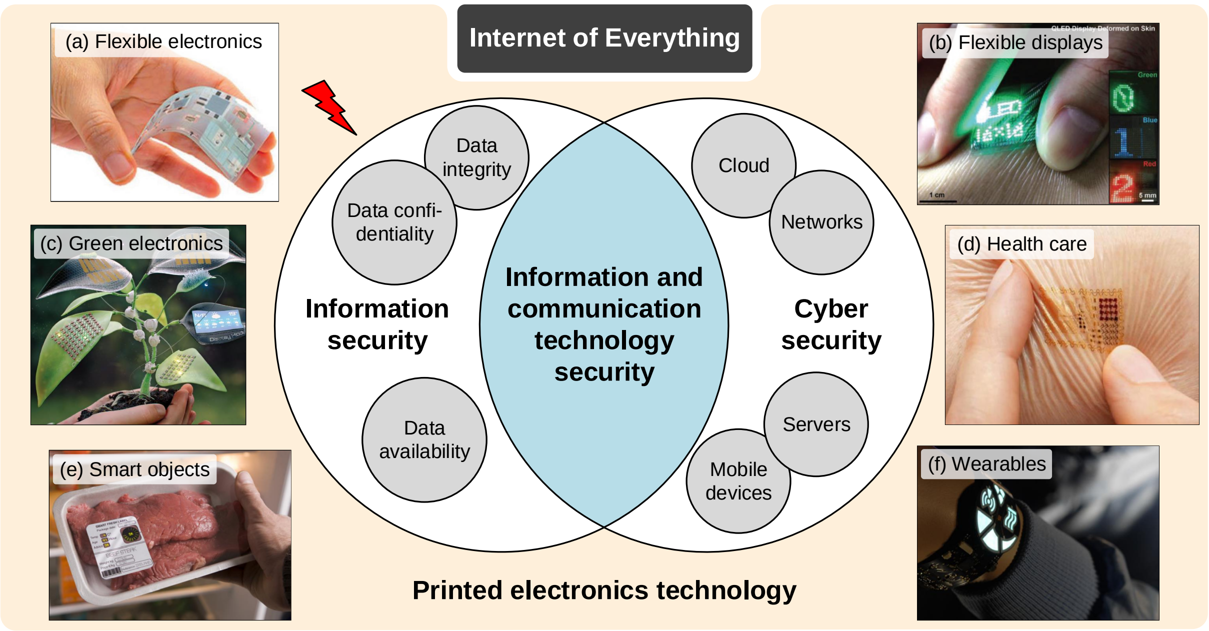


Figure 1.1: Internet of Everything and printed electronics technology. (a) Flexible electronic circuit [22], (b) printed flexible display [22], (c) example of PE-based green electronics [23], (d) printed patch with an integrated sensor [24], (e) smart packaging including a printed sensor [25], and (f) wearable with PE-based electronics [25].

Emerging technologies such as printed electronics (PE) bring innovations by enabling novel device types with free form factors, new materials, and based on large-area fabrication. PE is contrary to conventional silicon-based technology and therefore acts as a key enabler for electronic devices and systems that can be seamlessly integrated into our everyday environment. This will further push the evolution of the IoE by bringing billions of lightweight devices to the market. Potential target applications for PE technology include flexible electronics [22], flexible displays [22], green electronics [23], health care [24], smart objects [25], and wearables [25] as shown in Figure 1.1. Compared to lithographically structured devices, larger variations can be expected due to the additive manufacturing process [26–31]. Moreover, PE-based systems are often subject to strict design and performance constraints, which also limits the security capabilities. In this context, PUFs are promising candidates to overcome these issues and to provide security for lightweight PE-based electronic devices by benefiting from the high variations being used as a true source of randomness. Furthermore, the unique features of PE technology, such as decentralized manufacturing, help to establish root of trust (RoT) in the manufacturing supply chain. This thesis deals with the investigation of PE-based PUFs for the use as lightweight security primitives to enable information and cyber security.

1.2 Research Objectives

This work tackles the challenges arising from lightweight PE-based devices and systems in the IoE regarding their security. In this context, the term ’PE-based’ describes fully printed and hybrid systems incorporating silicon-based and printed components. The approaches and scientific results presented in this work are based on the subsequent research questions:

- **Q1: Which state of the art approaches are best suited to provide security features for PE-based devices and systems?**
  PE technology brings novel device types with free form factors, new materials, enables large-area fabrication, and therefore acts as a key enabler for the IoE. At the same time, PE technology is subject to strict design and performance constraints, which strengthens the need for lightweight security solutions. This analysis will help in finding promising technical solutions based on hardware-intrinsic security.
- **Q2: How can a PUF be designed to meet the requirements for PE fabrication?**
  To find a suitable PUF circuit design that can be fabricated with PE technology, it is required to investigate the variations of printed components based on simulations and experimental measurements.
- **Q3: How can the PUF characteristics be measured and the security performance be evaluated?**
  To assess the security performance of the PUF, it is essential to evaluate the security metrics and compare the results with other works.
- **Q4: Which security threats do arise for PE-based PUFs?**
  The research activities of PE-based PUFs are in the very beginning and the security threats might differ from silicon-based technology. It is required to investigate the vulnerabilities of the proposed PUF and compare the results with other works.
- **Q5: Which potential target applications do exist for the proposed PE-based PUF?**
  Based on the obtained results on the security metrics and the attack resistance, potential target application shall be identified.

1.3 Thesis Structure

In this thesis, we study PE-based PUF designs, security metrics, security threats as well as applications both from a conceptual and from a practical perspective. Figure 1.2 shows how the thesis is organized and these subjects relate to each other.

In Chapter 2, we introduce the foundations of security from a technical perspective with the focus on hardware-intrinsic security. In this respect, we focus on PE technology and its relevance as a key-driver for the IoE. This overview serves as an introduction into the state of the art of hardware-intrinsic security research.

In Chapter 3, we identify requirements on PUFs to qualify for specific applications. Based on our analysis on the requirements for PE-based PUFs, we introduce the Differential Circuit PUF (DiffC-PUF) design. To enable experimental evaluations on fabricated PUFs, a modular embedded PUF evaluation platform based on discrete silicon electronics is also introduced. We published the platform design and the corresponding software implementations in [32, 33]. Moreover, we explain the printing process to fabricate PE-based PUF core circuits and their integration into the evaluation platform.

In Chapter 4, we employ silicon-based PUF cores to investigate the performance in terms of security metrics. The embedded PUF evaluation platform is used to characterize the silicon-

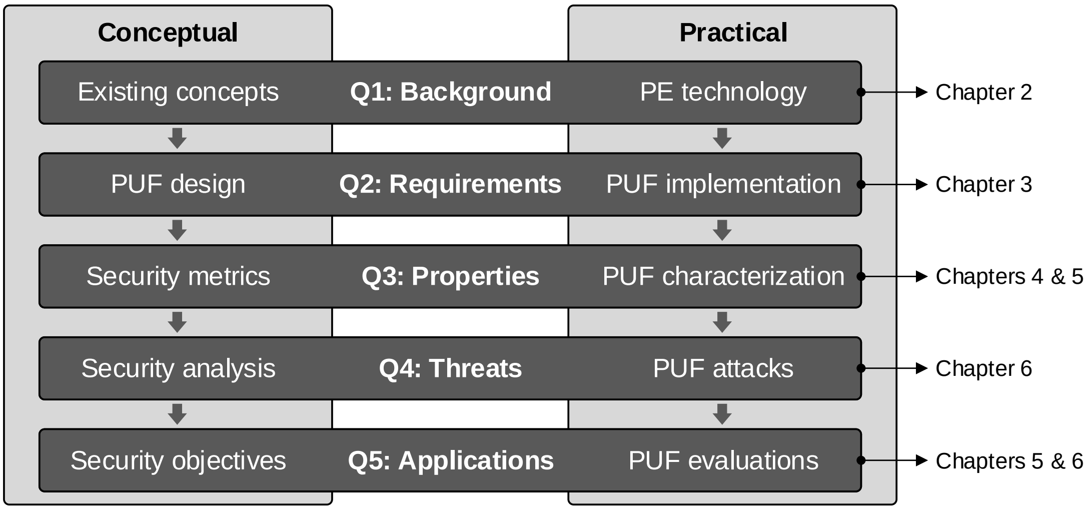


Figure 1.2: Organization of the research objectives in the thesis and its chapters.

based PUFs under changing operating conditions and obtain a data basis for statistical security metric evaluations. On that basis, the identification capabilities of the PUFs are assessed and compared with related works. The results discussed in this chapter are based on our published works in [33].

In Chapter 5, we employ printed PUF cores in combination with the silicon-based embedded evaluation platform to investigate the performance in terms of security metrics and identification capabilities.

In Chapter 6, we focus on security threats in general and emanating for PE-based PUFs. Based on the herein introduced PUF architecture, we investigate the entropy of the PUF responses and perform model-based attacks. This also includes a specially developed sorting algorithm as well as various machine learning (ML) techniques to model the PUF. To conclude, the performances of the employed algorithms are compared.

In Chapter 7, we conclude the most important findings of this thesis and propose interesting future research directions.

2 Background & State of the Art

2.1 Introduction

In the last decades wired and wireless communication technologies have become drivers of the IoE by enabling scalability and flexible deployment. Networks comprise heterogeneous devices and systems with diverse computing performance and design constraints. However, there is a number of challenges ahead in terms of security, privacy, and trust. The variety of parties being involved in the IoE makes it hard to establish consistent security standards. Furthermore, emerging technologies such as PE strengthen the need after security solutions for lightweight electronics. In the past two decades, hardware-intrinsic security emerged as a promising approach to inherently provide security functionalities to electronic devices. Various so-called physically unclonable function (PUF) constructions have been introduced for the use in different security applications.

Being the main subject of this thesis, it is important to introduce the basic concepts of hardware-intrinsic security in the light of PUFs. In the subsequent sections of this chapter, an overview of security in general, state of the art PUF designs, and security metrics is given. Furthermore, PE is introduced with regard to security as well as existing PE-based PUFs are reviewed. Finally, security threats in terms of eavesdropping and model-based attacks are presented. The herein outlined topics are the foundations for the subsequent chapters.

2.2 Security in the Age of Digitization

2.2.1 Security & Privacy

Security plays a major role in the modern world while touching our everyday life in a variety of aspects. As per definition, the term *security* relates to the physical protection of human beings or objects, but also covers observation, detection, and prevention. For example, to keep valuable assets secure one can register a bank account or rent a safe deposit locker for physical protection. The bank strictly limits the access to the bank's employees and logs all interactions to detect misbehavior. Since a bank robbery is per law defined as a criminal act, the asset is further protected by the legislator which allows for and enforces punishment for the caught culprit.

In the past, relatively simple *security* mechanisms were applicable for human non-digital interactions. In most cases, physical protection could be guaranteed based on entrance controls and face-to-face authentication. However, in our more and more digitized world, these *security* mechanisms are no longer sufficient to enable comprehensive *security*. Many interactions have been shifted to digital services in online systems, e.g. on websites or in smartphone applications. To stay with the former example, a bank's customer using the online banking system can not be authenticated face-to-face. Moreover, a digital thief could use the same login data of any other person and delegate money transfers. To detect such unauthorized access, *security* measures need to be introduced for the digital world. In this regard, many technical *security* solutions have been proposed in the past decades, such as multi-factor authentication methods [34], cryptography [35], or biometry [36]. Furthermore, the legislation must provide laws that allow for prosecution in cybercrime. This is a major issue, since cyber criminals are often spread around the world and it is difficult to locate them. Even when identified, cyber criminals often avoid being punished, due to the inconsistent legislation in different countries.

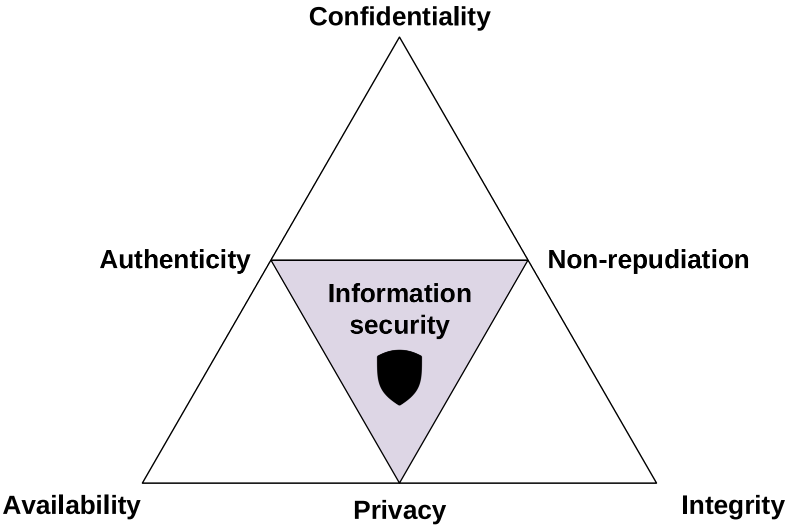


Figure 2.1: Information security CIA triad.

After this general discussion about the broad meaning of *security* in our everyday life, we now want to examine the basic protective goals of *information security* and *privacy*. This is very important due to the massive data exchange over highly heterogeneous distributed systems in the digitized world. Figure 2.1 shows the fundamental concepts of *information security*, which is also known as the CIA triad. The abbreviation CIA describes the properties *confidentiality*, *integrity*, and *availability*. Thereby, the essence of *confidentiality* is the access restriction to ensure that information is only shared with parties being authorized. *Integrity* ensures that information is not altered and truly represents what it is intended. The third property of the CIA triad is the *availability* describing that information can be accessed and modified by any authorized party within an appropriate time frame [37]. In [38] Cerdantseva et al. provide a comprehensive overview on *information security*. Because of the multidisciplinary field, the following extended version of the CIA triad can be found in literature: *confidentiality*, *integrity*, *availability*, *authenticity*, *non-repudiation*, and *privacy* [38, 39]. One of the fundamental tools to ensure *information security* is *authentication*. In this context, *authenticity* guarantees that no unauthorized party can gain access and modify private information, which is the basis for the CIA triad. *Non-repudiation* refers to the verifiability of the information, which can be achieved e.g. through electronic signatures. The *privacy* property is directly included to the *information security* requirements. In general, *privacy* relates to the right one has to control the personal information. It is less about protecting data from attacks than it provides transparency upon which data is collected, stored, and shared with others. In the next section, we elaborate more on the term *trust* and discuss its meaning for *security*.

2.2.2 Trust

The term *trust* describes the belief that someone or something is secure and reliable. Therefore, it is directly linked with security and forms the basis for authentication. The entire society is based on trust relations between individuals and complex systems. Because of this fact, manifold motives for being trustworthy do exist in the real world. For example, companies that want to sell products have more success if their image is good. Good images are mainly an outcome of the experience customers have made with the products of a brand. In this regard, many criminals try to copy original products and trade on the customer's *trust*. In the past, perpetrators could be detected more easily due to the direct relation between the interacting parties, e.g. the customer and the shop. In times of a widely interconnected world with complex and hence, often vast supply chains, distinguishing between originals and counterfeits can be very difficult. For example, many malicious traders in online shops advertise their counterfeits as originals and make use of the customer's *trust*. If we transfer this to digital, interconnected, and autonomously acting systems exchanging data, the trustworthiness of each single device and all data sources must be guaranteed. This highlights the need for trustworthy security solutions that can be applied to all parties. This is what we call *trust* by means of *security* in a pervasive manner.

In times of the Internet of Things (IoT) and the Internet of Everything (IoE), which describe the interconnection of human beings, devices, processes, data, and objects, securing the 'things' as well as the communication are vital factors. Many IoT devices are exposed to security vulnerabilities due to strict hardware limitations such as low computational performance and leakage of memory [40]. To provide standards on how to build secure IoT devices, design frameworks such as e.g. the Platform Security Architecture (PSA) by ARM Ltd [41] have been introduced. The aim of these design frameworks is to enable a strong and flexible protection for the *root of trust*, which is immutable over the lifetime of a device [42]. In this context, the terms *immutable root of trust* and *trust anchor* are widely used for the fixed and tamper resistant hardware security resources in a device. All subsequent *trust*, also called *chain of trust*, depends on this root/anchor. For the sake of simplicity, we prefer to use the term *root of trust (RoT)*. Figure 2.2 shows the relations between *root of trust*, physical security, information security, and privacy objectives.

In general, *RoT* is based on secrets also referred to as root keys. There are two traditional ways to generate root keys. The first method is to inject the keys into the devices during the manufacturing process. After injection, the root key is stored in a one-time programmable non-volatile memory (NVM). The drawbacks of this method are that runtime key generation is not possible and that the key itself does not originate from the device itself. In this case, the root key is similar to a programmed fingerprint, which implies a further security threat in terms of manipulation. In this context, please note that secret keys are just as trustworthy as their origin [33]. The second method to generate root keys is to use an internal random number generator (RNG). In this case, root keys can be changed by using the RNG. Furthermore, an NVM is required that can be reprogrammed, such as electrically erasable programmable read-only memory (EEPROM) and flash memory. The main drawback of this approach is the storage of the root keys which implies a vulnerability against reverse-engineering attacks.

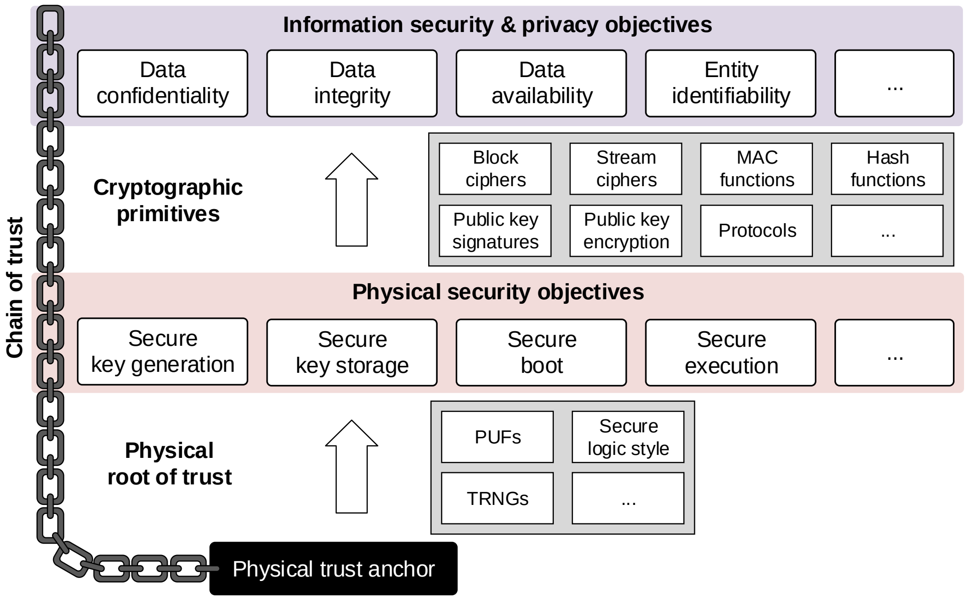


Figure 2.2: Relations between root of trust, physical security, information security, and privacy (cf. [43]).

2.2.3 Cryptology

Cryptology encompasses the subfields cryptography and cryptanalysis. Cryptography deals with the construction of protocols and algorithms to achieve information security goals. On the other hand, cryptanalysis analyzes the security of cryptographic constructions by attempting to break their security. The basic principle of cryptology is that a cryptographic construction can only be considered secure if its internal workings are general knowledge and have successfully withstood cryptanalysis attempts from independent parties [43].

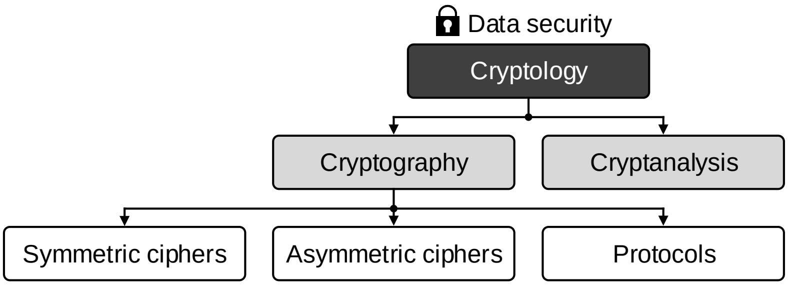


Figure 2.3: Classification of cryptology.

Cryptography was initially concerned with providing secrecy for written messages. In general, the secret information known only be the legitimate parties is the so-called key. The key is used to transform plaintext into a ciphertext (also called cipher), which is also referred to as encryption. In computer technology, it is distinguished between symmetric ciphers and asymmetric ciphers. The former includes algorithms such as the Advanced Encryption Standard (AES) [19], the

Data Encryption Standard (DES) [44], and Blowfish [18]. Widely used asymmetric ciphers are Rivest-Shamir-Adleman (RSA) [45], Digital Signature Standard (DSS) [46], and the Diffie-Hellman-Merkle key exchange protocol [47, 48]. For an extensive overview on cryptographic primitives please refer to [49].

2.2.4 One-Way Functions

Two-way functions are widely used in mathematics exhibiting a predictable dependency between the input and output variable, and vice versa. However, in information security it is not desired that generated keys are reversible. In contrast, a *one-way function (OWF)* is a function that is easy to compute in the forward direction, but hard or infeasible to invert. *OWFs* are widely used in the security area, such as cryptography to encrypt message transmission. In this context, *algorithmic one-way functions (AOWFs)* play a major role being defined as one-way functions that can be expressed as a probabilistic polynomial time algorithm. Basically, the theoretic one-way feature is not verifiable, but in practice it is typically sufficient to achieve a negligible probability of inversion. In this conjunction, the stringent property of one-wayness or non-invertibility is replaced by a probabilistic measure of unpredictability.
Besides *AOWFs*, the intrinsic random variations of physical materials or devices can be used to identify individuals, objects, or systems. For example in the nineteenth century, fingerprint identification of human beings have been introduced which has led to the research field of biometrics. In the later twentieth century, random patterns in material surfaces were used for unique identification based on optical inspections.

In 2001, Pappu [50] introduced a generic definition of *physical one-way functions (POWFs)*, which refers to the state of a physical system that may be dependent on the physical properties of the system itself.

Definition 2.1. *A function is a physical one-way function, if [50]:*

- there exists a deterministic physical interaction between the probe and the system which produces an output in constant time,
- inverting the function using either computational or physical means is difficult,
- simulating the physical interaction is computationally demanding,
- the physical system is easy to make but difficult to clone.

Another early work in this field was proposed by Gassend [51], introducing the term *physical random function (PRF)*. A *PRF* is a function that maps an input-stimulus, namely a challenge, to an output measure, also referred to as the response.

Definition 2.2. *A function is a physical random function, if [51]:*

- the physical device is capable of evaluating the function in a short amount of time (easy to evaluate),

- from a limited number of plausible physical measurements or queries of chosen challenge-response pairs (CRPs), an attacker who no longer has the device, and who can only use a limited amount of resources (time, money, raw material, etc.) can only extract a negligible amount of information about the response to a randomly chosen challenge (hard to characterize).

2.2.5 Security from Intrinsic Process Variations

In the past decades, physical attacks and information leakage turned out as possible security threats for integrated circuits. Many research groups started to develop and investigate countermeasures to these attacks. Particularly side-channel attacks gained a lot of attention. As a promising solution, the emerging research field of *hardware-intrinsic security* is dealing with secure key generation and storage. In this regard, secure keys are generated based on the intrinsic properties of materials and electronic devices, e.g. from physically unclonable functions (PUFs). In silicon technology, process variations can be categorized as wafer-to-wafer (W2W), die-to-die (D2D), and within-die (WID) variations [52]. WID process variations can be split into systematic and random components. The systematic component shows spatial correlations and leads to similar properties in devices that are laid out close. In contrast, the random component shows no correlations across devices and varies arbitrarily [53]. Several device parameters may vary due to process variations such as gate width, device threshold voltage, channel length, oxide thickness, to name but a few [52]. These facts play a major role in *hardware-intrinsic security*, which aims to utilize these phenomenons as a security feature.

As the unique identifiers/keys are inherently present in PUFs in the form of unique physical characteristics, the random intrinsic process variations are used as a pre-initialized non-volatile read-only memory. This means that no permanent key storage is required and that the keys are only present in the digital form for a limited time once generated. This denotes an important security advantage compared to non-volatile memory, whose contents are retained even after powering off the integrated circuit [54]. As a consequence, any physical attack attempting to extract information from the PUF must be carried out while the chip is powered on. It is difficult to execute invasive attacks without modifying the physical characteristics of the PUF itself. Compared to secure digital storage, no continually powered active anti-tamper mechanisms are required to secure the PUF [55]. Another advantage is that the keys can not be influenced from the outside, not even by the manufacturer. To that effect, the secure key derivation is shifted to the hardware, which makes PUFs suitable for lightweight devices and systems. When we talk about 'lightweight' in this context, we think of devices and systems that underlie strict constraints in terms of computing performance, memory, peripherals, area, and power consumption. This allows to utilize lightweight authentication protocols [56, 57] without the need to perform complex cryptographic operations. These unique properties make *hardware-intrinsic security* a promising research direction for the future with a highly practical relevance for many applications. PUF approaches can already be found in commercial products, as discussed in Section 2.5.4. For the sake of completeness, we also mention that other hardware-based concepts such as block and stream ciphers belong to the field of hardware security as well.

2.2.6 Fundamental Security Performance Measures

To assess the quality of security keys, a variety of performance measures do exist. The following definitions describe the fundamental security metrics, mainly originating from information theory.

Hamming Distance

The security keys used in computer technology are typically represented by digital bit strings, whose binary bit values are randomly distributed. Different forms of distance measures do exist to compute the distance $\mathrm{dist}(x, y)$ between two abstract elements x and y. In information theory the hamming distance (HD) is a widely used metric to measure the distance between two bit strings of equal length.

Definition 2.3. *The hamming distance between two binary bit strings $X = \{x_0, \ldots, x_{L-1}\}$ and $Y = \{y_0, \ldots, y_{L-1}\}$ of equal length L is:*

$$\mathrm{HD}(X, Y) = \sum_{l=0}^{L-1} x_l \oplus y_l. \tag{2.1}$$

In many cases it is useful to have a normalized distance metric, i.e. when comparing hamming distances obtained for different key bit widths. The so called fractional hamming distance (FHD) computes normalized distance values between $[0, 1]$.

Definition 2.4. *The fractional hamming distance between two binary bit strings X and Y of equal length L is:*

$$\mathrm{FHD}(X, Y) = \frac{1}{L} \cdot \mathrm{HD}(X, Y). \tag{2.2}$$

Entropy

In cyber security, *entropy* is a measure of the randomness of a data-generating function and represents the foundation for cryptographic functions [58]. Particularly with regard to one-way functions, full *entropy* means that no patterns can be found in the mathematical mapping. In contrast, low *entropy* means that patterns can be detected being used to predict other values. In cryptography, high *entropy* is needed to generate binary sequences used for encryption and hash functions. In this context, the term *entropy source* is frequently used in literature which describes the source of randomness. Potential *entropy sources* are numerous, but the most commonly used are based on hardware such as for example physical variations. In this context, it is distinguished between true sources of randomness and pseudo-randomness. The former is typically based on stochastic physical process variations in hardware. In contrast, pseudo-random numbers are mostly computer-generated using computational deterministic algorithms. The definition of *entropy* was introduced by Shannon in [59] with regard to data communication.

In the binary range of numbers, the *information entropy H* and the *maximum entropy $H_{\max}$* for N symbols are defined according to Equation (2.3) and Equation (2.4), respectively.

Definition 2.5. *The entropy H of discrete random variables (symbols) z_i of the alphabet Z is:*

$$H = -\sum_{z \in Z} P(z) \cdot \log_2(P(z)) \tag{2.3}$$

where $P(\cdot)$ is the probability mass function. An entropy value of 1 means that the keys exhibit the maximum information content.

Definition 2.6. *The maximum entropy $H_{\max}$ for N symbols is:*

$$H_{\max} = \log_2(N) \tag{2.4}$$

The *normalized entropy*, also referred to as *efficiency* η, is defined according to Equation (2.5).

Definition 2.7. *The entropy H of discrete random variables (symbols) z_i of the alphabet Z is:*

$$\eta = \frac{H}{H_{\max}} = -\sum_{z \in Z} P(z) \cdot \log_N(P(z)). \tag{2.5}$$

where $P(\cdot)$ is the probability mass function and N is the number of symbols.

Another option is to determine the so-called *minimum entropy (min-entropy)* of a binary source, as recommended in the NIST specification 800-90 [60]. The *min-entropy* estimate is a more conservative measure than the *Shannon entropy*, since the *min-entropy* value is always less. In the case of the binary range of numbers, for each binary value 0 and 1, the probabilities of occurrence p_0 and p_1 are calculated. The maximum probability $p_{\max} = \max(p_0, p_1)$ is used to estimate the *min-entropy*.

Definition 2.8. *The worst-case entropy, the so-called min-entropy $H_{\min}$, for a random variable is:*

$$H_{\min} = -\log_2(p_{\max}) \tag{2.6}$$

where $p_{\max}$ is the maximum probability value.

Bias
In cryptography, the binary values of the security keys should be equally distributed. If a key-generating function outputs bit strings that are biased towards 0 or 1, the overall key entropy is reduced. This means that attackers can find patterns and predict other keys. In general, the entropy and the *bias* metrics are strongly correlated when assessing the security performance. We decided to use the generic term *bias* in the context of security. Particularly in the field of PUFs the term *bit aliasing* is more common [61].

Definition 2.9. *The bias B_i for N keys of equal length at bit position i is:*

$$B_i = \frac{1}{N} \sum_{n=1}^{N} \Phi_{n,i} \tag{2.7}$$

where $\Phi_{n,i}$ is the n-th key. A bias value of 0.5 denotes that 0s and 1s are equally distributed. Bias values less or greater than 0.5 indicate that the corresponding bit position is biased towards 0 or 1, respectively.

2.3 Physically Unclonable Functions – Concepts and Definitions

2.3.1 PUF Definition & Properties

A physically unclonable function (PUF) is a one-way expression of an inherent and unclonable instance-specific feature of a physical object, comparable to biometric features of human beings like fingerprints. From a more technical point of view, a PUF is a physical device representing a function that maps challenges to responses. It should be easy to evaluate the function, but hard to characterize by measurements [62]. The term *physical(ly) unclonable function* (PUF) has established as the most commonly used denotation in literature.
A wide variety of PUF constructions have been proposed, covering many different manufacturing technologies, materials, and physical phenomenons. The earliest works presented by Pappu [50], Gassend [51], Maes et al. in [63], and Armknecht et al. [64] deal with the generic description of PUFs and the true properties being required. All definitions include the properties of *uniqueness*, *unpredictability*, and *unclonability*. In this section, we introduce the most important properties of PUFs based on a comprehensive literature research.

Uniqueness
The *uniqueness* property describes how uncorrelated PUF responses are across different hardware instances. In a given set of PUF instances, each single PUF shall be clearly recognizable due to its CRP set. The number of CRPs required to identify a PUF instance might differ depending on the *uniqueness* of the PUF responses. The *uniqueness* measure is provided by the inter hamming distance (inter-HD) introduced in Section 2.3.4.

Unpredictability
The *unpredictability* property is strongly connected with unclonability, but is not limited to it. In the context of PUFs, *unpredictability* means that CRPs must be independent to make it impossible for an attacker to predict other CRPs with that knowledge.

Unclonability
In most definitions, the *unclonability* property is the core property of a PUF and refers to the impossibility of an attacker to create a physical clone. Since PUFs rely on the random manufacturing variations of physical devices, *unclonability* also includes that the physical characteristics being used for the PUF output generation must be out of control from the manufacturer. This ensures that no specific replicates of PUFs can be fabricated. At this point we also want to discuss the difference between the terms *physical* and *physically* unclonable functions, which both can be found in literature. In literature the term *physical* is more widespread and defines a physical object that is hard to be cloned in any way. In this context, Maes et al. [63] bind the properties *uniqueness* with *physical unclonability* and *unpredictability* with *mathematical unclonability*. This definition seems to be more appropriate, especially in the light of recent research activities in this field. By definition it should be hard to create a *physical* clone of a PUF, even for the actual manufacturer. If we can not produce a *physical* clone we use the adverb and say that the PUF is *physically* unclonable. In this case we believe that the term *physically* is more fitting. This argument strengthens if we consider that most of the PUF designs have been mathematically cloned using model-based attacks.

Reproducibility
The *reproducibility* property describes that PUF responses should be equal (or at least close) when applying the same challenge. This property distinguishes PUFs from true random number generators (TRNGs), which are supposed to output random bit strings independent from outside influences. The *reproducibility* measure is provided by the intra hamming distance (intra-HD) introduced in Section 2.3.4.

One-Wayness
The *one-wayness* property goes back to the earliest definitions of PUFs which are described in Section 2.2.4. The origin of one-way functions can be found in cryptography.

Tamper Evidence
In the early years of PUF research, mainly optical PUF constructions have been proposed where *tamper evidence* was a useful property. Recent PUF constructions are mainly based on variations that lead to unique electrical characteristics of circuits. In this regard, *tamper evidence* is hard to achieve and therefore faded into the background in the past years. Since most of the PUF constructions do not provide this property, it does not qualify for a generic definition of PUF properties. Nonetheless, we want to mention that latest research activities in the field of novel material science are promising to provide *tamper evidence* for electrical PUFs in the future.

2.3.2 Challenges and Responses

A PUF is a physical one-way function that takes an input, the so-called *challenge*, and produces one or multiple output bits, namely the *response* R. Depending on the PUF construction, *challenges* can adopt different forms. For example in optical PUFs, *challenges* often consist of coordinates and angles to focus a laser beam on the surface to be evaluated [65]. In electrical PUFs, *challenges* mainly comprise binary bit strings that specify the internal PUF configuration. The tuples (C_i, R_i) are called challenge-response pairs (CRPs), where i denotes the index of the *challenge* and the corresponding *response*.

Definition 2.10. *The PUF response R_i for a given challenge C_i is:*

$$R_i = f_{\text{PUF}}(C_i) \tag{2.8}$$

where $f_{\text{PUF}}(\cdot)$ is the PUF behavior expressed as a function and i is the index of the challenge and the corresponding response.

2.3.3 Weak and Strong PUFs

In the past years, many PUF constructions have been introduced based on different methods to evaluate process variations. This led to the question which properties can be compared with each other. One comparable property is the number of CRPs that can be generated from a certain PUF. In this regard, the categorization of *weak* and *strong* PUFs was introduced.

Weak PUFs exhibit a low number of CRPs, in the extreme case just a single CRP. More specifically, in *weak* PUFs the CRP space scales polynomially (often linearly) with the area

footprint. *Weak* PUFs are also referred to as physical obfuscated keys (POKs) [51]. Typical application scenarios include private key generation. To protect the secret key(s) from attackers, the interfaces are often obfuscated by applying additional hash functions to the PUF responses. This PUF configuration is also called *controlled PUF* [51].
In contrast, *strong* PUFs can produce large numbers of individual CRPs and scale exponentially. The extent CRP space allows to use each CRP for a single time and then mark it as expired. In theory, the CRP must not even be hidden from attackers. Possible target applications include authentications of manufacturers to legitimate their products. However, the property of exhibiting a large CRP space can also become a security threat. Recently, many PUF constructions have faced model-based attacks to predict CRPs. We want to note that the terms *weak* and *strong* can be misleading. There is no implication that *weak* PUFs offer a lower degree of security than *strong* PUFs.

2.3.4 PUF-Specific Security Metrics

Various PUF security metrics have been defined by researchers in the community. Hori et al. in [66] and Maiti et al. in [61] proposed PUF metrics to assess and compare the performance of PUFs. For our evaluations, we utilize the security metrics *uniqueness*, *reliability*, *bit aliasing*, and *uniformity* defined by Maiti et al. [61], which are widely used in literature.

Uniqueness – Inter Hamming Distance Measure
The PUF property *uniqueness*, as described in Section 2.3.1, is a measure of how uncorrelated PUF responses are across different PUF instances using the same challenge. The corresponding mathematical measure is referred to as *inter hamming distance (inter-HD)*.

Definition 2.11. *The inter hamming distance* $\mathrm{HD}_{\mathrm{inter}}$ *for two PUF instances i and j is:*

$$\mathrm{HD}_{\mathrm{inter}} = \mathrm{FHD}(R_i, R_j) \tag{2.9}$$

where R_i and R_j are two responses from different PUF instances after applying the same challenge.

Definition 2.12. *The mean inter hamming distance* μ_{inter} *for a population of N PUF instances is:*

$$\mu_{\mathrm{inter}} = \frac{2}{N(N-1)} \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \mathrm{FHD}(R_i, R_j) \tag{2.10}$$

where i and j are two different PUF instances, each having L-bit responses R_i and R_j after applying the same challenge.

Reliability – Intra Hamming Distance Measure
In Section 2.3.1, we have described the PUF property *reproducibility* as a measure of how equal responses to the same challenge and PUF entity are. This means that the *reproducibility* is only dependent on the impacts affecting a single PUF instance. The corresponding mathematical measure is called *intra hamming distance (intra-HD)* which is the foundation for the *reliability* metric.

Definition 2.13. *The intra hamming distance* $\mathrm{HD}_{\mathrm{intra}}$ *for the PUF instance n is:*

$$\mathrm{HD}_{\mathrm{intra}}(n) = \frac{1}{T}\sum_{t=1}^{T} \mathrm{FHD}(R_n, R'_{n,t}) \tag{2.11}$$

where R_n *describes the reference response and* $R'_{n,t}$ *is the t-th PUF response of a total of T responses obtained from a repeatedly applied challenge.*

The mean *intra-HD* value corresponds to the bit error. To obtain the reliability of the PUF response generation, the μ_{intra} value (bit error) is subtracted from 1.

Definition 2.14. *The mean intra hamming distance* μ_{intra} *for a population of N PUF instances is:*

$$\mu_{\mathrm{intra}} = \frac{1}{N}\sum_{n=1}^{N} \mathrm{HD}_{\mathrm{intra}}(n). \tag{2.12}$$

Bit Aliasing

If single PUF response bits are strongly biased towards 0 or 1, different PUF instances produce nearly identical responses. Similarly, this also reduces the entropy of the responses. *Bit aliasing* can be caused by factors such as systematic process variations [67]. The *bit aliasing* metric is a measure of the 0's and 1's distribution for each single bit position in responses generated from *N* PUF instances for a fixed challenge.

Definition 2.15. *The bit aliasing* BA_l *for a population of N PUF instances is:*

$$\mathrm{BA}_l = \frac{1}{N}\sum_{n=1}^{N} r_{n,l} \tag{2.13}$$

where $r_{n,l}$ *is the l-th bit of a L-bit response of PUF instance n, obtained for a fixed challenge. The ideal value is 0.5, which denotes that 0 and 1 are equally distributed at PUF response bit position l.*

Uniformity

The *uniformity* metric is a measure of the balance of 0s and 1s in the response bits of a PUF. Ideally, for truly random PUF responses the proportion between 0s and 1s should be equal.

Definition 2.16. *The uniformity* U_n *for the PUF instance n is:*

$$U_n = \frac{1}{L}\sum_{l=0}^{L-1} r_{n,l} \tag{2.14}$$

where $r_{n,l}$ *is the l-th bit of a L-bit response. The ideal value is 0.5, which denotes that the numbers of 0s and 1s are equal for PUF instance n.*

2.3.5 PUF-Based Identification & Authentication

The terms *identification* and *authentication* have very broad meanings and therefore often lead to confusion when not described in more detail. In general, *identification* refers to the identity of a subject [68]. To clearly distinguish an object from others in a group, the identity must be uniquely assigned. To give an example, on website logins usually the email address is used as the user's identity. Based on the email address, the website provider can determine whether an account for the given user exists. On that note, the identity alone does not ensure that the user that has entered the email address is the owner of the login account. At this point, the *authentication* comes into play. Generally speaking, *authentication* proves that an identity is genuinely what it claims to be or counterfeit [69].

In information security, it is usually distinguished between *message authentication* and *entity authentication* [70]. The difference between both is that *message authentication* does not include any guarantee that proves when the message was created. In *entity authentication*, the verifying party can prove the identity in real-time through actual communications [49]. In the following discussions we focus on *entity authentication*, which is implied for PUF-based *authentication*. In the literature, the terms *identification* and *entity authentication* are often used synonymously. However, when we talk about *identification* we solely mean the identity of an object, whereas with *entity authentication* we intend the legitimation of an object's identity.

In electronic devices, identities are typically provisioned trough the assignment of identifiers to a device. The provisioning party generates an unique identifier, mostly by using monotonic counters or TRNGs. The identifiers must be stored permanently, which denotes an intrusion from the provisioning party into the actual device. In contrast, PUFs can provide *inherent identities* which connotes a practical advantage and brings a higher level of security. In [71], O'Neill has shown that PUFs can provide both device *identification* and *authentication*, while being tamper resistant. The process of generating inherent identities is called *enrollment*, which implies that the identity is only read from the device but not written to it. On the downside, *inherent identities* are completely out of control from the manufacturer. This can be an issue in cases where the identity should carry additional information about the device, such as a serial number that contains the device's production date. Another specialty of *inherent identities* is their *fuzzy* random behavior. In this context, the term *fuzzy* means that the identifiers are not entirely uniformly distributed and not perfectly reproducible [43]. In PUFs, the identifiers or responses are typically non-uniformly distributed and are subject to noise and environmental impacts.

To perform *identification* and *entity authentication* with PUFs, the *fuzziness* of the PUF responses must be determined. The intra-HD and inter-HD distributions describe the reproducibility and uniqueness of the PUF responses, as already introduced in Section 2.3.4. Ideally, the intra-HD would be zero, which means that the PUF responses can be reproduced reliably (without errors). This would also mean that the responses are not *fuzzy*. The inter-HD is ideally at exactly 50 % of the response bit width, which denotes uniformly random distributed responses. Although, this does not correspond to the reality. To use *inherent identities* in practical applications, the *fuzziness* has to be taken into account. During *identification*, the extracted PUF response is compared with the identifier obtained in the *enrollment* phase by using the hamming distance measure. In this context, we use the intra-HD and inter-HD distributions to show the coherence between the reproducibility and uniqueness measures. Figure 2.4 shows the example intra-HD and inter-HD distributions of a hypothetical PUF. Since the intra-HD is noticeably smaller than the inter-HD, there is some degree of identifiability in the system. The overlap between both distributions denotes *fuzzy* responses.

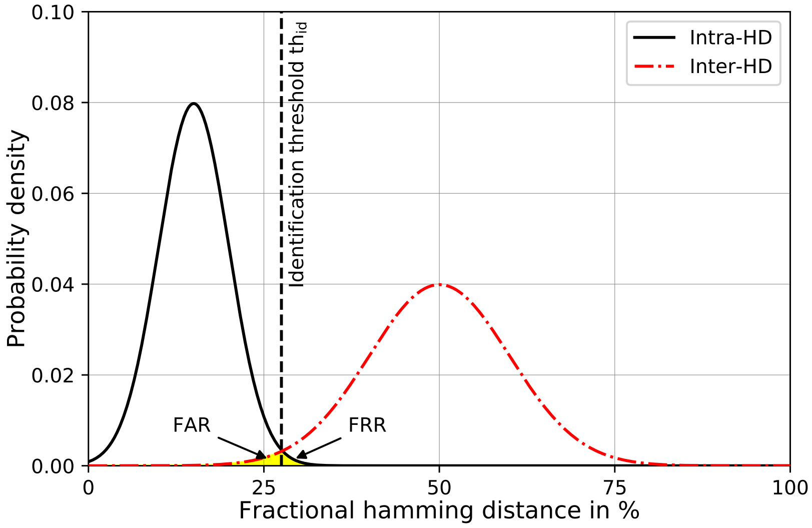


Figure 2.4: Exemplary intra-HD and inter-HD distributions for a PUF-based identification system. The overlapping region is split by the identification threshold into the false-acceptance-rate (FAR) and the false-rejection-rate (FRR).

To achieve a high probability of true identifications, typically a so called *identification threshold* value is used to distinguish between single entities and find matches. It is obvious that the optimum threshold value must be set somewhere in the area of the overlapping region of the intra-HD and inter-HD distributions. Thereby, the enclosed area is split into two sub-regions, where the left one is denoted as the *false-acceptance-rate* (FAR), and the right one is the *false-rejection-rate* (FRR). As a consequence, reducing the *identification threshold* also decreases the FAR and increases the FRR, and vice versa. In general, the trade-off to find the optimum FAR and FRR values is application-dependent. The FAR value is strongly related to security since false acceptances denote mistaken identifications. This means that in cryptographic applications, the FAR value ideally should be reduced to zero. On the other hand, the FRR value is connected with the convenience of an identification system. Increased *identification threshold* values lead to less false rejections. To sum up, we can say that the determination of an appropriate *identification threshold* is a trade-off between security (low *FAR*) and convenience (low FRR). In practice, it is often useful to minimize both values and therefore set the *identification threshold* to the point where FAR=FRR, which is also referred to as the *equal-error-rate (EER)* [72]. The corresponding *equal-error-threshold* value is denoted as $\mathrm{th_{EER}}$.

The exact values for FAR and FRR can be calculated by using the probability density functions $P_{\text{intra}}(\cdot)$ and $P_{\text{inter}}(\cdot)$ of the intra-HD and inter-HD distributions, respectively.

