Security Aspects of Printed Electronics Applications

Zur Erlangung des akademischen Grades eines

Doktors der Ingenieurwissenschaften

von der KIT-Fakultät für Informatik
des Karlsruher Instituts für Technologie (KIT)

genehmigte

Dissertation

von

Ahmet Turan Erozan

aus Sivas, Türkei

Tag der mündlichen Prüfung:	06.07.2020
Referent:	Prof. Dr. Mehdi Baradaran Tahoori, Karlsruhe Institute of Technology
Korreferent:	Prof. Dr. Jasmin Aghassi-Hagmann, Offenburg University of Applied Sciences, Karlsruhe Institute of Technology

To my family

Ahmet Turan Erozan
Tivoliplatz 1
76137 Karlsruhe

Hiermit erkläre ich an Eides statt, dass ich die von mir vorgelegte Arbeit selbstständig verfasst habe, dass ich die verwendeten Quellen, Internet-Quellen und Hilfsmittel vollständig angegeben haben und dass ich die Stellen der Arbeit - einschlielich Tabellen, Karten und Abbildungen - die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Karlsruhe, May 2020
Ahmet Turan Erozan

Acknowledgment

I would like to sincerely thank my advisers, Prof. Mehdi Tahoori and Prof. Jasmin Aghassi-Hagmann who continuously supported and encouraged me during my doctoral studies. I am grateful for insightful discussions we had throughout my research.

Words cannot express my gratitude to my family. Without them, this thesis would have been not possible. I am deeply grateful to my wife for her continuous support, understanding and technical discussions. My parents have always believed in me and encouraged me throughout my life for which I am thankful for. Besides, I thank my son who cheer me up in the last year of my PhD. I am indebted to them for their sacrifices to see me achieve this goal.

I would like to thank all of my colleagues in the Chair of Dependable Nano Computing and in MERAGEM Graduate School at Karlsruhe Institute of Technology for their technical as well as personal support. I especially thank Dr. Rajendra Bishnoi, Farhan Rasheed, Dr. Gabriel Cadilha Marques, Dr. Mohammad Saber Golanbari, Dennis Weller, Michael Hefenbrock, Dr. Arunkumar Vijayan, Dr. Shengcheng Wang, Dr. Anteneh Gebregiorgis, Sarath Mohanachandran Nair and Dr. Nour Sayed for their contributions, numerous technical discussions and invaluable support to my research.

I am thankful to Ms. Iris Schröder-Piepka and Ms. Siri Weiße for their friendly support and handling all the required documents during my PhD. I also thank Ms. Audrey Bohlinger for her help with the paperwork in the last months of my PhD.

Finally, I would like to thank The Ministry of Science, Research and Arts of the state of Baden-Württemberg for their financial support to my research in the form of MERAGEM Graduate School.

Abstract

Printed Electronics (PE) is an emerging technology that complements conventional technologies with its unique features, hence, the market of PE technology has rapidly increased from US$ 6B in 2010 to US$ 41B in 2019, and projected to grow US$ 153B in 2027. PE technology combines additive manufacturing and electronic functionality to enable the usage of various materials in the electronic components fabricated in the point-of-use, cost-effectively and environmentally friendly on a wide range of substrates that can be flexible, lightweight, transparent, large-area, and implantable. Therefore, PE technology enables the realization of envisioned applications such as smart packaging, disposables, smart labels, and electronic skin.

The progress of PE technology faces several challenges in yield, reliability, and performance that are primarily focused to advance PE technology. However, in recent years, the importance of security aspects of hardware platforms has been highlighted by numerous hardware-based attacks. Since the target PE applications can perform vital functionalities and contain sensitive information such as implantable devices and health monitoring patches, security flaws and trust issues in the supply chain can cause serious problems including fatality. Moreover, the unique features of PE technology such as additive manufacturing, larger feature sizes, fewer layers, and limited process steps result in more vulnerability to hardware-based attacks and new trust issues such as reverse engineering, counterfeiting, and hardware trojans. Besides, the adoption of countermeasures in conventional technologies is unsuitable and inefficient as such countermeasures introduce comparably high overhead to low-cost PE applications. Hence, this thesis provides a technology-specific assessment of hardware-level threats and their countermeasures in the form of resource-constrained hardware primitives to secure the supply-chain and functionalities of PE applications.