Definition 2.17. *The false-acceptance-rate (FAR) for a given identification threshold* $\mathrm{th_{id}}$ *is:*

$$\mathrm{FAR}(\mathrm{th_{id}}) = \int_0^{\mathrm{th_{id}}} P_{\text{inter}}(x)\ dx \tag{2.15}$$

where $P_{\text{inter}}(x)$ *is the probability density function for the inter-HD distribution.*

Definition 2.18. *The false-rejection-rate (FRR) for a given identification threshold* $\mathrm{th}_{\mathrm{id}}$ *is:*

$$\mathrm{FRR}(\mathrm{th}_{\mathrm{id}}) = \int_{\mathrm{th}_{\mathrm{id}}}^{L} P_{\mathrm{intra}}(x)\ dx \tag{2.16}$$

where $P_{\mathrm{intra}}(x)$ *is the probability density function for the intra-HD distribution and L is the PUF response bit width.*

We also want to note that the identifiability is strongly connected with the term 'easy to evaluate' which belongs to the basic properties of PUFs.

2.4 Printed Electronics

2.4.1 Printed Electronics and Silicon Electronics

In the past decades, printed electronics (PE) has gained a lot of attraction by research groups worldwide from academia and industries. PE promises to combine electronics manufacturing with additive graphic printing. This enables new form factors, large-area structures, flexible substrates, novel materials, and green or sustainable electronics [73]. Furthermore, PE benefits from low-cost and on demand fabrication at point-of-use [74]. Potential applications can be found in all market segments such as foldable displays [75] in consumer electronics, large-area sensor networks [76] in the industry, batteries [77], energy harvesters [78], and adhesive patches [79] in healthcare, to name but a few. In [73] Chang et. al review PE-based electronic standard components.

Recent progress in nanomaterial science has brought metallic, organic, and inorganic nanomaterials and their processes to PE. The more degrees of freedom also enable to print on rough substrates and under different angles, which makes PE technology also interesting for custom wire traces and interconnects [80]. Compared to conventional silicon-based chip manufacturing, different materials and processes can be used. Figure 2.5 compares the printing resolution among various printing techniques and shows their operational areas. Gravure printing [81], flexographic printing [82], screen printing [83], and nanoimprint lithography [84] belong to the class of contact printing, whereas inkjet-printing is a non-contact printing technique [85].

The current trend of digitization demands more electronic systems than already used today. Everyday objects will be equipped with some sort of intelligent electronics capable of communicating with other devices. In this regard, circuits must be thin, lightweight, and inexpensive. This depicts the unique feature of PE in contrast to silicon technology. Table 2.1 compares PE and conventional silicon-based electronics. The comparison clearly shows that both technologies are complementary. Hence, it is not expected that PE will substitute silicon-based electronics [86]. Instead it will develop entirely new markets and industries by opening new opportunities for high-volumne and low-cost printed circuits. On that note, new device architectures may combine the advantages of both technologies, which is also referred to as *hybrid systems*. In the subsequent section we focus on the inkjet-printing technology, which is widely used in research and development.

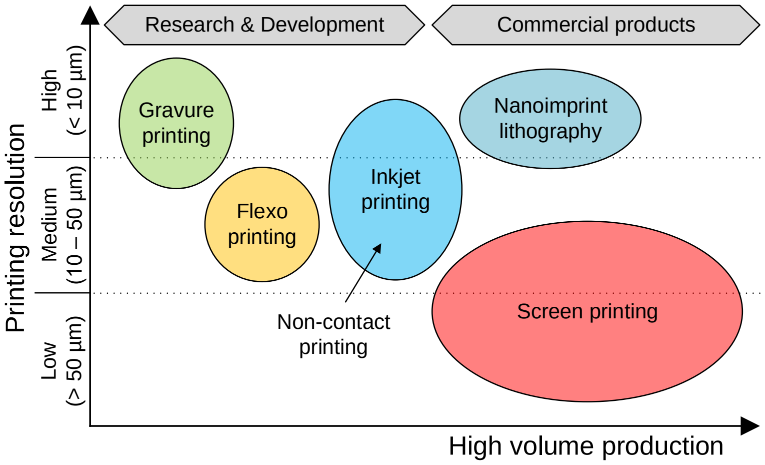


Figure 2.5: Printing resolution and high volume production capabilities for various printing techniques.

Table 2.1: Comparison of printed and conventional silicon-based (solid state) electronics.

	Printed Electronics	Silicon Electronics
Performance	Low	High
Design complexity	Low	High
Area per feature size	High	Low
Cost per unit area	Low	High
Device variations	High	Low
Throughput	High	Low
Substrate	Flexible	Rigid
Production site	Decentralized	Centralized
Lifetime	Short	Long

2.4.2 Inkjet-Printing Technology

Inkjet printing is a non-contact printing technology, where droplets of inks are precisely deposited from a nozzle onto the printing substrate. The printing system is controlled directly by an image processor that works on the basis of the digital print job format. Since inkjet-printing is entirely digitally and electronically controlled, it is also referred to as digital printing. Inkjet-printers can be classified either as continuous or drop-on-demand systems. The former provides a continuous stream of ink drops during the printing process. In drop-on-demand systems, the ink droplets are only generated if required. Nowadays, most of the commercially available inkjet-printers are drop-on-demand printers based on piezoelectric, thermal, or electrostatic systems. Figure 2.6 shows the functional principle of a piezoelectric inkjet-printer nozzle. The piezoelectric ceramic expands based on the printing signal and the ink droplet is deposited from the nozzle.

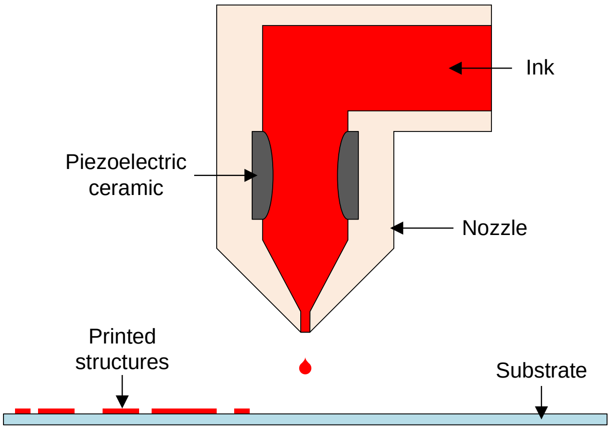


Figure 2.6: Schematic of the piezoelectric drop-on-demand inkjet-printing approach.

Inkjet-printers typically use liquid inks with low viscosity, which requires a further drying process through evaporation and absorption. The advantages of inkjet-printing technology include printing pattern adjustments and high quality prints on a variety of substrates. The major drawback is that the throughput is limited, even if using multiple print heads. For further information on inkjet-printing please refer to [87, 88].

2.4.3 Organic vs. Inorganic Semiconductor Materials

Semiconducting materials which change their conductivity with operating conditions are the basis for active electronic devices. Organic semiconductors may be deposited by low temperature and can be processed under less controlled environments than inorganic semiconductors, which makes them attractive for low-cost lightweight electronics [73, 89]. One of the major challenges in organic semiconductors is the material's instability to environmental conditions including atmospheric oxygen, ambient humidity, and light [90]. On the other hand, inorganic semiconductors show higher carrier-carrier mobilities, environmental stability, and superior electrical properties such as low-voltage operation [91]. These features make inorganic semiconductor materials suitable for higher performance electronic devices [92]. The low-voltage capabilities make inorganic semiconductors interesting for hybrid systems, due to the direct compatibility on the logic level of silicon and PE components.

To achieve a high lifetime of circuits incorporating active components, the materials and solvents have to be compatible and the semiconductors must be encapsulated from environmental impacts through additional passivation layers [88, 92–94]. A comprehensive introduction into organic and inorganic materials as well as decapsulation techniques is given in [95].

2.4.4 Electrolyte-Gated Field-Effect Transistors

The electrolyte-gated field-effect transistor (EGT) is a n-type transistor with an inorganic high intrinsic mobility semiconductor based on indium oxide (In_2O_3). Figure 2.7 shows the material stack of the EGT. The transistor's drain and source electrodes as well as the electric signal routing layer consists of laser-ablated indium tin oxide (ITO). The insulator between the semiconductor and the top-gate electrode is realized with a composite solid polymer electrolyte (CSPE), which provides a high gate capacitance. This allows for low voltage operation of the EGTs. The top-gate electrode is based on PEDOT:PSS. The inorganic semiconductor material including the electrolyte enables high performance at low supply voltages at ~ 1 V. Further information on the characteristics of EGTs can be found in [96, 97].

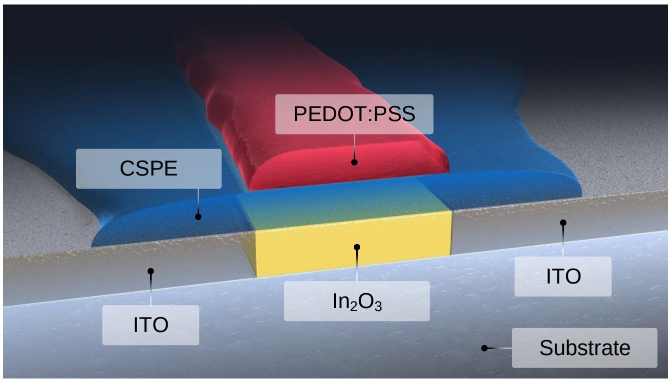


Figure 2.7: Material stack of the electrolyte-gated field-effect transistor (EGT) (cf. [98]).

2.4.5 Security for Printed Devices and Systems

In times of the IoE, devices are typically interconnected and managed through networks or via the Internet. One of the major challenges is therefore the exact identification of devices and to secure communication when using compromised communication channels such as wireless technology. Most of the conventional security solutions, such as asymmetric key establishment methods [47, 48], are based on mathematically proven foundations. More specifically, random numbers generated through software-based computational or hardware-based methods are the basis for cryptography. One well-known example is the Advanced Encryption Standard (AES) [19] that offers a high level of security.

Emerging technologies such as PE will further expand the IoE with new, especially lightweight devices that are subject to strict design and performance constraints. Because of the differences in fabrication and electrical characteristics between conventional silicon-based and PE technologies, existing security solutions cannot simply be adopted. In PE, particularly in digital printing, there are two shortcomings that lead to increased variations. First, the limiting printing resolution and second, the small quantities of materials in the form of nanoparticle-inks which show sensitive interactions with the substrate.

In this respect, hardware-intrinsic security presents a very promising research field for providing lightweight and high-quality security primitives. Furthermore, the PE's drawback of exhibiting high variations can be turned into a security feature when using the intrinsic variations as an entropy source for random number generation. In this regard, PUFs are very promising to provide security for PE-based devices and systems. Furthermore, also hybrid systems incorporating silicon-based and PE components can benefit from the increased variations of the printed part. At the same time, the decentralized manufacturing capabilities of PE technologies present a root of trust compared to foundry-fabricated fully silicon systems. In this context, PE offers to fabricate the printed circuits in-house, which pushes the concept of 'root of trust' to a higher level. If the device is powered off, no secret key can be found in any memory, which means that the root key is invisible.

In general, PE technology brings new security needs, constraints, risks and implications which need to be elaborated. Very recently, several researchers proposed first approaches for printed PUFs. Often it is not straightforward to clearly distinguish between printed PUFs and PUFs just based on novel materials. In Sections 2.5.2 and 2.5.3 we review and classify a selection of existing PUFs. In some cases, the crucial factor for a PUF to belong to the class of printed PUFs is the fabrication process. On that note, we assign PUFs that are based on novel materials but not printed to the class of novel material PUFs.

2.5 State of the Art of PUFs

2.5.1 Silicon-Based PUFs

This section gives an overview about different state of the art PUF types in silicon technology. At this point, we further distinguish between *electrical PUFs* and *optical PUFs*. The reason behind can be found in the evaluation complexity. While *electrical PUFs* leverage the unique electrical characteristics of integrated and compact hardware circuits to generate responses, *optical PUFs* use complex mechanisms to sense the surface of materials and objects. If we remember the PUF definition from Section 2.3.1, the attribute 'easy to evaluate' only holds true for *electrical PUFs* due to their integration capabilities and technology compatibility. Analog PUFs, arbiter PUFs, ring oscillator PUFs (RO-PUFs), memory-based PUFs, and coating PUFs belong to the class of *electrical PUFs*.

Analog PUFs
PUF designs that capture the variations as analog information are also referred to as analog PUFs [99]. Lofstrom et al. [100] introduced the integrated circuit identification (ICID) approach to generate unique and unclonable identifiers based on the intrinsic process variations of the silicon. This is the first implementation of an electrical PUF referring to intrinsic fingerprint extraction and unclonable identifiers. Saha et al. [101] proposed the threshold voltage PUF (TV-PUF), which is an advancement of the ICID approach. To magnify the impact of MOSFET threshold voltage variations, they use cascaded NMOS transistors in series. Vijayakumar et al. [99] investigated non-linear voltage transfer characteristics (NLVTC-PUF) to provide secure PUF authentication.

Arbiter PUFs
Arbiter PUFs are based on delay paths that are activated simultaneously. The response is decided on which path was dominating by having a faster signal propagation. Usually, the delay paths consist of numerous multiplexers that can be configured by an external challenge. The advantage of arbiter PUFs is that they have direct challenge and response interfaces without the need for a further evaluation logic. Lee et al. [102] and Lim et al. [103] proposed the first arbiter PUFs to build secret keys for identification and authentication applications, as shown in Figure 2.8. Typically, arbiter PUFs are used as strong PUFs where the CRPs are not further obfuscated and are publicly available. In various works, researchers have successfully attacked and modeled arbiter PUFs through machine learning attacks [104, 105]. As a countermeasure,

several variants of the arbiter PUF have been proposed to introduce additional non-linearity to provide more resistance [106, 107]. Nonetheless, also these variants have been successfully modeled by attackers [108, 109].

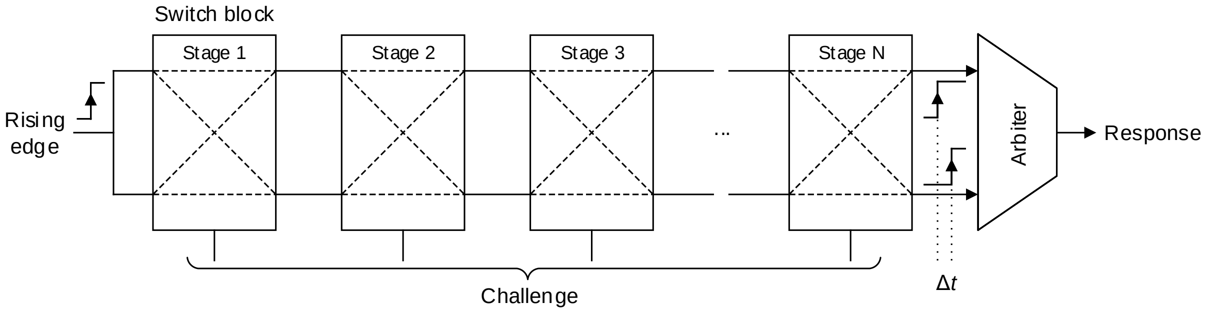


Figure 2.8: Basic N-stage arbiter PUF architecture.

Ring Oscillator PUFs

A ring oscillator (RO) is a chain with odd numbers of inverting logic elements. The output signal of the last inverter stage is fed back to the first element. As a consequence, the RO oscillates with a specific frequency that is variation-dependent. Suh et al. [110] introduced the first RO-PUF design, as shown in Figure 2.9. The RO-PUF consists of an array of identical ROs which can be arbitrarily addressed in pairs. Based on the challenge, the outputs of the addressed ROs are multiplexed to two counters to measure the oscillation frequencies. Based on which frequency was higher, a single response bit with the binary value 0 or 1 is generated.

RO-PUFs consist of standard logic elements that can be easily implemented in field programmable gate arrays (FPGAs), which is one of the main advantages. Since the CRP space of the architecture scales polynomially, RO-PUFs are weak PUFs. Nonetheless, many implementations target to extract low to medium numbers of keys [111–113], which makes it also interesting for attackers to model RO-PUFs [114].

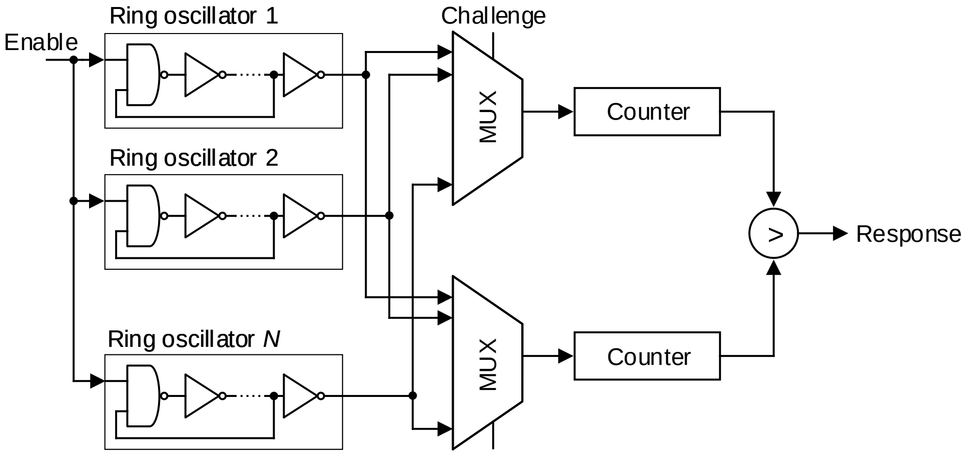
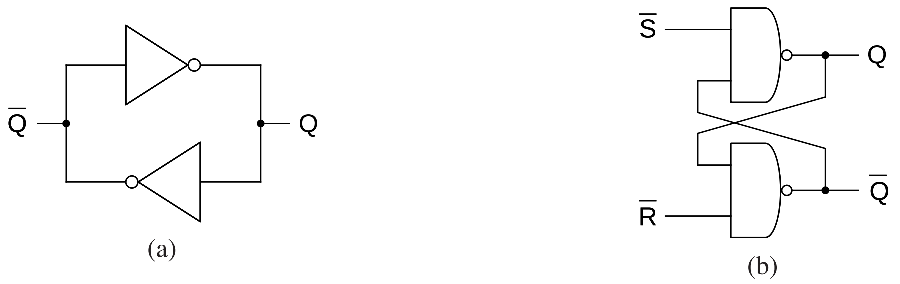


Figure 2.9: Basic RO-PUF architecture with N ring oscillators.

Memory-Based PUFs

Memory-based PUFs are based on the undefined power-up state of cross-coupled inverter cells. The first memory-based PUF using SRAM cells was introduced by Guarjardo et al. [115] to protect the intellectual property (IP) in FPGAs. Figure 2.10a shows the logical circuit of an SRAM cell. SRAM-PUFs [116] and butterfly PUFs [117] are the most widespread memory-based PUFs that can be found in literature and are also referred to as bistable PUFs. Butterfly PUFs are based on latch logic gates, as shown in Figure 2.10b. In memory-based PUFs, the challenge is the powering up of the supply voltage. The advantages of memory-based PUFs are that the response is directly available in the memory and that standard cells can be used to implement them into FPGAs. At this point we want to note that many FPGAs perform startup memory initialization when powering up the device, which hinders to implement PUF functionality. Furthermore, several works can be found in literature dealing with attacks on memory-based PUFs [118–120].



(a)

(b)

Figure 2.10: Basic logical circuits of (a) an SRAM cell and (b) a latch.

Coating PUFs
Coating PUFs have a layer wrapped around the integrated circuit or printed circuit board. Tuyls et al. [121] introduced the first coating PUF based on local variations in capacitances. The response is generated based on measurements of the unique pattern of the capacitances. The advantage of coating PUFs is that touching the security primitive can change the responses. This can be used to guarantee tamper-evidence. However, coating PUFs are relatively complex and therefore not often used.

Optical PUFs
Optical PUFs exploit imperfect speckle patterns as an entropy source to generate unique identifiers. The first optical PUF was proposed by Pappu et al. [122]. A challenge mainly comprises laser coordinates and angles to inspect the object carrying the variations to be evaluated. The advantage of optical PUFs is that no circuitry is required on the PUF-carrying object [65]. However, this research did not really proceed because of the many drawbacks that come with the optical inspections needed for PUF response generation. In the most cases, high-cost equipment such as microscopes, image processing, and optical readout for reliable key generation are required, which is disadvantageous for high-volume applications.

2.5.2 Printed PUFs

Printed PUFs is a very young research field in the scope of hardware-intrinsic security. Currently, there are two *electrical PUFs* based on memory cells and one *optical PUF* design that can be found in the literature.

Memory-Based PUFs
Guerin et al. [123] have designed and fabricated an all-organic sheet-to-sheet processed RFID tag incorporating an SRAM-PUF structure with four output bits. The PUF is used to generate random identification numbers for the RFID tags. No performance measures have been carried out in this work. Typically for organic PE, the supply voltage of 20 V is relatively high. For the special case of RFID technology, the increased supply voltage is no obstacle, since RFID tags are often powered by the reader device.
In another work, Erozan et al. [124, 125] have designed, fabricated, and evaluated an inkjet-printed memory-based PUF. The design is based on inorganic EGTs and shows good results regarding the uniqueness and reliability metrics. The advantage of this PUF implementation is that it can operate at supply voltages as low as 0.5 V. This makes the memory-based PUF suitable the integration into IoT devices and for lightweight authentication.

Optical PUFs
Liu et al. [126] have presented inkjet-printed anti-counterfeiting labels based on quantum dot fluorescent materials. For the PUF authentication, a (portable) microscope and artificial intelligence (AI) are required. The proposed security labels target applications where a line of sight between the label-equipped object and the authenticating device does exist.

2.5.3 Novel Material PUFs

Very recently, researchers have proposed PUF designs based on novel materials. The initial motivation for novel security primitives originates from the desire to achieve more secure, robust, and lightweight PUF designs. Novel materials offer unique properties such as substantial process variations, small footprints, multi-level bits capability of memory cells, reconfigurability, and lower energy consumption [127].

Carbon Nanotube PUFs
Konigsmark et al. [128] have presented the carbon nanotube PUF (CNPUF) based on carbon nanotube field-effect transistor (CNFET) characteristics. The advantages of the CNPUF include higher reliability against environmental variations and increased resistance against modeling attacks. Furthermore, they achieved a lower energy consumption compared to low-power silicon-based PUF designs. In [129] Hu et al. presented another PUF based on carbon nanotubes. In their work, they exploit the connection yield and switching behavior of carbon nanotube devices in an array structure to achieve a ternary-bit architecture. The ternary-bit logic strengthens the security capabilities of the PUF.

Memory-Based PUFs
Another promising research direction is the phase change memory PUF (PCM-PUF) utilizing the crystalline and amorphous nature of phase change materials [127]. The advantage of PCM is that each cell has the ability to store multiple bits. For response generation, the resistance of the PCM cells is measured and evaluated. Kursawe et al. [130] proposed the first PUF based on PCM cells, called reconfigurable PUF (rPUF). The advantage of their approach is that the phase change mechanism can be used to transform an rPUF into a new PUF with new unpredictable CRPs.

Memristor PUFs

In the past decade, memristors gained a lot of attraction in the research community. Several research groups have presented memristor PUFs (M-PUFs) as variants of memory-based PUFs [131–134]. The reconfigurability and reduction of area size compared to silicon-based electronics belongs to the main advantages.

Ring Oscillator PUFs

Kuribara et al. [135] have proposed an organic RO-PUF to generate unique identifiers. The ROs were fabricated using thermal evaporation and solution processes. At this point we want to note that their work does not include peripheral logic circuitry such as multiplexers and frequency counters. Although the RO-PUF offers the potential of being fabricated with PE technology, we categorize it into the novel materials section since it was not printed.

Optical PUFs

Optical PUFs face major drawbacks concerning the integration capabilities into electronic devices. Nonetheless, in the past years various optical PUF designs based on novel materials have been proposed. The reason for this development is that novel materials offer new possibilities to break the limitations of conventional technologies. In the literature, novel optical PUF designs can be found based on volumetric physical storage [136], randomly distributed nanowires [137], plasmonic nanoparticles [138], imaging of excitation-selected lanthanide luminescence [139], multi-mode optical waveguide [140], and biological human T-cells [141]. The advantages of these optical PUFs are mainly the huge CRP spaces (strong PUFs) and the tamper-evidence.

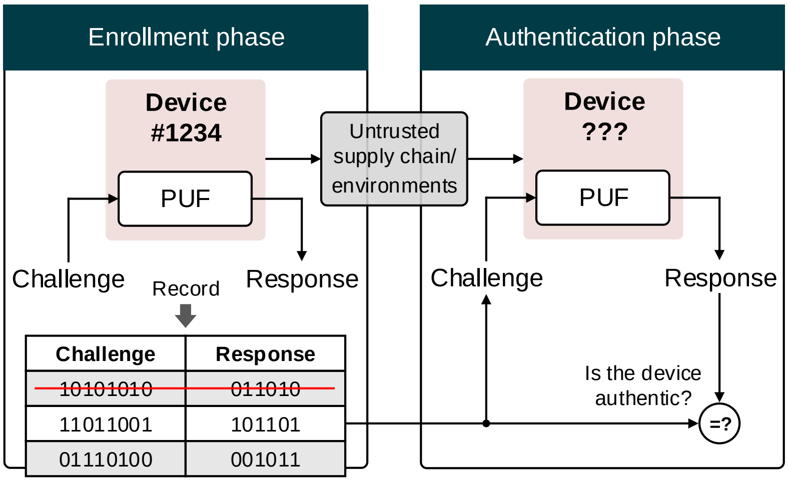
2.5.4 PUF Applications & Available Commercial Products

From the application perspective, weak PUFs are normally used in device identification, cryptographic key generation and storage, as well as IP protection. In the special case of cryptography, PUFs do not require expensive cryptographic hardware such as the secure hash algorithm (SHA) or public/private key encryption algorithms to generate secure keys [55]. On the other hand and due to the exponential CRP space, strong PUFs are mainly used for low-cost authentication, where each CRP is only used once in the lifetime of the PUF [142]. Figure 2.11 visualizes the device authentication scenario including a PUF. A comprehensive overview on cryptographic protocols including authentication can be found in [143].

PUFs can already be found in various commercially available products. This shows that the field of hardware-intrinsic security is not only attractive for academia but rather inspires engineers to bring this technology into products.

A product review regarding PUFs in commercial products shows that FPGA and system on a chip (SoC) manufacturers started to integrate PUFs into their boards natively. Examples include the Xilinx Zynq UltraScale+ FPGA devices [144] with a built-in PUF to derive strong and device-unique cryptographic keys. The Intel Stratix 10 FPGA/SoC platform [145] includes a PUF for key protection and hardware identity. The Microsemi Corporation integrated a PUF into their SmartFusion2 FPGA/SoC platform [146] to implement advanced security functions based on unique device biometrics. NXP integrates a PUF into the LPC54S0xx microcontroller family [147] to generate, store, and reconstruct keys.

The company Intrinsic ID, Inc. (USA) offers PUF-based unclonable identities for IoT devices.



Challenge	Response
~~10101010~~	~~011010~~
11011001	101101
01110100	001011

Figure 2.11: The mechanism of PUF authentication.

Their product portfolio mainly consists of memory-based PUFs, particularly SRAM-PUFs and butterfly PUFs, used to provide hardware-based root of trust. The products are available as the so called QuiddiKey hardware IP for direct integration into ICs as well as in the form of the Monark FPGA IP. Another company called PHYSEC GmbH (Germany) offers security solutions for the IoT including the Enclosure-PUF for tamper proof.

A patent review has shown that various semiconductor companies filed patents on PUFs in the past decade. This indicates a strong commercial interest in PUFs, which is mainly driven by providing secure device authentication. Table 2.2 shows a selection of patents.

Table 2.2: Selection of patents including PUFs.

Title	Assignee	Region	Year	PUF type	Invention	Ref.
Integrated physical unclonable function (puf) with combined sensor and display	Koninklijke Philips NV	US	2008	Optical PUF	Create challenge-response pairs for device authentication	[148]
Authentication of integrated circuits	Intrinsic ID BV, MIT	US	2010	Arbiter PUF	Authentication of integrated circuits	[149]
Secure authentication based on physically unclonable functions	Maxim Integrated Products Inc	US	2014	N/A	Use a challenge-response process to authenticate electronic devices	[150]
FET pair based physically unclonable function (PUF) circuit with a constant common mode voltage	International Business Machines Corp	US	2015	FET-pair PUF	PUF circuit design	[151]
Tamper-protected hardware and method for using same	EMSYCON GmbH	US	2015	N/A	Improve the tamper-resistibility of hardware	[152]
Physically unclonable function (PUF) with improved error correction	Intrinsic ID BV	US	2016	N/A	A cryptographic system for reproducibly establish a reliable data string	[153]
Quantum secure device, system and method for verifying challenge-response pairs using a physically unclonable function (PUF)	Twente Universiteit, Einhoven Technical University	EU	2016	Optical PUF	Verify challenge-response pairs using a PUF to provide authentication	[154]
PUF based boot-loading for data recovery on secure flash devices	NXP BV	US	2019	Memory-based	Provide data recovery on secure flash devices using PUF-based boot-loading	[155]

2.6 Security Threats

2.6.1 Security Threats for PE-Based Devices and Systems

In times of digitization and the IoE, electronic devices have become pervasive in our everyday life. This implicates that interconnected systems are embedded into our environment, with the aim to increase productivity to add value, to reduce cost, and to make our everyday life easier. However, the many advantages also bring vast security threats. The risks start at the manufacturing process of electronic devices, over often missing subsequent patching and update capabilities, physical security, while also affecting privacy and confidentiality issues as well as lack of user awareness and knowledge. In the IoE, all kind of data is exchanged through often compromised local and wide area networks, such as sensor networks and the Internet. In the past decades, information security, more specifically cryptography has further improved to authenticate devices, secure communication in the presence of third parties, and ensure data integrity. Most cryptographic systems are based on symmetric- (e.g. Advanced Encryption Standard (AES) [19]) or asymmetric-key (e.g. Diffie-Hellman-Merkle key exchange [47, 48]) algorithms. Various works can be found dealing with the security of symmetric- and asymmetric cryptography [156–158]. In general, cryptography is based on secret keys that are mainly generated through computational one-way functions or RNGs. The main drawback of these approaches is that the secret keys need to be stored in the devices. Basically, this is comparable to the root of trust issue that we have already discussed in Section 2.2.2. In NVMs it is also possible to reveal the memory contents when powered off, which makes them vulnerable against reverse-engineering attacks. In literature this is also referred to as *memory leakage* [63].

Under the assumption that many lightweight IoE devices will be available in the near future, the investigation of security models becomes a vital factor. Since the requirements of conventional cryptography solutions in terms of computation performance are often hard to met in lightweight devices, we mainly concentrate on hardware-intrinsic security primitives. In general, in terms of security threats we distinguish between two classes. The first class is the *provision of information*, which includes non-invasive-, semi-invasive-, and invasive attacks. In security models, these attacks are used to reveal secrets from a device. We use the overall term *eavesdropping* for these techniques. The second class of threats is the *learning* or *cloning*, which can either be model-based or physical cloning of the device properties. It should be noted that *eavesdropping* is the basis for *learning* and *cloning*. PUFs store secrets in a non-volatile manner, but in contrast to NVMs, the secret key is only available in binary form once needed. Moreover, the source of uniqueness in PUFs is very hard to observe without altering or even destroying the PUF. However, invasive attacks are often not reasonable since expensive equipment is needed and the original PUF circuit will be destroyed. Figure 2.12 visualizes the general procedure for cloning PUFs.

In the next sections we focus on *eavesdropping* and *model-based attacks*, which are widely used by the research community to assess the resilience of security primitives against attacks.

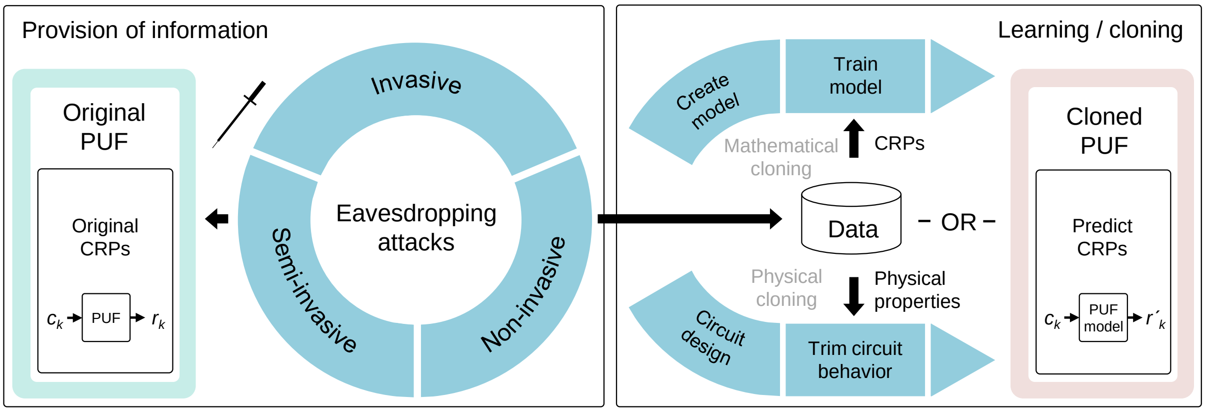


Figure 2.12: Procedure of eavesdropping and cloning PUFs.

2.6.2 Eavesdropping Attacks

In the scope of PUFs, *eavesdropping* describes the provision of information, particularly of CRPs. Thereby, attackers might *eavesdrop* either the operations between the PUF and the surrounding circuitry or the communication channels between PUF-equipped devices. Depending on the security-level, the responses of strong PUFs are often utilized as single-use keys which are discarded after usage. On the first sight this enables a high security-level in bilateral communication. One possible application scenario would be device authentication, where the manufacturer extracts CRPs after production and stores them in a database. For authentication, the manufacturer transmits one of the challenges to the PUF, which replies with its response. Since the CRP is only used once, the data transmission has not to be encrypted, which makes it easy to properly authenticate lightweight devices. However, if there are dependencies between the PUF CRPs, an adversary can use *eavesdropped* data to draw conclusions about other, not yet exchanged CRPs.

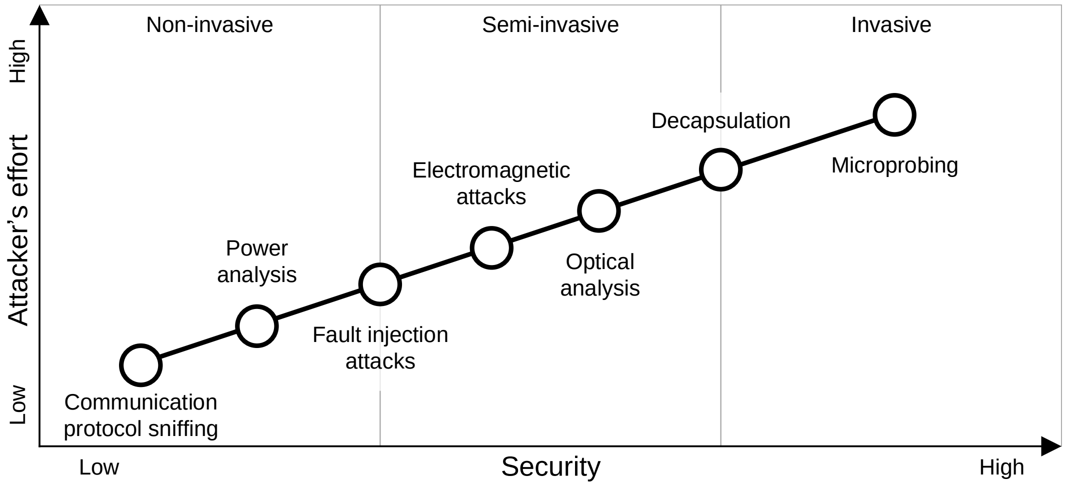


Figure 2.13: Overview on eavesdropping attacks.

In general, *eavesdropping* techniques are classified into *non-invasive*, *semi-invasive*, and *invasive attacks*. Figure 2.13 classifies the available attacks in a trade-off between security and the attacker's effort. *Non-invasive attacks* are per definition neither disrupting the operation of the affected device, nor do they damage the internal physical structure [159]. Widely used *non-invasive* techniques include side-channel analysis [160–162] based on communication protocol sniffing [163], power analysis [164, 165], electromagnetic interference-based fault injection [159], and fault attacks [166]. The benefits of these attacks are that in the case of *eavesdropping* the communication protocol, no direct physical access to the device is required. Furthermore, low-cost equipment is sufficient and *non-invasive* attacks leave no evidence that an attack has happened.

In contrast, *invasive attacks* physically break into a device and thereby modify its internal structure. For example, Helfmeier et al. [119] have successfully attacked an SRAM-PUF and produced a physical clone of it. For the characterization of the PUF they used invasive decapsulation in conjunction with microprobing. This process is also called *reverse-engineering*. High-precision and high-cost equipment is needed to expose the layers of the internal PUF circuit and measure its characteristics, which also implies physical access to the device. In many cases, *non-invasive attacks* are inappropriate and *invasive attacks* are too expensive. As a further security threat, in [167] Skorobogatov has introduced *semi-invasive attacks*. Thereby, depackaging of the offended chip is necessary, but no electrical contact to the internal wirings is required. Typical attacks are based on electromagnetic (EM) [168–170] and optical analysis [119]. The benefits of this technique are that the functionality of the original device is not affected and that low-cost is possible. However, the attacker must gain physical access to the device.

If all CRPs of a PUF were *eavesdropped*, the adversary is able to create a physical clone. However, most often it is impossible to *eavesdrop* all CRPs, particularly if the number of PUF CRPs is high. Typically, just a small subset of the actual CRP space is used in practice. Especially if the attacker is limited to passive *eavesdropping* and cannot control the challenges actively. In this case, one possible solution is to find interdependencies between the revealed CRPs, e.g. by using model-based attacks, which is explained in the next section.

2.6.3 Model-Based Attacks

Model-based attacks attempt to estimate the unknown model parameters as a function of the observed CRPs [43]. It is required that a subset of CRPs has already been eavesdropped from a specific PUF entity. In the past years, various *model-based attacks* on PUF designs have been proposed by researchers to break with security. Given a subset of CRPs from a PUF, the goal is to find a model in the form of an algorithm which behaves indistinguishably from the original PUF [114]. The most commonly used attacks are based on machine learning (ML) techniques. In general, ML is a very powerful tool to create and improve a model based on training data and make predictions or decisions. In this context, the term *modeling attacks* is widely used to describe methods based on mathematical or numerical PUF models using optimization algorithms. Please note that we use the more general term *model-based attacks*, since the attacks must not necessarily be based on ML techniques. For example in Section 6.4, we show that for some PUF types *sorting attacks* can be a good alternative. Furthermore, methods based on linear programming [103, 171, 172] have been proposed by researchers to model PUFs. Originally, *model-based attacks* were introduced for strong PUF implementations with a huge CRP space, which in many cases offer a publicly accessible challenge-response interface. On the other hand, weak PUFs can produce only a small number of CRPs and are typically embedded into a controlled environment. However, weak PUFs may also provide hundreds or thousands of

CRPs, which raises the threats emanating from *model-based attacks* as well.
Different PUF types have individual vulnerabilities against *model-based attacks*. For example in arbiter PUFs, each challenge involves all stages which means that each response carries information about the entire PUF's delay behavior for that special configuration. This allows to describe the functionality of arbiter PUFs with a linear delay model [103, 172, 173]. On the other hand, the challenges of analog PUFs and RO-PUFs typically include just a subset of the arbitrarily addressable cells, i.e. MOSTFETs or ring oscillators. In this case, the adversary has to eavesdrop more CRPs to draw conclusions about the internal PUF characteristics.
Another important measure to assess the vulnerabilities of PUFs against *model-based attacks* is the entropy analysis. The entropy of a PUF is a measure of the statistical independency of its CRPs. If a PUF exhibits a low entropy score, this can be seen as an indicator that *model-based attacks* can break the PUF. At the same time, achieving a high entropy score does not necessarily imply immunity. This means that the security of a PUF is not solely dependent on the entropy but rather the internal functionality plays a major role. Furthermore, if the 0s and 1s are unevenly distributed over the PUF responses, in other words if the PUF responses are biased, an attacker can guess others with a higher probability. In conclusion, PUF clones can impersonate original PUFs, which holds true for model-based and physical clones. However, model-based clones can be arbitrarily duplicated and distributed with low effort and at low cost.

If we remember the *unclonability* property of PUFs from Section 2.3.1, we have bound *unpredictability* with *mathematical unclonability*. The circumstance that PUFs are provably vulnerable against *model-based attacks* is a further indication that the wording *physically unclonable function* is more suitable than *physical unclonable function*.

2.6.4 Machine Learning-Based Attacks

Machine learning is used in a wide range of applications, where it is difficult to describe a specific functionality by using conventional algorithms. The application fields include image [174] and speech recognition [175], medical diagnosis [176], email spam filtering [177], product recommendations [178], traffic prediction [179], to name but a few. In the ML context, the term learning involves the representation, evaluation, and optimization [180]. The representation is the ML algorithm that describes the behavior to be modeled in a formal language. In the next step, the evaluation is needed to assess and distinguish between ML models. Finally, the optimization is the basis for the learning capability and determines its efficiency. Typically, machine learning algorithms are classified into supervised learning [181], unsupervised learning [182], and reinforcement learning [183]. Figure 2.14 shows the ML classes and a selection of ML algorithms. More detailed information on ML algorithms can be found in [184].

In this work, we focus on the most widely used ML technique: classification. In [180], Domingos et al. present an overview on available ML classifiers. In general, an ML classifier is a function that takes input data in the form of a feature vector, also referred to as training data, and outputs the class it belongs to. Classification is a supervised learning technique, where the training data comprises the feature vectors (inputs) and the corresponding observations (outputs). Typically, ML classifiers are trained through optimization based on error minimization. In the following, we will concentrate on logistic regression (LR) [185], random forest (RF), and perceptron-based ML algorithms.

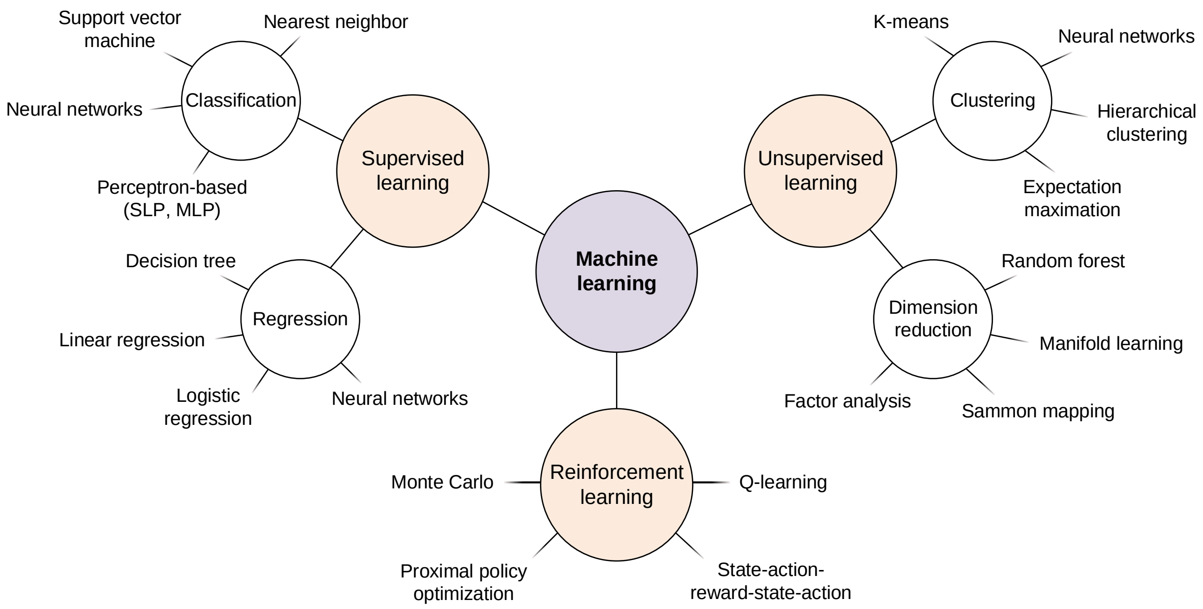


Figure 2.14: Machine learning classes and selection of algorithms.

Logistic Regression

LR belongs to the class of supervised learning algorithms. Technically speaking, it is not a ML classifier, but it can be used for binary classification by choosing a decision value that separates between the two classes. Therefore, the term *logistic regression classifier* is often used in literature. In general, an LR classifier takes an input vector $\vec{\mathbf{x}}$ and assigns it to the discrete class C_2, which is also referred to as categorical data with two values. The core cost/activation function is the so-called logistic function, more particularly the sigmoid function $f_\sigma(z)$.

Definition 2.19. *The sigmoid function is defined as:*

$$f_\sigma(z) = \frac{1}{1+e^{-z}}. \tag{2.17}$$

The hypothesis function $h_\theta(\vec{\mathbf{x}}) = f_\sigma(\vec{\theta}^T\vec{\mathbf{x}})$ limits the cost function to binary values between 0 and 1. The transposed vector $\vec{\theta}^T$ denotes the regression coefficients (weights) adjusted by the optimizer algorithm to find suitable decision boundaries for the classifier. In the context of PUFs, LR is one of the most often used ML algorithm to model the challenge-response behavior [104, 114, 186].

Random Forest

RF is an unsupervised learning algorithm based on decision trees. A decision tree is a directed graph, where each path splits into branches following the decision rules to map the desired behavior. Figure 2.15 shows a sample decision tree. The appearance of a decision tree depends on the training data that determines the decision rules and the order of the branches. This means that single decision trees might perform worse. However, the RF technique overcomes this issue. It assumes that a crowd of randomly created decision trees can achieve better matching predictions by using majority voting.

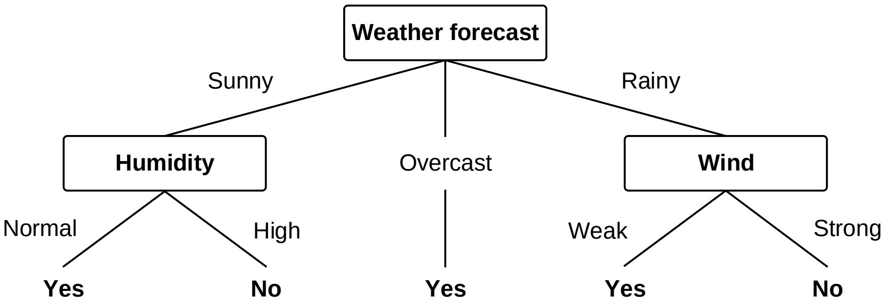


Figure 2.15: Sample decision tree for playing tennis on weather conditions (cf. [187]).

RF is mainly used for classification and regression tasks. In general, the RF classifier is an ensemble of individual decision trees, each making a class prediction. Finally, majority voting is used to determine the overall class prediction of the RF classifier. One of the main advantages of the RF classifier is its efficiency on large data sets. In the context of PUF modeling attacks, various PUF designs have been attacked by the RF algorithm [188–190].

Perceptron-Based Learning

Perceptron-based learning algorithms belong to the class of supervised learning. Figure 2.16a visualizes the perceptron as proposed by Minsky et al. in [191] as well as the artificial neuron as firstly introduced by McCulloch et al. in [192], which are the fundamental units of artificial neural networks (ANNs). The difference between both is the activation function. While perceptrons utilize the step function as the activation function to distinguish between two classes at the output, artificial neurons typically make use of smoother variants. The most commonly used activation function is the sigmoid function (see Definition 2.17), which is a special case of the logistic function. Figure 2.16b shows the step and sigmoid functions for a given bias w_0.

In the ML context, it is distinguished between single-layer perceptrons (SLPs) and multi-layer perceptrons (MLPs). SLPs are classifiers that are limited to learning linear separable patterns. The so-called activation potential of a neuron is denoted as $z = \sum_{i=1}^{n} w_i \cdot x_i + w_0$, where w_i are the weights, x_i are the input values, and w_0 is the bias. According to the step function, the classification is set to 1 (true) if the sum z exceeds the decision threshold value, and 0 (false) otherwise. SLPs can comprise an arbitrary number of perceptrons, where all are arranged in a single-layer architecture.

MLPs are finite directed acyclic graphs that include at least one additional hidden layer between the input and the output layers, as shown in Figure 2.17. Typically, artificial neurons based on non-linear activation functions are used.

Definition 2.20. *The mathematical description of an artificial neuron is:*

$$\widehat{y} = f_{\text{act}}(\vec{\mathbf{w}}^T\vec{\mathbf{x}} - w_0) = f_{\text{act}}\left(\sum_{i=1}^{n} w_i \cdot x_i + w_0\right) \tag{2.18}$$

where $f_{\text{act}}(\cdot)$ is the activation function, $\vec{\mathbf{x}} = (x_1, \ldots, x_n)$ is the input vector with n values, $\vec{\mathbf{w}} = (w_1, \ldots, w_n)$ is the weight vector, and w_0 is the bias.

The input values $\vec{\mathbf{x}}$ pass through the first layer whose outputs are the inputs of the subsequent layer. This repeats until the output layer is reached. Adding more hidden layers allows to learn

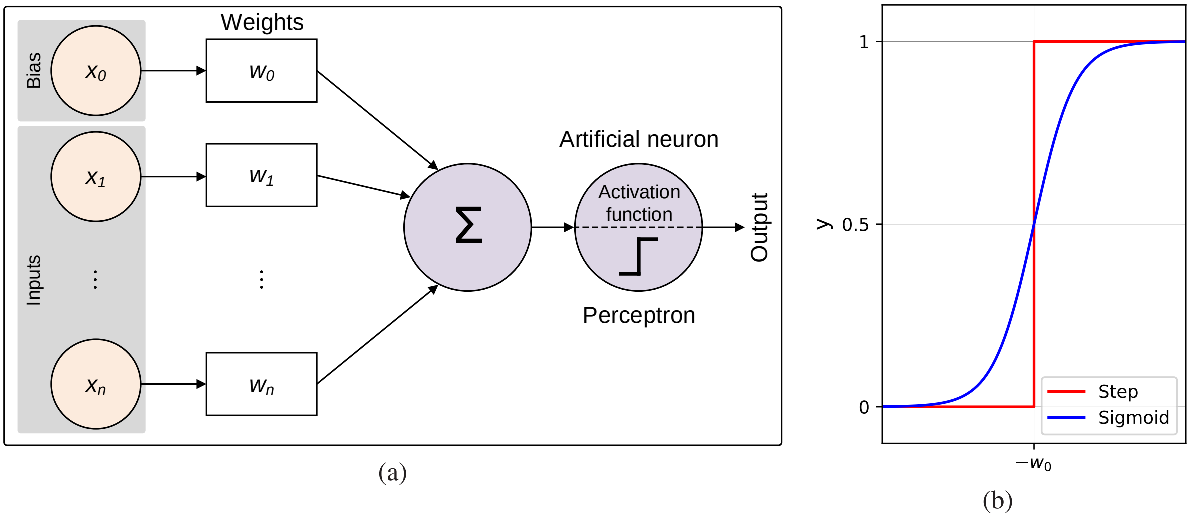


Figure 2.16: (a) Visualization of a perceptron with the input feature vector $\vec{\mathbf{x}} = \{x_1, \ldots, x_n\}$ and the weight vector $\vec{\mathbf{w}} = \{w_1, \ldots, w_n\}$ with the bias w_0. Perceptrons use the step activation function, whereas artificial neurons typically use smoother functions such as the sigmoid. (b) Step and sigmoid activation functions.

more complex patterns, which is also referred to as deep learning. The learning capability comes from the backpropagation algorithm that recalculates the weights vector $\vec{\mathbf{w}}$ based on error or loss minimization from back to front of the network. To perform backpropagation, the error function must be differentiable in order to calculate the gradients. More detailed information on error functions and backpropagation can be found in [193, 194]. For more details on perceptron-based learning in general please refer to [195].

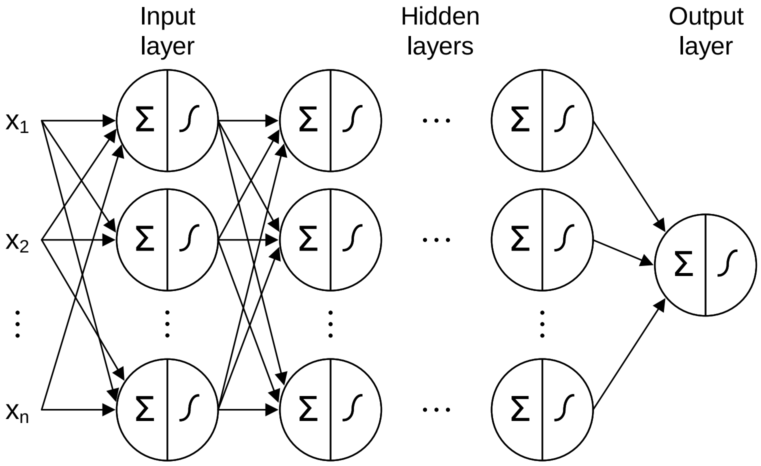


Figure 2.17: Multi-layer perceptron architecture.

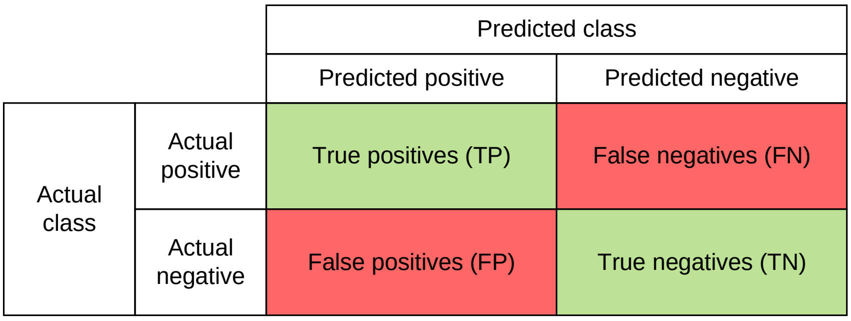
Perceptron-based learning algorithms in the form of SLPs and MLPs are widely used to model PUFs [196–200]. The main advantage of perceptron-based attacks is that ANNs can learn complex patterns and non-linear correlations. The broad applicability makes them a good choice independent from the actual PUF type.

2.6.5 Machine Learning Metrics

In general, machine learning techniques can be versatile with manifold application fields. A variety of machine learning metrics have been proposed for different machine learning models such as classification metrics [201], regression metrics [202], ranking metrics [203], to name but a few. In this work we focus on classification metrics, since our ML attacks on PUFs are based on ML classifiers.

Confusion Matrix

The basic concept to assess the classification performance is the so-called *confusion matrix*. The *confusion matrix* is a tabular comparison between a model's ground truth labels (the actual class) and the predictions. Figure 2.18 shows an exemplary *confusion matrix* for a binary classifier (two classes).



		Predicted class	
		Predicted positive	Predicted negative
Actual class	Actual positive	True positives (TP)	False negatives (FN)
	Actual negative	False positives (FP)	True negatives (TN)

Figure 2.18: Confusion matrix for a binary classifier [204].

The predictions are classified into true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN). These *confusion matrix* values are the basis for other types of classification metrics.

True positives (TP): The actual class is positive and the predicted class was also positive.

False positives (FP): The actual class is positive, but the prediction was negative.

True negatives (TN): The actual class is negative and the predicted class was also negative.

False negatives (FN): The actual class is negative, but the predicted class was positive.

Classification Accuracy

The *classification accuracy* is an intuitive performance measure considering correct predictions in relation to the total number of predictions made. In literature the terms *prediction accuracy* and *accuracy* are widely used.

Definition 2.21. *The classification accuracy is:*

$$\text{Classification accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{2.19}$$

where TP are the true positives, FP are the false positives, TN are the true negatives, and FN are the false negatives, respectively.

Area Under Receiver Operating Characteristic Curve

The *area under receiver operating characteristic curve (AUROC)* is widely used to assess binary classifications. The shortened term *area under curve (AUC)* can be found very often in literature, which is in our opinion bad practice. AUC could mean any curve, whereas AUROC uniquely defines that the area under a receiver operating characteristic (ROC) curve is meant.

In binary classifications, the classifier boundary to distinguish between classes is determined by a threshold value. According to the previously shown confusion matrix, a binary classifier always has four possible outcomes (TP, TN, FP, FN). The ROC curve is used to determine the ideal threshold value for the classifier. This is done by a trade-off between the ratio of actual positive classes that were correctly predicted as positive and the ratio of actual negative classes that were mistakenly predicted as positive. The former is referred to as the true-positive-rate (TPR), whereas the latter denotes the false-positive-rate (FPR), respectively.

Definition 2.22. *The true-positive-rate (TPR), also called sensitivity, describes the probability of detection and is defined as:*

$$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{2.20}$$

where TP are the true positives and FN are the false negatives, respectively.

Definition 2.23. *The false-positive-rate (TPR), also called specificity, is also known as probability of false alarm and is defined as:*

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \tag{2.21}$$

where TN are the true negatives and FP are the false positives, respectively.

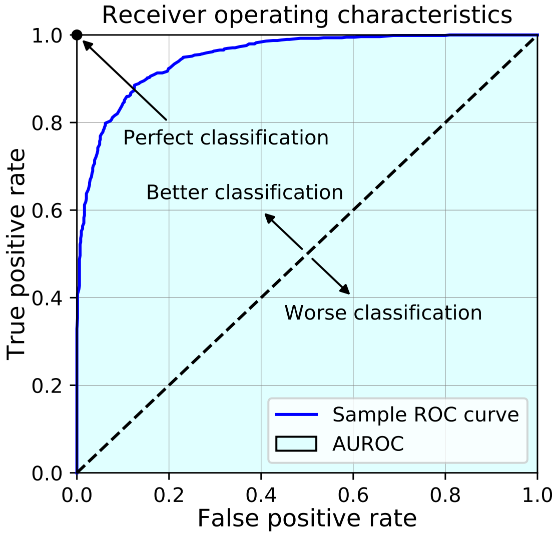


Figure 2.19: Sample receiver operating characteristics (ROC) curve and area under ROC (AUROC).

The ROC curve is a plot showing the TPR against the FPR for various threshold values. Figure 2.19 shows a sample ROC curve (blue line) and the corresponding AUROC. The upper left black point denotes a perfect classification, where the TPR is 1 and the FPR is 0. The dashed black line indicates a random guess with equal TPR and FPR values. If the bending of the ROC curve is steady, the TPR and FPR values are uniformly distributed. In the machine learning community ROC curves are often used for model comparison.

2.7 Conclusion

In this chapter, we have introduced the basic concepts of security in general and hardware-intrinsic security in particular, as well as studied state of the art PUFs. Furthermore, we elaborated on the differences between PE and silicon electronics, inkjet-printed inorganic transistors, and the need for lightweight security solutions for PE-based electronic devices and systems. Finally, we have explored potential security threats existing for PUFs.

The presented overview provides all the information necessary to understand the subsequent chapters and therefore serves as a convenient reference work. We have also introduced the mathematical foundations in the form of security and performance metrics to assess the qualities of the PUF constructions and to compare them with related works.

3 PUF Design & Fabrication

3.1 Introduction

In the previous chapter, we have discussed the significance of security in the digitized world. For the time being, the research field of hardware-intrinsic security primitives based on novel materials is in the early stages. Since PE is a key driver for the IoE, the demand for lightweight security solutions is expected to be enormous in the future. In many application scenarios, such as printed large-area sensors, printed antennas in communication devices, etc., PE technology goes hand in hand with conventional silicon-based electronics. In this manner, the unique features of two worlds can be combined in a single operating device. Most of the novel material PUFs belong to the class of optical PUFs that require complex evaluation systems. This strictly limits the applicability for lightweight devices and systems, as emerging from PE technology in the scope of the IoE. In the past years, first printed electrical PUFs have been proposed in literature, showing promising performance in terms of the PUF security metrics. The better integration capabilities of electrical PUFs, compared to optical PUFs, make them promising candidates as lightweight security primitives. In this context, the additive manufacturing processes used in PE lead to larger device variations compared to lithographically structured devices. The source of variations reaches from discrete droplet size of the printed ink, the surface roughness of printed layers, the quality of the interfaces between the layers in general, up to scaling errors in the channel width-to-length ratio of printed transistors, to name but a few [26–31]. In this chapter we aim to:

- Present the fundamentals of the Differential Circuit PUF (DiffC-PUF) including the design rationale, requirements, as well as the challenge and response generation.
- Give detailed insights into the implementation architecture of the DiffC-PUF as an embedded system. This also includes the hardware design and fabrication of the PUF as a fully silicon system and as a hybrid PUF incorporating silicon-based and printed components.
- Present the high-level software architecture by describing the components and parameters being involved into the PUF response generation mechanism.

3.2 PUF Design

3.2.1 Design Rationale & Requirements

The rationale behind PUF designs is a trade-off between many different factors. In the following, we present six quality parameters to determine the essential requirements on PUFs for a specific application scenario. The quality parameters include the *security level*, *tamper evidence*, *simpli-*

city, *scalability*, *cost effectiveness*, and *integrability*. Figure 3.1 visualizes the quality parameters, each being ranked by low, medium, or high. The shaded surface shows the ranking carried out in the decision phase for a PUF based on PE technology.

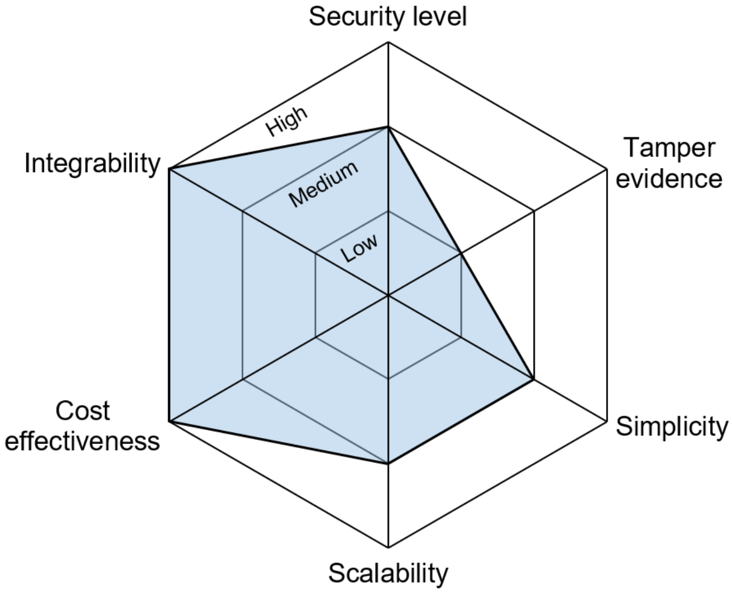


Figure 3.1: Radar chart of the PUF quality parameters. The ranking indicated by the shaded surface shows the requirements selected for a PE-based PUF.

Table 3.1 shows the PUF qualities and a list of possible rankings. In general, the *security level* refers to the security capabilities of different PUF constructions. In the context of lightweight PE-based security primitives, cryptographic applications are too complex for the time being. Therefore, the target *security level* is set to medium, which enables device authentication. Please note that a medium *security level* does not directly imply that authentication is less secure than cryptography. In contrast to authentication, cryptographic keys must satisfy more strict requirements in terms of entropy, uniformity, etc. and are the basis for authentication protocols. As initially discussed in Section 2.3.1, *tamper evidence* is hard to achieve with electronic PUFs and often not required. For that reason it is set to low. *Simplicity* relates to the circuit and key derivation complexity of PUFs. In general, this quality parameter refers to the Kerckhoffs's principle which states that security should not only come from 'security through obscurity' [205]. In other words: 'The simpler the secrets that one must keep to ensure system security, the easier it is to maintain system security' [206]. For example, memory-based PUFs exhibit high *simplicity*, since the challenge complexity is limited to the powering-up state of the memory cells and the response is directly accessible in binary form. However, the *simplicity* is set to medium to obtain an additional degree of freedom that comes with the challenge addressing capability, which enables non-linear scaling of the CRP space. The *scalability* is well defined by the weak and strong PUF classifications (please refer to Section 2.3.3 for more details). Weak PUFs with very low numbers of responses are also referred to as POKs. Strong PUFs typically comprise a large number of complex circuit components, which detracts the suitability for PE technology. Therefore, the *scalability* requirement is set to medium. Finally, the *cost effectiveness* and *integrability* qualities are set to high. This is a consequence of the unique properties originating from PE technology such as mass production, customizability, and on demand fabrication. The ranking of these two qualities are in contrast to silicon PUFs, which often suffer from high integration and fabrication costs.

Table 3.1: PUF qualities and possible rankings. Please note that the list is not comprehensive.

	Low	Medium	High
Security level	Identification	Authentication	Cryptography
Tamper evidence	No explicit tamper evidence	Key derivation may fail on interaction	PUF irreversibly destroyed
Simplicity	High complexity	Medium complexity	Low complexity
Scalability	POK	Weak PUF	Strong PUF
Cost effectiveness	High cost	Medium cost	Low cost
Integrability	Redesign required	PUF can be integrated into existing designs	PUF reuses existing circuitry

Since PE technology faces limitations in terms of circuit complexity and performance, it is challenging to construct a PUF design offering a large CRP space. Nonetheless, many applications require either large key bit widths, or the opportunity to generate a number of different keys. One typical example for the former case is device identification, where a larger bit width of the identifier (key) typically leads to a larger number of devices that can be uniquely distinguished. One possible solution is to use memory-based PUFs, e.g. as introduced by Guerin et al. in [123] and Erozan et al. in [124, 125]. However, the drawback of memory-based PUFs is their linear scaling of the CRP space, which causes high area consumption, if using PE technology to achieve large key bit widths. In identification tasks, the main requirement to be achieved is that the generated keys must be unique and reproducible, while other security measures such as uniformity are of lower priority. This means that key derivation techniques become applicable that provide non-linear bit width scaling, as long as the uniqueness of the resulting key is sufficient to meet the application requirements. If targeting authentication and cryptographic key generation tasks, it is often required to generate several security keys. For example in PUF-based authentication protocols it is often intended to utilize single-use CRPs in order to uniquely authenticate devices. This also applies to cryptographic key generation, where various keys might be required, e.g. for encryption and decryption of data.

The herein derived requirements for PE-based PUFs as determined above are based on the assumption, that as many target applications as possible can be targeted by the resulting PUF construction. Referring to the RO-PUF construction as introduced by Suh et al. in [110], in the next section we introduce the Differential Circuit PUF (DiffC-PUF) design. The aim of the DiffC-PUF construction is to provide the first PE-based PUF that offers non-linear scaling of the CRP space and therefore enables versatile adaptation to a wide field of potential target applications, that could not be addressed before. Additionally, the aim is to use standard components and simple circuit design to enable the potential of being fully fabricated with PE technology.

3.2.2 Differential Circuit PUF

The DiffC-PUF is designed based on the requirements obtained from the previous analysis. The design utilizes a resistor-transistor-logic (RTL) inverter array, also referred to as the PUF core. Array structures enable scaling of the PUF CRP space. In general, each RTL inverter consists of a resistor and a metal-oxide-semiconductor field-effect transistor (MOSFET). If the input of the inverter is set to a logical high level, a voltage divider is formed between the resistor and the drain-source resistance of the transistor. As a consequence, the logical low level of the RTL inverter does not reach electrical ground. Due to process variations, the transistors' threshold voltages differ slightly. This leads to variations in the drain currents and thus results in varying inverter output voltages. The existence of threshold variations in transistors was firstly utilized by Lofstrom et al. in [100] to identify integrated circuits. If the magnitude of the variations is very small, the evaluation logic must be of high precision. In the context of security primitives for lightweight devices and systems, this is an important factor to be considered. Using RTL inverter arrays instead of transistor arrays additionally includes resistance variations from the resistors. This results in higher magnitudes of variations. A simple comparator can be used to compare the output voltages of two inverters and generate one digital response bit.

Figure 3.2 shows the basic DiffC-PUF design. Bidirectional multiplexers (BIMUXs) are used to arbitrarily select a pair of any two different inverters. In the input path, a predefined inverter biasing voltage V_{in} is routed to the inputs of the two addressed inverters with the addresses a_k and b_k. Correspondingly, the output signals of the addressed inverters are forwarded to a comparator (COMP). The COMP generates one digital bit based on its input voltages. The term 'Differential Circuit PUF' originates from the pairwise voltage comparison approach used for PUF response generation. The advantage of this differential technique is that fluctuations of the PUF core's supply voltage VDD_{core} and its impact on the inverter output voltage are suppressed. Thus, the voltage difference at the comparator inputs $\Delta V_{\text{out}} = V_{\text{out},a_k} - V_{\text{out},b_k}$ is kept stable over all operating conditions [33].

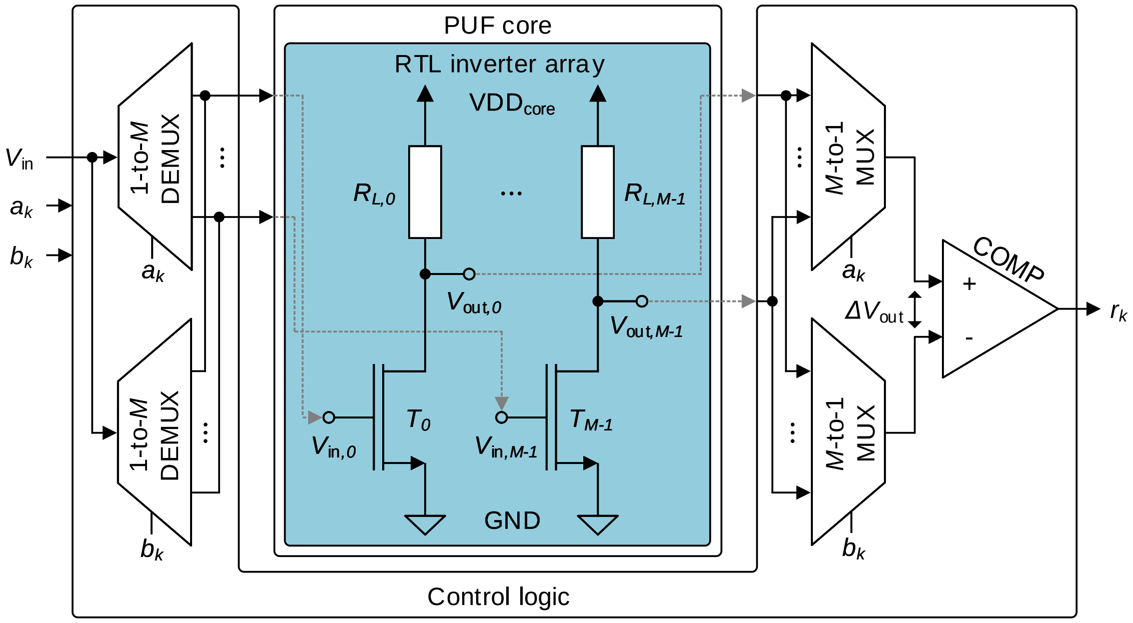


Figure 3.2: DiffC-PUF design including the PUF core inverter array and the control logic (cf. [207]).

3.2.3 Challenge and Response Generation

The DiffC-PUF challenges can be configured through the selection of the inverter pairs to be evaluated. A challenge C comprises a set of sub-challenges c_k, where each sub-challenge consists of the inverter addresses a_k, b_k, and the inverter biasing voltage V_{in}. The sub-challenge c_k is defined according to Equation (3.1) [33]. The inverter biasing voltage V_{in} can be used to obtain an additional degree of freedom in challenge configuration. Since this increases the complexity of the control logic, e.g. by using additional digital-to-analog-converters (DACs) to adjust V_{in} during operation, the inverter biasing voltage is typically fixed.

Definition 3.1. *The k-th DiffC-PUF sub-challenge c_k is defined as:*

$$c_k = (a_k, b_k, V_{in}) \mid a_k, b_k \in \{0, 1, \dots, M-1\} \tag{3.1}$$

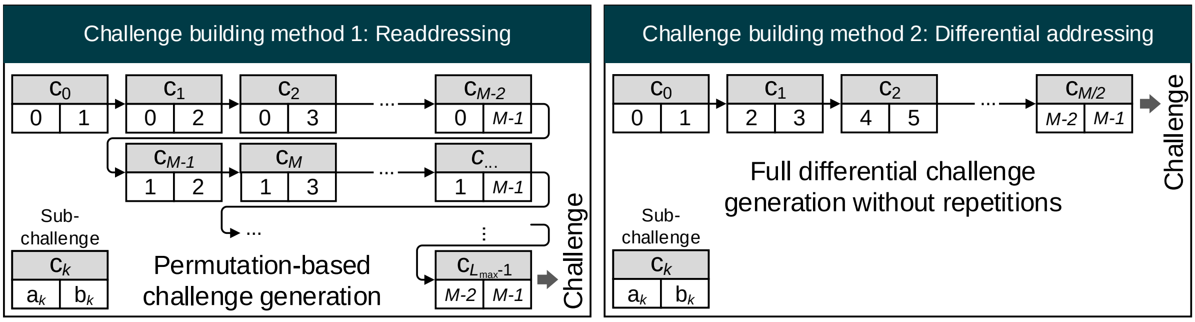
where a_k and b_k are the inverter addresses of the selected pair, V_{in} is the inverter biasing voltage, and M denotes the number of PUF core inverters.

For each challenge, one PUF response R is generated, including the sub-responses r_k. In general, the 1-bit sub-response r_k is a function of the sub-challenge c_k.

Definition 3.2. *The k-th DiffC-PUF sub-response r_k to sub-challenge c_k is defined as:*

$$r_k = f(c_k). \tag{3.2}$$

The DiffC-PUF's control logic allows to address the inverters arbitrarily, which enables free challenge configurations. Basically, two addressing methods for challenge building are possible:


Challenge building method 1: Readdressing
c0
0 1
c1
0 2
c2
0 3
...
cM-2
0 M-1
cM-1
1 2
cM
1 3
...
c...
1 M-1
...
⋮
Sub-challenge
ck
ak bk
Permutation-based challenge generation
cLmax-1
M-2 M-1
Challenge
Challenge building method 2: Differential addressing
c0
0 1
c1
2 3
c2
4 5
...
cM/2
M-2 M-1
Challenge
Full differential challenge generation without repetitions
Sub-challenge
ck
ak bk

(a) (b)

Figure 3.3: PUF challenge building methods. (a) Visualization of the permutation-based readdressing method. (b) Visualization of the differential addressing method.

Challenge Building Method 1: Readdressing

The readdressing method allows all possible unique permutations of inverter address pairs, as visualized in Figure 3.3a. In general, two inverter addresses can either be addressed in the combination (a_k, b_k) or (b_k, a_k). Reversing the addresses leads to inverted sub-response bits, which degrades the information content in proportion to the absolute response bit width. Therefore, each address combination may only occur once in the set of all sub-challenges provided by the PUF. In a mathematical sense, this can be expressed by $(a_k, b_k) = (b_k, a_k)$. In the readdressing method, the maximum response bit width (single response) can be achieved. In this case, the response bit width $L_{\max}$ equals the number of possible sub-challenges and is determined by Equation 3.3.

Definition 3.3. *The maximum response bit width of a DiffC-PUF with M inverters if using the readdressing method is limited to:*

$$L_{\max} = \frac{M \cdot (M-1)}{2}. \tag{3.3}$$

Challenge Building Method 2: Differential Addressing

In the differential addressing method, each inverter address is used only once among all sub-challenges, as visualized in Figure 3.3b. The maximum response bit width that can be achieved for a single response is limited to $L_{\max} = M/2$ (Equation (3.4)), where M is the number of PUF core inverters. At a first glance, this method seems to be inefficient. However, if an unauthorized party (attacker) reveals information about some CRPs, it would be almost impossible to draw conclusions about other internal dependencies of the PUF. In this regard, further discussions about the entropy of the PUF responses can be found in Section 6.2.2.

Definition 3.4. *The maximum response bit width of a DiffC-PUF with M inverters if using the differential addressing method is limited to:*

$$L_{\max} = \frac{M}{2}. \tag{3.4}$$

3.3 Embedded PUF Platform Implementation

3.3.1 Implementation Rationale & Requirements

In the previous section the basic DiffC-PUF design based on the acquired requirements was described. The rationale behind the hardware and software implementations of the DiffC-PUF is mainly described by the following considerations:

- The DiffC-PUF design is split into the following building blocks: Microcontroller, control logic, and PUF core. The modular platform architecture enables large-scale characterization of the fabricated PUF cores.
- The DiffC-PUF core circuit design is kept minimalist to enable PE fabrication. The circuit design complexity of the control logic is reduced to standard components to offer the potential of being fully printed in the future.
- An off-the-shelf microcontroller with standard components that is widely used in the IoE area is utilized to ensure compatibility with existing systems.
- The systematic errors in the evaluation electronics are reduced by using silicon components with low variations as well as equal temperature and humidity coefficients.
- The DiffC-PUF evaluation platform can be configured and controlled by a personal computer (PC).

3.3.2 Top-Level Architecture

The DiffC-PUF design imposes the following requirements to be considered in the embedded PUF platform architecture: (1) *Scalability*: The DiffC-PUF is a weak PUF design enabling non-linear scaling of the CRP space. (2) *Differential response generation*: The PUF response bits are generated utilizing a differential evaluation approach to mitigate supply voltage variations (please refer to Section 3.2.2 for more information). (3) *Modularity*: The functionality of the embedded PUF platform can be split into the control unit (PC and microcontroller), the addressing and bit generation logic, and the PUF core circuit. (4) *Automation*: Computer-driven platform configuration and statistical readout.

The design goal of the embedded PUF platform architecture is to perform the first comprehensive statistical analysis in terms of security metrics on PE-based PUFs. This enables expressive comparison with other PUFs.

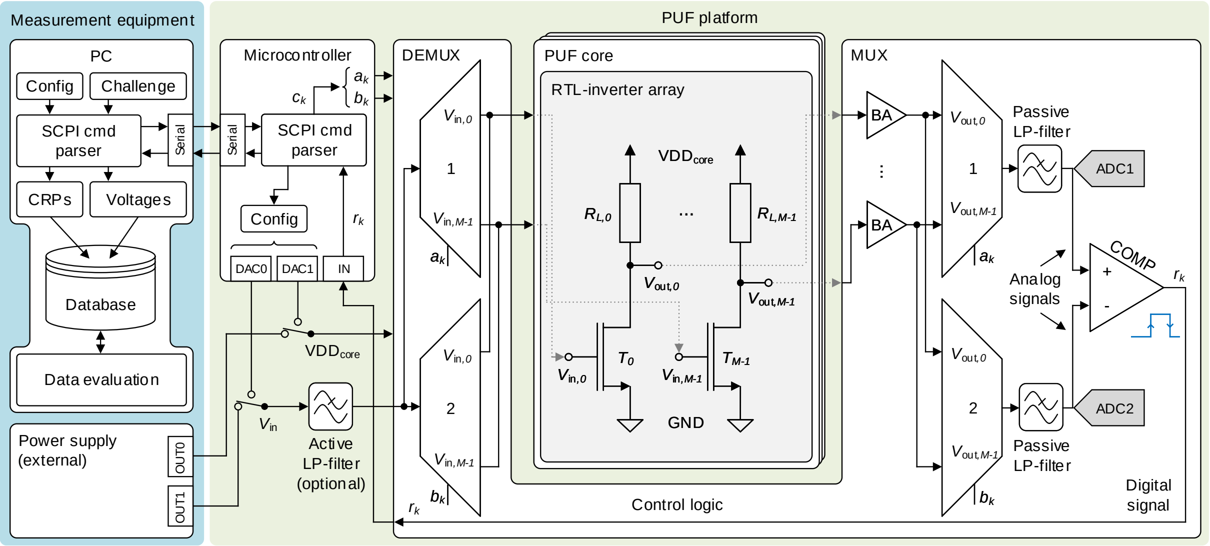
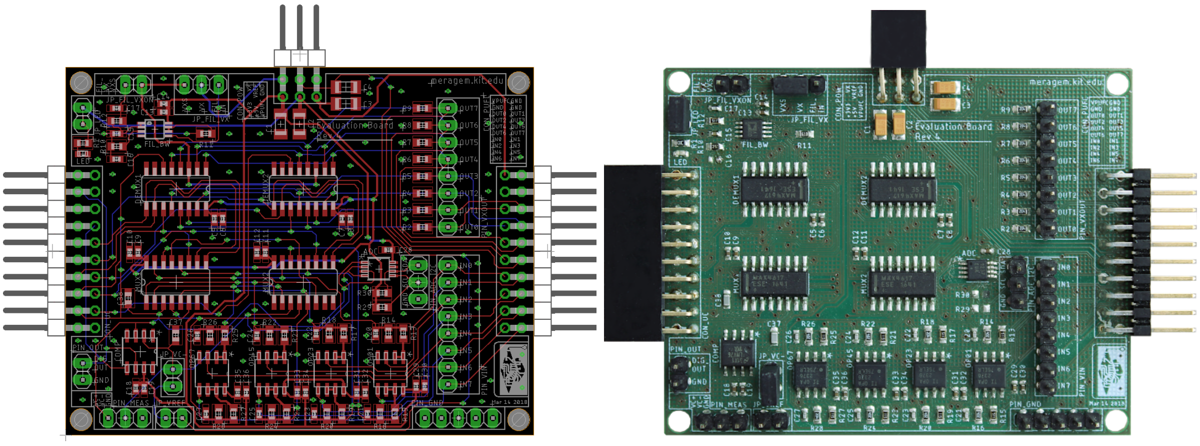


Figure 3.4: DiffC-PUF platform block diagram (cf. [33]). DAC: Digital-to-analog converter, ADC: Analog-to-digital converter, MUX: Multiplexer, DEMUX: Demultiplexer, BA: Buffer amplifier.

Figure 3.4 shows the top-level architecture of the embedded DiffC-PUF platform. All configuration and data communication between the PC and the microcontroller is done through the Universal Serial Bus (USB) interface. The communication protocol is based on the Standard Commands for Programmable Instruments (SCPI), that provides a common syntax, command structure, and data formats [208]. The power supply voltages for the control logic and PUF core can be configured by the user and is provided by digital-to-analog converters (DACs). Alternatively, external power supplies can be attached to the platform. The output voltages of the selected inverter pairs are passed through a first-order RC low-pass filter with a cut-off frequency of $f_c \approx 10\,\text{kHz}$, to limit the signal bandwidth of the readout path [33]. The voltages at the comparator input terminals can be measured by on-board ADCs. The intention behind the integration of the ADCs is to enable large-scale characterization. The platform can be fully configured via a single interface, which allows to change the operating conditions (the PUF core supply voltage VDD$_{\text{core}}$ and the inverter biasing voltage V_{in}) during operation.

3.3.3 Silicon-Based PUF Platform Implementation

The DiffC-PUF platform comprises three printed circuit boards (PCBs). The microcontroller is a Silicon Labs EFM32LG on the STK3600 development board [209]. The control logic includes the addressing and response bit generation components and is hosted on a separate PCB, the so-called Evaluation Board. The Evaluation Board is set up with discrete components with low variations and equal temperature as well as humidity coefficients. The cautious choice of the components reduces the systematic failures of the evaluation platform when being operated under different environmental conditions. Figure 3.5 shows the PCB layout of the Evaluation Board.


(a)

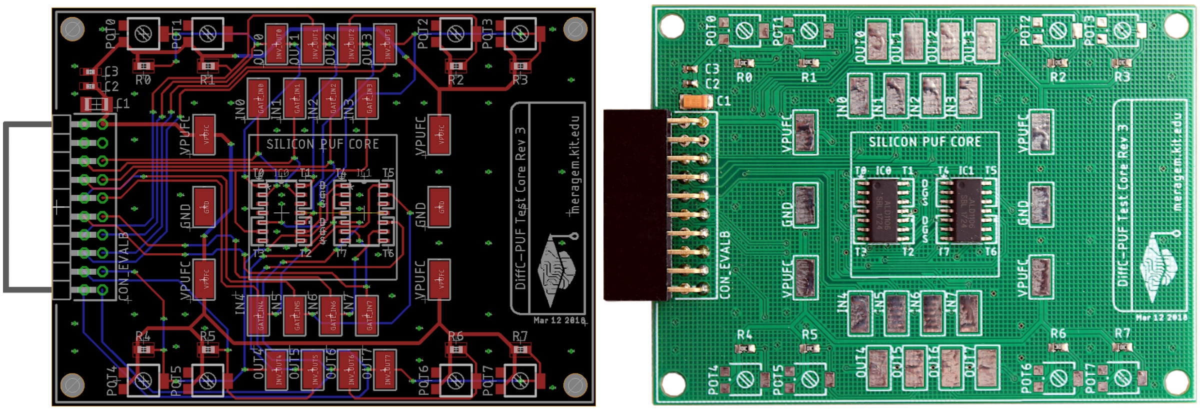
(b)

Figure 3.5: Silicon-based DiffC-PUF Evaluation Board (Revision 4) PCB. (a) PCB layout. (b) Top view on the fabricated PCB.

The hardware configuration incorporates the PUF core inverter array with eight RTL inverters, which are hosted on a third PCB. Two 1-to-8 demultiplexers (DEMUXs) are used to arbitrarily address the inputs of one inverter pair. Two 8-to-1 multiplexers (MUXs) route the outputs of the addressed inverters to the comparator inputs, correspondingly. Buffer amplifiers are used to separate the electrical load between the Evaluation Board and the PUF core.
Figure 3.6 shows the PCB layout of the silicon-based PUF core. Since this is a prototype implementation, large-area metal pads are carried out to the design to enable manual measurements. For the RTL inverters, surface-mounted device (SMD) resistors with 10 kΩ and 1 % variation from one batch and a MOSFET transistor array (ALD1106) are used. The partitioned design allows to substitute each of the three modules, which enables large-scale characterization. Please refer to Chapter 4 for the statistical results of the fabricated silicon-based PUF cores.

3.3.4 Hybrid PUF Implementation

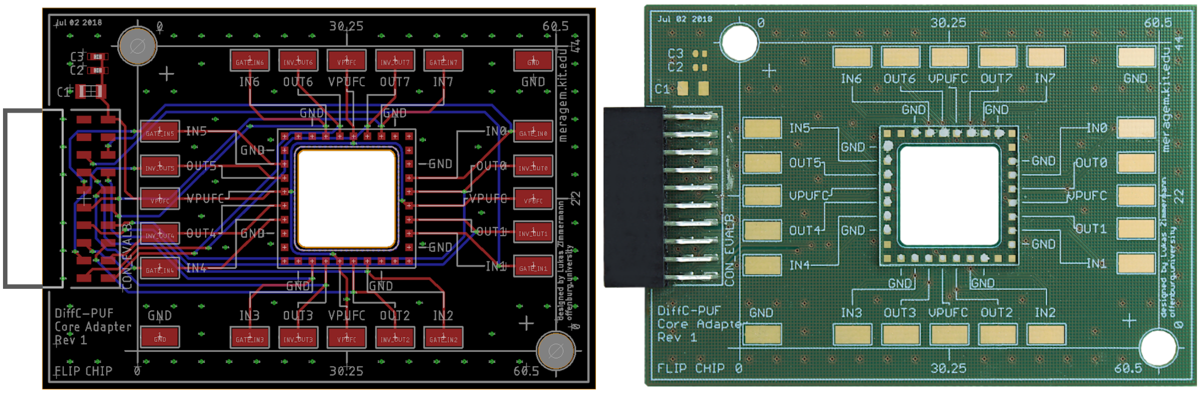
One of the major challenges to enable large-scale characterization of electronics based on novel materials is the missing integration capability. When attaching a printed to a silicon-based circuit, the materials must be compatible and the interface must be defined. The herein used printing substrate is an ITO-covered 20 mm × 20 mm glass (PGO CEC020S) with a layer thickness of



(a) (b)

Figure 3.6: Silicon-based DiffC-PUF core PCB. (a) PCB layout. (b) Top view on the fabricated PCB.

100 nm. In our lab setup, these dimensions are the basis for all printing tasks. To integrate the substrate hosting the printed PUF core circuit into the PUF evaluation platform, a silicon-based adapter PCB is designed. The adapter PCB layout is shown in Figure 3.7. The design offers 36 gold-coated bonding pads that are used to establish a connection between the PE-based and the silicon-based interfaces. Additionally, the adapter PCB exhibits large-area pads for manual measurements.



(a) (b)

Figure 3.7: Silicon-based DiffC-PUF core adapter PCB. (a) PCB layout of the flip chip adapter PCB. (b) Top view on the fabricated PCB for printed PUF core integration.

In this context, we use the term *hybrid PUF* to describe the DiffC-PUF incorporating silicon-based and PE components. The PUF core circuit is fabricated with inkjet-printing technology. Similar to its silicon-based counterpart, it consists of an RTL inverter array. The inverters are realized with EGTs and resistive indium tin oxide (ITO) meander structures as load resistors. Figure 3.8 shows the simplified fabrication process of the printed PUF core and its integration onto the adapter PCB.

In step 1, the signal routing, the resistor meander structures, and the transistor electrodes are laser-ablated from an ITO-covered glass substrate, using a Trumpf TruMicro5000 laser.

In step 2, the EGT's seminconductor channel (indium oxide – In_2O_3), the electrolyte (composite solid polymer electrolyte – CSPE), and the top gate (poly(3,4ethylenedioxythiophene):poly(styrenesulfonate) – PEDOT:PSS) are printed. The inkjet-printer Fujitsu Dimatix DMP-2850 is used to perform all printing steps. The placement of the components follows a symmetrical alignment. Thereby, the input/output (I/O) terminals of all inverters are connected to bonding pads. This reduces the integration complexity into the silicon-based circuits. Furthermore, no printed crossovers are needed, which is an example for hybrid systems where the advantages of both technologies can be combined.

In step 3, the printed PUF core is integrated onto the adapter PCB by using a mounting technique derived from the flip chip technology [210]. The flip chip approach allows automatic integration at ambient room temperatures. The process includes adhesive dispensing on the adapter PCB as well as precise alignment and mounting of the PUF core substrate onto the PCB.