In the first contribution of this dissertation, we propose a printed Physical Unclonable Function (pPUF) design to provide secure keys that are used in several countermeasures such as authentication and fingerprinting. Also, we optimize the multi-bit pPUF design and achieve 31% area save for 16-bit key generation. Moreover, we develop an analysis framework including a Monte Carlo simulation flow for pPUF and perform simulation and fabrication-based analyses. The results show that pPUF has sufficient uniqueness and reliability metrics, and operates at the supply voltage of down to 0.5 V.

In the second contribution of this dissertation, we propose a compact printed True Random Number Generator (pTRNG) design to generate unpredictable keys for cryptographic functions and random authentication challenges. The pTRNG design mitigates the process variation using a printed resistor tuning method enabled by the customizable fabrication feature of PE so that the generated bits are mostly based on the random noise in the circuit, providing a true random behaviour. The simulation results demonstrate that the overall process variation of the TRNGs is mitigated by 110 times, and the generated bitstreams of TRNGs pass the National

Institute of Standards and Technology Statistical Test Suite. Moreover, the characterization results of fabricated TRNGs prove that the TRNGs generate random bitstreams at the supply voltage of down to 0.5 V.

The third contribution of this dissertation is to describe the unique features of PE circuit design and fabrication which differ from conventional technologies resulting in the necessity of a new reverse engineering (RE) methodology. Hereof, we propose a robust RE methodology based on supervised learning for PE circuits to demonstrate their vulnerabilities to RE attacks. The RE results show that the proposed methodology reverse engineers numerous PE circuits without complex and expensive tools.

In the last contribution, we propose a one-time programmable printed Look-up Table (pLUT) that implements any printed digital circuits and enables countermeasures such as camouflaging, split manufacturing, and watermarking against various hardware-level attacks. The comparison of the PE implementation of the existing and the proposed pLUT designs shows that the proposed pLUT outperforms other designs in terms of area usage, worst-case delay, and power consumption. The proposed pLUT design is simulated, fabricated, and programmed with inkjet-printed conductive ink to implement XNOR, XOR, and AND gates to prove the programmability of the proposed design. The simulation and characterization results prove the functionality of the pLUT at 1 V.

Zusammenfassung

Gedruckte Elektronik (Printed Electronics (PE)) ist eine neu aufkommende Technologie welche komplementär zu konventioneller Elektronik eingesetzt wird. Dessen einzigartigen Merkmale führten zu einen starken Anstieg von Marktanteilen, welche 2010 \$6 Milliarden betrugen, \$41 Milliarden in 2019 und in 2027 geschätzt \$153 Milliarden. Gedruckte Elektronik kombiniert additive Technologien mit funktionalen Tinten um elektronische Komponenten aus verschiedenen Materialien direkt am Verwendungsort, kosteneffizient und umweltfreundlich herzustellen. Die dabei verwendeten Substrate können flexibel, leicht, transparent, großflächig oder implantierbar sein. Dadurch können mit gedruckter Elektronik (noch) visionäre Anwendungen wie Smart-Packaging, elektronische Einmalprodukte, Smart Labels oder digitale Haut realisiert werden.

Um den Fortschritt von gedruckten Elektronik-Technologien voranzutreiben, basierten die meisten Optimierungen hauptsächlich auf der Erhöhung von Produktionsausbeute, Reliabilität und Performance. Jedoch wurde auch die Bedeutung von Sicherheitsaspekten von Hardware-Plattformen in den letzten Jahren immer mehr in den Vordergrund gerückt. Da realisierte Anwendungen in gedruckter Elektronik vitale Funktionalitäten bereitstellen können, die sensible Nutzerdaten beinhalten, wie zum Beispiel in implantierten Geräten und intelligenten Pflastern zur Gesundheitsüberwachung, führen Sicherheitsmängel und fehlendes Produktvertrauen in der Herstellungskette zu teils ernsten und schwerwiegenden Problemen. Des Weiteren, wegen den charakteristischen Merkmalen von gedruckter Elektronik, wie zum Beispiel additive Herstellungsverfahren, hohe Strukturgröße, wenige Schichten und begrenzten Produktionsschritten, ist gedruckte Hardware schon per se anfällig für hardware-basierte Attacken wie Reverse-Engineering, Produktfälschung und Hardware-Trojanern. Darüber hinaus ist die Adoption von Gegenmaßnahmen aus konventionellen Technologien unpassend und ineffizient, da solche zu extremen Mehraufwänden in der kostengünstigen Fertigung von gedruckter Elektronik führen würden. Aus diesem Grund liefert diese Arbeit eine Technologie-spezifische Bewertung von Bedrohungen auf der Hardware-Ebene und dessen Gegenmaßnahmen in der Form von Ressourcen-beschränkten Hardware-Primitiven, um die Produktionskette und Funktionalitäten von gedruckter Elektronik-Anwendungen zu schützen.

Der erste Beitrag dieser Dissertation ist ein vorgeschlagener Ansatz um gedruckte Physical Unclonable Functions (pPUF) zu entwerfen, welche Sicherheitsschlüssel bereitstellen um mehrere sicherheitsrelevante Gegenmaßnahmen wie Authentifizierung und Fingerabdrücke zu ermöglichen. Zusätzlich optimieren wir die multi-bit pPUF-Designs um den Flächenbedarf eines 16-bit-Schlüssels-Generators um 31% zu verringern. Außerdem entwickeln wir ein Analyse-Framework basierend auf Monte Carlo-Simulationen für pPUFs, mit welchem wir Simulationen und Herstellungs-basierte Analysen durchführen können. Unsere Ergebnisse haben gezeigt, dass die pPUFs die notwendigen Eigenschaften besitzen um erfolgreich als Sicherheitsanwendung eingesetzt zu werden, wie Einzigartigkeit der Signatur und ausreichende Robustheit. Der

Betrieb der gedruckten pPUFs war möglich bis zu sehr geringen Betriebsspannungen von nur 0.5 V.

Im zweiten Beitrag dieser Arbeit stellen wir einen kompakten Entwurf eines gedruckten physikalischen Zufallsgenerator vor (True Random Number Generator (pTRNG)), welcher unvorhersehbare Schlüssel für kryptographische Funktionen und zufälligen "Authentication Challenges" generieren kann. Der pTRNG Entwurf verbessert Prozess-Variationen unter Verwendung von einer Anpassungsmethode von gedruckten Widerständen, ermöglicht durch die individuelle Konfigurierbarkeit von gedruckten Schaltungen, um die generierten Bits nur von Zufallsrauschen abhängig zu machen, und damit ein echtes Zufallsverhalten zu erhalten. Die Simulationsergebnisse legen nahe, dass die gesamten Prozessvariationen des TRNGs um das 110-fache verbessert werden, und der zufallsgenerierte Bitstream der TRNGs die "National Institute of Standards and Technology Statistical Test Suit"-Tests bestanden hat. Auch hier können wir nachweisen, dass die Betriebsspannungen der TRNGs von mehreren Volt zu nur 0.5 V lagen, wie unsere Charakterisierungsergebnisse der hergestellten TRNGs aufgezeigt haben.

Der dritte Beitrag dieser Dissertation ist die Beschreibung der einzigartigen Merkmale von Schaltungsentwurf und Herstellung von gedruckter Elektronik, welche sehr verschieden zu konventionellen Technologien ist, und dadurch eine neuartige Reverse-Engineering (RE)-Methode notwendig macht. Hierfür stellen wir eine robuste RE-Methode vor, welche auf Supervised-Learning-Algorithmen für gedruckte Schaltungen basiert, um die Vulnerabilität gegenüber RE-Attacken zu demonstrieren. Die RE-Ergebnisse zeigen, dass die vorgestellte RE-Methode auf zahlreiche gedruckte Schaltungen ohne viel Komplexität oder teure Werkzeuge angewandt werden kann.