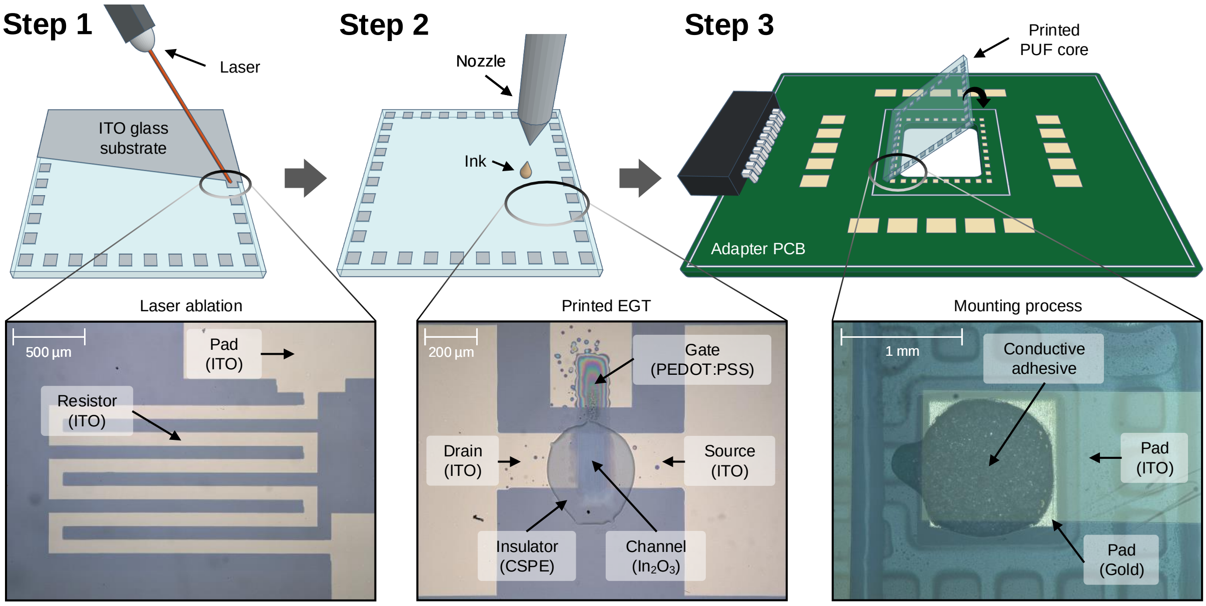
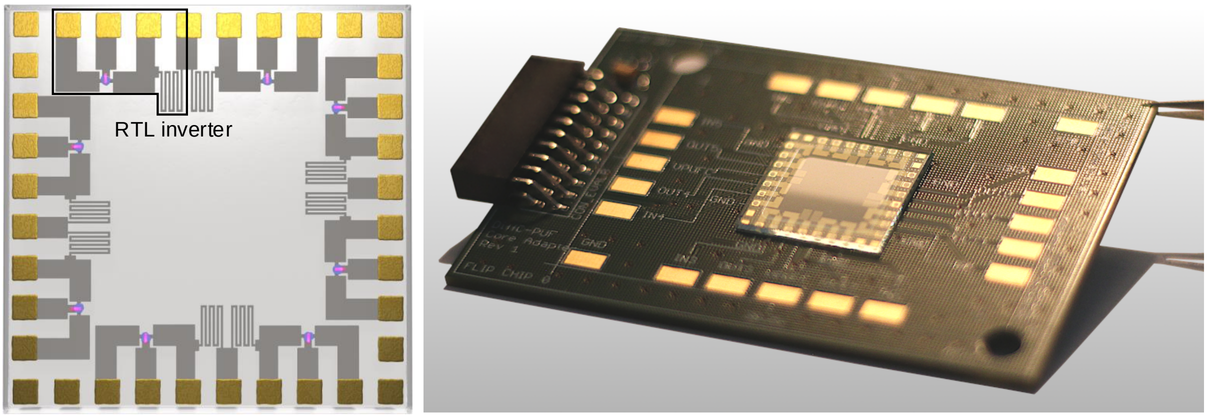


Figure 3.8: Fabrication process of the printed PUF core and integration onto the adapter PCB. Step 1: ITO structuring by laser ablation of the PUF core circuit including routing strips, resistors, I/O, and transistor terminals. Step 2: Inkjet-printing of the EGT layers, such as In_2O_3 (channel), electrolyte (gate insulation), and top gate (PEDOT:PSS). Step 3: Flip chip adopted mounting process of the inkjet-printed PUF core onto the adapter PCB using conductive adhesive (cf. [98]).

Figure 3.9a shows a rendering of the printed PUF core with eight RTL inverters on a glass substrate. Each inverter is connected to four bonding pads (gold-colored), where three pads are occupied by the transistor's drain (V_{out}), gate (V_{in}), source (GND) electrodes, and the fourth pad is connected to the PUF core supply voltage (VDD_{core}). Figure 3.9b shows a photograph of a fabricated PUF core mounted onto an adapter PCB. The mounted adapter PCB can be attached to the silicon-based PUF evaluation platform by a connector. This allows to substitute the printed PUF cores, which accelerates the large-scale characterization process. Please refer to Chapter 5 for the statistical results on printed PUF cores. At this point we want to note that the circuit complexity of the Evaluation Board is kept as low as possible to offer the potential of being fully fabricated with PE technology in the near future.

Figure 3.10 shows the scanning electron microscopy (SEM) image of a printed EGT. The image displays the non-uniformity of the semiconductor/electrolyte interface, which is used as intrinsic variation source of the PUF. The inlet close-up image shows the ITO film with the known 100 nm layer thickness as a reference. The inkjet-printed thin-film semiconductor (In_2O_3) layer has a determined thickness of ≈50 nm.



(a)

(b)

Figure 3.9: (a) Rendering of a printed PUF core on a glass substrate. (b) Photograph of a fabricated PUF core mounted onto an adapter PCB.

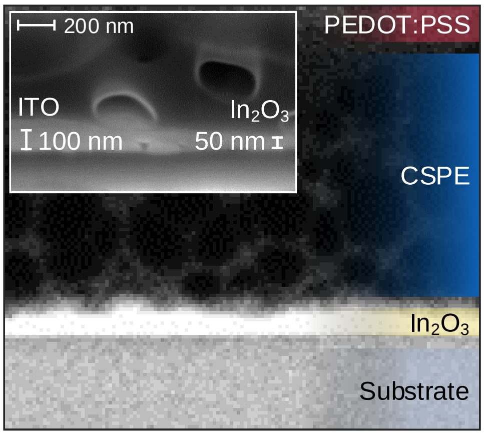


Figure 3.10: Scanning electron microscopy (SEM) image of a printed EGT showing the non-uniformity of the semiconductor/electrolyte interface (cf. [98]).

3.3.5 Software Implementation

The DiffC-PUF platform can be fully controlled from a PC via the USB interface. The PC software implementation offers the functionality to configure the PUF platform, send challenges, receive responses, and trigger voltage measurements. The entire data communication between the PC and the microcontroller is based on SCPI commands.

Figure 3.11 shows the software components of the microcontroller implementation. The PUF platform framework includes the high-level functionalities that are visible for the user. The control unit processes the challenge configuration and handles the corresponding PUF response. The supply and measurement unit configures the PUF-internal supply voltages (inverter biasing voltage V_{in} and PUF core supply voltage VDD_{core}) as well as the optional analog voltage measurements with the on-board 12-bit ADCs. The minimum resolvable signal by the ADC is 500 µV. To reduce ADC quantization errors, averaging over eight measurements is performed [33]. The platform can be configured either for manual or automatic operation. In the manual operation mode, the sub-challenges are entered via buttons and the Liquid Crystal Display (LCD). In the automatic operation mode, the platform is controlled by a PC. The user can enter challenges through challenge configuration files, or use the implemented random challenge generator. Challenges and measured responses are stored in a file database. If additional analog voltage measurements are performed, the corresponding digitalized values are also stored for further evaluations.

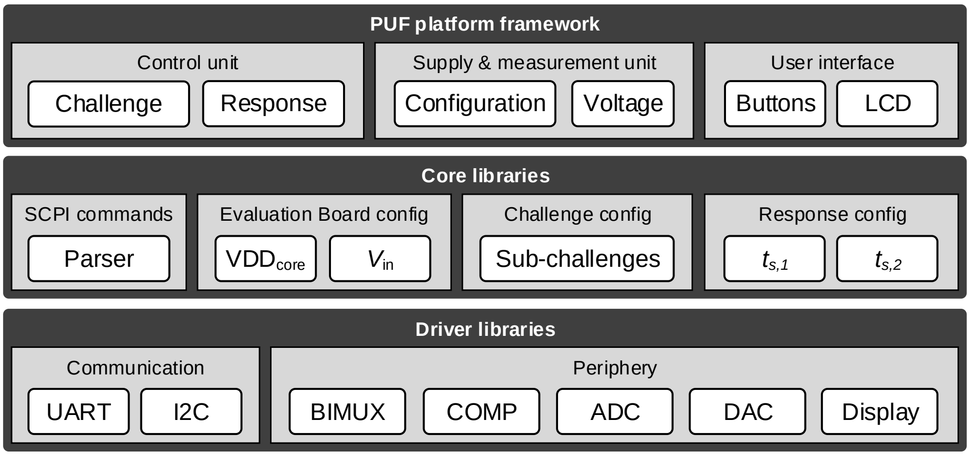


Figure 3.11: Software components of the microcontroller implementation.

The core libraries include basic functionalities, such as the SCPI command parser and the platform configurations. The lowermost layer shows the driver libraries required for communication and the periphery components. The UART interface is used in combination with an UART-to-USB converter for the communication with the PC. Figure 3.12 visualizes the challenge-response generation procedure of the DiffC-PUF. The sub-challenge c_k determines the selected inverter pair with the address tuple (a_k, b_k). The analog inverter output signals ($V_{\text{comp},+}$ and $V_{\text{comp},-}$) at the comparator input terminals change based on the inverter addressing configuration. The sampling time t_{sample} determines the point in time where the response bit r_k is read by the microcontroller and the ADCs convert the inverter output voltages to binary 12-bit values. In the shown scenario, the voltage difference at the comparator input terminals ΔV_{comp} is positive, which leads to the sub-response bit $r_k = 1$.

The timing of the sub-response bit and ADC sampling can be configured through SCPI commands by adjusting the $t_{s,1}$ and $t_{s,2}$ delay parameters, as shown in Figure 3.13. The $t_{s,1}$ value describes the time gap between applying the inverter addresses to the BIMUXs and the sampling time t_{sample}. The choice of this parameter depends on the used technology. The MOSFETs used in the silicon-based PUF core offer a high switching speed, which means that the inverter output signal remains stable after a very short time period. As a consequence, the $t_{s,1}$ parameter can be set to a small value. On the other hand, the printed EGTs offer a relatively low switching speed. Therefore, the sampling time $t_{s,1}$ should be increased to achieve reliable response bits. The timing parameter $t_{s,2}$ is mainly used to realize delays between the single sub-challenges.

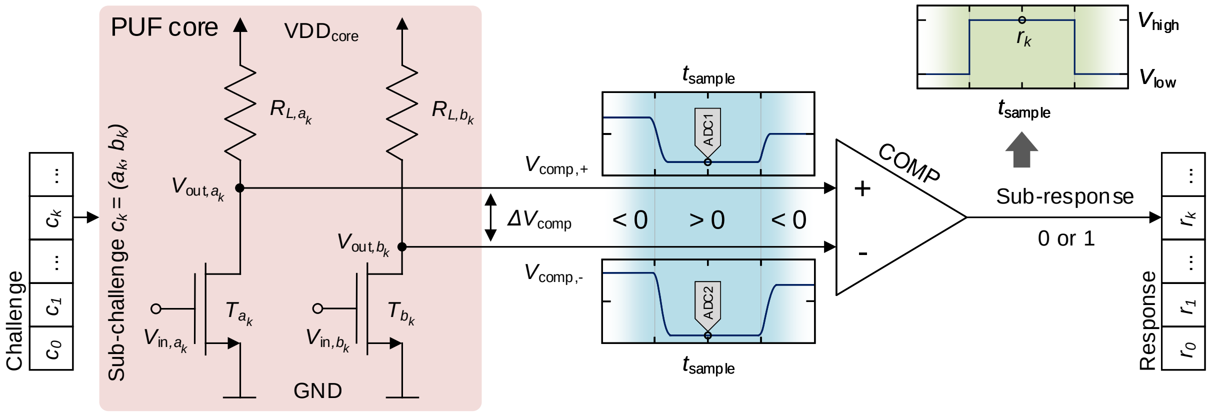


Figure 3.12: DiffC-PUF signal path for response generation. The PUF challenge is split into sub-challenges c_k to address pairs of inverters (a_k, b_k). The comparator (COMP) generates the digital sub-response bit r_k (cf. [98]).

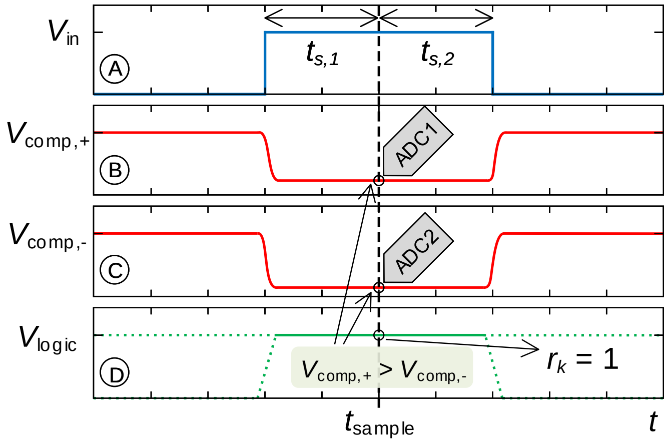


Figure 3.13: Exemplary timing diagram of the response generation (cf. [33]).

Figure 3.14 shows the simplified flow diagrams of the PC (Figure 3.14a) and microcontroller (Figure 3.14a) software implementations. The PC sends a PUF challenge command. The microcontroller receives the command and starts to process the challenge. After all sub-response bits have been generated, the response is returned to the PC.

3.4 Conclusion

In this chapter we have identified the essential requirements on PUFs suitable for PE technology. On that basis, we have presented detailed features on the DiffC-PUF design as well as the top-level architecture of the hardware and software implementations. The evaluation platform is split into three building blocks: (1) Microcontroller, (2) evaluation board, and (3) the PUF core. The implemented hardware design is based on eight PUF core inverters in resistor-transistor-logic. The microcontroller and the evaluation board are based on silicon electronic components, whereas the PUF core can either be fabricated with silicon or printed inverters. The PE-based circuits are printed onto ITO-covered 20 mm × 20 mm glass substrates. To integrate the PE circuit

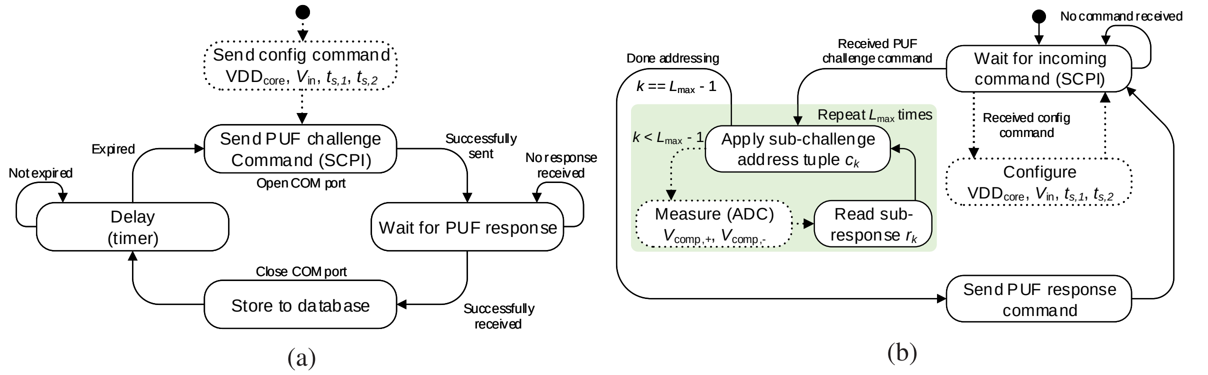


Figure 3.14: DiffC-PUF platform software implementation. Simplified flow diagrams of (a) the PC software and (b) the microcontroller software (cf. [33]). The dotted frames indicate optional processing steps.

into the evaluation system, a specially designed flip chip adapter PCB have been designed. This modular design enables large-scale characterization of fully silicon and PE-based hybrid PUFs, since the PUF cores can be substituted on demand. The embedded evaluation platform can be fully controlled by a computer via the USB interface. The software components and the bit generation process are shown and described in detail. This is the basis for the evaluations carried out in the subsequent chapters.

4 Silicon PUF Characterization & Security Evaluation

4.1 Introduction

In the previous chapters we have outlined the background of security in general, the state of the art in PUFs as well as arising security threats. Moreover, in Chapter 3 we have introduced the DiffC-PUF design and developed the modular embedded PUF platform for the evaluation of silicon as well as PE-based hybrid PUFs. Most of the PUFs reported in literature are based on silicon electronics and obtain their unique PUF characteristics from variations induced during the manufacturing process. To create a basis of comparison with other silicon-based PUF design, in this chapter the embedded PUF platform will be evaluated using discretely constructed silicon-based PUF cores. To assess the identification capabilities of the DiffC-PUF, the FAR and FRR values are computed and compared with related works. In this chapter we aim to:

- Employ fabricated silicon PUF cores for statistical tests under realistic operating conditions.
- Conduct a comprehensive experimental analysis by defining the experiment goals.
- Present statistical analysis of the PUF security metrics including uniqueness, reproducibility, bit aliasing, and uniformity based on experimental data.
- Investigate and assess the biometric identification capabilities of the fabricated silicon-based DiffC-PUFs by computing the FAR and FRR values.

4.2 Experimental Analysis

4.2.1 Experiment Goals

The goal of the experiments on the silicon-based DiffC-PUF is to assess the security capabilities of fabricated PUF core instances under realistic operating conditions. To compare our evaluation results with other works, we use the well-established PUF security metrics, as introduced in Section 2.3.4. In the literature, different PUF types are often compared and ranked only based on their security metric performances. At this point we want to mention that an objective comparison should also consider the envisioned target applications of the PUFs. For example, the security requirements might differ between identification and cryptographic applications. For many identification tasks, strong PUFs with huge CRP spaces are not required and their integration could even fail due to cost constraints. Here, we will provide an experimental analysis of the uniqueness, reliability, bit aliasing, and uniformity metrics. Furthermore, a comprehensive bit error analysis is conducted. Based on our statistical evaluations, we will identify possible target applications for the silicon-based DiffC-PUF.

4.2.2 Experiment Setup

To empirically evaluate the characteristics of the fabricated silicon-based PUF core instances, we have fabricated 30 samples and tested them under varying operating conditions. We consider variations of the ambient temperature in the range of −20 °C up to 80 °C. Furthermore, the PUF core supply voltage ($\mathrm{VDD}_{\mathrm{core}}$) and the inverter biasing voltage (V_{in}) are varied by ±10 %, respectively. Table 4.1 shows the test configurations applied in our experiments. The reference test case P_{11} denotes nominal conditions, where the ambient temperature is 25 °C, the PUF core supply voltage is $\mathrm{VDD}_{\mathrm{core}} = 1.0\,\mathrm{V}$, and the inverter biasing voltage is $V_{\mathrm{in}} = 1.0\,\mathrm{V}$. The other test cases represent corner conditions. The following methodology is used to generate PUF responses for our statistical security metric evaluations:

1. *Reference challenge*: A fixed reference challenge is built using the readdressing method and applied to the PUFs. The reference challenge includes all combinations of inverter address pairs without repetitions.
2. *Reference response*: For each PUF core instance a reference response is extracted by applying the reference challenge. The reference response is determined through majority voting among 125 PUF responses extracted under nominal operating conditions.
3. *Data aquisition*: For each PUF core instance and experimental test case, the PUF response is extracted 125 times by applying the reference challenge. The resulting responses are stored in a database.
4. *Evaluation*: The PUF responses are evaluated in terms of the PUF security metrics. The uniqueness, reliability, bit aliasing, and uniformity metrics are computed and evaluated.

The fabricated PUF cores incorporate eight RTL inverters, as explained in Section 3.3.3. The maximum bit width that can be achieved for a single PUF response by using the readdressing method is 28-bit (according to Equation (3.3)). Figure 4.1 shows a photograph of the fabricated silicon-based DiffC-PUF platform.

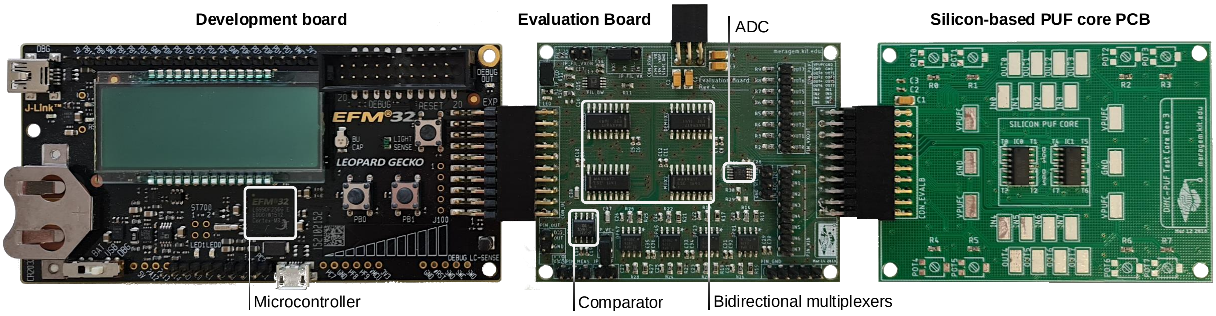


Figure 4.1: Photograph of the DiffC-PUF platform including the EFM32 development board, the silicon-based Evaluation Board, and the silicon-based PUF core PCB (from left to right).

In total, $15 \times 125 \times 30 = 56,250$ PUF responses with a length of 28 bits are evaluated for the statistical analysis of the security metrics. For our evaluations, the PUFs are operated in a Weiss WK3 climatic chamber to have a controlled ambient environment. The supply voltages of the Evaluation Board and the PUF cores are provided by a Keithley HM80403 triple power supply [33].

Table 4.1: Experiment setup for the PUF security metric evaluations.

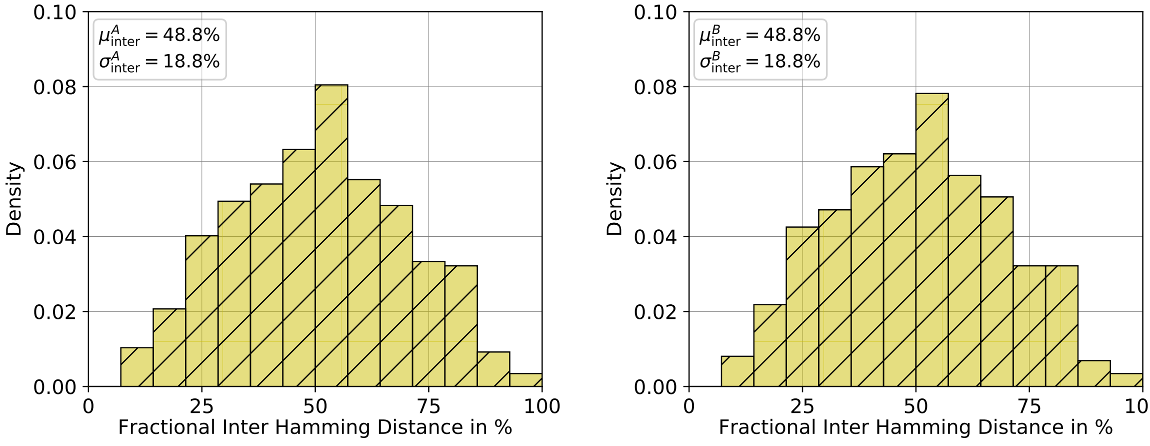
	Test	**Ambient Temperature**							**VDD$_{\text{core}}$**			**V_{in}**		
	case	**−20°C**	**0°C**	**20°C**	**25°C***	**40°C**	**60°C**	**80°C**	**0.9 V**	**1.0 V***	**1.1 V**	**0.9 V**	**1.0 V***	**1.1 V**
Temperature variations	P_1	×								×			×	
	P_2		×							×			×	
	P_3			×						×			×	
	P_4					×				×			×	
	P_5						×			×			×	
	P_6							×		×			×	
Supply voltage variations	P_7				×				×			×		
	P_8				×				×				×	
	P_9				×				×					×
	P_{10}				×					×		×		
	P_{11}				×					×			×	
	P_{12}				×					×				×
	P_{13}				×						×	×		
	P_{14}				×						×		×	
	P_{15}				×						×			×

Note: *Nominal operating conditions.

4.3 Experimental Security Metrics Results

4.3.1 Uniqueness Results

As defined in Equation (2.10), the uniqueness metric is determined by the mean value of the inter-HD distribution. A uniqueness value close to 50 % indicates unique PUF responses. Typically, the uniqueness is measured at nominal operating conditions, which corresponds to test case P_{11} from Table 4.1. We apply a fixed reference challenge (including all 28 possible sub-challenges) to each PUF instance and measure the responses. In total, we evaluate the responses of 30 fabricated PUF cores with the DiffC-PUF platform and two Evaluation Boards A and B. Figure 4.2a and Figure 4.2b show the inter-HD distributions measured with two identically constructed Evaluation Boards A and B, respectively. Both computed uniqueness values are similar with a mean of $\mu^{A}_{\text{inter}} = \mu^{B}_{\text{inter}} = 48.8$ % and a standard deviation of $\sigma^{A}_{\text{inter}} = \sigma^{B}_{\text{inter}} = 18.8$ %. The similar values imply that the uniqueness is not negatively affected by variations in the Evaluation Board circuitry and components. This is consistent with our design goal of reducing systematic errors in the DiffC-PUF platform.



(a) (b)

Figure 4.2: Inter-HD distributions for the reference responses of 30 fabricated silicon-based DiffC-PUFs using (a) Evaluation Board A (cf. [33]) and (b) Evaluation Board B.

4.3.2 Reproducibility Results

The reproducibility of a PUF is determined by the intra-HD distribution and the bit errors that occur due to changing operating conditions or aging. To compute the reliability metric according to Equation (2.12), we use the test cases P_1 to P_{15} from Table 4.1 to measure the PUF responses from 10 fabricated PUF cores. The reason for using 10 instead of all 30 fabricated DiffC-PUF cores for our reproducibility investigations is the high complexity of the evaluation process in terms of measurement equipment and time. We calculate the intra-HDs between the PUF responses measured under nominal (P_{11}) and corner conditions. Figure 4.3a shows the intra-HD distribution for the PUF responses. Figure 4.3b shows the calculated reliability values.

The resulting mean reliability value is $\mu_{\text{intra}} = 99.2\,\%$ which is close to ideal. This means that the PUF responses are reproducible.

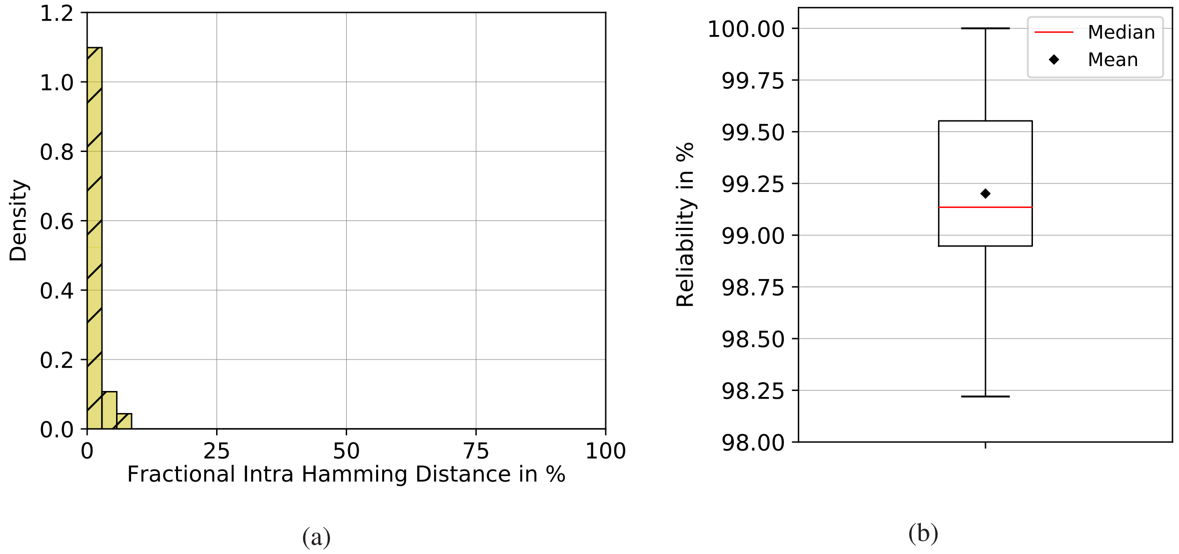


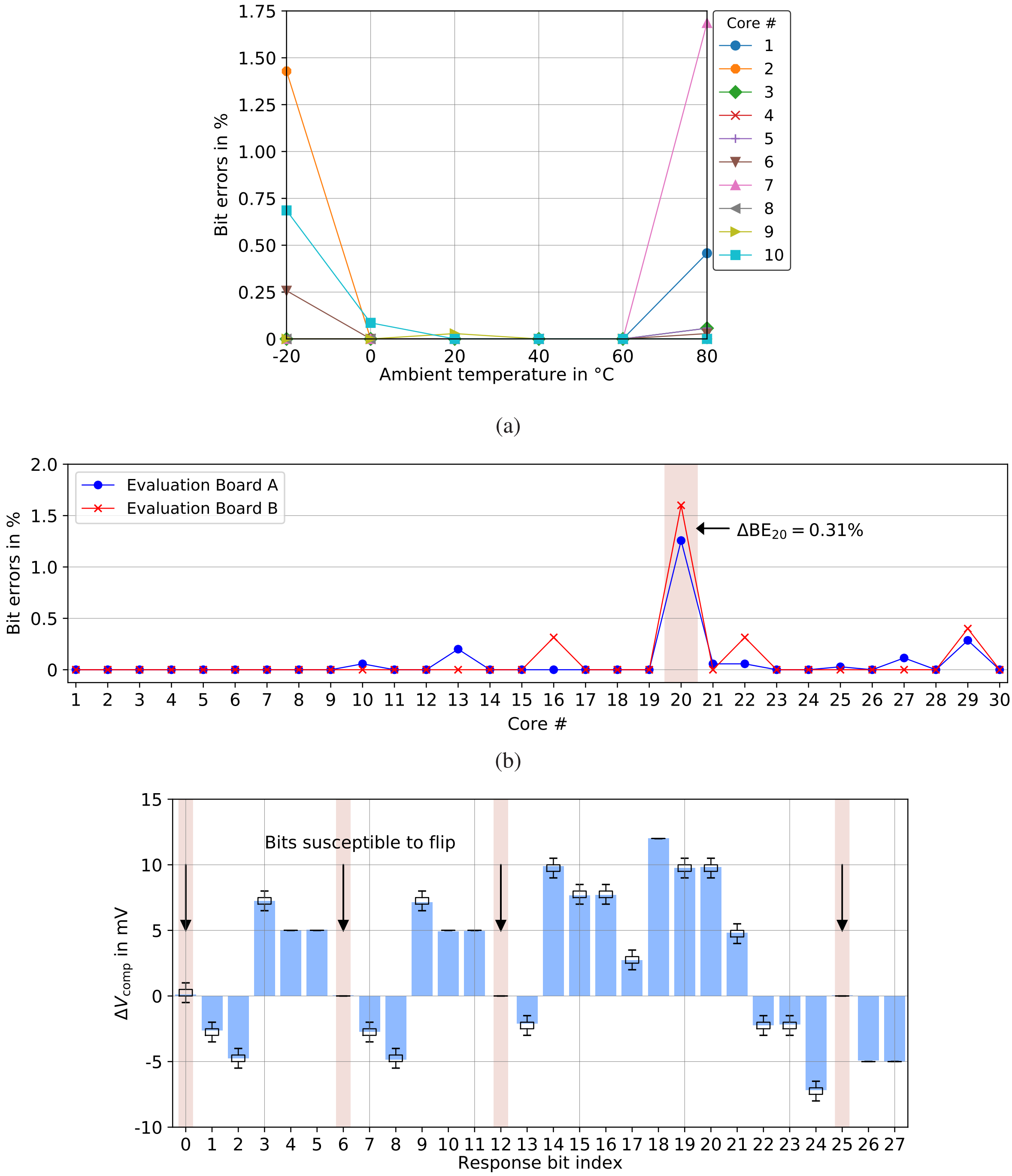
Figure 4.3: (a) Intra-HD distribution and (b) reliability values for 10 fabricated silicon-based DiffC-PUF core instances (cf. [33]).

It is often useful to gain more insight into the bit errors that occur while re-extracting PUF responses. Typical causes for evoking bit errors include noise, environmental effects, and aging. For our bit error evaluation, we apply a fixed reference challenge to all PUF instances. The PUF responses are re-extracted 125 times under different ambient temperatures (P_1 to $P6$). Figure 4.4a shows the bit errors computed from the PUF responses. The plot shows increased bit error values at ambient temperatures of −20 °C and 80 °C. The results show that the responses can be generated reproducibly in the ambient temperature range of 0 °C and 60 °C.

In a further experiment, we investigate the dependency between the occurence of bit errors and the used Evaluation Board. Therefore, we operate the 30 fabricated DiffC-PUF core instances at nominal conditions (P_{11}) by utilizing two identically constructed Evaluation Boards A and B, respectively. Figure 4.4b shows the resulting mean bit error values across the measured PUF cores. The bit errors remain stable if comparing the measurements of both Evaluation Boards. PUF core 20 shows the largest bit error values. In this context we want to note, that the herein used PUF platform also measures the comparator input voltages that cause response bit generation. Figure 4.4c shows the corresponding comparator input voltage differences ΔV_{comp} for each single PUF response bit. The sub-response bit positions r_0, r_6, r_{12}, and r_{25} show small values below 200 µV. The whiskers of the box plots indicate that the comparator input voltage difference ΔV_{comp} sometimes changes from positive to negative, and vice versa. This leads to bit errors in the binary PUF responses.

4.3.3 Bit Aliasing Results

The bit aliasing metric measures the distribution of 0s and 1s for each single PUF response bit index. In this context, a bit aliasing value of 0 % for bit position i means that all PUF instances



(a)

(b)

(c)

Figure 4.4: (a) Bit errors across ambient temperature for 10 fabricated silicon-based DiffC-PUF core instances. (b) Bit errors across 30 fabricated PUF core instances and two Evaluation Boards. (c) Comparator input voltage differences ΔV_{comp} per response bit position of PUF core 20 (cf. [33]).

produce a 0. Accordingly, a bit aliasing value of 100 % indicates a fixed bit value of 1. Both cases are referred to as ’complete bit aliasing’. For our evaluations, we compute the bit aliasing metric for 30 fabricated PUF cores according to Equation (2.13). A fixed reference challenge is applied to the PUFs and the responses are generated under nominal operating conditions. Figure 4.5

shows the resulting bit aliasing values for each response bit index. The mean bit aliasing value is 45.6 %, which is close to the ideal value of 50 %. The minimum and maximum bit aliasing values are 26.7 % and 63.3 %, respectively. These results show, that no complete bit aliasing happens, which means that the uniqueness metric is not negatively affected by frozen bits.

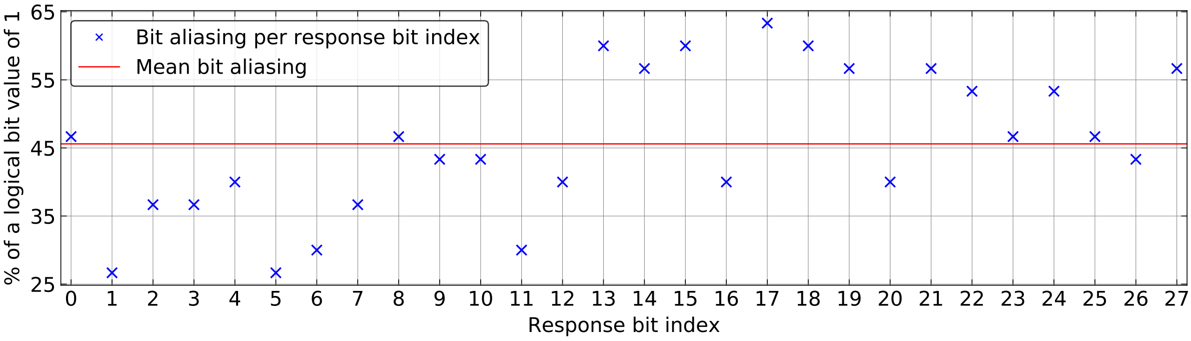


Figure 4.5: Bit aliasing values for 28-bit responses generated under nominal operating conditions.

4.3.4 Uniformity Results

The uniformity metric is a measure of the 0s and 1s distribution of the PUF response bits. Based on the envisioned target application of a PUF, specific requirements on the uniformity of the PUF responses do arise. For example, RNGs should ideally produce unpredictable binary bit sequences where the 0s and 1s occur equiprobable. The performance of a PUF in terms of the uniformity of its PUF responses is important for applications that require true random numbers, such as cryptography. For our analysis, we operate 30 fabricated PUF cores under nominal conditions (P_{11}). A fixed reference challenge is applied to the PUFs and the responses are extracted. According to Equation (2.14), the resulting mean uniformity value is 45.6 %. The boxplot in Figure 4.6 shows the uniformity values. The range of the whiskers is relatively wide, which means that some PUFs generate responses that are non-uniform. This fact limits possible target applications to tasks where a lower security level is sufficient. Further discussions on the applicability of the silicon-based DiffC-PUF will be carried out in the next section.

4.4 Identification Capabilities

In Section 2.3.5, various performance metrics to assess the identification and authentication capabilities of a PUF were presented. Thereby, the reproducibility and the uniqueness of the PUF responses are of major interest. Hence, the fuzziness of the PUF responses, described by the overlapping region between the intra-HD and inter-HD distributions, determine the identifiability of the PUF. For our evaluations, we consider an identification system based on silicon-based DiffC-PUFs with eight PUF core inverters, as proposed in the previous sections. Figure 4.7 shows the intra-HD (black line) and inter-HD (dash-dot red line) distributions for the responses obtained from fabricated DiffC-PUFs. The black dashed line indicates the point, where both distributions intersect. At this point we want to note that the raw PUF response data is used to investigate the performance capabilities. The FAR and FRR values are calculated according to

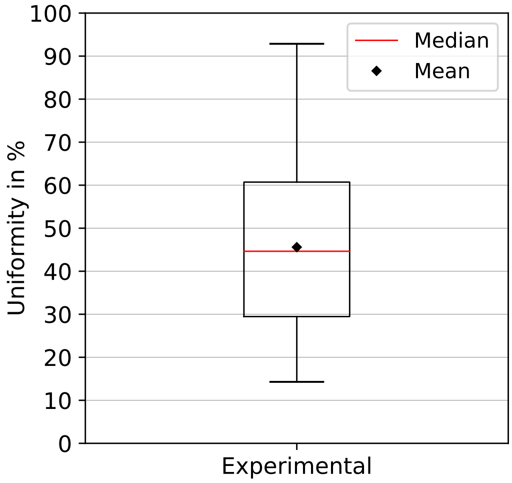


Figure 4.6: Boxplot of the uniformity values.

Equation (2.15) and Equation (2.16), respectively. Firstly, we calculate the FAR and FRR values for the intersection point of both distributions. The determined FAR value is 2.14 % (-1.67), whereas the FRR value is 0.47 % (-2.33). Typically, the percentual values are converted to the $\log_{10}(\cdot)$ notation, as denoted by the values in the brackets. The corresponding identification threshold is at 12.14 %. Secondly, we determine the point, where FAR=FRR, the so-called EER. The resulting FAR and FRR values are 1.57 % (-1.80), respectively. In this case, the identification threshold decreases slightly to 10.16 %.

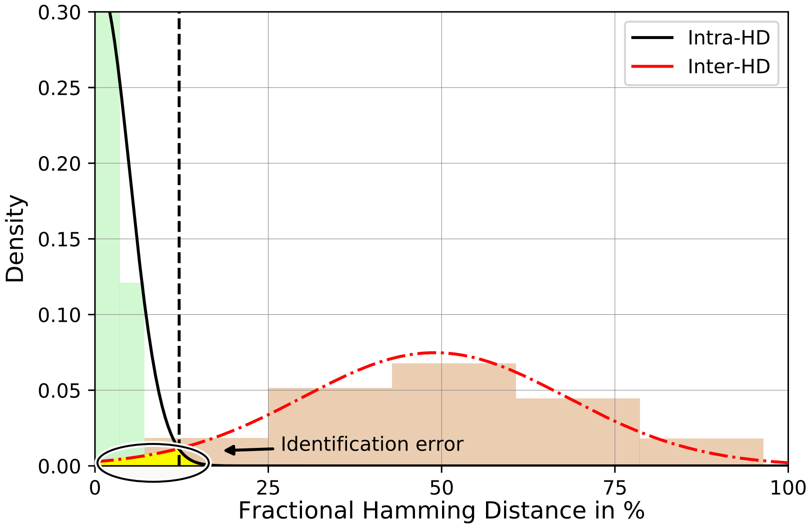


Figure 4.7: Intra-HD and inter-HD distributions for the measured PUF responses. The overlapping region is split by the identification threshold into the false-acceptance-rate (FAR) and the false-rejection-rate (FRR).

In general, the required identification performance (FAR and FRR) as well as the optimal identification threshold $\mathrm{th}_{\mathrm{id}}$ of an identification system depend on the actual target application. In many cases, FAR and FRR values of $\leq 10^{-6}$ are minimally desired [43]. To reach such values, additional post-processing, such as error-correction techniques, can further improve the identifiability of the identification system. Please note, that post-processing is not part of this work and is therefore not discussed. However, the herein presented FAR, FRR, and EER values allow to compare the identification performances between the silicon-based and the hybrid DiffC-PUFs. Futhermore, the identification threshold based on the raw response data is also an important factor to be considered when constructing a suitable error-correction.

4.5 Conclusion

In this chapter, we have presented the statistical analysis based on experimental response data obtained from 30 fabricated silicon-based PUF cores. The PUFs were operated in a climatic chamber under controlled ambient conditions. A large-scale characterization has been performed. The response data produced by the PUFs in various experiments (see Table 4.1) were evaluated in terms of the security metrics including uniqueness, reproducibility, bit aliasing, and uniformity. Finally, the identification capabilities to provide secure entity identification of the silicon-based DiffC-PUFs have been investigated. The most relevant results are shown in Table 5.6, including other related works. Please note that our evaluations are based on raw PUF responses without additional post-processing such as error correction. Nonetheless, the silicon-based DiffC-PUF shows nearly ideal values in terms of uniqueness and reliability. In order to obtain a cryptographic level of authentication security (FAR and FRR values), we propose to apply further post-processing on the PUF responses.

5 Hybrid PUF Characterization & Security Evaluation

5.1 Introduction

Most of the currently known PUF designs based on novel materials and PE technology feature promising physical characteristics for providing hardware-intrinsic security. However, the assessment of the security capabilities requires comprehensive statistical analysis, which has not been addressed for any novel material PUF, yet. In this chapter, we extract physical randomness from printed thin-film metal-oxide devices. At this point it should be noted that there are no datasheets available for the utilized printed PUF core inverters. Simulations help to investigate the characteristics of electronic circuits and to determine the best operating point. This knowledge can then be applied to fabricated devices. Since the herein discussed PUF evaluation platform enables large-scale characterization, a large number of PUF responses can be generated automatically. This allows for comprehensive statistical evaluations on the security metrics and the identification capabilities, which is important for authentication tasks. Furthermore, we validate the randomness of the PUF responses and investigate the suitability for cryptography. Finally, the performance in terms of security metrics of the hybrid PUF is compared with a selection of other related PUFs. In this chapter we aim to:

- Introduce an evaluation workflow to simulate hybrid PUFs from the analog voltage level up to the digital PUF responses. Furthermore, we perform Monte Carlo simulations to investigate the random variations of the printed PUF core inverters.
- Evaluate the hybrid PUF based on simulations in terms of the security metrics including uniqueness, reproducibility, bit aliasing, and uniformity.
- Determine the best operating point of the printed PUF cores, where the variations are maximum.
- Employ fabricated hybrid PUFs for statistical tests at the best operating point and under varying operating conditions.
- Evaluate the fabricated hybrid PUFs in terms of the security metrics including uniqueness, reproducibility, bit aliasing, and uniformity.
- Investigate and assess the biometric identification capabilities of the fabricated hybrid PUFs by computing the FAR and FRR.
- Validate the randomness of the PUF responses using the NIST Statistical Test Suite (NIST-STS).
- Compare the hybrid PUF with other PUFs in terms of the security metrics and the identification capabilities.