Der letzte Beitrag dieser Arbeit ist ein vorgeschlagenes Konzept für eine "one-time programmable" gedruckte Look-up Table (pLUT), welche beliebige digitale Funktionen realisieren kann und Gegenmaßnahmen unterstützt wie Camouflaging, Split-Manufacturing und Watermarking um Attacken auf der Hardware-Ebene zu verhindern. Ein Vergleich des vorgeschlagenen pLUT-Konzepts mit existierenden Lösungen hat gezeigt, dass die pLUT weniger Flächenbedarf, geringere worst-case Verzögerungszeiten und Leistungsverbrauch hat. Um die Konfigurierbarkeit der vorgestellten pLUT zu verifizieren, wurde es simuliert, hergestellt und programmiert mittels Tintenstrahl-gedruckter elektrisch leitfähiger Tinte um erfolgreich Logik-Gatter wie XNOR, XOR und AND zu realisieren. Die Simulation und Charakterisierungsergebnisse haben die erfolgreiche Funktionalität der pLUT bei Betriebsspannungen von nur 1 V belegt.

Table of Contents

List of Figures

List of Tables

1 Introduction

In the era of digitalization, products enabled by the advances in electronics have massively driven the market in almost every application fields such as communication, household appliances, automotive, internet of things, education, research, medical, and security. Moreover, the rapid growth in the semiconductor field, as projected in Moore's law, has enabled the development of new products or upgrading the existing ones in terms of functionality, speed and compactness [18, 19, 20]. However, conventional electronics has become incapable in addressing the increased demand for emerging applications such as the internet of disposable things (IoDT) [21] and electronic skin (e-skin) [22] due to their complex fabrication processes, mechanical properties, and minimum cost limitations.

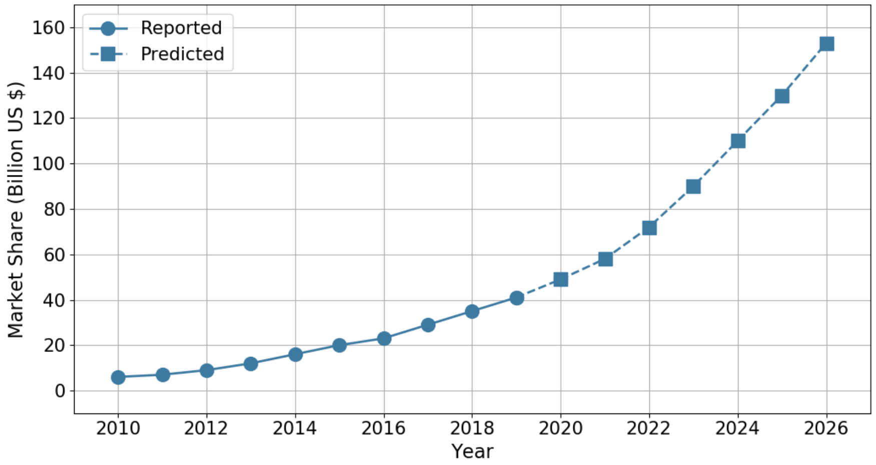


Figure 1.1: Reported and predicted market growth of Printed Electronics [1, 2].

Printed Electronics (PE) is a complementary technology of conventional silicon-based electronics, targeting several emerging applications. The market for PE has increased from US$ 6B in 2010 to US$ 41B in 2019, and is projected to grow US$ 153B in 2027 [1, 2], as shown in Figure 1.1. PE employs additive printing techniques, broadly known for conventional printing, in the manufacturing of electronics. The combination of additive manufacturing and electronic functionality allows the usage of various functional materials in fabricating electronic components on a broad range of substrates such as glass, flexible foil, textiles, and paper. This provides advantages or new functionalities such as low-cost, on-demand, customizable fabrication, and mechanical flexibility that are unachievable by other manufacturing processes. PE applications can be flexible, stretchable, lightweight, transparent, large-area, bio-compatible, and/or implantable and manufactured in point-of-use, cost-effective, and environmentally friendly processes. Therefore, the realization of several envisioned applications such as smart packaging [23], e-skin [22], health monitoring patches [24], smart cards [25], smart labels [26] and IoDT [21] can benefit from the promising features of PE [27]. Figure 1.2 presents some examples of

PE applications developed by industry and research institutions.