5.2 Experimental Analysis

5.2.1 Experiment Goals

The goal of the experiments on the hybrid PUF incorporating printed PUF cores is to asses its security capabilities. For the sake of simplicity, from here on we use the term ’hybrid PUF’ to describe the DiffC-PUF comprising the silicon-based Evaluation Board and the integrated printed PUF core. The main objective is to analyze the characteristics of the printed PUF cores. In this context, Monte Carlo (MC) simulations will be performed to investigate the RTL inverter characteristics. To assess the security performance capabilities of the hybrid PUF, the MC simulation results on the analog voltage level must be transferred to binary PUF responses. Therefore, an evaluation tool is required to simulate the complete PUF behavior, including the Evaluation Board logic components and the response bit generation. At this point, the goal is to provide a scalable evaluation tool that is not exclusively limited to the hybrid PUF configuration as used for the fabricated devices. On that basis, the simulated hybrid PUF will be evaluated in terms of security metrics and the theoretical best operating point will be determined. This is an important step, since the simulation-based statistical results will be the basis for the subsequent experimental characterization of the fabricated hybrid PUFs. In total, 15 fabricated hybrid PUFs will be operated under changing operating conditions. Based on the measured PUF responses, the security capabilities will be determined. Finally, possible target applications will be defined and the performance will be compared with related PUF designs.

5.2.2 Simulation Environment & Setup

To gain insights into the printed PUF core circuit behavior, the transfer characteristics of the printed RTL inverters are investigated. To analyze the effects of printing process variations, we perform MC simulations. The MC simulations are based on the Enz-Krummenacher-Vittoz semi-physical model developed by Rasheed et al. in [211]. Further information on the used variation model for the EGTs can be found in [212]. For temperature modeling, we use the coefficient-based approach introduced by Erozan et al. in [124, 125]. Figure 5.1 shows the workflow used for the hybrid PUF simulations.

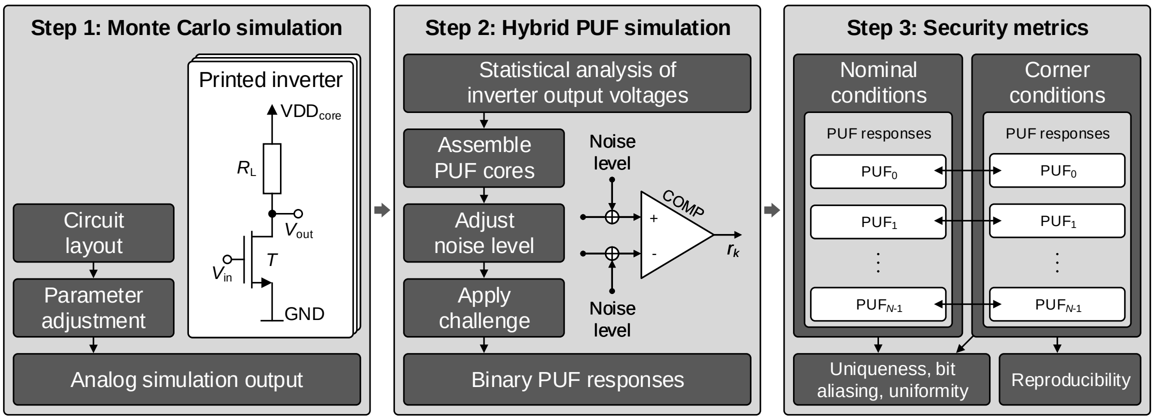


Figure 5.1: Monte Carlo simulations of printed RTL inverters and evaluation workflow of hybrid PUFs (cf. [207]).

In step 1, MC simulations are carried out for different simulation parameters, including the inverter biasing voltage V_{in}, the PUF core supply voltage VDD_{core}, and the PUF core temperature T_{core}. The parameters represent the nominal and corner conditions for PUF operation, which are used to compute the PUF security metrics. Table 5.1 shows the simulation parameters with the corresponding value ranges. The resistor R_L is set to a fixed value of 10 kΩ. For all parameter combinations, the inverter output voltages are simulated and stored in a database.

Table 5.1: Monte Carlo simulation parameters and value range.

Parameter	Value range	Description
V_{in}	0 V, 0.1 V, . . . 1.0 V	Inverter biasing voltage
VDD_{core}	0.9 V, 1.0 V*, 1.1 V	Inverter supply voltage
T_{core}	−20 °C, 23 °C*, 60 °C	PUF core temperature

Note: *Nominal conditions.

In step 2, the PUF cores are assembled by grouping the inverter output voltages obtained from the MC simulations. In general, the number of PUF core inverters can be chosen arbitrarily. The functionality of the Evaluation Board including the addressing and bit generation is implemented in Python. To consider noise in the bit generation logic, an additional noise level can be specified. Figure 5.2 shows how the noise level V_ϵ affects the comparator input voltages $V_{\text{comp},+}$ and $V_{\text{comp},-}$. The comparator input voltages are defined according to Equations (5.1) and (5.2).

$$V_{\text{comp},+} = V_{\text{out},a_k} \pm V_\epsilon \tag{5.1}$$

$$V_{\text{comp},-} = V_{\text{out},b_k} \pm V_\epsilon \tag{5.2}$$

For the simulations, different noise levels in the range of $V_\epsilon = \{0\,\text{mV}, 0.5\,\text{mV}, 1.0\,\text{mV}, \ldots 10.0\,\text{mV}\}$ are applied, whereas a noise level of 0 mV denotes nominal conditions. All permutations of possible noise level allocations are used, as shown in Table 5.2.

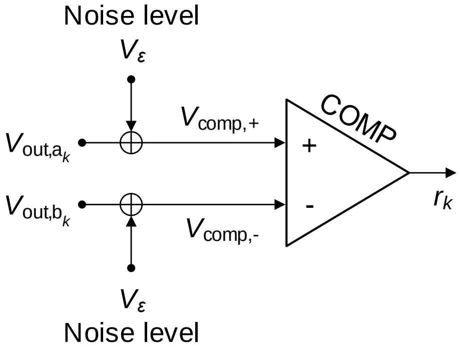


Figure 5.2: Hybrid PUF comparator input noise level modeling. (cf. [207]).

The PUF responses are generated based on inverter output voltage comparisons and under consideration of the noise levels. The following methodology is used to generate PUF responses for further evaluations:

1. *Reference challenge:* A fixed reference challenge is applied, including all combinations of inverter address pairs without repetitions (readdressing method).
2. *Reference response:* For each simulated PUF core instance and under nominal conditions a reference response is extracted by applying the reference challenge.
3. *Data acquisition:* For each simulated PUF core instance, inverter biasing voltage, corner condition, and noise level the PUF response is re-extracted by applying the reference challenge. The resulting responses are stored in a database.

Table 5.2: Impacts of the noise level (NL) on the comparator input voltages.

Quantity	**Noise level allocation**					
	NL1	**NL2**	**NL3**	**NL4**	**NL5**	**NL6**
V_{out,a_k}	$+V_\epsilon$	$-V_\epsilon$			$+V_\epsilon$	$-V_\epsilon$
V_{out,b_k}			$+V_\epsilon$	$-V_\epsilon$	$-V_\epsilon$	$+V_\epsilon$

In step 3, the simulation results at nominal and corner conditions are separated. Finally, the security metrics are computed and evaluated. In total, $102 \times 6 \times 150 = 91,800$ PUF responses with 28-bit are considered in the statistical evaluations of the security metrics [207].

5.2.3 Experiment Setup

To empirically evaluate the characteristics of the 15 fabricated printed DiffC-PUF core instances, they are tested under varying operating conditions. For our evaluations we consider variations of the ambient temperature in the range of 20 °C up to 60 °C. The printed EGTs are typically operated at a relative humidity of 50 % and show sensitivity to humidity changes. To capture this effects in our evaluations, we operate the hybrid PUFs in a climatic chamber and vary the relative humidity in the range of 45 % to 55 %. Furthermore, the PUF core supply voltage ($\mathrm{VDD}_{\mathrm{core}}$) is varied by ±10 %. Table 5.3 shows the test configurations applied in our experiments. The reference test case $\tilde{P}_1$ denotes nominal conditions where the ambient temperature is 20 °C, the relative humidity is 50 %, and the PUF core inverter supply voltage is $\mathrm{VDD}_{\mathrm{core}} = 1.0\,\mathrm{V}$. Similar to our silicon-based DiffC-PUF evaluations, the following methodology is used to generate PUF responses for our statistical security metric evaluations on the hybrid PUF:

1. *Reference challenge:* A fixed reference challenge is generated and applied to the hybrid PUFs. The reference challenge includes all combinations of inverter address pairs without repetitions (readdressing method).
2. *Reference response:* For each printed PUF core instance a reference response is extracted by applying the reference challenge. The reference response is determined through majority voting among 20 PUF responses extracted under nominal operating conditions.
3. *Data acquisition:* For each printed PUF core instance and experimental test case, the PUF response is extracted 20 times by applying the reference challenge. The resulting responses are stored in a database.

4. *Evaluation:* The PUF responses are evaluated in terms of the PUF security metrics. The uniqueness, reproducibility, uniformity, and bit aliasing metrics are computed and evaluated.

The fabricated printed PUF cores incorporate eight RTL inverters. Figure 5.3 shows a photograph of the fabricated hybrid DiffC-PUF platform. As described in Section 3.3.4, the printed PUF core is mounted onto the silicon-based adapter PCB. Please note that the ITO strips are not visible in the picture due its transparency.

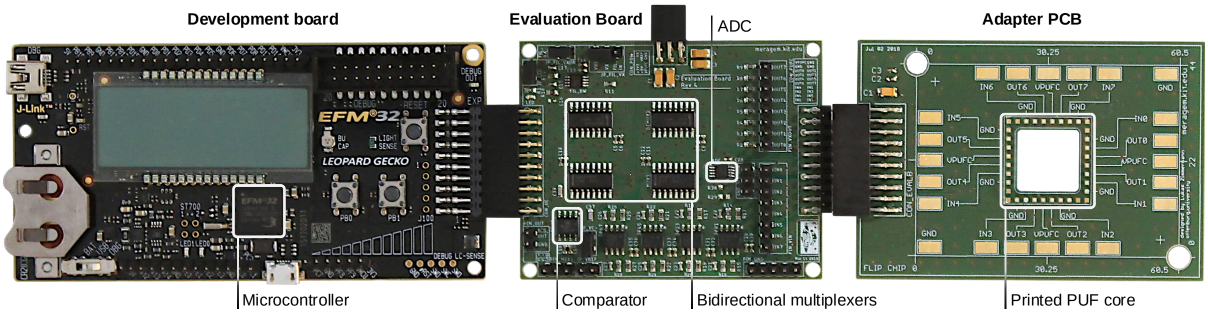


Figure 5.3: Photograph of the hybrid PUF platform including the EFM32 development board, the silicon-based Evaluation Board, and the adapter PCB incorporating the printed PUF core (from left to right) (cf. [98]).

For our evaluations, the PUFs are operated in a Weiss WK3 climatic chamber to have a controlled ambient environment in terms of temperature and relative humidity. The microcontroller development board is powered by the USB interface. The Evaluation Board is powered using the microcontroller development board's internal 5 V and 3.3 V supply pins. To dynamically adjust the inverter biasing voltage (V_{in}) and the PUF core inverter supply voltage (VDD_{core}), two internal 12-bit DACs of the microcontroller board are utilized. For the statistical analysis in terms of security metrics, in total $11 \times 20 \times 15 = 3,300$ PUF responses with 28-bit are evaluated.

5.3 Simulation-Based Security Metrics Results

5.3.1 Best Operating Point Determination

Before evaluating the PUF security metrics, first of all we want to investigate the variations in the PUF core inverter output voltages. In the hybrid PUF, the response bit generation is based on pairwise voltage comparisons. In technical systems, the maximum resolution is limited by the electrical characteristics of the components. The comparator resolution of our PUF platform setup (please refer to Section 3.3.3 for more information) is limited by the input offset voltage of 200 µV. As a consequence, higher magnitudes of variations reduce bit errors and lead to a better reproducibility of the PUF responses. As stated in Section 2.3.1, achieving a good reproducibility is one of the most important properties that distinguishes PUFs from RNGs.
Figure 5.4 shows the standard deviation of the inverter output voltages V_{out} for different inverter biasing voltages V_{in}, PUF core supply voltages VDD_{core}, and PUF core temperatures T_{core}. For all temperatures, the maximum standard deviations are reached in the range of $V_{\text{in}} = [0.3\,\text{V}, 0.5\,\text{V}]$. The best operating point can be found within this range. From a theoretical point of view, it is preferable to choose a robust operating point. In general, using the middle of the aforementioned

Table 5.3: Experiment setup for the hybrid PUF security metric evaluations.

Test	**Ambient Temperature**			**Rel. humidity**			**VDD$_{\text{core}}$**		
case	**20°C***	**40°C**	**60°C**	**45 %**	**50 %***	**55 %**	**0.9 V**	**1.0 V***	**1.1 V**
$\tilde{P}_1$	×				×			×	
$\tilde{P}_2$	×			×				×	
$\tilde{P}_3$	×					×		×	
$\tilde{P}_4$	×				×		×		
$\tilde{P}_5$	×				×				×
$\tilde{P}_6$		×			×			×	
$\tilde{P}_7$		×			×		×		
$\tilde{P}_8$		×			×				×
$\tilde{P}_9$			×		×			×	
$\tilde{P}_{10}$			×		×		×		
$\tilde{P}_{11}$			×		×				×

Note: *Nominal operating conditions.

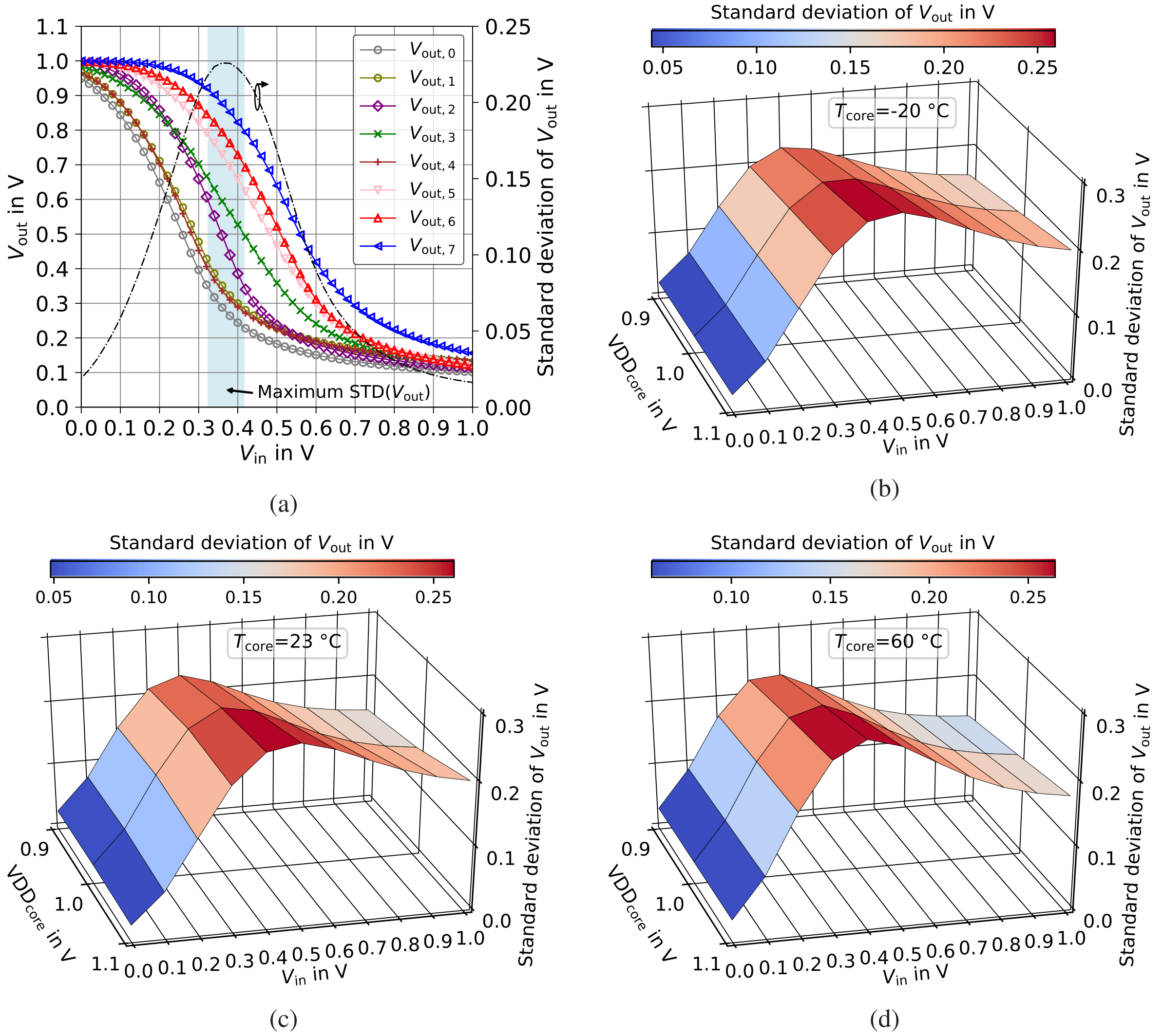
range provides a margin that prevents from unstable PUF responses, even if the inverter biasing voltage drifts due to environmental impacts.

5.3.2 Uniqueness Results

The uniqueness metric is computed according to Equation (2.10), based on PUF responses generated under nominal operating conditions. In total, we evaluate the reference responses of 150 simulated hybrid PUFs. Figure 5.5 shows the inter-HD distribution for an inverter biasing voltage of 0.4 V. The uniqueness metric is determined by the mean inter-HD value $\mu_{\text{inter}} = 50.0\,\%$ with a standard deviation of $\sigma_{\text{inter}} = 14.4\,\%$. The mean value shows that the PUF responses are distinguishable. Table 5.4 shows the uniqueness results for inverter biasing voltages in the range of $V_{\text{in}} = [0.2\,\text{V}, 1.0\,\text{V}]$.

5.3.3 Reproducibility Results

For the reproducibility evaluation, we compute the reliability metric according to Equation 2.12, based on the responses of 150 simulated hybrid PUFs. We calculate the intra-HDs between the PUF reference responses generated under nominal operating conditions and the corner responses extracted under the corner conditions. As described in Section 5.2.2, the nominal conditions comprise a PUF core inverter supply voltage of VDD$_{\text{core}}$ = 1.0 V and a PUF core temperature of $T_{\text{core}} = 23\,°\text{C}$. The inverter biasing voltage is gradually increased in 100 mV steps in the range of $V_{\text{in}} = [0.2\,\text{V}, 1.0\,\text{V}]$. Figure 5.6 shows the mean reliability values in dependency of the noise level and the inverter biasing voltage. If increasing the noise level, the mean reliability values



(a)

(b)

(c)

(d)

Figure 5.4: (a) Measured transfer curves of eight fabricated PUF core inverters, including the standard deviation (STD(V_{out})). (b) – (d) Standard deviations of V_{out} across different inverter biasing voltages V_{in}, PUF core supply voltages VDD$_{core}$, and PUF core temperatures T_{core} (cf. [213]).

decrease for all V_{in}. The results show that the maximum mean reliability values are reached when biasing the PUF core inverters with $V_{in} = 0.4$ V, which coincides with the best operating point determined in Section 5.3.1.

When calculating mean values, outliers might be compensated, which could falsify the results. Thereby, the minimum reliability value that can be expected limits the field of possible target applications. Figures 5.7a and 5.7b show the mean and minimum reliability values over different noise levels and inverter biasing voltages (V_{in}), respectively. All corner conditions are included in the results. Even for higher noise levels (≥ ±5 mV), the best reliability values are achieved at $V_{in} = 0.4$ V. At the best operating point, the mean reliability value is 98.4 %, whereas the minimum reliability value is 93.7 % at a noise level of ±10 mV. The minimum reliability value is an indicator for the requirements an error correction must fulfill to achieve error-free reproducibility of the PUF responses. The histogram in Figure 5.7c shows distribution of the

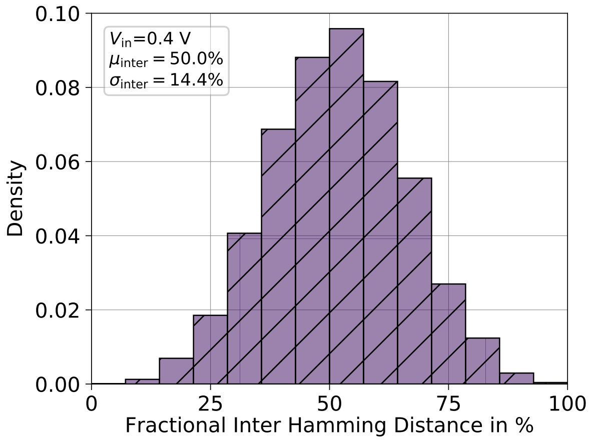
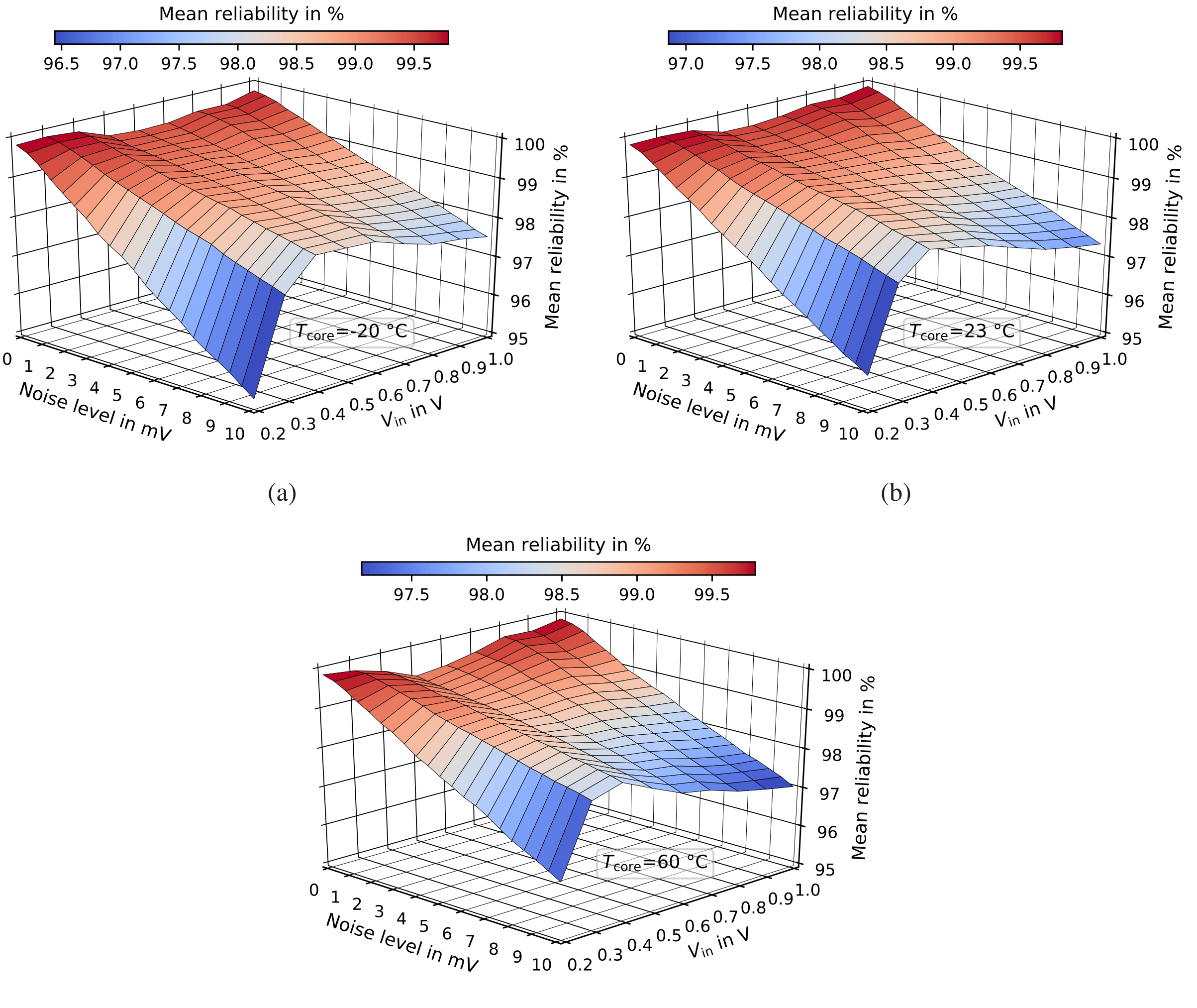


Figure 5.5: Inter-HD distribution for the reference responses of 150 simulated hybrid PUFs (cf. [213]).



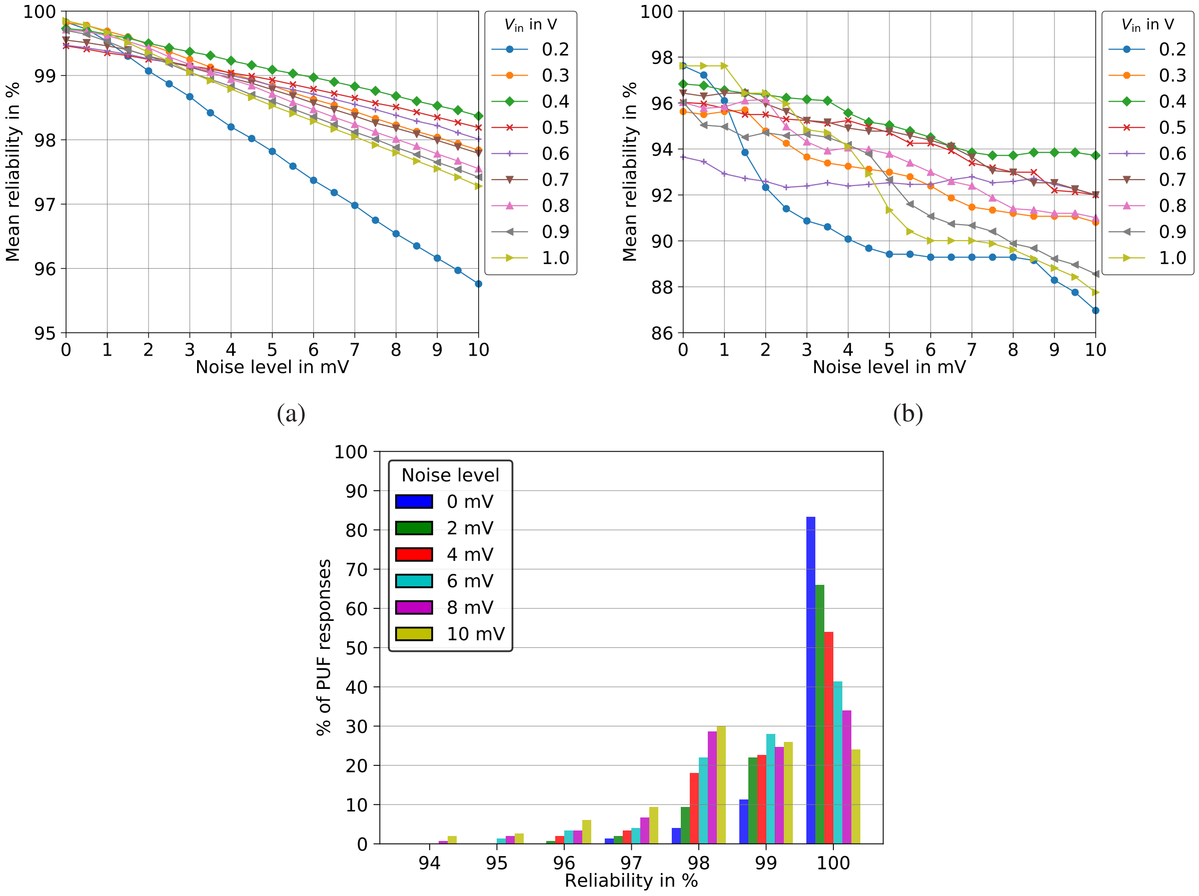
(a)

(b)

(c)

Figure 5.6: Mean reliability values across different noise levels, inverter biasing voltages V_{in}, and PUF core temperatures T_{core}. (a) T_{core} = −20 °C. (b) T_{core} = 23 °C. (c) T_{core} = 60 °C (cf. [213]).

reliability values at the best operating point and for different noise levels. Increasing the noise level degrades the robustness of the response generation. In summary it can be said, that the reliability results are close to the ideal value of 100 %, which means that the PUF responses are reproducible.



(a)

(b)

(c)

Figure 5.7: (a) Mean reliability values and (b) minimum reliability values across different noise levels and inverter biasing voltages. (c) Histogram of the mean reliability values for $V_{\text{in}} = 0.4$ V and different noise levels (cf. [213]).

5.3.4 Bit Aliasing Results

The bit aliasing metric determines the bias of each single PUF response bit. In this context, a bit aliasing value of 0 % for bit position i means that all PUF instances produce a 0. Accordingly, a bit aliasing value of 100 % indicates a fixed bit value of 1. Both cases are referred to as 'complete bit aliasing'. Our bit aliasing evaluation is based on responses extracted from 150 simulated hybrid PUFs under nominal operating conditions. According to Equation (2.13), the bit aliasing is calculated for each single PUF response bit index. We compute the bit aliasing values for inverter biasing voltages in the range of $V_{\text{in}} = [0.2\,\text{V}, 1.0\,\text{V}]$. With a minimum value of 38.7 % and a maximum value of 60.7 %, no complete bit aliasing happens in the hybrid PUFs. This implies that there are no frozen bits that negatively affect the uniqueness metric results.

Figure 5.8 shows the bit aliasing values for an inverter biasing voltage of $V_{\text{in}} = 0.4\,\text{V}$. The mean bit aliasing value is 49.8 %, which is close to the ideal value of 50 %. The minimum bit aliasing value is 42.7 %, whereas the maximum value is 58.0 %, respectively. The good results can be explained by the nature of printed device fabrication. Because of the additive manufacturing process with solution-processable materials, each device exhibits its own intrinsic variation probability distribution [213].

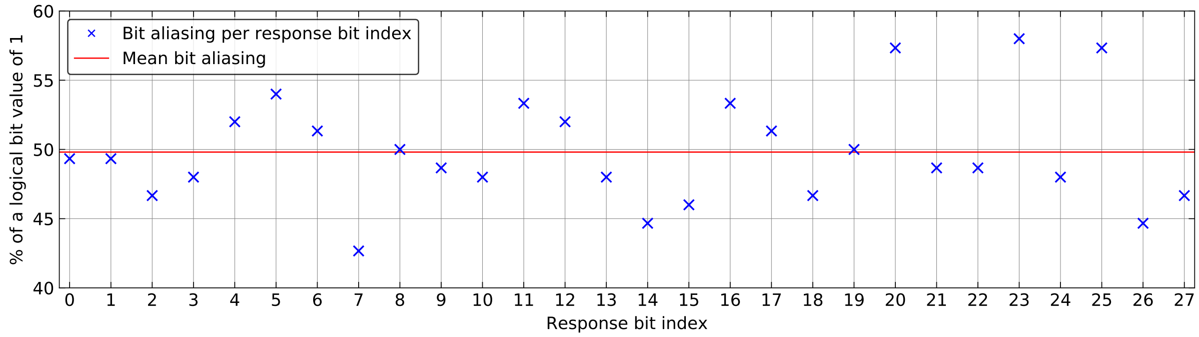


Figure 5.8: Bit aliasing values for 28-bit PUF responses at $V_{\text{in}} = 0.4\,\text{V}$ and nominal operating conditions (cf. [213]).

5.3.5 Uniformity Results

The uniformity metric is computed using the responses of 150 simulated hybrid PUFs under nominal operating conditions, according to Equation (2.14). The resulting mean uniformity values for inverter biasing voltages in the range of $V_{\text{in}} = [0.2\,\text{V}, 1.0\,\text{V}]$ are close to the ideal value of 50 %. The boxplot in Figure 5.9 shows the uniformity values for $V_{\text{in}} = 0.4\,\text{V}$.

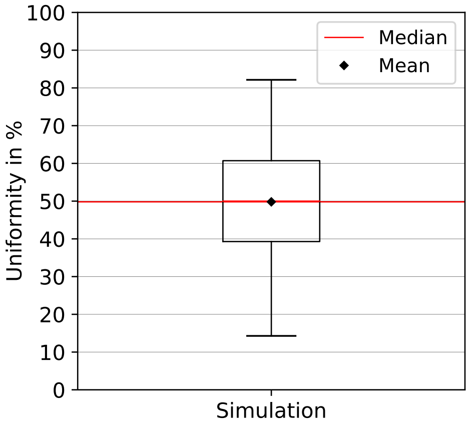


Figure 5.9: Boxplot of the uniformity values at $V_{\text{in}} = 0.4\,\text{V}$ and nominal operating conditions.

The mean value is 49.8 %, whereas the spread of the uniformity values is wide, which denotes that some PUF responses are non-uniform. This limits the suitability of the hybrid PUF to applications where the uniformity feature is less relevant, such as identification and authentication. However, at this point we must consider that the evaluations shown in this work are based on raw PUF responses without additional post-processing. Please note that the uniformity can be further improved through techniques such as the entropy distiller as introduced in [214, 215].

Table 5.4: Security metrics for the simulated hybrid PUF.

$\mathbf{V_{in}}$	**Uniqueness**		**Reliability**		**Bit aliasing**			**Uniformity**		
	μ_{inter}	σ_{inter}	**Min.**	**Mean**	**Min.**	**Mean**	**Max.**	**Min.**	**Mean**	**Max.**
0.2 V	50.0 %	14.3 %	87.0 %	95.8 %	39.3 %	49.5 %	58.0 %	10.7 %	49.5 %	92.9 %
0.3 V	50.1 %	14.3 %	90.8 %	97.8 %	41.3 %	49.4 %	57.3 %	10.7 %	49.4 %	85.7 %
0.4 V	50.0 %	14.4 %	93.7 %	98.4 %	42.7 %	49.8 %	58.0 %	7.1 %	49.8 %	82.1 %
0.5 V	50.0 %	14.4 %	92.0 %	98.2 %	43.3 %	49.4 %	60.0 %	7.1 %	49.4 %	85.7 %
0.6 V	50.0 %	14.4 %	92.0 %	98.0 %	44.7 %	49.6 %	60.0 %	7.1 %	49.6 %	85.7 %
0.7 V	50.0 %	14.4 %	92.0 %	97.8 %	44.0 %	49.8 %	59.3 %	7.1 %	49.8 %	85.7 %
0.8 V	50.0 %	14.4 %	91.0 %	97.6 %	44.7 %	49.6 %	60.7 %	10.7 %	49.6 %	85.7 %
0.9 V	50.0 %	14.4 %	88.6 %	97.4 %	43.3 %	49.7 %	60.7 %	10.7 %	49.7 %	82.1 %
1.0 V	49.9 %	14.4 %	87.8 %	97.3 %	42.7 %	49.7 %	60.0 %	14.3 %	49.7 %	82.1 %

5.4 Experimental Security Metrics Results

5.4.1 Uniqueness Results

The uniqueness metric is determined by the mean inter-HD value according to Equation (2.10). The experiments performed to evaluate the uniqueness metric are described in Section 5.2.3. A fixed reference challenge is applied to 15 fabricated hybrid PUFs under nominal operating conditions (test case $\tilde{P}_1$ from Table 5.3). The inverter biasing voltage is set to the best operating point $V_{\text{in}} = 0.4\,\text{V}$, as explored in our prior simulations (see Section 5.3). Figure 5.10 shows the inter-HD distribution based on the experimental results and the outcomes of the simulations. The resulting experimental uniqueness value is $\mu^{e}_{\text{inter}} = 51.1\,\%$ with a standard deviation of $\sigma^{e}_{\text{inter}} = 15.5\,\%$. These values are in good agreement with both the simulation results and the theoretical ideal value of 50 %, which shows that the PUF responses from different entities can be distinguished.

5.4.2 Reproducibility Results

For the reproducibility evaluations, we operate four fabricated hybrid PUFs in the controlled ambient environment of a climatic chamber. The test cases used for the experiments are shown in Table 5.3, whereas test case $\tilde{P}_1$ deenotes nominal operating conditions. The reason for using four instead of all 15 fabricated PUF cores is the high complexity of the evaluation process in terms of measurement equipment and time. We compute the reliability metric according to Equation (2.12). The inverter biasing voltage is consecutively set to the values

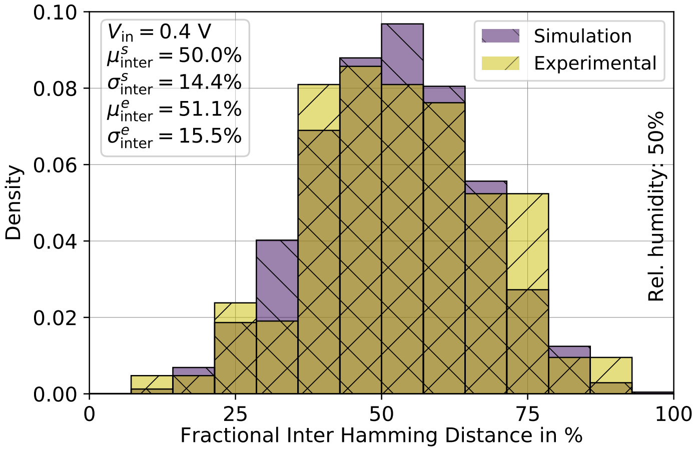
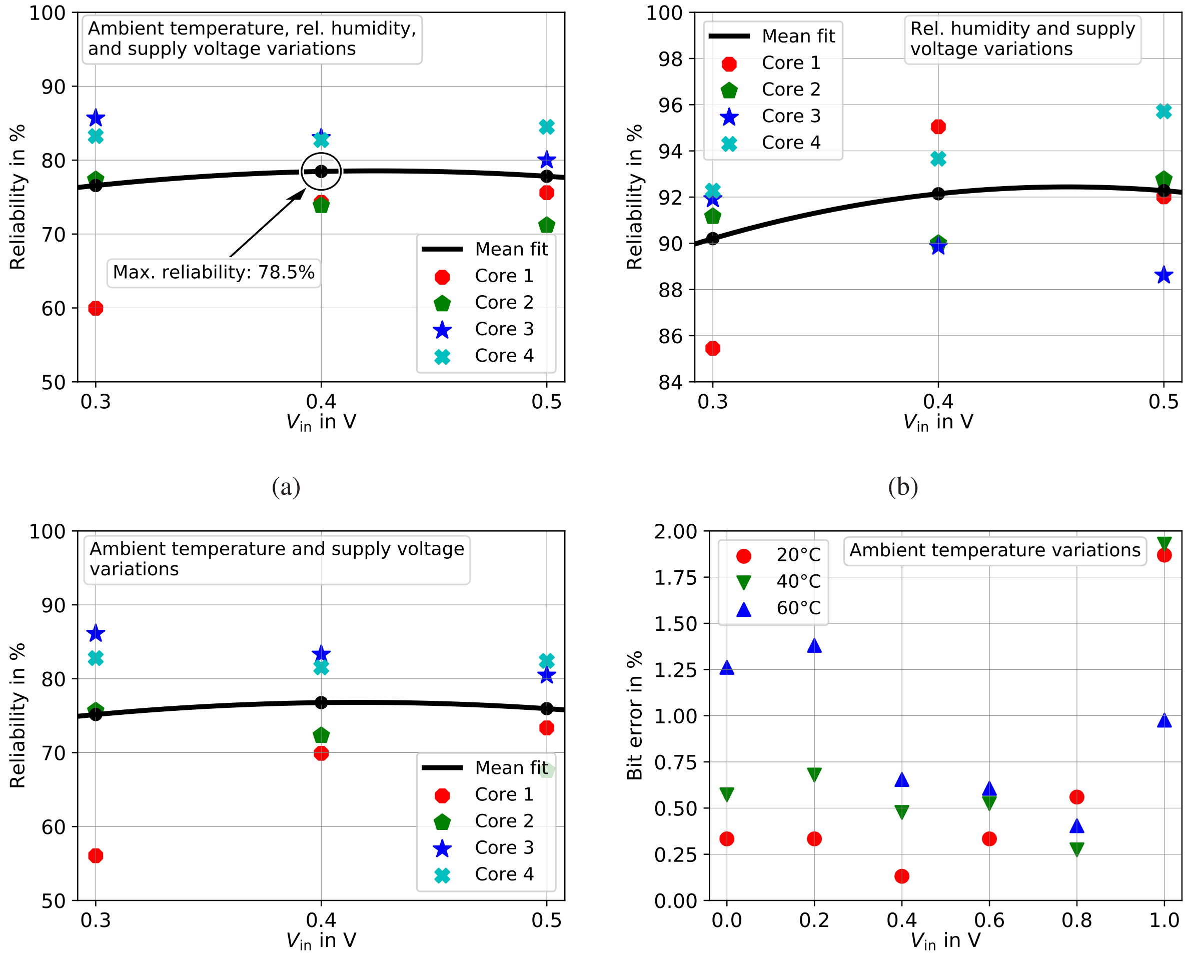


Figure 5.10: Inter-HD distribution for the responses of 15 fabricated hybrid PUFs generated under nominal conditions (test case $\tilde{P}_1$) as well as the simulation results for comparison (cf. [98]).

$V_{in} = \{0.3\,\text{V}, 0.4\,\text{V}, 0.5\,\text{V}\}$, to investigate the robustness around the best operating point determined in our prior simulations (see Section 5.3). Figure 5.11a shows the mean reliability values for each single tested PUF core. In this experiment, all test cases $\tilde{P}_1$ to $\tilde{P}_{11}$ are used. The thick black line represents a second-order regression model fit of the calculated mean reliability values. The maximum fitted mean reliability value is 78.5 % reached at $V_{in} = 0.4$ V. However, the simulations indicated a minimum reliability value of 93.7 %, which is far apart from the experimental results. At this point we want to note that no passivation layer to protect the active materials of the EGTs from environmental impacts is available for the fabricated devices. This explains the relatively low experimental reliability values. To further investigate the impacts of the different ambient conditions, we re-evaluate the reliability metric under non-consideration of changes in the ambient temperature and relative humidity. Figure 5.11b shows the mean reliability values for each PUF core based on the responses extracted under varied relative humidity and supply voltages (test cases $\tilde{P}_1$ to $\tilde{P}_5$). The maximum mean reliability value is 92.3 % at $V_{in} = 0.5$ V. The results show that the bit flips are mainly caused by the influence of ambient temperatures variations. Figure 5.11c shows the mean reliability values for PUF responses extracted under ambient temperature and supply voltage variations. The maximum mean reliability value is 76.8 % at $V_{in} = 0.4$ V, which is a further evidence for the temperature dependency of the PUF responses. The actual bit errors over the inverter biasing voltage V_{in} and for different ambient temperatures are shown in Figure 5.11d. The relative humidity is 50 % and the inverter supply voltage is $\text{VDD}_{core} = 1.0$ V. The inverter biasing voltage is gradually increased in the range of $V_{in} = [0.0\,\text{V}, 1.0\,\text{V}]$. For this evaluation, the reference responses are generated for each temperature level in order to investigate the robustness of the PUF response generation. The plot shows that the bit errors strongly increase between $V_{in} = [0.8\,\text{V}, 1.0\,\text{V}]$. This effect happens because the PUF core inverters have already reached their logical low levels, where the magnitude of the variations is small. If a single bit in a 28-bit response flips its binary value, it causes a bit error of ≈ 3.6 %. The experimentally determined mean bit error is below < 2 % for the full range of inverter biasing voltages, which means that in the average case less than one bit is flipped per re-extraction of the PUF response.

In summary, the results show that the bit errors are mainly caused by variations of the ambient temperature. The impacts of altered relative humidity and inverter supply voltage variations are low. Larger reliability values can be expected once passivation and encapsulation is available for the EGT technology.



(a)

(b)

(c)

(d)

Figure 5.11: (a) Reliability values for ambient temperature, relative humidity, and supply voltage variations (test cases $\tilde{P}_1 - \tilde{P}_{11}$). (b) Reliability values for relative humidity and supply voltage variations (test cases $\tilde{P}_1 - \tilde{P}_5$). (c) Reliability values for ambient temperature and supply voltage variations (test cases $\tilde{P}_1$, $\tilde{P}_4 - \tilde{P}_{11}$). (d) Bit errors across different ambient temperatures (test cases $\tilde{P}_1$, $\tilde{P}_6$, and $\tilde{P}_9$) (cf. [98]).

5.4.3 Bit Aliasing Results

To evaluate the bit aliasing metric, the responses of 15 fabricated hybrid PUFs are utilized. The PUF responses are extracted under nominal operating conditions (test case $\tilde{P}_1$). The inverter biasing voltage is fixed to the best operating point at $V_{\text{in}} = 0.4\,\text{V}$. Figure 5.12 shows the distribution of the bit aliasing values (according to Equation (2.13)), computed based on experimental response data. The resulting experimental mean bit aliasing value is $\mu^e_{\text{BA}} = 44.5\,\%$ with a standard deviation of $\sigma^e_{\text{BA}} = 9.3\,\%$. The ideal bit aliasing value is 50 %, which shows that the PUF responses are biased towards 0. Nonetheless, the results show good statistical coverage with the simulations (see Section 5.3).

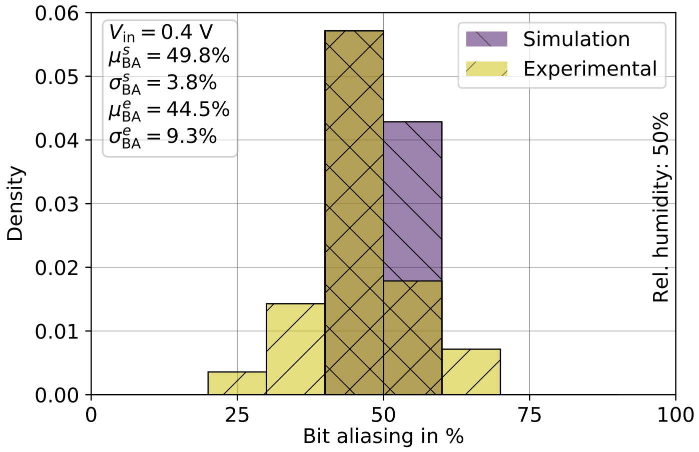


Figure 5.12: Bit aliasing at $V_{in} = 0.4$ V and nominal operating conditions (test case $\tilde{P}_1$) (cf. [98]).

5.4.4 Uniformity Results

Similar to the bit aliasing metric, the uniformity metric is computed based on PUF responses generated from 15 fabricated hybrid PUFs. The hybrid PUFs are operated under nominal conditions (test case $\tilde{P}_1$) and the inverter biasing voltage is set to the best operating point $V_{in} = 0.4$ V. The resulting experimental mean uniformity is 44.5 %. The minimum and maximum values are 17.9 % and 89.3 %, respectively, which denotes that some PUF responses are non-uniform. The boxplot in Figure 5.13 shows the spread of the uniformity values. The results on the raw PUF responses without additional post-processing imply that the hybrid PUF is not suitable for applications that require uniform PUF responses, such as cryptography.

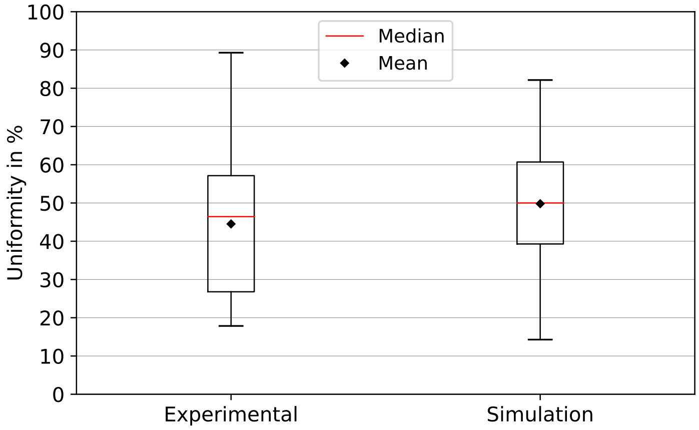
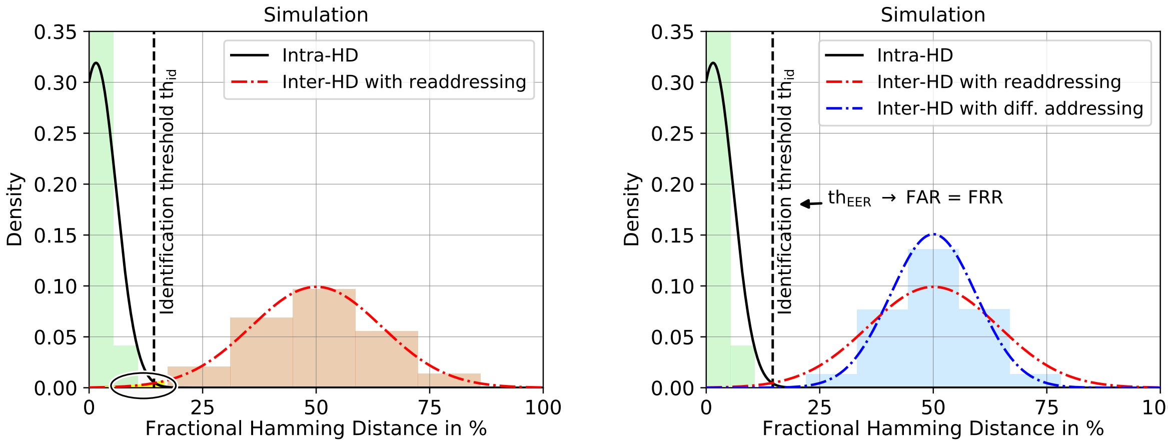


Figure 5.13: Boxplot of the uniformity values at $V_{in} = 0.4$ V and nominal operating conditions (test case $\tilde{P}_1$).

5.5 Identification Capabilities

In general, the identification capabilities of PUFs are determined by the fuzziness of the PUF responses. To determine a theoretical figure of merit in terms of the identification capabilities of the hybrid PUF, we utilize the intra-HD and inter-HD distributions obtained from the simulations in Section 5.3. In Section 3.2.3, we have introduced two challenge building methods. For our first evaluations, we use the readdressing method to build the PUF challenges and generate the corresponding responses from hybrid PUFs with eight core inverters.



(a)

(b)

Figure 5.14: Intra-HD and inter-HD distributions based on simulations when using (a) the readdressing method and (b) the differential addressing method to build the PUF challenges (cf. [216]).

Figure 5.14a shows the intra-HD (solid black line) and inter-HD (dash-dot red line) distributions for the generated PUF responses. Both distributions are overlapping and enclose an area that is divided by the dashed black line into the FAR (left) and FRR (right) regions. More information on FAR and FRR can be found in Section 2.3.5. The FAR and FRR values are calculated according to Equation (2.15) and Equation (2.16), respectively. Both values are dependent from the chosen identification threshold th_{id}. Typically, the threshold value is either set to the intersection point of the intra-HD and inter-HD distributions or to the point where FAR=FRR, the so-called EER. Firstly, we compute the FAR and FRR values for the intersection point $th_{id} = 14.29\,\%$ of both distributions. The resulting values are FAR = 0.61 % (-2.21) and FRR = 0.21 % (-2.68). The values in the brackets represent the $\log_{10}(\cdot)$ notation of the percentual values, which is widely used to improve the readability and to ease comparability. Furthermore, we determine the identification threshold th_{EER} for the EER. The resulting values are $th_{EER} = 13.1\,\%$ and FAR = FRR = 0.48 % (-2.32).

For the second evaluations, the differential addressing method is used to build the PUF challenges. To obtain comparable 28-bit responses, we simulate hybrid PUFs with 56 core inverters. Figure 5.14b shows the intra-HD (solid black line) and inter-HD (dash-dot blue line) distributions for the generated PUF responses. For comparison purposes, the dash-dot red line indicates the inter-HD distribution when using the readdressing method. The differential addressing method leads to a reduced standard deviation of the inter-HD distribution, which is a consequence of the increased entropy of the PUF responses. For further evaluations on the PUF entropy, please refer to Section 6.2.2. Since there is no visible overlap between both distributions, we set the identification threshold to the value that leads to the EER. The resulting threshold value is th_{EER} = 17.08 % with FAR = FRR = 0.02 % (-3.61).

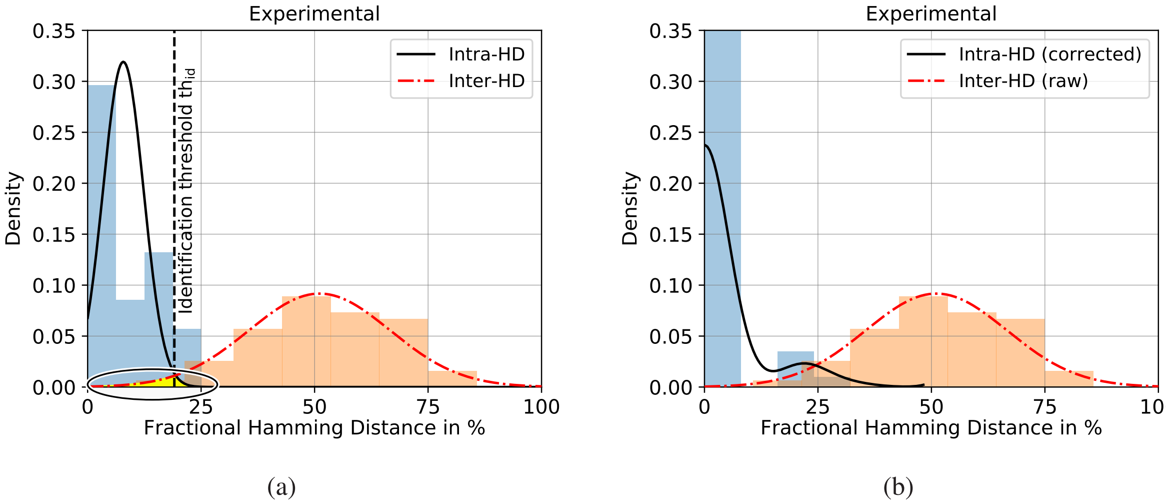


Figure 5.15: Intra-HD and inter-HD distributions based on experimental data when using the readdressing method for (a) raw PUF responses and (b) corrected PUF responses.

Figure 5.15a shows the intra-HD (solid black line) and inter-HD (dash-dot red line) distributions based on the experimental responses of fabricated hybrid PUFs with eight core inverters. The readdressing method is used for challenge building. Similar to our prior evaluations, we firstly set the identification threshold to the intersection point of both distributions th_{id} = 19.11 %. The results are FAR = 0.59 % (-2.23) and FRR = 1.92 % (-1.71). The identification threshold value that leads to the EER is th_{EER} = 17.56 % with FAR = FRR = 1.50 % (-1.83).
The experimental results are in good agreement with the simulations in general. However, the greater mean value of the intra-HDs moves the distribution to the right, which increases the FAR and FRR areas. This can be attributed to the missing passivation layer for the fabricated PUF core inverter's EGTs. Due to the relatively low FAR and FRR values, the hybrid PUF is not suitable for cryptographic applications, but qualifies for identification tasks. Nonetheless, the relatively low design complexity and the non-linear bit width scaling property make the hybrid PUF a promising candidate as a lightweight security primitive suitable for identification tasks.

Please note that the results for both, the simulations and the experimental data, are based on raw PUF responses without additional post-processing, such as error-correction. Figure 5.15b shows the intra-HD (solid black line) and inter-HD (dash-dot red line) distributions for PUF responses that were post-processed by an exemplary 5-bit error-correction, based on Bose-Chaudhuri-Hocquenghem (BCH) codes. Figure 5.16 shows the response enrollment and the response extraction phase including an error-correction.
Since the intra-HD values of various PUF responses are still greater than the maximum number of bit errors that can be corrected by the BCH code, the area enclosed with the inter-HD distribution does not decrease. This descriptive example shows that the error-correction must offer an upper margin in terms of bits that can be corrected. Thereby, the identification threshold serves as the lower boundary, indicating the minimum number of bits an error-correction must be capable

to correct. For the fabricated hybrid PUF, the potential operational areas are limited to indoor applications unless a passivation layer is available to protect the EGTs from environmental effects.

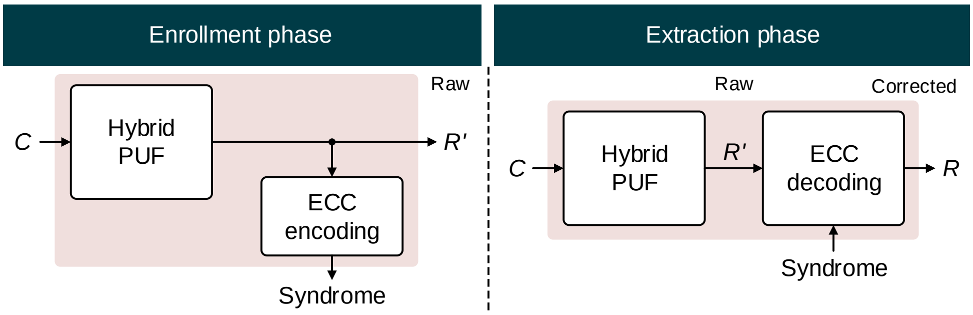


Figure 5.16: Enrollment phase: Raw PUF response extraction R' and syndrome computation by the error correcting code (ECC). Extraction phase: Raw PUF response extraction R' and error correction using the syndrome to obtain the stable response R.

5.6 NIST Randomness Tests

To determine the randomness of the response bits generated by hybrid PUFs, we use the NIST-STS. The NIST-STS defines various tests to assess the uniformity of the generated bits and to find patterns in bit sequences. There are 15 tests specified in the NIST-STS to judge on the randomness. For a comprehensive description of the single NIST tests please refer to the NIST 800-22 specification in [217]. Since some NIST tests require a very large bit sequence, our evaluation is limited to seven tests. For each test, a P-value is determined quantifying the confidence in whether or not the null hypothesis, i.e., that the data is in fact random, is true [218]. This is the case if the P-value is greater than 0.01.

Table 5.5 shows the NIST test results for simulated hybrid PUFs using the differential addressing method (refer to Section 3.2.3 for more information). The key length for performing the NIST tests was set to 256 bits. The tested bit sequence comprises 31,976 bits generated by 1,142 hybrid PUF entities. The results show, that the bit sequence generated by the hybrid PUFs satisfies the NIST test requirements and are random.

Similarly, we have performed NIST tests by using the readdressing method for challenge building. The tested bit sequence includes 224,000 bits generated by 8,000 hybrid PUF entities. In this case, all tests failed, which means that the generated bit sequence is non-random. This can be explained by the multiple reuse of inverter addresses, which degrades the entropy of the PUF responses (please refer to Section 6.2.2 for a detailed discussion about entropy).

In summary, our NIST test evaluations show that the hybrid PUF is capable of producing responses offering enough randomness as required in cryptography, if the differential addressing method is used.

Table 5.5: NIST test results based on simulated hybrid PUFs using the differential addressing method for challenge building.

NIST statistical test	P-value (> **0.0001**)	Proportion (> **119**)	Result
Frequency (Monobit)	0.141256	123/124	Pass
Block frequency	0.637119	124/124	Pass
Cumulative sums	0.407091	122/124	Pass
Runs	0.105618	121/124	Pass
Longest run of ones	0.941144	121/124	Pass
Approximate entropy	0.875539	124/124	Pass
Serial	0.033288	123/124	Pass

5.7 Performance Comparison of Different PUFs

To assess the performance of the silicon-based DiffC-PUF and the hybrid PUF incorporating inkjet-printed PUF cores, we compare our results with other PUFs. Table 5.6 shows the performance values of various PUFs based on silicon technology, novel materials, and printed electronic components. It should be noted that this comparison only covers a selection of different PUF designs. The PUFs are assessed regarding their security metrics and identification system capabilities. In general, most of the works in the literature either concentrate on the security metrics or the PUF as part of an identification system. Most often it is not clear how exactly the PUF responses were generated and whether additional post-processing techniques or majority voting was used to stabilize the responses. Our evaluations are based on raw PUF responses without any post-processing.

In the case of silicon-based PUFs, various works are available that show figures of merit for the security metrics and the identification capabilities. The herein presented silicon-based DiffC-PUF (see Section 4.2) achieves security metric results close to the ideal values. However, the results regarding the identification capabilities do not reach the other PUFs' performances. At this point it must be considered that the silicon-based DiffC-PUF is a prototype system set up with discrete components. Silicon-based PUFs do compete with sophisticated key generation techniques, which are mainly based on well-recognized mathematical foundations and random numbers. On the other hand, PUFs based on novel materials and printing technology are in the very early stages. This makes it hard to compare the performance between the different technologies for the time being.

In the context of PE-based PUFs, the organic RO-PUF presented by Kuribara et al. in [135] is the first PUF that was suggested for PE fabrication. Their security metric evaluations are based on manual frequency measurements of the ROs.
The first fully printed PUFs are based on memory cells. Firstly, the RFID SRAM-PUF was pro-

posed without showing any PUF-specific performance results. The later on introduced memory-based PUF's security metrics are based on simulations, but serve as a performance indicator for PE-based electrical PUFs. The herein presented hybrid PUF shows performance values in terms of security metrics similar to the printed memory-based PUF. To the best of our knowledge, the hybrid PUF is the first PE-based PUF that has been investigated regarding its security metrics and identification capabilities. Therefore, the identification capabilities can not be stressed against other related PUFs.

5.8 Conclusion

In this chapter, we have initially performed statistical analysis based on simulations to investigate the characteristics of the inkjet-printed PUF cores. Monte Carlo (MC) simulations on printed inverters were performed with varying parameters (see Table 5.1). The aim of the simulation-based evaluations was to determine the best operating point of the hybrid PUF under consideration of the security metrics including uniqueness, reproducibility, bit aliasing, and uniformity. The results are close to the ideal values, showing that the hybrid PUF is a promising candidate for being used as a security primitive. The best operating point in terms of robustness is reached at a inverter biasing voltage of $V_{\text{in}} = 0.4\,\text{V}$. On that basis, we have performed statistical analysis on experimental response data obtained from 15 fabricated hybrid PUFs. The PUFs were operated in a climatic chamber under controlled ambient conditions including temperature and humidity variations (see Table 5.3 for the experiments). The calculated security metric values for the uniqueness, bit aliasing, and uniformity show good agreement with the simulations. The reproducibility, more particularly the mean reliability value is relatively low. This effect mainly stems from the missing passivation and encapsulation of the printed transistors, which can be improved in the future. Finally, we have investigated the identification capabilities of the hybrid PUF based on simulations and raw experimental response data. The relatively low FAR and FRR values show that the hybrid PUF is not suitable for cryptographic applications. This is caused by the low reliability value. However, we want to note that the security metric evaluations are based on raw response data without additional post-processing. The reliability as well as the identification capabilities (FAR and FRR) can be expected better once passivation, encapsulation, and error correction is available for the hybrid PUF. The results obtained from NIST tests show, that the responses generated by the hybrid PUF are random and satisfy the requirements to be suitable for cryptography, if the differential addressing method is used to build the PUF challenges. Table 5.6 summarizes the most important results obtained from our evaluations including a comparison with other works.

Table 5.6: Performance comparison between a selection of PUFs in terms of security metrics and identification capabilities.

PUF type	Data basis	Category	Security metrics				Identification system			Ref.
			Uniqueness	Reliability	Bit aliasing	Uniformity	FAR*	FRR*	EER*	
Pseudo LFSR-PUF*	Experimental	Weak	62.7 %	97.3 %	-	-	-2.96	-3.05	-	[219]
SRAM-PUF*	Experimental	Weak	-	-	-	-	-4.01	-4.03	-4.01	[72]
PUF sensor*	Experimental	Weak	31.0 %	92.8 %	-	-	-6.04	-6.02	-6.01	[220]
DiffC-PUF*	Experimental	Weak	48.8 %	99.2 %	45.6 %	45.6 %	-1.67	-2.33	-1.80	This work
Organic RO-PUF$^\diamond$	Experimental	Weak	30.0 %	99 %	-	-	-	-	-	[135]
CN-PUF$^\diamond$	Simulation	Weak	49.7 %	96.5 %	-	-	-	-	-	[128]
Memristor-PUF$^\diamond$	Simulation	Strong	49.9 %	99.0 %	52.4 %	50.6 %	-	-	-	[134]
RFID SRAM-PUF†	-	Weak	-	-	-	-	-	-	-	[123]
Memory-based PUF†	Simulation	Weak	49.8 %	92.6 %	-	-	-	-	-	[125]
Inkjet-printed labels†	Experimental	Strong	-	-	-	-	-	-	-	[126]
Hybrid PUF†	Simulation	Weak	50.0 %	98.4 %	49.8 %	49.8 %	-2.21	-2.68	-3.61	This work
	Experimental	Weak	51.1 %	78.5 %	44.5 %	44.5 %	-2.23	-1.71	-1.83	This work

Note: *Silicon-based PUFs. $^\diamond$Novel material PUFs. †Printed/Hybrid PUFs. $^*\log_{10}(\cdot)$ of the value.

6 Attacks Against PUFs

6.1 Introduction

In the previous chapters, we focused on the design, simulation, fabrication, and evaluation of PUFs. From the outside point of view, a PUF is a black box that is stimulated with an input (challenge) and replies with an output (response). The internal device-specific characteristics are hidden and seem to be unpredictable. However, non-idealities such as systematic variations might cause correlations between CRPs, which are actually expected to be independent. This circumstance opens doors for attackers whose aim is to create a clone that behaves like the original PUF. As discussed in Section 2.6, for an attacker it is of substantial importance to leak CRPs from the PUF in order to draw conclusions about the challenge-response behavior. The procedure of leaking CRPs is also referred to as eavesdropping attacks and is extensively discussed in Section 2.6.2. Many works dealing with attacks on PUFs can be found in the literature [104, 114, 118, 221, 222]. Most of them concentrate on strong PUFs that exhibit large CRP spaces, where the challenge-response interfaces are typically publicly accessible. Up to now, there are no works addressing attacks on PE-based PUFs. In this chapter, we aim to:

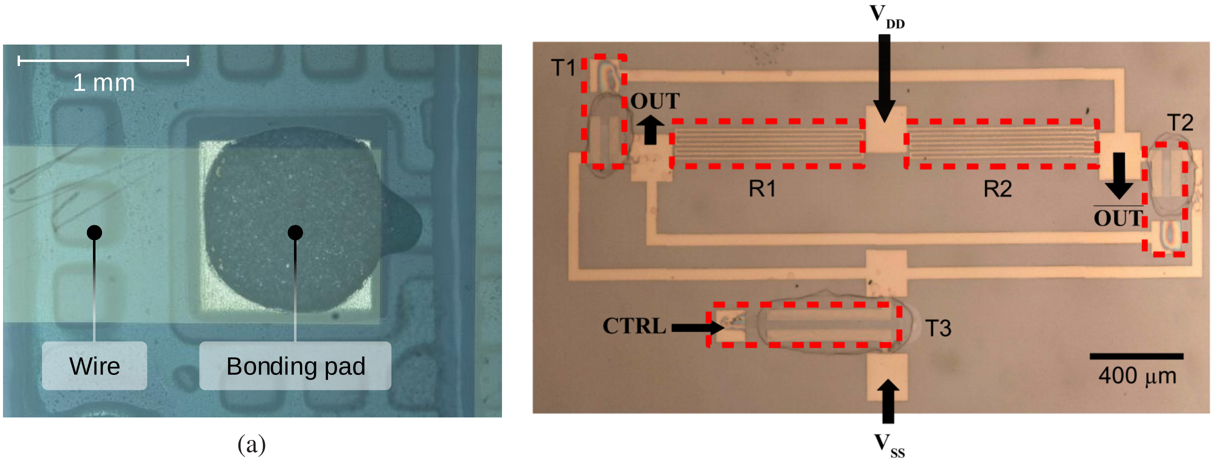
- Give a detailed security analysis on the herein presented PUF design with special emphasis on the PE-based hybrid PUF. The analysis will also include entropy and bias investigations of the PUF responses.
- Introduce a sorting algorithm that can be used to model the challenge-response behavior of the PUF. This analysis will also include performance results in terms of prediction accuracy.
- Perform model-based attacks by means of supervised machine learning algorithms and evaluate the performances of the different models.
- Compare and discuss the performance of the sorting algorithms and the employed machine learning algorithms.

6.2 Security Analysis

6.2.1 Security Challenges for PE-Based PUFs

Silicon-based PUFs are typically fabricated as encapsulated multi-layer integrated circuits (ICs). The packaged design makes it difficult and therefore expensive for attackers to eavesdrop CRPs, since invasive attacks are required to get access to the internal wirings. As a consequence, attackers are often limited to semi-invasive and non-invasive attacks, especially if there is no physical access to the PUF. For example, strong PUFs are often used for device authentication, where each CRP is just used once in the lifetime of the device. Theoretically, there is no need to encrypt the challenge and the resulting response data between the PUF-equipped device and the authentication party. Simple and low-cost non-invasive attacks are sufficient to eavesdrop the communication. The attacker might draw conclusions about the challenge-response behavior of the PUF and try to derive/predict other CRPs. This would only be possible if there were dependencies between the CRPs. In this context, the entropy and the bias of the PUF responses are important measures to assess the learnability.

Contrary to silicon technology, which offers high integration densities, PE enables large-area fabrication. Printed electronic systems include large-area structures, e.g. in the form of bonding pads and/or wires visible with the naked eye. As a consequence, they can be accessed with little effort, e.g. with standard measurement probes, which implies that there is an aggravated risk against invasive eavesdropping attacks. Figure 6.1a shows the microscope image of a wire and bonding pad on an ITO substrate structured via laser ablation. The substrate hosts the inkjet-printed electronic, which is connected to a PCB using conductive adhesive.



(a)

(b)

Figure 6.1: (a) Microscope image of a wire and bonding pad on an ITO substrate structured via laser ablation. The substrate hosts the inkjet-printed electronic, which is connected to a PCB using conductive adhesive. (b) Microscope image of an inkjet-printed single-bit memory-based PUF circuit © 2018 IEEE [125].

The herein presented DiffC-PUF design belongs to the group of weak PUFs. As described in Section 2.6.3, weak PUFs are often used in a controlled PUF environment to obfuscate the challenge and response interfaces. However, weak PUFs can exceed hundreds or even thousands of CRPs, making them also candidates for being attacked and cloned [223]. This is an important information since all yet introduced PE-based PUF designs are weak PUFs. The reason behind is that PE technology faces limitations in terms of yield and integration density. Figure 6.1b shows the image of an inkjet-printed single-bit memory-based PUF circuit [125]. The dimensions of the pads and wirings are magnitudes larger than comparable widths used in silicon-based technology.

Furthermore, additive manufacturing capabilities can be used to tune [224] or manipulate the characteristics of printed circuits. This must be considered when integrating printed electronic devices into products. Possible countermeasures are protective coatings to detect invasive attacks.

6.2.2 Entropy of PUF Responses

To assess the entropy of responses produced by the hybrid PUF, the normalized entropy η is calculated according to Equation (2.5). Since the challenge building method has direct impacts on the entropy determination, we distinguish between the readdressing and the differential addressing methods (please refer to Section 3.2.3 for more information on the challenge building techniques).

Challenge Building Method 1: Readdressing

In the readdressing method (see Section 3.2.3 for more information), the alphabet consists of the M inverter addresses and is defined as $Z = \{z_0, \ldots, z_{M-1}\}$. The number of symbols is $|Z| = M$. For our entropy estimation, we use a challenge that leads to the maximum response bit width L_{max}. Since each sub-challenge includes two inverter addresses, the total number of symbols to be considered is $N = 2 \cdot L_{\text{max}}$. Each inverter address occurs exactly $M - 1$ times in a challenge, which implies that the probabilities of occurrence are equally distributed over all symbols. The resulting probabilities are constant and can be determined according to Equation (6.1):

$$P(z_i) = \frac{M - 1}{N}. \tag{6.1}$$

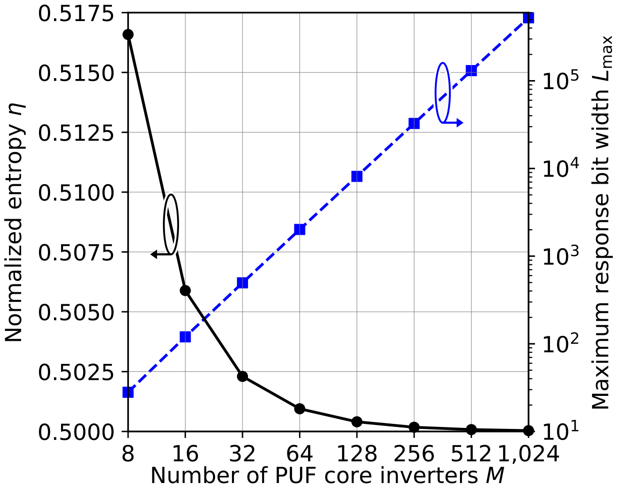


Figure 6.2: Normalized entropy as defined by Shannon (solid black line) and maximum response bit width using the readdressing method (dashed blue line).

The solid black line in Figure 6.2 shows the normalized entropy for different numbers of PUF core inverters (M). If M is increased, the normalized entropy decreases slightly. In general, the curve shows that the entropy of the PUF responses is reduced to nearly 50 %. The reason behind is the readdressing method used for challenge building. The results show, that correlations between the sub-challenges do exist and that the PUF is vulnerable against model-based attacks. For $M = 8$ PUF core inverters, the normalized entropy is $\eta = 0.517$. The dashed blue line shows the maximum response bit width L_{max} that can be achieved with a specific number of PUF core inverters. The previously shown results on the entropy estimation for the PUF responses originated from the employed challenge building method. The obtained theoretical entropy values do not consider the statistical characteristics of the PUF responses. Therefore, we compute the minimum entropy (min-entropy) to determine the lower bound of unpredictability of the responses. The mean bit aliasing value (Equation (2.13)) gives the bias of the PUF responses. On the basis of our simulation results from Section 5.3.4, we get the probabilities of occurrence $p_0 = 0.502$ and $p_1 = 0.498$. Correspondingly, the maximum probability is $p_{\max} = 0.502$. The resulting min-entropy value of the PUF responses is $H_{\min} = 0.994$.

Challenge Building Method 2: Differential Addressing

As described in Section 3.2.3, in the differential addressing method each inverter address is just used once among all challenges. In this case, the alphabet also consists of M inverter addresses and is defined as $Z = \{z_0, \ldots, z_{M-1}\}$, whereas the number of symbols is $|Z| = M$. To estimate the entropy we use a challenge that leads to the maximum response bit width, which is defined as $L_{\max} = M/2$. Since each inverter address is used exactly once, the probability of occurrence calculates according to Equation (6.2):

$$P(z_i) = \frac{1}{M}. \tag{6.2}$$

The resulting entropy value is 1, which is obvious since all challenges are completely independent. To estimate the min-entropy for the differential addressing method, we simulate 1,000 hybrid PUFs. To be able to compare the PUF responses, we increase the number of PUF core inverters to $M = 56$, which leads to a maximum response bit width of $L_{\max} = 28$. Figure 6.3 shows the distribution of the resulting bit aliasing values. The mean bit aliasing value is 49.7 %, which leads to the probabilities of occurrence $p_0 = 0.503$ and $p_1 = 0.497$. The resulting maximum probability is $p_{\max} = 0.503$ and causes a min-entropy value of $H_{\min} = 0.991$. Table 6.1 shows the entropy results for the silicon-based DiffC-PUF and the PE-based hybrid PUF.

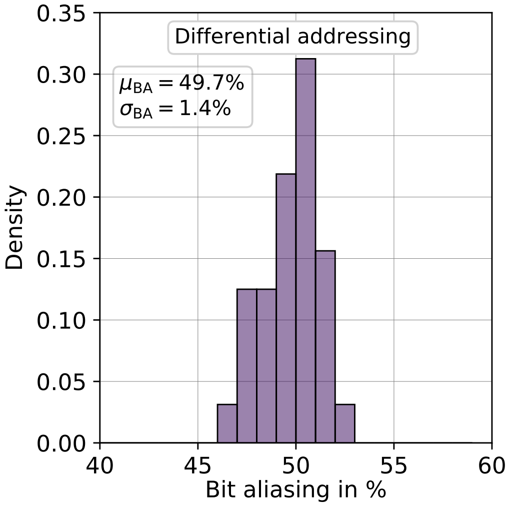


Figure 6.3: Bit aliasing for a hybrid PUF when using the differential addressing method for challenge building.

Table 6.1: Comparison of the Shannon entropy and min-entropy values.

PUF type	**Data basis**	**Addressing method**	**Inverters M**	**Bit aliasing**	**Entropy η**	**H_{min}**
DiffC-PUF*	Experimental	Readdressing	8	45.6 %	0.517	0.878
Hybrid PUF†	Simulation	Readdressing	8	49.8 %	0.517	0.994
	Simulation	Differential	56	49.7 %	1	0.991
	Experimental	Readdressing	8	44.5 %	0.517	0.849

Note: *Silicon-based PUF. †Printed/Hybrid PUF.

6.3 PUF Attack Methodology

In this section, we introduce the attack methodology that is used for the further evaluations. We distinguish between the enrollment phase and the model-based attack phase. In the former, the CRP data is generated from the original PUFs and stored in a database. In the attack phase, the CRP data is prepared as required by the employed models. In Section 2.6.3, we have reviewed various model-based attacking methods. The herein employed techniques are based on sorting and machine learning. To simulate the effects of fuzzy PUF responses or noisy eavesdropping channels, we artificially introduce bit error-inflicted CRPs by randomly flipping response bits. On that basis, PUF responses are predicted using the trained model. To assess the prediction capabilities, various performance metrics are computed and compared against each other. Model-based training techniques mainly depend on the quality and quantity of the training data.
Performing model-based attacks on hybrid PUFs (with $M = 8$ PUF core inverters) and a maximum single response bit width of 28-bit would be non-productive. To provide meaningful statistics we increase the number of PUF core inverter to $M = 64$, which leads to the maximum number of 2,016 sub-CRPs. According to Equation (3.3), in total 2,016 sub-challenges and sub-responses can be generated with this configuration and with the readdressing method. In sum, 1,000 hybrid PUFs are simulated under nominal operating conditions, as presented in Section 5.2.2.

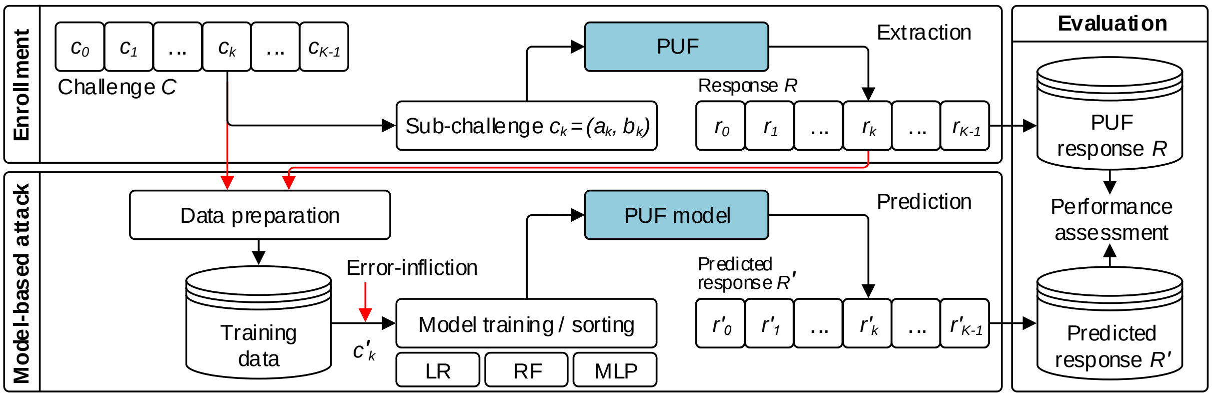


Figure 6.4: Methodology for our model-based attack evaluations. In the data preparation building block, the raw extracted PUF challenge-response data is encoded into the representation that fits the model best.

Raw Training Data
PUF responses extracted from the original PUFs without additional post-processing are called raw responses. In this context, the term raw training data refers to CRPs that comprise one sub-challenge c_k and the corresponding genuine sub-response bit r_k, as shown in Figure 6.4.

Error-Inflicted Training Data
Attackers might sometimes face eavesdropping errors due to environmental impacts, such as noise or fuzzy responses. To assess the prediction performance of the employed model-based attacks, we deliberately introduce error-inflicted sub-CRPs. In particular, randomly selected response bits are flipped in the training data. For the further evaluations, we run experiments with bit error rates (BERs) of 10 % and 20 %. At this point we want to note that the herein considered BER is an independent probability per sub-response bit. This assumption is helpful for the statistical evaluation and assessment of the learning capabilities of the employed model-based cloning techniques, but does not reflect the real situation an attacker might be exposed to.

6.4 Sorting Attacks

6.4.1 Binary Relations Sorting Algorithm

In general, with the readdressing method to build PUF challenges, the DiffC-PUF design is comparable with the ring oscillator selection in RO-PUFs [110]. The RO-PUF design has been demonstrated to be vulnerable against machine learning attacks by Ruehrmair et al. [114]. Moreover, the authors stated that sorting attacks can also be used to estimate the internal oscillating frequency order of the ROs. In this section, we introduce an online sorting algorithm that is capable of modeling hybrid PUFs.

In the following we assume that an attacker is able to eavesdrop sub-challenges and sub-responses from the hybrid PUF. The combination of both is called sub-CRP comprising the tuple (a_k, b_k, r_k), where a_k and b_k are two PUF core inverter addresses and r_k is the sub-response bit. It is assumed that the exact inverter output voltages are not known by the attacker. However, each sub-CRP represents a mathematical binary relation in the form of Equation (6.3).

$$c_k = (a_k, b_k) \begin{cases} V_{\text{out}}(a_k) > V_{\text{out}}(b_k), & \text{if } r_k = 1 \\ V_{\text{out}}(a_k) < V_{\text{out}}(b_k), & \text{if } r_k = 0 \end{cases} \tag{6.3}$$

The transitivity of these binary relations can be used to create a sorted list of the relative PUF core inverter output voltages. It is assumed that in a real attack scenario the adversary is limited to passive eavesdropping and can not select the sub-challenges arbitrarily. Thereby, the eavesdropped sub-CRPs drop in an uncontrolled manner, which raises the need for direct processing of the binary relations into model training. Online sorting algorithms are promising that can process input elements provided piece-by-piece by keeping the sequence sorted as more elements are added. The insertion sort algorithm [225] offers online functionality and can sort lists as it receives the elements.

We introduce the binary relations sort (BR-sort) algorithm, which uses insertion sort as the core sorting algorithm. For each PUF core inverter address, we store a list of all occurring binary relations with other inverter addresses. This enables to sort the inverter addresses regarding their inverter output voltages. Figure 6.7 shows the flowchart of the function INSERT_CRP($\cdot$) to add sub-CRPs to the sorted inverter address list S. The globally defined list S is built up line-by-line and holds the current set of already inserted inverter addresses in ascending order. Please note that the algorithm sorts the inverter addresses based on binary relations, more particularly the relative inverter output voltages. This means that the inverter addresses themselves are typically not arranged in ascending order in the sorted list S. Each time a sub-CRP is added to the sorted list, the function BR_UPDATE($\cdot$) is called, which keeps track of all binary relations that have already been inserted. The flowchart in Figure 6.8 shows the function BR_SORT($\cdot$) to sort on the basis of binary relations.

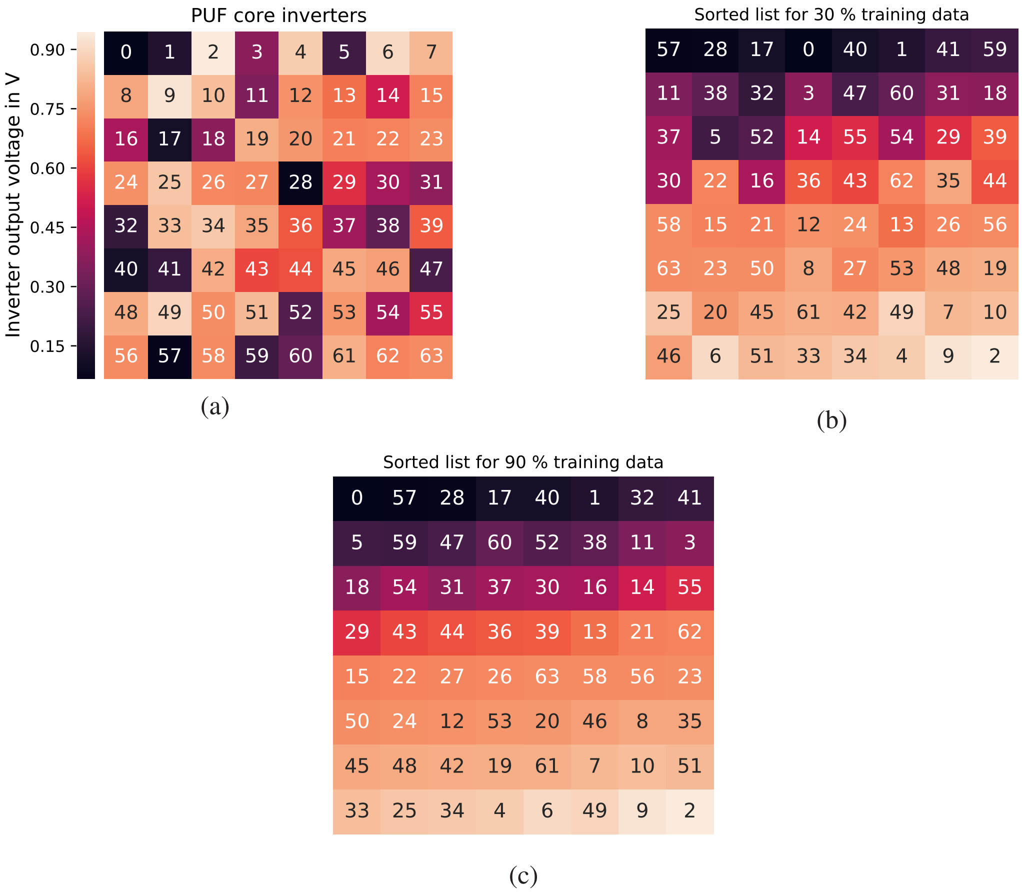
In a real attack scenario, the adversary might eavesdrop faulty sub-CRPs due to noisy side-channels. Faulty sub-CRPs would lead to contradictions in the sorting algorithm. For the attacker it would be hard to detect it if a contradiction was caused by the last recently inserted sub-CRP or if the corrupted sub-CRP was already part of the binary relations list. To improve the sorting quality, our algorithm tries to reduce the impact of corrupted sub-CRPs. For example, if $(a_k, b_k, 1) \rightarrow V_{\text{out}}(a_k) > V_{\text{out}}(b_k)$ causes a contradiction with the current binary relations list BR, then our algorithm checks whether b_k can be moved into the opposite direction towards a_k. This approach triggers a further update of the BR list, which improves the consistency of the sorted inverter address list S. Since the proposed binary relation sorting algorithm is based on the insertion sort algorithm, the worst case runtime complexity is $\mathrm{O}(n^2)$.

6.4.2 Performance Results

To assess the performance of the proposed BR-sort algorithm, the accuracy of its PUF response prediction capabilities is computed. The predictions are made on the basis of the sorted PUF core inverter address list. The prediction accuracy is computed according to Equation (2.19). Therefore, the predicted PUF responses are classified into the number of TP, TN, FP, and FN, as introduced in Section 2.6.5. In this respect, the attack methodology introduced in Section 6.3 is used with the CRPs of 1,000 simulated hybrid PUFs. The hybrid PUFs are set up with $M = 64$ PUF core inverters. The heatmap in Figure 6.5a shows one example output of a hybrid PUF with $M = 64$ PUF core inverters visualized by an 8×8 array. The numbers denote the inverter address, whereas the colors indicate the corresponding inverter output voltage. Figure 6.5b and Figure 6.5c show the sorted list S after using 30 % and 90 % of the sub-CRPs as training data.

When initializing the BR-sort algorithm, the sorted inverter address list S is empty and grows with new binary relations of sub-CRPs. If the number of sub-CRPs eavesdropped by an attacker is low enough, some of the PUF core inverter addresses might not be part of the sorted list S. Missing inverter addresses can not be resolved and may cause wrong predictions. One possible solution to overcome this issue is to preinitialize the sorted list S randomly with the number of inverter addresses. This is only applicable if the attacker knows about the hybrid PUF architecture. For our evaluations, we distinguish between the following two methods to start sorting with:

- *Initialization method 1*: Empty list S.
- *Initialization method 2*: Preinitialized list S.



(a)

(b)

(c)

Figure 6.5: Heatmaps showing the simulated inverter output voltage variations of a hybrid PUF with 64 core inverters. The colors indicate the inverter output voltages, whereas the numbers show the corresponding inverter address. (a) Heatmap of the actual PUF inverter output voltages. (b) Heatmap of the sorted list with 30 % training data. (c) Heatmap of the sorted list with 90 % training data.

Furthermore, we distinguish between error-free (raw) and error-inflicted training data, as described in Section 6.3. Please consider that we use the term training data synonymously to describe the insertion of sub-CRPs in the BR-sort algorithm. The prediction accuracies are calculated for different ratios of training and test data sizes ($q_{\text{train}}/q_{\text{test}}$). The training data comprises the sub-CRPs of 1,000 simulated hybrid PUFs. For model training using the BR-sort algorithm, the sub-CRPs are randomly chosen in the range of $q_{\text{train}} = [10\,\%, 90\,\%]$ with steps of 5 %.

Raw Training Data

Figure 6.6a shows the prediction accuracy values. The orange line indicates the results if sorting starts with an empty list S (method 1). The green line shows the results in case of a start with a preinitialized list (method 2). The markers represent the mean accuracy values, whereas the error bars indicate the standard deviations. The numbers below the error bars display the predictions failed due to too small training data q_{train}. In these cases, not all inverter addresses have already been present in the sorted list S. In contrast, the results when preinitializing the list S are slightly better for small training set sizes $q_{\text{train}} = [10\,\%, 20\,\%]$. From an attackers point of view, in the best case unknown sub-CRPs can be predicted with an accuracy of $\geq 90\,\%$, if at least 25 % of the total sub-CRPs were eavesdropped and used for model training.