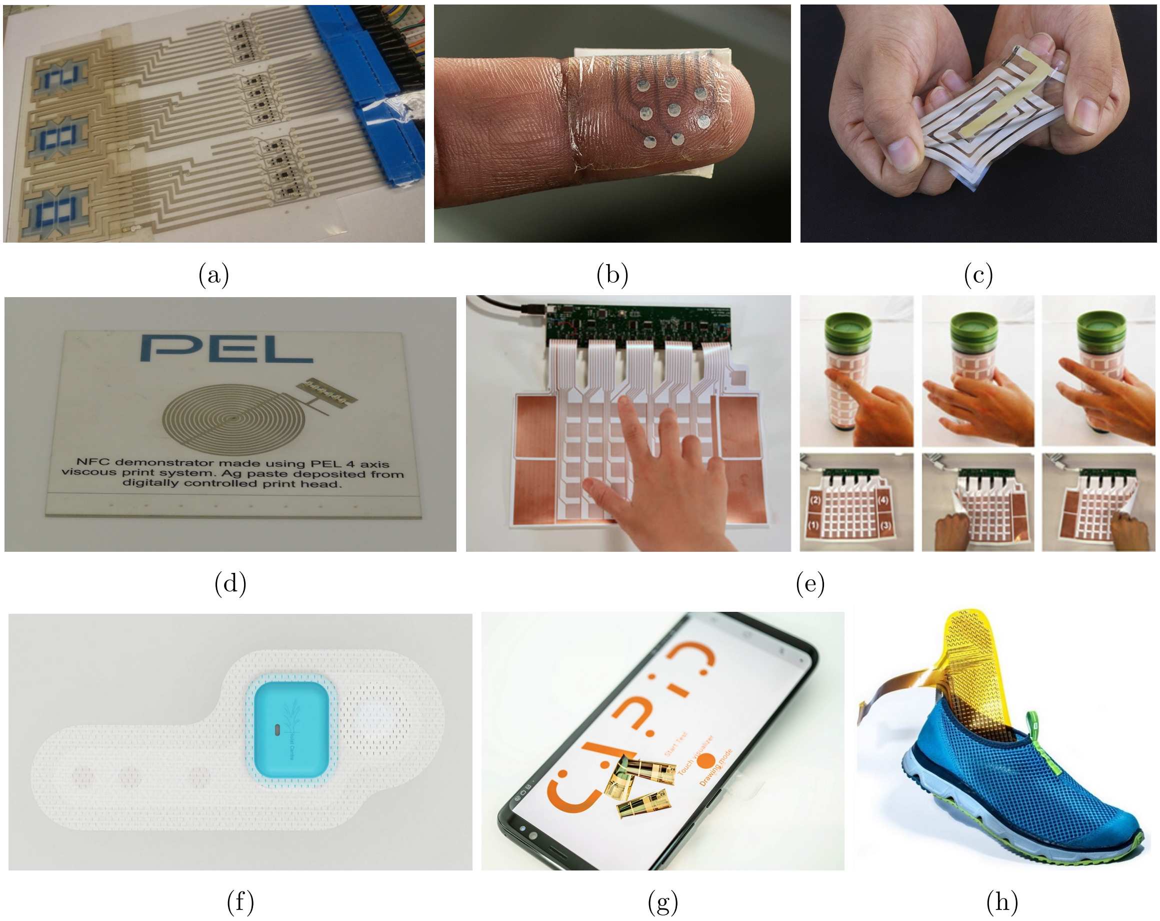

(a)
(b)
(c)
PEL
NFC demonstrator made using PEL 4 axis viscous print system. Ag paste deposited from digitally controlled print head.
(1)
(2)
(3)
(4)
(d)
(e)
(f)
(g)
(h)

Figure 1.2: Examples of Printed Electronics applications. (a) Printed electrochromic display on flexible substrate [3]. (b) Tacttoo: thin and feel-through tattoo for on-skin tactile output [4]. (c) BodyNet sticker: wireless sensors that stick to skin to track health indicators [5]. (d) Printed energy harvesting circuit [3]. (e) PrintSense: on-surface sensing technique for planar, curved and flexible surfaces [6]. (f) Comfortable, disposable health patch with long battery life to measure vital signs [7]. (g) Flexible tags that communicate with standard touch screens [8, 9]. (h) Intelligent shoe sole that measures distribution of pressure of foot [10].