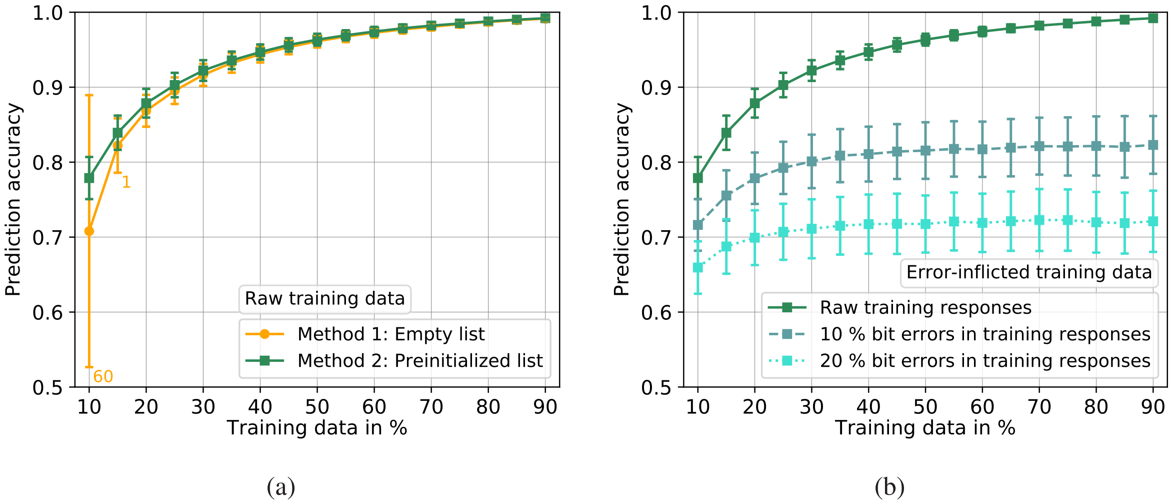


Figure 6.6: Prediction accuracies of the proposed binary relation sorting algorithm for **(a)** raw training data and **(b)** error-inflicted training data.

Error-Inflicted Training Data

To assess the prediction performance of the BR-sort algorithm under the impact of error-inflicted training data, we deliberately flip the response bits of sub-CRPs. Similar to the prior evaluations on raw response data, we choose the sub-CRPs randomly in the range of q_{train}. Figure 6.6b shows the prediction accuracies for BERs of 10 % and 20 %. The results show that the prediction performance of the BR-sort algorithm decreases if bit errors occur in the training data. Table 6.2 shows the obtained best, median, and mean prediction accuracy values for different BERs. The table shows the percentual training data required for model training to achieve a prediction accuracy of $\geq 90\,\%$. Table 6.3 shows the detailed results for the quality metrics. If increasing the BER, the TP and TN values decrease, while the FP and FN values increase. This causes the classification accuracy (see Equation (2.19)) to decrease.

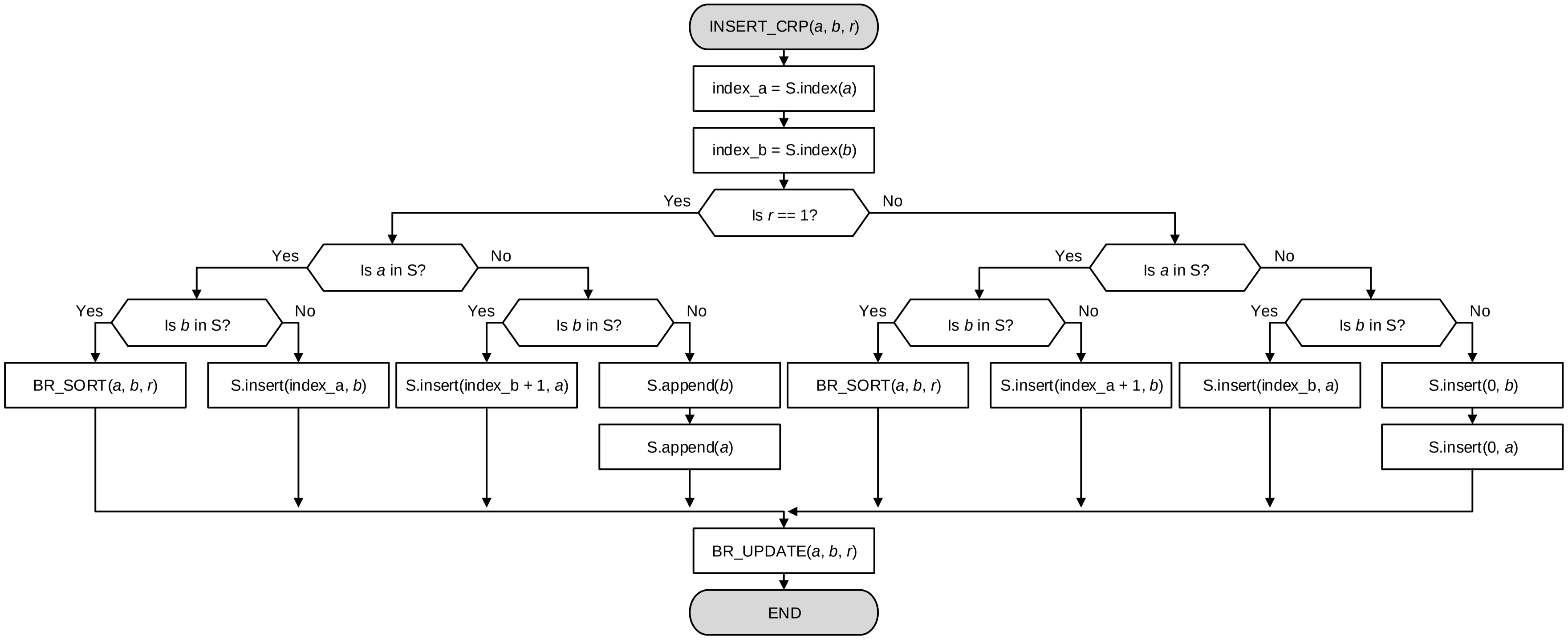


Figure 6.7: Flowchart diagram of the INSERT_CRP($\cdot$) function to insert sub-CRPs to the sorted inverter address list S.

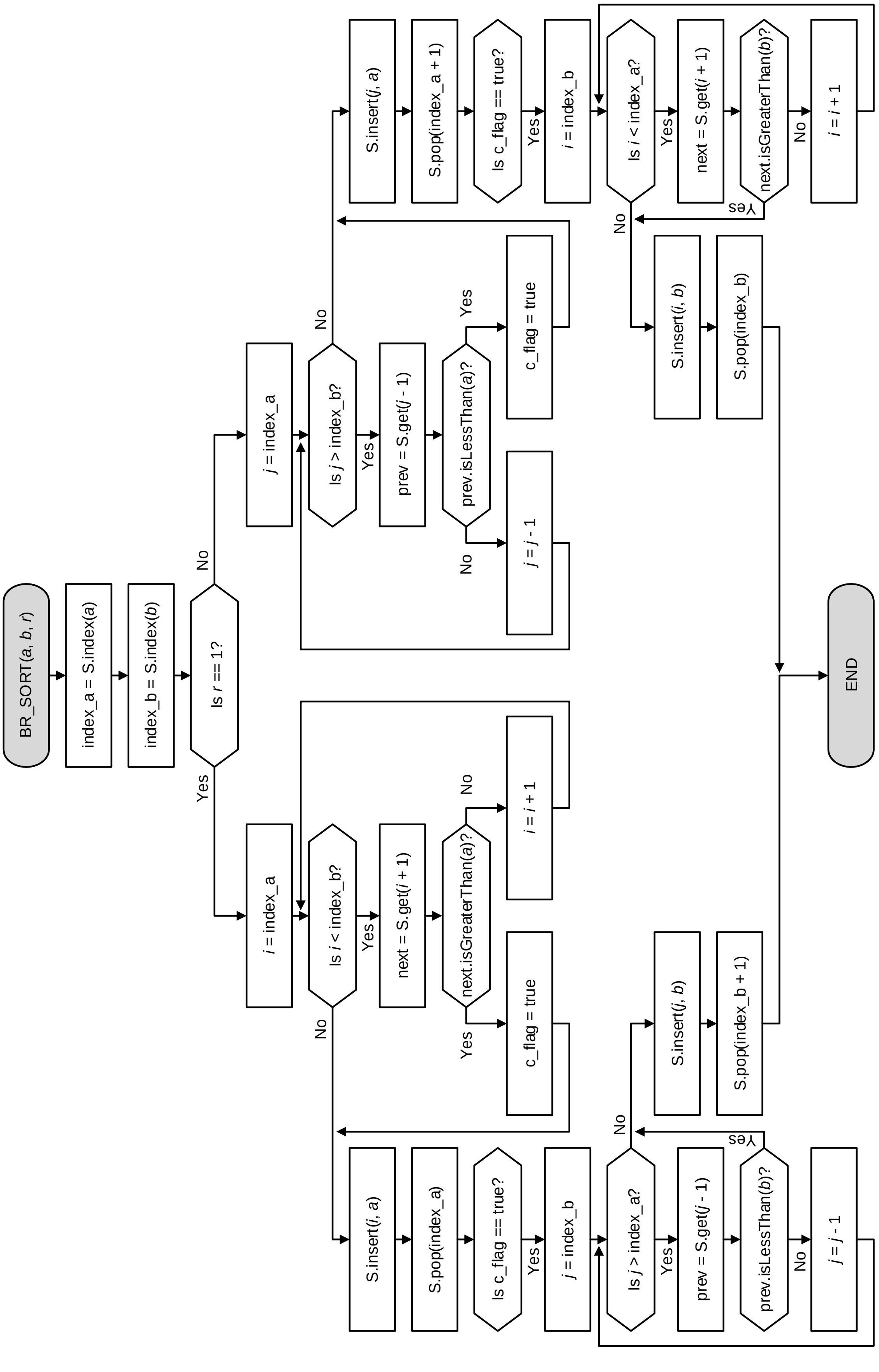


Figure 6.8: Flowchart diagram of the BR_SORT(·) algorithm to sort inverter addresses based on binary relations represented by the sub-CRPs.

6.5 Machine Learning Attacks

6.5.1 Data Preparation

In general, machine learning algorithms use inputs to create outputs. The input data must be prepared in a form that is compatible with the requirements of the ML methods. This data preparation procedure is called feature engineering and can also improve the performance of the prediction accuracies. In the following, we describe the binary and one-hot encoding representation of numbers in general and hybrid PUF sub-challenges in particular. As introduced in Section 3.2.3, each sub-challenge comprises the tuple $c_k = (a_k, b_k)$, where a_k and b_k are PUF core inverter addresses. Typically, these addresses are displayed in integer or binary representation to improve human readability. Using the binary encoding directly as inputs for the ML models causes that a natural ordering between the categories (in this case the inverter addresses) is assumed. However, this is not the desired behavior of the ML models, since the inverter output voltages are completely independent from the actual inverter address. For example, in the case of the three inverter addresses $a_0 = 1$, $a_1 = 2$, and $a_2 = 3$ the ML model would think that $a_0 = 1$ is more similar to $a_1 = 2$ than to $a_2 = 3$ due to the smaller difference. In this context, the one-hot encoding is widely used in ML to circumvent such effects [226, 227]. For our further evaluations, we choose the one-hot encoding representation, which is widely used for representing categorical data.

Binary Representation
The binary representation of the PUF sub-challenges consists of the two j-bit inverter addresses $a_k^0\, a_k^1 \ldots a_k^{j-1} \mid (a_k^i \in \{0,1\})$ and $b_k^0\, b_k^1 \ldots b_k^{j-1} \mid (b_k^i \in \{0,1\})$. As a result, each sub-challenge c_k comprises the bit sequence denoted by Equation (6.4):

$$c_k = a_k^0\, a_k^1 \ldots a_k^{j-1}\, b_k^0\, b_k^1 \ldots b_k^{j-1} \tag{6.4}$$

$$\text{where } a_k^i \neq b_k^i \ (0 \leq i \leq j-1) \text{ and } j = \log_2(M).$$

One-Hot Encoding Representation
One-hot encoded bit strings exhibit exactly one 1, whereas all other bit values are 0. As a consequence, the minimum bit width of one-hot encoded bit strings equals the number of different classes to be distinguished. In the case of the hybrid PUF, each binary j-bit inverter address is converted to its M-bit one-hot representation using the mapping function $f_{\text{one-hot}}$ from Equation (6.5):

$$f_{\text{one-hot}} : \{0,1\}^j \rightarrow \{0,1\}^M. \tag{6.5}$$

The mapping function converts the binary inverter address $a_k^0\, a_k^1 \ldots a_k^{j-1}$ to its one-hot encoded representation $\dot{a}_k^0\, \dot{a}_k^1 \ldots \dot{a}_k^{M-1}$, and in the same way $b_k^0\, b_k^1 \ldots b_k^{j-1}$ to $\dot{b}_k^0\, \dot{b}_k^1 \ldots \dot{b}_k^{M-1}$. Each sub-challenge only includes two single bits with the binary values of 1, which determine the two inverter addresses. This means that only these two sub-challenge addresses are considered by the ML algorithm, which makes the learning more efficient.

In general, the challenge-response behavior of the ML models can be expressed as $f_{\text{model}} : C'_K \rightarrow R'$, where $R' = \{0, 1\}$ and $C'_K = \{0, 1\}^K$ denotes the set of all K sub-challenges c'_k. Equation (6.6) and Equation (6.7) show the (predicted) sub-response r'_k as a function of the sub-challenge using binary and one-hot encoded inverter addresses:

$$r'_k = f_{\text{model}}(a_k^0\ a_k^1 \ldots a_k^{j-1}\ b_k^0\ b_k^1 \ldots b_k^{j-1}), \tag{6.6}$$

$$r'_k = f_{\text{model}}(\dot{a}_k^0\ \dot{a}_k^1 \ldots \dot{a}_k^{M-1}\ \dot{b}_k^0\ \dot{b}_k^1 \ldots \dot{b}_k^{M-1}). \tag{6.7}$$

6.5.2 Employed Machine Learning Algorithms

The LR, RF, and MLP classifiers are interesting machine learning techniques to model complex behavior. These techniques have been demonstrated in the literature to effectively model different types of PUFs. In the following, we describe the configuration used for our ML-based attacks. For our implementations of the ML algorithms we use the Python-based *scikit-learn* library [228]. Please refer to Section 2.6.4 for more basic information on the employed ML algorithms.

Logistic Regression (LR) Configuration
To model the challenge-response behavior of hybrid PUFs, we employ the LR algorithm using the limited-memory Broyden-Fletcher-Goldfarb-Shanno (L-BFGS) optimization algorithm [229], due to its fault tolerance in step size control.

Random Forest (RF) Configuration
For our evaluations with the RF algorithm, we use ten decision trees to model the hybrid PUF's challenge-response behavior.

Multi-Layer Perceptron (MLP) Configuration
Figure 6.9 shows the MLP architecture used to model hybrid PUFs with 64 PUF core inverters. The MLP is set up with two hidden layers comprising 128 and 64 perceptrons. We use 128 perceptrons in the first hidden layer, since the one-hot encoded challenges comprise 128 bits. The output layer is a single perceptron. We use the sigmoid (logistic) activation function for the perceptrons and the gradient-based adaptive moment estimation (Adam) [230] optimization algorithm to optimize the edge weights and perceptron biases.

6.5.3 Performance Results

To assess the performance of the employed ML algorithms, the prediction accuracy and the quality of the classification is computed according to Equation (2.19). In this regard, the TP, TN, FP, and FN values are calculated according to Section 2.6.5. To assess the quality of the classification, the ROC curves and AUROC values are computed for each ML algorithm. The attack methodology depicted in Figure 6.4 is used to perform the model-based attacks. In total, the CRPs of 1,000 simulated hybrid PUFs with $M = 64$ PUF core inverters provide the data basis for our evaluations. The performance of the ML algorithms is evaluated for different ratios of training and test data sizes ($q_{\text{train}}/q_{\text{test}}$). The training data comprises randomly chosen sub-CRPs in the range of $q_{\text{train}} = [10\,\%, 90\,\%]$ in steps of $5\,\%$.

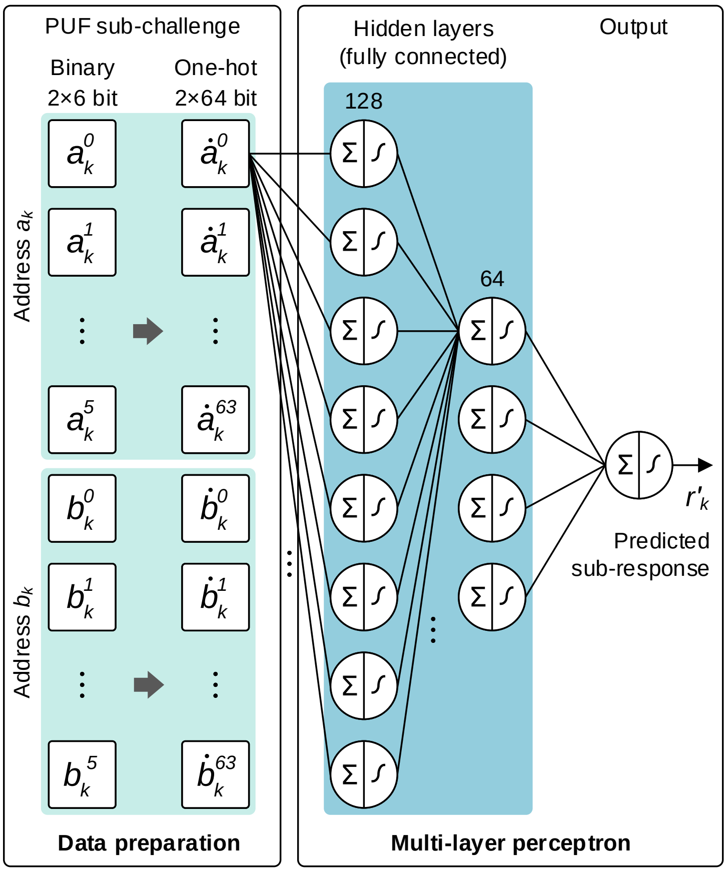
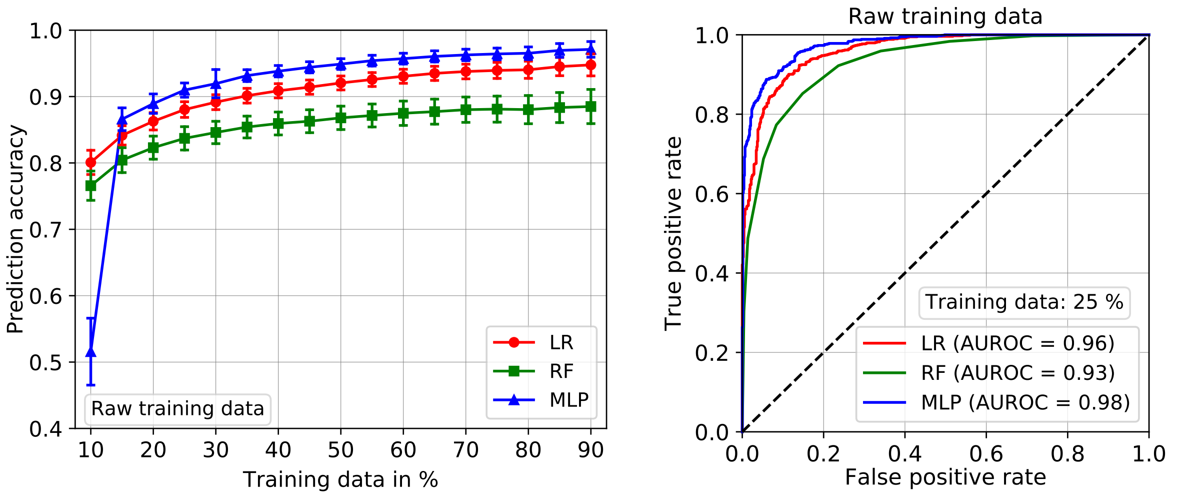


Figure 6.9: Multi-layer perceptron (MLP) architecture.

Raw Training Data

Figure 6.10a shows the classification accuracies of the three employed ML algorithms. The markers represent the mean values, whereas the error bars indicate the standard deviations of the corresponding data points. The MLP (red line and point markers) classifier shows the best classification performance and reaches mean accuracies of $\geq$ 90 % when being trained with $q_{\text{train}} = 25\,\%$ of the sub-CRPs of a hybrid PUF. The LR (blue line and triangle markers) algorithm requires at least $q_{\text{train}} = 35\,\%$ of the sub-CRPs to break through this line. Finally, the RF (green line and square markers) shows the lowest performance in terms of classification accuracies. The results show, that the hybrid PUFs can be successfully modeled by attackers if using the readdressing method to build PUF challenges. This is in good agreement with our entropy analysis in Section 6.2.2.

To assess the quality of the classification we compute the true-positive-rate (TPR) and the false positive rate (FPR) according to Equation (2.20) and Equation (2.21), respectively. From an attackers point of view, it is desired to use the model-based attack that offers the best classification quality while requiring the least training data. From our prior evaluations on the prediction accuracies, we determined the MLP as the best predictive model. Therefore, we use the MLP model as the benchmark for our classification quality assessment. Figure 6.10b shows the ROC curves for the LR, RF, and MLP classifiers when training the ML models with $q_{\text{train}} = 25\,\%$ of the total sub-CRPs. All AUROC values are close to the ideal value of 1, which implies that the classification of the ML models is accurate.



(a)

(b)

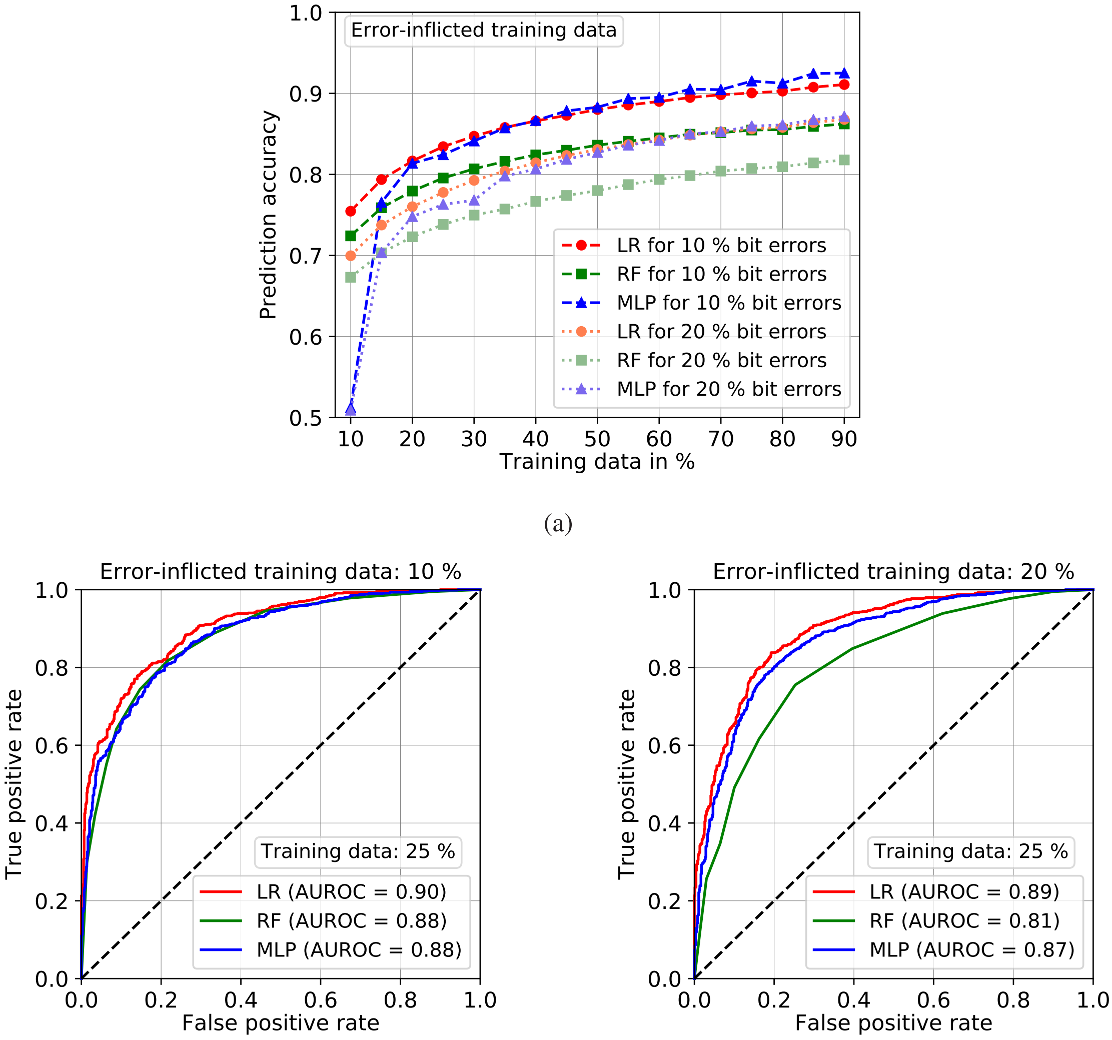
Figure 6.10: (a) Prediction accuracies of the LR, RF, and MLP machine learning methods for raw training data. (b) ROC curves for the LR, RF, and MLP machine learning methods for raw training data.

Error-Inflicted Training Data

To simulate the effects of noisy side-channels, we randomly flip response bits of the sub-CRPs used as training data. Figure 6.11a shows the prediction accuracies for the three employed ML algorithms after introducing BERs of 10 % (dashed lines) and 20 % (dotted lines), respectively. The results show, that increasing bit errors reduce the prediction accuracies. The MLP and LR classifiers achieve similar results and reach mean accuracies of ≥ 90 %, if at least $q_{\text{train}} = 70\,\%$ of the sub-CRPs are used for model training. The following correlation can be seen: The greater the BER, the smaller the gap between the MLP and LR accuracies. In this case, the lower training complexity in terms of computing power and time consumption makes the LR algorithm the most appropriate choice for attackers. Analog to our evaluation results based on raw training data, the RF classifier shows worse performance. Table 6.2 shows the obtained best, median, and mean prediction accuracies for different BERs. Furthermore, the table shows the relative training data required ($q_{\text{train}}/q_{\text{test}}$) to achieve a mean prediction accuracy of ≥ 90 %.
Similar to our evaluations based on the raw training data, we plot the ROC curves for the ML classifiers for error-inflicted training data. Figure 6.11b and Figure 6.11c show the resulting ROC curves when using $q_{\text{train}} = 25\,\%$ training data. Even if increasing the BER in the training data, the LR and MLP models outperform the RF classifier. Although the AUROC values decrease, the distance between the ROC curves and the diagonal black dashed line is still large, which implies accurate predictive models. Table 6.3 shows the detailed results for the quality metrics.

6.6 Performance Comparison

In the previous sections, we have performed model-based attacks on hybrid PUFs, using the BR-sort algorithm as well as different machine learning techniques. When using the raw training data, our evaluation results show that the BR-sort algorithm reaches prediction accuracies similar to the MLP classifier. If we consider the mean training times required by both models, the sorting



(a)

(b)

(c)

Figure 6.11: (a) Mean prediction accuracies of the LR, RF, and MLP machine learning methods for error-inflicted training data. ROC curves for the LR, RF, and MLP machine leaning methods for error-inflicted training data with bit errors rates (BERs) of (b) 10 %, and (c) 20 %.

algorithm offers ≈ 428-times faster training. This makes the BR-sort algorithm a promising alternative to the MLP classifier. The LR models' mean training time is in the range of the BR-sort algorithm. However, the minimum training data required to achieve prediction accuracies of ≥ 90 % is at $q_{\text{train}} = 35$ %, which is 10 % higher than for the BR-sort and MLP models. This means additional efforts for attackers in terms of eavesdropping CRP data. The RF classifier is outperformed by all other model-based attacks. If introducing bit errors to the training data, the performance of the BR-sort algorithm reduces strongly. The results imply that the ML classifiers should be preferred by attackers to attain high predictive models. Table 6.4 compares different works on model-based PUF attacks that can be found in the literature. Compared to other PUF types, the hybrid PUF design is less vulnerable against model-based attacks. This can be explained by the architecture of the hybrid PUF, where inverter cells can be addressed arbitrarily. In contrast, in arbiter PUFs each challenge involves all PUF logic components, which reveals information about the internal characteristics of the entire PUF circuit.

Table 6.2: Comparison of the prediction accuracy values of the BR-sort algorithm and different machine learning methods. The training data indicates the minimum relative portion of the total sub-CRPs required for model training to achieve a mean prediction accuracy score of ≥ 90 %.

Learning	**Training**	**Accuracy**	**Error-infliction (BER)**			**Training**
method	**data**	**score**	**0 %**	**10 %**	**20 %**	**time**
BR-sort (method 1)	30 %	Best	95.6 %	89.9 %	81.1 %	14.2 ms
		Median	91.8 %	79.1 %	70.5 %	
		Mean	91.6 %	79.1 %	70.4 %	
BR-sort (method 2)	25 %	Best	94.7 %	88.5 %	81.7 %	12.4 ms
		Median	90.4 %	79.6 %	70.9 %	
		Mean	90.3 %	79.2 %	70.7 %	
LR	35 %	Best	94.5 %	91.4 %	85.4 %	13.7 ms
		Median	90.2 %	85.8 %	80.4 %	
		Mean	90.1 %	85.8 %	80.4 %	
RF	90 %	Best	95.5 %	93.6 %	90.6 %	16.4 ms
		Median	88.6 %	86.1 %	81.7 %	
		Mean	88.4 %	86.2 %	81.8 %	
MLP	25 %	Best	94.8 %	88.6 %	82.7 %	5.3 s
		Median	91.0 %	82.4 %	76.4 %	
		Mean	90.1 %	82.4 %	76.3 %	

Table 6.3: Quality metrics of the classification for the BR-sort algorithm as well as the LR, RF, and MLP classifiers based on raw and error-inflicted training data. The training data indicates the minimum relative portion of the total sub-CRPs required for model training to achieve a mean prediction accuracy score of ≥ 90 %.

Learning method	**Training data**	**Confusion matrix term**	**Error-infliction (BER)**		
			0 %	**10 %**	**20 %**
BR-sort (method 1)	30 %	TP	45.8 %	39.8 %	35.2 %
		TN	46.4 %	40.3 %	36.1 %
		FP	3.6 %	9.7 %	13.9 %
		FN	4.2 %	10.2 %	14.8 %
BR-sort (method 2)	25 %	TP	44.8 %	39.2 %	35.1 %
		TN	45.4 %	39.9 %	35.9 %
		FP	4.6 %	10.1 %	14.1 %
		FN	5.2 %	10.8 %	14.9 %
LR	35 %	TP	45.1 %	42.9 %	40.2 %
		TN	45.1 %	42.9 %	40.3 %
		FP	4.9 %	7.1 %	9.7 %
		FN	4.9 %	7.1 %	9.8 %
RF	90 %	TP	43.2 %	41.8 %	39.0 %
		TN	45.3 %	44.4 %	43.0 %
		FP	4.6 %	5.4 %	6.8 %
		FN	6.9 %	8.4 %	11.2 %
MLP	25 %	TP	45.5 %	41.1 %	38.1 %
		TN	45.5 %	41.3 %	38.2 %
		FP	4.5 %	8.7 %	11.8 %
		FN	4.5 %	8.9 %	11.9 %

Table 6.4: Comparison between different silicon-based PUFs and the DiffC-PUF/hybrid PUF including model-based attacks.

PUF type	**Modeling**	**Training**	**Prediction**	**Training**	**Ref.**
	method	**data**	**accuracy**	**time**	
Arbiter PUF (64 stages)	LR	$\approx 3.5 \times 10^{-15}$ %	95 %	10 ms	[114]
XOR arbiter PUF (64 stages)	LR	$\approx 6.5 \times 10^{-14}$ %	99 %	3:42 min	[114]
FF-arbiter PUF (64 stages)	MLP	$\approx 5.4 \times 10^{-14}$ %	94.2 %	6.2 s	[231]
RO-PUF (256 ROs)	Quick sort	43.1 %	99 %	-	[114]
DiffC-PUF / Hybrid PUF (64 inverters)	BR-sort (method 1)	30 %	91.6 %	14.2 ms	This work
	BR-sort (method 2)	25 %	90.3 %	12.4 ms	This work
	LR	35 %	90.1 %	13.7 ms	This work
	RF	90 %	88.4 %	16.4 ms	This work
	MLP	25 %	90.1 %	5.3 s	This work

6.7 Conclusion

The security level of PUFs is mainly dependent on the vulnerabilities against physical and mathematical cloning. In this chapter, we have investigated and discussed the vulnerabilities of the hybrid PUF against model-based attacks. From an attacker's point of view, the internal characteristics of a PUF are not visible and appear to be totally random. However, all PUFs are subject to limited one-wayness, e.g. caused by systematic variations that lead to interdependencies between CRPs, biased responses, and reduced entropy. In this chapter, we have discussed eavesdropping techniques to leak CRPs and uncover correlations using model-based attacks. At this point we want to note, that PE-based PUFs face special security challenges due to the relatively low printing resolutions, large structures and components. Furthermore, we have performed entropy analysis based on different challenge building methods as well as minimum entropy (min-entropy) estimations. The results are shown in Table 6.1 and imply that the PUF response entropy mainly depends on the employed challenge building method. Having a reduced entropy implies that the interdependencies between the CRPs can be utilized to predict others.

While most of the state of the art model-based attacks are solely based on machine learning algorithms, we have introduced a sorting algorithm to model the internal behavior of hybrid PUFs (and RO-PUFs). Furthermore, we have employed the logistic regression (LR), random forest (RF), and multi-layer perceptron (MLP) classifiers to model hybrid PUFs. To assess and compare their performances in terms of prediction accuracies, an evaluation methodology was presented. The results (see Table 6.2 and Table 6.3) show, that the hybrid PUF is vulnerable against model-based attacks. Nonetheless, it is less vulnerable than many other PUF types (see Table 6.4). The sorting algorithm benefits from shorter training times compared to the ML algorithms. However, if the eavesdropped CRPs are erroneous, the ML techniques outperform the sorting algorithm.

7 Conclusion and Future Work

7.1 Conclusion

Printed electronics (PE) is a young research field compared to conventional silicon-based electronics and is considered as a key enabler for the Internet of Everything (IoE). A variety of novel materials and new fabrication methods enable flexible substrates, new form factors, large-area fabrication, and decentralized manufacturing.

These unique features bring new device types and develops new markets. In the scope of the IoE, devices are interconnected and managed in networks. The heterogeneity of devices with diverse computing performance and design constraints raise challenges in terms of security. In this context, constrained lightweight devices and systems are especially threatened.

To overcome these issues and to provide security also for low-complexity PE-based devices and systems, hardware-intrinsic security is a promising research direction. In this context, physically unclonable functions (PUFs) enable trust in the context of key derivation, generation, and secure storage. Firstly introduced for silicon technology to enable root of trust and to provide a device-specific inherent source of randomness for key derivation, the research field of printed PUFs is in the very early days. This thesis deals with PUFs based on hybrid electronics and has provided the following scientific contributions, in particular: (1) Determination of hardware-intrinsic security, particularly PUFs, as promising security primitives to be utilized in lightweight PE-based devices and systems. (2) Investigation of the requirements on PUF designs to meet the criteria of PE technology. Development of concepts for a PE-based PUF comprising silicon-based and printed components. (3) Implementation and evaluation of an embedded evaluation platform to enable large-scale characterization for fabricated silicon-based and PE-based PUFs. (4) Implementation of a simulation environment to investigate and evaluate the security metrics of the PE-based PUF. (5) Fabrication of PE-based PUFs and evaluation of the security metrics. (6) Determination of potential security threats arising for PE-based PUFs and investigation of vulnerabilities. Finally, (7) Implementation and evaluation of attacks against the introduced PE-based PUF and determination of potential target applications. The research questions outlined in Chapter 1 have been answered in the following way:

- **Q1: Which state of the art approaches are best suited to provide security features for PE-based devices and systems?**
  Printed electronics is a key enabling technology for the IoE. The pervasive interconnection of devices and the deployment in untrusted environments strengthen the need for security solutions suitable for lightweight electronic systems. The relatively strict design and performance constraints provided by PE limits the applicability of conventional security approaches. Originally emerged from silicon technology, hardware-intrinsic security, particularly PUFs, make use of the random intrinsic variations of integrated circuits and components to reproducibly derive device-specific identifiers. In Chapter 2 of this the-

sis, a comprehensive overview of state of the art PUF types is given. Firstly introducing silicon-based PUFs, the literature review also includes PUFs based on PE technology and novel materials. It is further distinguished between electrical and optical PUFs. The major drawback of optical PUFs is their high complexity especially for readout, making them non-applicable for the integration into lightweight electronic devices and systems. In particular, PE-based electrical PUFs can benefit from larger variations compared to silicon counterparts, which makes hardware-intrinsic security very promising. Since the variations are induced randomly and uncontrollably during the manufacturing process, no additional non-volatile memory (NVM) is necessary to store the identifiers. The identifiers are derived from the inherent variations on demand and discarded in the binary form if not used. This prevents from attacks such as memory leakage, which is one of the major security threats when using NVMs even if the device is powered off. Due to the so-called ’chain of trust’ the genuineness of the immutable identifiers belonging to the root of trust is of the greatest importance. Printed PUFs in combination with decentralized manufacturing further strengthen the root of trust compared to foundry-fabricated silicon-based systems.

- **Q2: How can a PUF be designed to meet the requirements for PE fabrication?**
  Printed electronics technology exhibits strict design and performance constraints, imposing special requirements regarding viable PUF types. The PUF quality parameters introduced in Chapter 3 help to determine the essential requirements on PUFs for a specific application scenario. Prior works introduced memory-based PUFs based on PE technology. The advantage of using memory cells is their relatively simple challenge-response interface. Thereby, the powering on of the memory cells is the challenge and the response is directly accessible in binary form. However, the scaling factor is very low if using memory cells to implement PUFs. For many applications it is desired to achieve non-linear challenge-response pair (CRP) growth when scaling up the PUF circuit. As a consequence, the design requirements on PE-based PUFs are mainly dependent on the desired scalability and simplicity of the challenge-response interface, which is the basis for the DiffC-PUF design. The DiffC-PUF is based on inverter structures, each comprising one resistor and one field effect transistor. The architecture allows arbitrary addressing and grouping of inverter pairs to be evaluated for response generation. As a consequence, the CRP space increases non-linearly with the number of PUF core inverters used.

- **Q3: How can the PUF characteristics be measured and the security performance be evaluated?**
  To enable large-scale characterization it is essential to develop an evaluation platform, as introduced in Chapter 3. The PUF characteristics are experimentally measured for silicon-based PUF cores in Chapter 4. Based on the PUF responses extracted under different operating conditions, the security metrics can be evaluated as introduced in Chapter 2. In Chapter 5, in the first instance the hybrid PUF incorporating printed PUF cores is characterized based on simulations. This allows to verify the characteristics to be expected from the fabricated devices. To evaluate the security metrics, it is essential to consider all possible operating conditions. Finally, the fabricated hybrid PUFs are characterized under changing operating conditions, including variations in the ambient temperature, relative humidity, and inverter supply voltage. The investigated security metrics include uniqueness, reproducibility, bit aliasing, and uniformity. The computed

metrics based on the experimental data obtained from the silicon-based PUF cores show values close to ideal. The experimental results for the PE-based hybrid PUFs show an almost ideal uniqueness value of 51.1 %. The bit aliasing and uniformity values show, that the measured PUF responses are biased towards 0. Nonetheless, the results are in good statistical agreement with the simulations. The determined security metrics show promising results and indicate the suitability of the hybrid PUF as a security primitive. The investigations of the reproducibility show, that the missing passivation for the EGTs degrades the robustness of the PUF response generation. In particular, changing ambient conditions such as temperature and humidity have effects on the electrical characteristics of the PE-based PUF core circuit. With a mean reliability value of 78.5 %, the hybrid PUF's operational areas are currently limited to indoor applications, where the ambient operating conditions are more stable. Compared to other works, this is the first comprehensive study on PE-based PUFs in terms of security metrics, computed on the basis of experimentally measured PUF responses.

- **Q4: Which security threats do arise for PE-based PUFs?**
  In Chapter 2, a comprehensive overview on security threats for PUFs in general including eavesdropping, model-based, and machine learning attacks is given. The security analysis in Chapter 6 deals with security threats against PE-based PUFs. Due to the contrary properties of PE compared to silicon technology, new security threats do arise, especially concerning invasive attacks and tampering. The large-area fabrication capabilities, which is one of the major advantages of PE technology, allows to measure internal circuit characteristics with relatively low equipment overhead, if the attacker has physical access to the PUF. Furthermore, the eavesdropped information can be used to perform model-based attacks, e.g. by using sorting algorithms or by training machine learning models including logistic regression (LR), random forest (RF), and multi-layer perceptron (MLP). Thereby, the learnability of the PUF-internal behavior mainly depends on the employed challenge building method, as described in Section 3.2.3. If using the readdressing method, the binary relations (BR) sorting algorithm and the MLP achieve prediction accuracies of $\geq 90\,\%$ if at least 25 % of the sub-CRPs are used for model training. Compared to other PUF types such as arbiter PUFs, our results show that the hybrid PUF is less vulnerable against model-based attacks. From an attacker's point of view, the BR-sort algorithm is a promising alternative to machine learning algorithms, since it exhibits shorter training times and it requires less computational performance.

- **Q5: Which potential target applications do exist for the proposed PE-based PUF?**
  In general, PUFs are used for identification, authentication, and cryptographic key generation. In identification and authentication, the uniqueness and reproducibility of the generated keys are of greatest importance. On the other hand, cryptography impose requirements in terms of unpredictability and uniformity. Potential target applications can be determined on the basis of the security metrics. In this context, the intra hamming distance (intra-HD) and inter-HD distributions of the PUF responses play a major role, as introduced in Section 2.3.4. In Chapter 4 and Chapter 5 the evaluation methodologies are given. The results of the experimental data obtained from silicon-based PUF cores using the readdressing method show a false-acceptance-rate (FAR) and a false-rejection-rate (FRR) of 1.57 % (-1.80) at the equal-error-rate (EER), respectively. The values in the brackets indicate the $\log_{10}(\cdot)$ notation of the percentual values. For the PE-based PUF cores,

the simulation results show FAR and FRR values of 0.48 % (-2.32) at the EER for the readdressing method. The experimental values are FAR=FRR=1.50 % (-1.83) and show good agreement with the simulations. Another option is to use the differential challenge building method, which improves the results to FAR=FRR=0.02 % (-3.61). Thereby, the standard deviation of the inter-HD distribution is smaller, which reduces both the FAR and FRR values. Many applications require FAR and FRR values of −6 or lower, which can be achieved through additional post-processing steps, such as error-correction of the PUF responses. Additional evaluations on the randomness of the PUF responses (please refer to Section 5.6 for more information) show, that the differential addressing method is capable of generating bit sequences that satisfy the NIST randomness tests for cryptography. The main limitation for the fabricated hybrid PUFs arises from the relatively low reliability value, which is caused by the missing passivation of the printed electrolyte-gated field-effect transistors (EGTs). For the time being, the requirements holding for identification tasks can be addressed with the DiffC-PUF design. It is expected that authentication and cryptographic applications can be targeted once passivation for the EGTs and post-processing on the PUF responses are available. In Chapter 6, it has been found that PE-based PUFs are vulnerable against invasive attacks, which is an issue to be addressed in the future. Possible countermeasures include large-area printed protective coatings to prevent from physical access.

In this thesis, we have performed statistical evaluations of the security metrics as well as a comprehensive security analysis. In conclusion, we have shown that the PUF designed, simulated, and fabricated in this thesis, has the potential to improve security for lightweight PE-based electronic devices and systems.

7.2 Future Work

During the project, a number of additional questions came up. In the future, various research directions can be pursued to improve the security capabilities of the PE-based PUF presented in this thesis. This would also help to address applications, such as authentication and cryptographic key generation.

- **Transistor passivation and encapsulation**
  Introducing transistor (EGT) passivation and encapsulation would increase the resilience against impacts originating from changing environmental conditions and aging. It is also expected that bit errors are reduced and the reproducibility of the PUF responses can be improved in general.
- **Fully printed PUF**
  Since the research field of PE is still in the early stages compared to silicon technology, many standard components such as multiplexers, operational amplifiers, and comparators are missing or compatibility between different materials is not given. To reach the next step of PUF-based security in lightweight printed electronic systems, it would be interesting to push the potential of being fully printed to the next level.

- **Post-processing of PUF responses**
  Responses generated by PUFs are typically fuzzy, due to changing environmental impacts, changing operating conditions, and aging effects. In silicon-based PUFs, it is common practice to employ post-processing in terms of error correction to obtain stable responses. This improves the reproducibility of the PUF responses by reducing the bit errors. As a consequence, the intra-HD distribution changes and the mean value is likely to be decreased. This should also improve the false-acceptance-rate (FAR) and false-rejection-rate (FRR) values, which is necessary to improve the security capabilities by qualifying for authentication and cryptographic applications.
- **Tamper protection**
  In contrast to conventional silicon technology, printed electronics exhibits large-area structures. This raises security threats in terms of invasive attacks that can be performed with relatively low effort and equipment overhead. One possible countermeasure could be printed protective coatings to detect or prevent from invasive attacks and provide tamper protection.

Besides these future directions, the foundations acquired in this thesis are interesting for the research community in the field of cyber security. The comprehensive statistical analysis on the basis of simulations and experimental data obtained from fabricated PE-based PUFs denote a milestone towards security for lightweight devices and systems in the IoE.

References

[1] V. L. Kalyani and D. Sharma, "Iot: machine to machine (m2m), device to device (d2d) internet of everything (ioe) and human to human (h2h): future of communication," *J. Manag. Eng. Inf. Technol*, vol. 2, pp. 17–23, 2015.

[2] D. Pavithra and R. Balakrishnan, "Iot based monitoring and control system for home automation," in *2015 global conference on communication technologies (GCCT)*. IEEE, 2015, pp. 169–173.

[3] S. Pirbhulal, H. Zhang, M. E. E Alahi, H. Ghayvat, S. C. Mukhopadhyay, Y.-T. Zhang, and W. Wu, "A novel secure iot-based smart home automation system using a wireless sensor network," *Sensors*, vol. 17, no. 1, p. 69, 2017.

[4] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm," in *2014 IEEE international conference on industrial engineering and engineering management*. IEEE, 2014, pp. 697–701.

[5] A.-R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta, and M. Alikarar, "A smart home energy management system using iot and big data analytics approach," *IEEE Transactions on Consumer Electronics*, vol. 63, no. 4, pp. 426–434, 2017.

[6] S. H. Sutar, R. Koul, and R. Suryavanshi, "Integration of smart phone and iot for development of smart public transportation system," in *2016 International Conference on Internet of Things and Applications (IOTA)*. IEEE, 2016, pp. 73–78.

[7] C. Badii, P. Bellini, A. Difino, and P. Nesi, "Sii-mobility: An iot/ioe architecture to enhance smart city mobility and transportation services," *Sensors*, vol. 19, no. 1, p. 1, 2019.

[8] M. Lom, O. Pribyl, and M. Svitek, "Industry 4.0 as a part of smart cities," in *2016 Smart Cities Symposium Prague (SCSP)*. IEEE, 2016, pp. 1–6.

[9] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0," *IEEE industrial electronics magazine*, vol. 11, no. 1, pp. 17–27, 2017.

[10] N. E. Maghawry and S. Ghoniemy, "A proposed internet of everything framework for disease prediction," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 15, no. 04, pp. 20–27, 2019.

[11] S. Ansari, T. Aslam, J. Poncela, P. Otero, and A. Ansari, "Internet of things-based healthcare applications," in *IoT Architectures, Models, and Platforms for Smart City Applications*. IGI Global, 2020, pp. 1–28.

[12] D. Liu and G. Hong, "Wearable electromechanical sensors and its applications," in *Wearable Devices-the Big Wave of Innovation*. IntechOpen, 2019.

[13] A. Iqbal, F. Ullah, H. Anwar, A. Ur Rehman, K. Shah, A. Baig, S. Ali, S. Yoo, and K. S. Kwak, "Wearable internet-of-things platform for human activity recognition and health care," *International Journal of Distributed Sensor Networks*, vol. 16, no. 6, p. 1550147720911561, 2020.

[14] S. L. Kinney, *Trusted platform module basics: using TPM in embedded systems*. Elsevier, 2006.

[15] R. Ross, M. McEvilley, and J. Oren, "Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems," National Institute of Standards and Technology, Tech. Rep., 2016.

[16] T. Phinney, "Iec 62443: Industrial network and system security," *Last accessed July*, vol. 29, 2013.

[17] P. Barrett, "Implementing the rivest shamir and adleman public key encryption algorithm on a standard digital signal processor," in *Conference on the Theory and Application of Cryptographic Techniques*. Springer, 1986, pp. 311–323.

[18] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (blowfish)," in *International Workshop on Fast Software Encryption*. Springer, 1993, pp. 191–204.

[19] "Announcing the advanced encryption standard (aes)," in *Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST)*, 2001.

[20] S. Mittal and A. I. Alsalibi, "A survey of techniques for improving security of non-volatile memories," *Journal of Hardware and Systems Security*, vol. 2, no. 2, pp. 179–200, 2018.

[21] B. Willsch, "Integration of physically unclonable functions (pufs) in cmos," Ph.D. dissertation, Universität Duisburg-Essen, 2019.

[22] Y. Khan, A. Thielens, S. Muin, J. Ting, C. Baumbauer, and A. C. Arias, "A new frontier of printed electronics: flexible hybrid electronics," *Advanced Materials*, vol. 32, no. 15, p. 1905279, 2020.

[23] M. Irimia-Vladu, ""green" electronics: biodegradable and biocompatible materials and devices for sustainable future," *Chemical Society Reviews*, vol. 43, no. 2, pp. 588–610, 2014.

[24] K. Suganuma, *Introduction to printed electronics*. Springer Science & Business Media, 2014, vol. 74.

[25] W. Clemens, D. Lupo, K. Hecker, and S. Breitung, "White paper oe-a roadmap for organic and printed electronics," *Organic Electronics Association (OE-A). http://www. vdma. org/wps/myportal/Home/en/Datenbanken/Downloads*, 2009.

[26] M. Bartzsch, H. Kempa, M. Otto, A. Hübler, and D. Zielke, "Device and circuit simulation of printed polymer electronics," *Organic electronics*, vol. 8, no. 4, pp. 431–438, 2007.

[27] P. H. Lau, K. Takei, C. Wang, Y. Ju, J. Kim, Z. Yu, T. Takahashi, G. Cho, and A. Javey, "Fully printed, high performance carbon nanotube thin-film transistors on flexible substrates," *Nano letters*, vol. 13, no. 8, pp. 3864–3869, 2013.

[28] X. Zhang, T. Ge, and J. S. Chang, "Fully-additive printed electronics: Transistor model, process variation and fundamental circuit designs," *Organic Electronics*, vol. 26, pp. 371–379, 2015.

[29] J. Zhou, T. Ge, E. Ng, and J. S. Chang, “Fully additive low-cost printed electronics with very low process variations,” *IEEE Transactions on Electron Devices*, vol. 63, no. 2, pp. 793–799, 2015.

[30] J. Noh, M. Jung, Y. Jung, C. Yeom, M. Pyo, and G. Cho, “Key issues with printed flexible thin film transistors and their application in disposable rf sensors,” *Proceedings of the IEEE*, vol. 103, no. 4, pp. 554–566, 2015.

[31] E. Sowade, E. Ramon, K. Y. Mitra, C. Martínez-Domingo, M. Pedró, J. Pallarès, F. Loffredo, F. Villani, H. L. Gomes, L. Terés *et al.*, “All-inkjet-printed thin-film transistors: manufacturing process reliability by root cause analysis,” *Scientific reports*, vol. 6, p. 33490, 2016.

[32] A. Scholz, L. Zimmermann, A. Sikora, M. Tahoori, and J. Aghassi-Hagmann, “Demonstration of differential circuit (diffc)-puf addressing and readout platform,” EasyChair Preprint no. 1571, EasyChair, 2019.

[33] L. Zimmermann, A. Scholz, A. Sikora, M. B. Tahoori, and J. Aghassi-Hagmann, “Embedded analog physical unclonable function system to extract reliable and unique security keys,” *Applied Sciences*, vol. 10, no. 3, p. 759, 2020.

[34] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-factor authentication: A survey,” *Cryptography*, vol. 2, no. 1, p. 1, 2018.

[35] G. C. Kessler, “An overview of cryptography,” 2003.

[36] D. Bhattacharyya, R. Ranjan, F. Alisherov, M. Choi *et al.*, “Biometric authentication: A review,” *International Journal of u-and e-Service, Science and Technology*, vol. 2, no. 3, pp. 13–28, 2009.

[37] D. T. Bourgeois, “Information systems for business and beyond,” 2018.

[38] Y. Cherdantseva and J. Hilton, “Information security and information assurance. the discussion about the meaning, scope and goals.(may, 2012).”

[39] Y. Sattarova Feruza and T.-h. Kim, “It security review: Privacy, protection, access control, assurance and system security,” *International journal of multimedia and ubiquitous engineering*, vol. 2, no. 2, pp. 17–32, 2007.

[40] J. Jung, J. Cho, and B. Lee, “A secure platform for iot devices based on arm platform security architecture,” in *2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM)*. IEEE, 2020, pp. 1–4.

[41] A. Ltd, “Platform security architecture overview,” *ARM Ltd, Cambridge, UK, White Paper June 2019 (Revision 1.3)*, 2019.

[42] R. T. Tiburski, C. R. Moratelli, S. F. Johann, M. V. Neves, E. de Matos, L. A. Amaral, and F. Hessel, “Lightweight security architecture based on embedded virtualization and trust mechanisms for iot edge devices,” *IEEE Communications Magazine*, vol. 57, no. 2, pp. 67–73, 2019.

[43] R. Maes, *Physically unclonable functions: Constructions, properties and applications*. Springer Science & Business Media, 2013.

[44] D. E. Standard *et al.*, “Data encryption standard,” *Federal Information Processing Standards Publication*, p. 112, 1999.

[45] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[46] C. Nist, "The digital signature standard," *Communications of the ACM*, vol. 35, no. 7, pp. 36–40, 1992.

[47] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[48] R. C. Merkle, "Secure communications over insecure channels," *Communications of the ACM*, vol. 21, no. 4, pp. 294–299, 1978.

[49] A. J. Menezes, J. Katz, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[50] R. Pappu, "Physical one-way functions', 2001," *Massachusetts Institute of Technology*.

[51] B. L. P. Gassend, "Physical random functions," Ph.D. dissertation, Massachusetts Institute of Technology, 2003.

[52] S. Mittal, "A survey of architectural techniques for managing process variation," *ACM Computing Surveys (CSUR)*, vol. 48, no. 4, pp. 1–29, 2016.

[53] K. A. Bowman, S. G. Duvall, and J. D. Meindl, "Impact of die-to-die and within-die parameter fluctuations on the maximum clock frequency distribution for gigascale integration," *IEEE Journal of solid-state circuits*, vol. 37, no. 2, pp. 183–190, 2002.

[54] D. Nedospasov, J.-P. Seifert, C. Helfmeier, and C. Boit, "Invasive puf analysis," in *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE, 2013, pp. 30–38.

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

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

[57] M.-D. Yu, M. Hiller, J. Delvaux, R. Sowell, S. Devadas, and I. Verbauwhede, "A lockdown technique to prevent machine learning on pufs for lightweight authentication," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 3, pp. 146–159, 2016.

[58] T. W. Edgar and D. O. Manz, *Research methods for cyber security*. Syngress, 2017.

[59] C. E. Shannon, "A mathematical theory of communication," *Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[60] E. Barker, L. Feldman, and G. Witte, "Recommendation for random number generation using deterministic random bit generators," National Institute of Standards and Technology, Tech. Rep., 2015.

[61] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded systems design with FPGAs*. Springer, 2013, pp. 245–267.

[62] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 148–160.

[63] P. Tuyls, *Towards hardware-intrinsic security: foundations and practice*. Springer Science & Business Media, 2010.

[64] F. Armknecht, R. Maes, A.-R. Sadeghi, F.-X. Standaert, and C. Wachsmann, “A formal foundation for the security features of physical functions,” 05 2011, pp. 397–412.

[65] U. Rührmair, C. Hilgers, S. Urban, A. Weiershäuser, E. Dinter, B. Forster, and C. Jirauschek, “Optical pufs reloaded,” *Eprint. Iacr. Org*, 2013.

[66] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, “Quantitative and statistical performance evaluation of arbiter physical unclonable functions on fpgas,” in *2010 International Conference on Reconfigurable Computing and FPGAs*. IEEE, 2010, pp. 298–303.

[67] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, “A large scale characterization of ro-puf,” in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 2010, pp. 94–99.

[68] N. A. Lal, S. Prasad, and M. Farik, “A review of authentication methods,” *International Journal of Scienctific and Technology Research (IJSTR)*, vol. 5, no. 11, pp. 246–249, 2016.

[69] M. Lehtonen, T. Staake, and F. Michahelles, “From identification to authentication–a review of rfid product authentication techniques,” in *Networked RFID Systems and Lightweight Cryptography*. Springer, 2008, pp. 169–187.

[70] G. Di Crescenzo, R. Graveman, R. Ge, and G. Arce, “Approximate message authentication and biometric entity authentication,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2005, pp. 240–254.

[71] M. O’Neill *et al.*, “Insecurity by design: Today’s iot device security problem,” *Engineering*, vol. 2, no. 1, pp. 48–49, 2016.

[72] Y. Gao, H. Ma, S. F. Al-Sarawi, D. Abbott, and D. C. Ranasinghe, “Detecting recycled commodity socs: Exploiting aging-induced sram puf unreliability,” *arXiv preprint arXiv:1705.07375*, 2017.

[73] J. S. Chang, A. F. Facchetti, and R. Reuss, “A circuits and systems perspective of organic/printed electronics: Review, challenges, and contemporary and emerging design approaches,” *IEEE Journal on emerging and selected topics in circuits and systems*, vol. 7, no. 1, pp. 7–26, 2017.

[74] W. Wu, “Inorganic nanomaterials for printed electronics: a review,” *Nanoscale*, vol. 9, no. 22, pp. 7342–7372, 2017.

[75] J. C. Lee, S. E. Hudson, and E. Tse, “Foldable interactive displays,” in *Proceedings of the 21st annual ACM symposium on User interface software and technology*, 2008, pp. 287–290.

[76] S. Khan, L. Lorenzelli, and R. S. Dahiya, “Technologies for printing sensors and electronics over large flexible substrates: a review,” *IEEE Sensors Journal*, vol. 15, no. 6, pp. 3164–3185, 2014.

[77] A. M. Gaikwad, D. A. Steingart, T. Nga Ng, D. E. Schwartz, and G. L. Whiting, “A flexible high potential printed battery for powering printed electronics,” *Applied Physics Letters*, vol. 102, no. 23, p. 104_1, 2013.

[78] R. Xu, A. Lei, C. Dahl-Petersen, K. Hansen, M. Guizzetti, K. Birkelund, E. V. Thomsen, and O. Hansen, “Screen printed pzt/pzt thick film bimorph mems cantilever device for vibration energy harvesting,” *Sensors and Actuators A: Physical*, vol. 188, pp. 383–388, 2012.

[79] J. van den Brand, M. de Kok, M. Koetse, M. Cauwe, R. Verplancke, F. Bossuyt, M. Jablonski, and J. Vanfleteren, “Flexible and stretchable electronics for wearable health devices,” *Solid-State Electronics*, vol. 113, pp. 116–120, 2015.

[80] J. Perelaer, P. J. Smith, D. Mager, D. Soltman, S. K. Volkman, V. Subramanian, J. G. Korvink, and U. S. Schubert, “Printed electronics: the challenges involved in printing devices, interconnects, and contacts based on inorganic materials,” *Journal of Materials Chemistry*, vol. 20, no. 39, pp. 8446–8453, 2010.

[81] E. B. Secor, S. Lim, H. Zhang, C. D. Frisbie, L. F. Francis, and M. C. Hersam, “Gravure printing of graphene for large-area flexible electronics,” *Advanced materials*, vol. 26, no. 26, pp. 4533–4538, 2014.

[82] X. Liu and J. Guthrie, “A review of flexographic printing plate development,” *Surface Coatings International Part B: Coatings Transactions*, vol. 86, no. 2, pp. 91–99, 2003.

[83] A. Eshkeiti, A. S. Reddy, S. Emamian, B. B. Narakathu, M. Joyce, M. Joyce, P. D. Fleming, B. J. Bazuin, and M. Z. Atashbar, “Screen printing of multilayered hybrid printed circuit boards on different substrates,” *IEEE transactions on components, packaging and manufacturing technology*, vol. 5, no. 3, pp. 415–421, 2015.

[84] S. H. Ahn and L. J. Guo, “Large-area roll-to-roll and roll-to-plate nanoimprint lithography: a step toward high-throughput application of continuous nanoimprinting,” *ACS nano*, vol. 3, no. 8, pp. 2304–2310, 2009.

[85] N. Saengchairat, T. Tran, and C.-K. Chua, “A review: Additive manufacturing for active electronic components,” *Virtual and Physical Prototyping*, vol. 12, no. 1, pp. 31–46, 2017.

[86] J. Krumm, “Printed electronics-from vision to first products,” in *4th European Workshop on RFID Systems and Technologies*. VDE, 2008, pp. 1–3.

[87] E. Tekin, P. J. Smith, and U. S. Schubert, “Inkjet printing as a deposition and patterning tool for polymers and inorganic particles,” *Soft Matter*, vol. 4, no. 4, pp. 703–713, 2008.

[88] M. Singh, H. M. Haverinen, P. Dhagat, and G. E. Jabbour, “Inkjet printing—process and its applications,” *Advanced materials*, vol. 22, no. 6, pp. 673–685, 2010.

[89] C. Kagan, D. Mitzi, and C. Dimitrakopoulos, “Organic-inorganic hybrid materials as semiconducting channels in thin-film field-effect transistors,” *Science*, vol. 286, no. 5441, pp. 945–947, 1999.

[90] M. Jang, J. H. Park, S. Im, S. H. Kim, and H. Yang, “Critical factors to achieve low voltage- and capacitance-based organic field-effect transistors,” *Advanced Materials*, vol. 26, no. 2, pp. 288–292, 2014.

[91] Y. Sun and J. A. Rogers, “Inorganic semiconductors for flexible electronics,” *Advanced materials*, vol. 19, no. 15, pp. 1897–1916, 2007.

[92] G. A. T. Sevilla and M. M. Hussain, “Printed organic and inorganic electronics: Devices to systems,” *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 7, no. 1, pp. 147–160, 2016.

[93] A. C. Arias, F. Endicott, and R. A. Street, "Surface-induced self-encapsulation of polymer thin-film transistors," *Advanced Materials*, vol. 18, no. 21, pp. 2900–2904, 2006.

[94] Z. Liu, J. Xu, D. Chen, and G. Shen, "Flexible electronics based on inorganic nanowires," *Chemical Society Reviews*, vol. 44, no. 1, pp. 161–192, 2015.

[95] Z. Cui, *Printed electronics: Materials, technologies and applications*. John Wiley & Sons, 2016.

[96] G. C. Marques, S. K. Garlapati, D. Chatterjee, S. Dehm, S. Dasgupta, J. Aghassi, and M. B. Tahoori, "Electrolyte-gated fets based on oxide semiconductors: Fabrication and modeling," *IEEE Transactions on Electron Devices*, vol. 64, no. 1, pp. 279–285, 2016.

[97] G. Cadilha Marques, S. K. Garlapati, S. Dehm, S. Dasgupta, H. Hahn, M. Tahoori, and J. Aghassi-Hagmann, "Digital power and performance analysis of inkjet printed ring oscillators based on electrolyte-gated oxide electronics," *Applied Physics Letters*, vol. 111, no. 10, p. 102103, 2017.

[98] A. Scholz, L. Zimmermann, U. Gengenbach, L. Koker, Z. Chen, H. Hahn, A. Sikora, M. B. Tahoori, and J. Aghassi-Hagmann, "Hybrid low-voltage physical unclonable function based on inkjet-printed metal-oxide transistors," *Nature Communications*, vol. 11, no. 1, pp. 1–11, 2020.

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

[100] K. Lofstrom, W. R. Daasch, and D. Taylor, "Ic identification circuit using device mismatch," in *2000 IEEE International Solid-State Circuits Conference. Digest of Technical Papers (Cat. No. 00CH37056)*. IEEE, 2000, pp. 372–373.

[101] V. Sehwag and T. Saha, "Tv-puf: a fast lightweight analog physical unclonable function," in *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*. IEEE, 2016, pp. 182–186.

[102] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525)*. IEEE, 2004, pp. 176–179.

[103] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.

[104] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 237–249.

[105] J. Delvaux and I. Verbauwhede, "Side channel modeling attacks on 65nm arbiter pufs exploiting cmos device noise," in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 2013, pp. 137–142.

[106] S. S. Zalivaka, A. A. Ivaniuk, and C.-H. Chang, "Fpga implementation of modeling attack resistant arbiter puf with enhanced reliability," in *2017 18th International Symposium on Quality Electronic Design (ISQED)*. IEEE, 2017, pp. 313–318.

[107] C. Zhou, K. K. Parhi, and C. H. Kim, “Secure and reliable xor arbiter puf design: An experimental study based on 1 trillion challenge response pair measurements,” in *Proceedings of the 54th Annual Design Automation Conference 2017*, 2017, pp. 1–6.

[108] A. Mahmoud, U. Rührmair, M. Majzoobi, and F. Koushanfar, “Combined modeling and side channel attacks on strong pufs.” *IACR Cryptology ePrint Archive*, vol. 2013, p. 632, 2013.

[109] G. T. Becker, “The gap between promise and reality: On the insecurity of xor arbiter pufs,” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2015, pp. 535–555.

[110] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 9–14.

[111] C.-E. D. Yin and G. Qu, “Lisa: Maximizing ro puf’s secret extraction,” in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 2010, pp. 100–105.

[112] A. Maiti and P. Schaumont, “Improved ring oscillator puf: An fpga-friendly secure primitive,” *Journal of cryptology*, vol. 24, no. 2, pp. 375–397, 2011.

[113] M. Gao, K. Lai, and G. Qu, “A highly flexible ring oscillator puf,” in *Proceedings of the 51st Annual Design Automation Conference*, 2014, pp. 1–6.

[114] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, “Puf modeling attacks on simulated and silicon data,” *IEEE transactions on information forensics and security*, vol. 8, no. 11, pp. 1876–1891, 2013.

[115] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, “Fpga intrinsic pufs and their use for ip protection,” in *International workshop on cryptographic hardware and embedded systems*. Springer, 2007, pp. 63–80.

[116] D. E. Holcomb, W. P. Burleson, and K. Fu, “Power-up sram state as an identifying fingerprint and source of true random numbers,” *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2008.

[117] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, “The butterfly puf protecting ip on every fpga,” in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE, 2008, pp. 67–70.

[118] D. Karakoyunlu and B. Sunar, “Differential template attacks on puf enabled cryptographic devices,” in *2010 IEEE International Workshop on Information Forensics and Security*. IEEE, 2010, pp. 1–6.

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

[120] A. Roelke and M. R. Stan, “Attacking an sram-based puf through wearout,” in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2016, pp. 206–211.

[121] P. Tuyls, G.-J. Schrijen, B. Škorić, J. Van Geloven, N. Verhaegh, and R. Wolters, “Read-proof hardware from protective coatings,” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2006, pp. 369–383.

[122] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical one-way functions,” *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[123] M. Guerin, E. Bergeret, E. Bènevent, P. Pannier, A. Daami, S. Jacob, I. Chartier, and R. Coppard, “Design of organic complementary circuits for rfid tags application,” in *Proceedings of the IEEE 2012 Custom Integrated Circuits Conference*. IEEE, 2012, pp. 1–4.

[124] A. T. Erozan, M. S. Golanbari, R. Bishnoi, J. Aghassi-Hagmann, and M. B. Tahoori, “Design and evaluation of physical unclonable function for inorganic printed electronics,” in *2018 19th International Symposium on Quality Electronic Design (ISQED)*. IEEE, 2018, pp. 419–424.

[125] A. T. Erozan, G. C. Marques, M. S. Golanbari, R. Bishnoi, S. Dehm, J. Aghassi-Hagmann, and M. B. Tahoori, “Inkjet-printed egfet-based physical unclonable function—design, evaluation, and fabrication,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 12, pp. 2935–2946, 2018.

[126] Y. Liu, F. Han, F. Li, Y. Zhao, M. Chen, Z. Xu, X. Zheng, H. Hu, J. Yao, T. Guo *et al.*, “Inkjet-printed unclonable quantum dot fluorescent anti-counterfeiting labels with artificial intelligence authentication,” *Nature communications*, vol. 10, no. 1, p. 2409, 2019.

[127] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, “Emerging physical unclonable functions with nanotechnology,” *IEEE access*, vol. 4, pp. 61–80, 2016.

[128] S. C. Konigsmark, L. K. Hwang, D. Chen, and M. D. Wong, “Cnpuf: A carbon nanotube-based physically unclonable function for secure low-energy hardware design,” in *2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2014, pp. 73–78.

[129] Z. Hu, J. M. M. L. Comeras, H. Park, J. Tang, A. Afzali, G. S. Tulevski, J. B. Hannon, M. Liehr, and S.-J. Han, “Physically unclonable cryptographic primitives using self-assembled carbon nanotubes,” *Nature nanotechnology*, vol. 11, no. 6, p. 559, 2016.

[130] K. Kursawe, A.-R. Sadeghi, D. Schellekens, B. Skoric, and P. Tuyls, “Reconfigurable physical unclonable functions-enabling technology for tamper-resistant storage,” in *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE, 2009, pp. 22–29.

[131] G. S. Rose, N. McDonald, L.-K. Yan, B. Wysocki, and K. Xu, “Foundations of memristor based puf architectures,” in *2013 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH)*. IEEE, 2013, pp. 52–57.

[132] G. S. Rose, N. McDonald, L.-K. Yan, and B. Wysocki, “A write-time based memristive puf for hardware security applications,” in *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2013, pp. 830–833.

[133] P. Koeberl, Ü. Kocabaş, and A.-R. Sadeghi, “Memristor pufs: a new generation of memory-based physically unclonable functions,” in *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2013, pp. 428–431.

[134] J. Mathew, R. S. Chakraborty, D. P. Sahoo, Y. Yang, and D. K. Pradhan, “A novel memristor-based hardware security primitive,” *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 14, no. 3, pp. 1–20, 2015.

[135] K. Kuribara, Y. Hori, T. Katashita, K. Kakita, Y. Tanaka, and M. Yoshida, “Organic physically unclonable function on flexible substrate operable at 2 v for iot/ioe security applications,” *Organic Electronics*, vol. 51, pp. 137–141, 2017.

[136] R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assawaworrarit, and C. Yang, “Physical key-protected one-time pad,” *Scientific reports*, vol. 3, p. 3543, 2013.

[137] J. Kim, J. M. Yun, J. Jung, H. Song, J.-B. Kim, and H. Ihee, “Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires,” *Nanotechnology*, vol. 25, no. 15, p. 155303, 2014.

[138] A. F. Smith, P. Patton, and S. E. Skrabalak, “Plasmonic nanoparticles as a physically unclonable function for responsive anti-counterfeit nanofingerprints,” *Advanced Functional Materials*, vol. 26, no. 9, pp. 1315–1321, 2016.

[139] M. R. Carro-Temboury, R. Arppe, T. Vosch, and T. J. Sørensen, “An optical authentication system based on imaging of excitation-selected lanthanide luminescence,” *Science advances*, vol. 4, no. 1, p. e1701384, 2018.

[140] C. Mesaritakis, M. Akriotou, A. Kapsalis, E. Grivas, C. Chaintoutis, T. Nikas, and D. Syvridis, “Physical unclonable function based on a multi-mode optical waveguide,” *Scientific reports*, vol. 8, no. 1, p. 9653, 2018.

[141] A. Wali, A. Dodda, Y. Wu, A. Pannone, L. K. R. Usthili, S. K. Ozdemir, I. T. Ozbolat, and S. Das, “Biological physically unclonable function,” *Communications Physics*, vol. 2, no. 1, p. 39, 2019.

[142] C.-H. Chang, Y. Zheng, and L. Zhang, “A retrospective and a look forward: Fifteen years of physical unclonable function advancement,” *IEEE Circuits and Systems Magazine*, vol. 17, no. 3, pp. 32–62, 2017.

[143] M. van Dijk and U. Rührmair, “Physical unclonable functions in cryptographic protocols: Security proofs and impossibility results.” *IACR Cryptol. EPrint Arch.*, vol. 2012, p. 228, 2012.

[144] N. Menhorn, “External secure storage using the puf,” *Xilinx, San Jose, CA, USA, Application Note XAPP1333 (v1.0) June 26, 2018*, 2018.

[145] T. Lu, R. Kenny, and S. Atsatt, “Secure device manager for intel stratix 10 devices provides fpga and soc security,” *Intel, Santa Clara, CA, USA, White Paper WP-01252-1.2*, 2018.

[146] Microsemi, “Overview of data security using microsemi fpgas and soc fpgas,” *One Enterprise, Aliso Viejo, CA, USA*, 2013.

[147] N. Semiconductors, “Secure storage with sram puf on nxp lpc54s0xx,” *NXP Semiconductors, San Jose, CA, USA, Application Note AN12292 (v1.0) November 06, 2018*, 2018.

[148] W. G. Ophey, B. Skoric, P. T. Tuyls, and A. H. M. Akkermans, “Integrated physical unclonable function (puf) with combined sensor and display,” Sep. 25 2008, uS Patent App. 12/090,414.

[149] D. Clarke, B. Gassend, M. Van Dijk, and S. Devadas, “Authentication of integrated circuits,” Nov. 23 2010, uS Patent 7,840,803.

[150] C. Tremlet, “Secure authentication based on physically unclonable functions,” Sep. 18 2014, uS Patent App. 14/202,239.

[151] H. H. Chi, H. O. Dai, K. D. Feng, and D. J. Papae, "Fet pair based physically unclonable function (puf) circuit with a constant common mode voltage," Jan. 27 2015, uS Patent 8,941,405.

[152] H. Kreft, "Tamper-protected hardware and method for using same," Jun. 30 2015, uS Patent 9,071,446.

[153] V. Van Der Leest, B. K. B. Preneel, and E. Van Der Sluis, "Physically unclonable function (puf) with improved error correction," Jul. 19 2016, uS Patent 9,396,357.

[154] P. W. Pinkse, A. P. Mosk *et al.*, "Quantum secure device, system and method for verifying challenge-response pairs using a physically unclonable function (puf)," Sep. 13 2016, uS Patent 9,444,632.

[155] T. Wille and B. Murray, "Puf based boot-loading for data recovery on secure flash devices," Oct. 8 2019, uS Patent 10,437,524.

[156] Z. Ramzan and L. Reyzin, "On the round security of symmetric-key cryptographic primitives," in *Annual International Cryptology Conference*. Springer, 2000, pp. 376–393.

[157] Z. Brakerski, Y. T. Kalai, J. Katz, and V. Vaikuntanathan, "Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage," in *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*. IEEE, 2010, pp. 501–510.

[158] S. Dai, H. Li, and F. Zhang, "Memory leakage-resilient searchable symmetric encryption," *Future Generation Computer Systems*, vol. 62, pp. 76–84, 2016.

[159] Y.-i. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki, and H. Sone, "Non-invasive emi-based fault injection attack against cryptographic modules," in *2011 IEEE International Symposium on Electromagnetic Compatibility*. IEEE, 2011, pp. 763–767.

[160] D. Merli, D. Schuster, F. Stumpf, and G. Sigl, "Side-channel analysis of pufs and fuzzy extractors," in *International Conference on Trust and Trustworthy Computing*. Springer, 2011, pp. 33–47.

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

[162] U. Rührmair, X. Xu, J. Sölter, A. Mahmoud, M. Majzoobi, F. Koushanfar, and W. Burleson, "Efficient power and timing side channels for physical unclonable functions," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2014, pp. 476–492.

[163] U. Rührmair and M. van Dijk, "Pufs in security protocols: Attack models and security evaluations," in *2013 IEEE symposium on security and privacy*. IEEE, 2013, pp. 286–300.

[164] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual International Cryptology Conference*. Springer, 1999, pp. 388–397.

[165] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*. Springer Science & Business Media, 2008, vol. 31.

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

[167] S. P. Skorobogatov, “Semi-invasive attacks-a new approach to hardware security analysis. university of cambridge,” *computer laboratory: Technical report (04 2005)*, 2005.

[168] L. Sauvage, S. Guilley, and Y. Mathieu, “Electromagnetic radiations of fpgas: High spatial resolution cartography and attack on a cryptographic module,” *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, vol. 2, no. 1, pp. 1–24, 2009.

[169] D. Merli, D. Schuster, F. Stumpf, and G. Sigl, “Semi-invasive em attack on fpga ro pufs and countermeasures,” in *Proceedings of the Workshop on Embedded Systems Security*, 2011, pp. 1–9.

[170] P. Bayon, L. Bossuet, A. Aubert, and V. Fischer, “Electromagnetic analysis on ring oscillator-based true random number generators,” in *2013 IEEE International Symposium on Circuits and Systems (ISCAS2013)*. IEEE, 2013, pp. 1954–1957.

[171] E. Öztürk, G. Hammouri, and B. Sunar, “Towards robust low cost authentication for pervasive devices,” in *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 2008, pp. 170–178.

[172] M. Majzoobi, F. Koushanfar, and M. Potkonjak, “Testing techniques for hardware security,” in *2008 IEEE International Test Conference*. IEEE, 2008, pp. 1–10.

[173] M. Majzoobi and F. Koushanfar, “Lightweight secure pufs,” in *2008 IEEE/ACM International Conference on Computer-Aided Design*. IEEE, 2008, pp. 670–673.

[174] G. Koch, R. Zemel, and R. Salakhutdinov, “Siamese neural networks for one-shot image recognition,” in *ICML deep learning workshop*, vol. 2. Lille, 2015.

[175] L. Deng and X. Li, “Machine learning paradigms for speech recognition: An overview,” *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 21, no. 5, pp. 1060–1089, 2013.

[176] I. Kononenko, “Machine learning for medical diagnosis: history, state of the art and perspective,” *Artificial Intelligence in medicine*, vol. 23, no. 1, pp. 89–109, 2001.

[177] E. Blanzieri and A. Bryl, “A survey of learning-based techniques of email spam filtering,” *Artificial Intelligence Review*, vol. 29, no. 1, pp. 63–92, 2008.

[178] Y.-J. Park and K.-N. Chang, “Individual and group behavior-based customer profile model for personalized product recommendation,” *Expert Systems with Applications*, vol. 36, no. 2, pp. 1932–1939, 2009.

[179] J. Rzeszótko and S. H. Nguyen, “Machine learning for traffic prediction,” *Fundamenta Informaticae*, vol. 119, no. 3-4, pp. 407–420, 2012.

[180] P. Domingos, “A few useful things to know about machine learning,” *Communications of the ACM*, vol. 55, no. 10, pp. 78–87, 2012.

[181] T. Hastie, R. Tibshirani, and J. Friedman, “Overview of supervised learning,” in *The elements of statistical learning*. Springer, 2009, pp. 9–41.

[182] Z. Ghahramani, “Unsupervised learning,” in *Summer School on Machine Learning*. Springer, 2003, pp. 72–112.

[183] P. Y. Glorennec, “Reinforcement learning: An overview,” in *Proc. of ESIT*, vol. 2000. Citeseer, 2000, pp. 17–35.

[184] H. Kour and N. Gondhi, "Machine learning techniques: A survey," in *Innovative Data Communication Technologies and Application*, J. S. Raj, A. Bashar, and S. R. J. Ramson, Eds. Cham: Springer International Publishing, 2020, pp. 266–275.

[185] C. M. Bishop, *Pattern recognition and machine learning*. Springer, 2006.

[186] P. H. Nguyen and D. P. Sahoo, "An efficient and scalable modeling attack on lightweight secure physically unclonable function." *IACR Cryptology ePrint Archive*, vol. 2016, p. 428, 2016.

[187] N. Pendar and C. A. Chapelle, "Investigating the promise of learner corpora: Methodological issues," *CALICO journal*, vol. 25, no. 2, p. 189, 2008.

[188] J. Miao, M. Li, S. Roy, and B. Yu, "Lrr-dpuf: Learning resilient and reliable digital physical unclonable function," in *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2016, pp. 1–8.

[189] J. Miao, M. Li, S. Roy, Y. Ma, and B. Yu, "Sd-puf: Spliced digital physical unclonable function," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 5, pp. 927–940, 2017.

[190] Y. Tanaka, S. Bian, M. Hiromoto, and T. Sato, "Coin flipping puf: a novel puf with improved resistance against machine learning attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 5, pp. 602–606, 2018.

[191] M. Minsky and S. A. Papert, *Perceptrons: An introduction to computational geometry*. MIT press, 2017.

[192] W. S. McCulloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity," *The bulletin of mathematical biophysics*, vol. 5, no. 4, pp. 115–133, 1943.

[193] R. Caruana, S. Lawrence, and C. L. Giles, "Overfitting in neural nets: Backpropagation, conjugate gradient, and early stopping," in *Advances in neural information processing systems*, 2001, pp. 402–408.

[194] D. E. Rumelhart, R. Durbin, R. Golden, and Y. Chauvin, "Backpropagation: The basic theory," *Backpropagation: Theory, architectures and applications*, pp. 1–34, 1995.

[195] I. Stephen, "Perceptron-based learning algorithms," *IEEE Transactions on neural networks*, vol. 50, no. 2, p. 179, 1990.

[196] G. Hospodar, R. Maes, and I. Verbauwhede, "Machine learning attacks on 65nm arbiter pufs: Accurate modeling poses strict bounds on usability," in *2012 IEEE international workshop on Information forensics and security (WIFS)*. IEEE, 2012, pp. 37–42.

[197] D. Schuster and R. Hesselbarth, "Evaluation of bistable ring pufs using single layer neural networks," in *International Conference on Trust and Trustworthy Computing*. Springer, 2014, pp. 101–109.

[198] Y. Ikezaki, Y. Nozaki, and M. Yoshikawa, "Deep learning attack for physical unclonable function," in *2016 IEEE 5th Global Conference on Consumer Electronics*. IEEE, 2016, pp. 1–2.

[199] M. S. Mispan, H. Su, M. Zwolinski, and B. Halak, "Cost-efficient design for modeling attacks resistant pufs," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2018, pp. 467–472.

[200] S. Kumar and M. Niamat, "Machine learning based modeling attacks on a configurable puf," in *NAECON 2018-IEEE National Aerospace and Electronics Conference*. IEEE, 2018, pp. 169–173.

[201] M. David, "Powers. 2011. evaluation: From precision, recall and f-score to roc, informedness, markedness & correlation," *Journal of Machine Learning Technologies*, vol. 2, no. 1.

[202] P. Stalph, *Analysis and design of machine learning techniques: evolutionary solutions for regression, prediction, and control problems*. Springer Science & Business Media, 2014.

[203] T.-Y. Liu *et al.*, "Learning to rank for information retrieval," *Foundations and Trends® in Information Retrieval*, vol. 3, no. 3, pp. 225–331, 2009.

[204] T. Fawcett, "An introduction to roc analysis," *Pattern recognition letters*, vol. 27, no. 8, pp. 861–874, 2006.

[205] R. T. Mercuri and P. G. Neumann, "Security by obscurity," *Communications of the ACM*, vol. 46, no. 11, p. 160, 2003.

[206] A. Kerckhoffs, *La cryptographie militaire, ou, Des chiffres usités en temps de guerre: avec un nouveau procédé de déchiffrement applicable aux systèmes à double clef*. Librairie militaire de L. Baudoin, 1883.

[207] L. Zimmermann, A. Scholz, A. Sikora, and J. Aghassi-Hagmann, "A hybrid system architecture for the readout of a printed physical unclonable function," in *2018 International Conference on Electronics Technology (ICET)*. IEEE, 2018, pp. 11–14.

[208] S. Consortium *et al.*, "Standard commands for programmable instruments," 1999.

[209] *Starter Kit EFM32LG-STK3600 User Manual*, Silicon Laboratories Inc., 2013.

[210] D. F. Baldwin and L. M. Higgins, *Electronic packaging and interconnection Handbook*. McGraw–Hill Handbooks, 2007, vol. 4, ch. Chip Scale, Flip Chip, and Advanced Chip Packaging Technologies, pp. 8.1–8.147.

[211] F. Rasheed, M. S. Golanbari, G. C. Marques, M. B. Tahoori, and J. Aghassi-Hagmann, "A smooth ekv-based dc model for accurate simulation of printed transistors and their process variations," *IEEE Transactions on Electron Devices*, vol. 65, no. 2, pp. 667–673, 2018.

[212] F. Rasheed, M. Hefenbrock, M. Beigl, M. B. Tahoori, and J. Aghassi-Hagmann, "Variability modeling for printed inorganic electrolyte-gated transistors and circuits," *IEEE Transactions on Electron Devices*, no. 99, pp. 1–7, 2018.

[213] L. Zimmermann, A. Scholz, M. B. Tahoori, J. Aghassi-Hagmann, and A. Sikora, "Design and evaluation of a printed analog-based differential physical unclonable function," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 11, pp. 2498–2510, 2019.

[214] C.-E. Yin, "A regression-based entropy distiller for ro pufs," Tech. Rep., 2011.

[215] C.-E. Yin and G. Qu, "Improving puf security with regression-based distiller," in *Proceedings of the 50th Annual Design Automation Conference*, 2013, pp. 1–6.

[216] L. Zimmermann, A. Scholz, M. B. Tahoori, A. Sikora, and J. Aghassi-Hagmann, "Hardware-intrinsic security with printed electronics for identification of ioe devices," in *2020 European Conference on Circuit Theory and Design (ECCTD)*. IEEE, 2020, pp. 1–4.

[217] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-allen and hamilton inc mclean va, Tech. Rep., 2001.

[218] L. T. Clark, S. B. Medapuram, and D. K. Kadiyala, "Sram circuits for true random number generation using intrinsic bit instability," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 10, pp. 2027–2037, 2018.

[219] Y. Hori, H. Kang, T. Katashita, and A. Satoh, "Pseudo-lfsr puf: A compact, efficient and reliable physical unclonable function," in *2011 International Conference on Reconfigurable Computing and FPGAs*. IEEE, 2011, pp. 223–228.

[220] Y. Gao, H. Ma, D. Abbott, and S. F. Al-Sarawi, "Puf sensor: Exploiting puf unreliability for secure wireless sensing," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 9, pp. 2532–2543, 2017.

[221] U. Ruhrmair and J. Solter, "Puf modeling attacks: An introduction and overview," in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2014.

[222] D. P. Sahoo, P. H. Nguyen, D. Mukhopadhyay, and R. S. Chakraborty, "A case of lightweight puf constructions: Cryptanalysis and machine learning attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 8, pp. 1334–1343, 2015.

[223] S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything you wanted to know about pufs," *IEEE Potentials*, vol. 36, no. 6, pp. 38–46, 2017.

[224] A. T. Erozan, R. Bishnoi, J. Aghassi-Hagmann, and M. B. Tahoori, "Inkjet-printed true random number generator based on additive resistor tuning," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2019, pp. 1361–1366.

[225] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT press, 2009.

[226] J. E. Beck and B. P. Woolf, "High-level student modeling with machine learning," in *International Conference on Intelligent Tutoring Systems*. Springer, 2000, pp. 584–593.

[227] W. Zhang, T. Du, and J. Wang, "Deep learning over multi-field categorical data," in *European conference on information retrieval*. Springer, 2016, pp. 45–57.

[228] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg *et al.*, "Scikit-learn: Machine learning in python," *the Journal of machine Learning research*, vol. 12, pp. 2825–2830, 2011.

[229] D. C. Liu and J. Nocedal, "On the limited memory bfgs method for large scale optimization," *Mathematical programming*, vol. 45, no. 1-3, pp. 503–528, 1989.

[230] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.

[231] M. S. Alkatheiri and Y. Zhuang, "Towards fast and accurate machine learning attacks of feed-forward arbiter pufs," in *2017 IEEE Conference on Dependable and Secure Computing*. IEEE, 2017, pp. 181–187.

[232] A. Scholz, D. Gerig, L. Zimmermann, M. Seiberlich, N. Strobel, G. Hernandez-Sosa, and J. Aghassi-Hagmann, “A hybrid optoelectronic sensor platform with an integrated solution-processed organic photodiode,” *Advanced Materials Technologies*, p. 2000172, 2020.

[233] A. Sikora, A. Walz, and L. Zimmermann, “Research aspects for secure communication in the industrial internet of things,” in *2020 International Conference on Dependable Systems, Services and Technologies (DESSERT2020)*. IEEE, 2020, pp. 1–6.

[234] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, “A review on internet of things (iot), internet of everything (ioe) and internet of nano things (iont),” in *2015 Internet Technologies and Applications (ITA)*. IEEE, 2015, pp. 219–224.

[235] B. Alluhaybi, M. S. Alrahhal, A. Alzhrani, and V. Thayananthan, “A survey: Agent-based software technology under the eyes of cyber security, security controls, attacks, and challenges.”

[236] M. Tehranipoor and C. Wang, *Introduction to hardware security and trust*. Springer Science & Business Media, 2011.

[237] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, “A review on authentication methods,” 2013.

[238] S. Bhunia, S. Ray, and S. Sur-Kolay, *Fundamentals of IP and SoC security*. Springer, 2017.

[239] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making use of manufacturing process variations: A dopingless transistor based-puf for hardware-assisted security,” *IEEE Transactions on Semiconductor Manufacturing*, vol. 31, no. 2, pp. 285–294, 2018.

[240] H. Ma, Y. Gao, O. Kavehei, and D. C. Ranasinghe, “A puf sensor: Securing physical measurements,” in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 2017, pp. 648–653.

[241] A. Aysu and P. Schaumont, “Hardware/software co-design of physical unclonable function based authentications on fpgas,” *Microprocessors and Microsystems*, vol. 39, no. 7, pp. 589–597, 2015.