PE components are manufactured using several printing processes instead of complex photolithography based subtractive process which are expensive as well as environmentally hazardous. Some prominent examples of additive printing processes are screen printing, flexography printing, offset printing, gravure printing, and inkjet printing [27]. Depending on the application, one or multiple printing methods can be used in the manufacturing process. Due to their maskless fabrication process, some of these processes such as inkjet printing enable a highly demanding feature that is customizable/personalized fabrication at the point-of-use [27, 28]. Personalized fabrication allows users to select their material and substrate according to their application, and fabricate fully custom designs without profound expertise, sophisticated and extremely expensive manufacturing tools.

Various printed transistors such as p-type organic-based thin-film transistors (OTFTs) [29], organic field-effect transistors (OFETs) [30], and n-type organic transistors [31, 32] are demonstrated to construct functional PE circuits. However, these transistors mostly suffer from the high supply voltage and low mobility making them unsuitable for low-power applications. On the other hand, inorganic semiconductor-based transistors combined with an electrolyte gate, called electrolyte-gated transistors (EGTs), provide high mobility and require low supply voltage ($\leq 1\,\mathrm{V}$), paving the way for low-power PE applications [12]. Due to their promising electrical characteristics, the fabrication of proposed circuits in this thesis are performed using EGTs.

Although PE is a promising field, several challenges have to be addressed by a wide range of experts from different scientific backgrounds to advance this technology. Yield, reliability, performance, supply-chain, and life-cycle aspects are some examples of challenges that need to be thoroughly considered while developing PE technology. However, given the fact that the target applications of PE can perform vital functionalities such as implantable devices for healthcare and/or contain sensitive information such as health monitoring patches, the security aspects of PE applications should be also carefully examined while advancing the technology. Thus, while PE fundamentally transforms the usage areas of electronics, it should exhibit trusted and secure applications.

1.1 Problem Statement and Objective

The advancement of PE brings about security concerns since most of PE applications are pervasive, containing vital functionalities and sensitive information. Any security flaw or trust issue in the supply chain can cause severe problems including fatality. While developing such technologies, the security challenges of their applications should be equally considered with other fundamental challenges such as yield, reliability, and performance. On the other hand, unlike the cost of silicon-based integrated circuits (ICs) applications such as server chips, these applications are expected to be highly cost-effective. For instance, PE applications like the Internet of Disposable Things (IoDT) target cost-effective products, and the overhead of securing the product should not exceed a certain percentage of such product costs. Therefore, the security aspects of PE should be carefully examined, and lightweight and compact security solutions have to be provided.

The security aspects of PE differ from the security of silicon-based ICs in terms of technical properties and supply chain. The unique features of PE such as additive manufacturing, larger feature sizes, transparent layers, fewer layers, and limited process steps contrast to that of the silicon-based ICs such as subtractive manufacturing, packaging, smaller feature sizes down to nanometers, opaque and stacked layers and various process steps These differences make PE applications more vulnerable to hardware-based attacks such as reverse engineering, counterfeiting, and malicious circuit modification. Moreover, although the point-of-use manufacturing of PE allows removing the cost of transportation from the overall cost of products, it can lead to new intellectual property (IP) piracy and IC overbuilding models at the point-of-use which does not exist in the supply chain of silicon-based ICs. Also, the direct adoption of existing countermeasures is comparably unsuitable in terms of overhead considering the cost-effectiveness of PE applications. Therefore, the technology-specific threat models against the security of PE applications should be reconsidered, and the compact countermeasures to thwart such threats should be provided in a way that they secure the PE applications with the help of compact hardware primitives, in other words, resource-constrained circuits.

The objective of the thesis is to provide a technology-specific assessment of hardware-level threats and their countermeasures in the form of resource-constrained circuits to secure the supply-chain and functionalities of PE applications at the hardware level. In this regard, we have proposed a printed Physical Unclonable Function (PUF) and a printed True Random Number Generator (TRNG) that generates unclonable and random keys to utilize in several countermeasures against hardware-based attacks and provide secure communication and authentication to PE applications. Moreover, we have proposed a robust reverse engineering method for PE circuits and demonstrated their vulnerability to such attacks. Furthermore, we have proposed a printed Look-up Table based programmable circuit that can be used to thwart hardware-based attacks including reverse engineering, IP piracy, and overbuilding in the supply chain. The common property of proposed hardware primitives is their low-overhead designs compared to silicon-based counterparts, which are achieved by exploiting the technology-specific features of PE. The overview of possible hardware-level attacks, corresponding countermeasures, and the usage of proposed hardware primitives in such countermeasures in the context of PE security is shown in Figure 1.3. The detailed contributions of this thesis are elaborated in the following section.

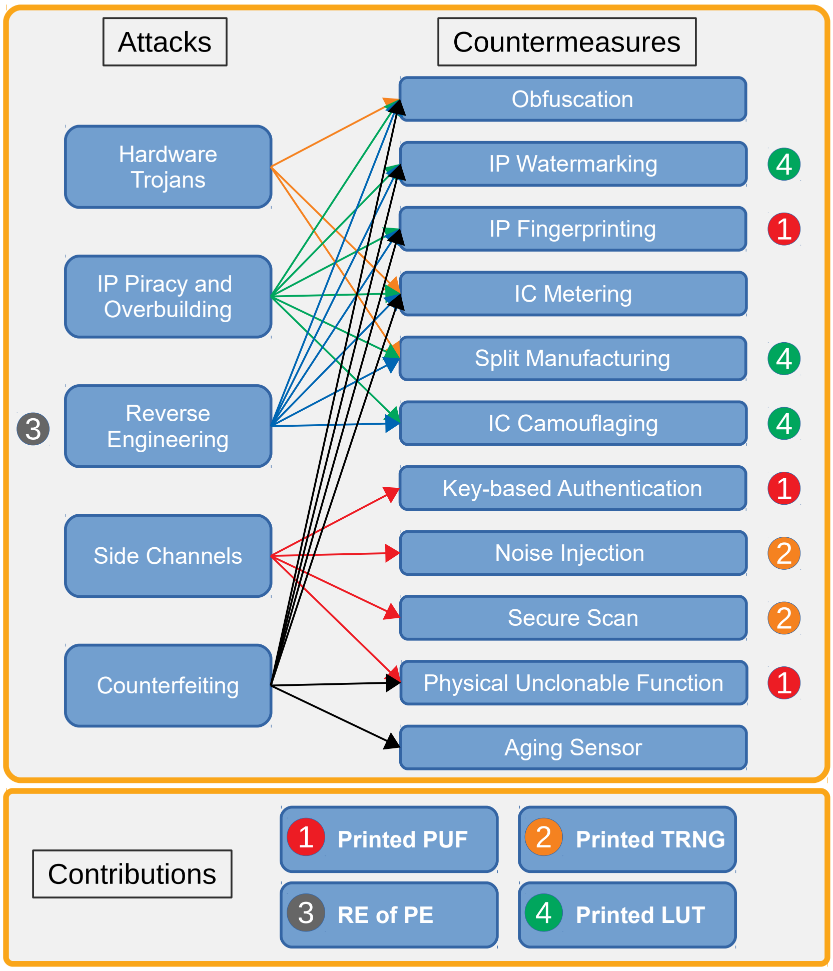


Figure 1.3: Overview of hardware-level attacks, countermeasures, and contributions of this thesis in different security aspects of printed electronics. (1) Printed Physical Unclonable Function, (2) Printed True Random Number Generator, (3) Reverse Engineering of Printed Electronics, (4) Printed Look-up Table

1.2 Thesis Contributions

1.2.1 Inkjet-Printed Physical Unclonable Function

Since pervasive PE applications need secure communication and/or authentication, it is imperative to embed security primitives for cryptographic key and authentication purposes into the applications. Physical unclonable functions (PUFs) have been adopted widely to provide secure keys, which are extracted from uncontrollable process variations in manufacturing. This work presents the design, simulation, fabrication, and measurements of a printed PUF [13, 33, 12]. A comprehensive framework, including Monte Carlo simulations calibrated on real device measurements, is developed to evaluate the proposed PUF. Moreover, a multi-bit printed PUF design is proposed to optimize the area usage. Our simulation results show that the printed PUF has ideal uniqueness (50.1%) and good reliability (89%). Moreover, the proposed multi-bit printed PUF reduces the area usage around 30%. The proposed PUF was fabricated and the experimental results confirm that the printed PUF can operate reliably at as low as 0.5 V, and hence, it is a remarkable candidate to be utilized in low-power PE applications.

1.2.2 Compact True Random Number Generator based on Inkjet-Printing Technology

True Random Number Generators (TRNGs) are required to generate unpredictable random bits by digitizing unpredictable natural phenomenons (entropy source) such as thermal noise to random bits for security purposes such as cryptographic functions, random challenges for authentication, and noise injection for side-channel attacks, which secure the operation of pervasive PE applications. Since the digitization of entropy sources must be performed in a way that the bias introduced by TRNGs is negligible, the process variation of TRNGs should be mitigated. However, since the additive fabrication processes of PE circuits result in high intrinsic variation due to the random dispersion of the printed inks on the substrate, constructing a printed TRNG is challenging. In this work, we propose a compact TRNG design, which exploits the additive customizable fabrication feature of inkjet printing [34, 35]. We propose an additive resistor tuning flow for the TRNG circuit to mitigate the overall process variation of the TRNG so that the generated bits are mostly based on the random noise in the circuit, providing a true random behavior. The simulation results show that the overall process variation of the TRNGs is mitigated by 110 times, and the generated bitstream of tuned TRNGs pass the National Institute of Standards and Technology Statistical Test Suite. For proof-of-concept, the proposed TRNG circuit was fabricated and tuned. The characterization results of tuned TRNGs prove that the TRNGs generate random bitstreams at the supply voltage of down to 0.5 V. Furthermore, the proposed TRNG occupies 4.59 mm^2 which is less than 1% of the area usage of PE implementation of a silicon-based counterpart. Hence, the proposed TRNG design is a promising candidate to secure low-power applications in this domain.

1.2.3 Reverse Engineering of Printed Electronics Circuits

The custom fabrication is a key feature of PE technology, enabling customization per application, even in small quantities due to low-cost printing compared to lithography. However, the personalized and on-demand fabrication, the non-standard circuit design and the limited number of printing layers with larger geometries compared to traditional silicon-based ICs, open doors for new and unique reverse engineering (RE) schemes for this technology. In this work, we present a robust RE methodology based on supervised machine learning, starting from image acquisition to netlist extraction of PE circuits to demonstrate their vulnerability to RE attacks [36]. The results show that the proposed RE methodology can reverse engineer numerous PE circuits with very limited manual effort, and is robust against non-standard circuit design, customized layouts and high variations resulting from the inherent properties of PE manufacturing processes.

1.2.4 Printed Look-Up Table-based Programmable Printed Digital Circuit

The supply-chain of PE applications is vulnerable to several attacks due to the properties of PE such as larger feature sizes, transparent and fewer layers, and limited process steps. Therefore, attacks like reverse engineering, counterfeiting, IP piracy, and overbuilding are rather easy. PE applications that are used in critical functionalities have to be protected against such attacks since they can lead to severe problems. In this work, we propose a one-time programmable printed Look-up Table (pLUT) that implements any printed digital circuits and can be used for IC camouflaging, split manufacturing and IP watermarking to thwart the attacks in the supply-chain [37]. The proposed pLUT implementation is simulated, fabricated, and programmed with inkjet-printed conductive ink as XNOR, XOR, and AND logic gate functionalities to prove the programmability of the proposed pLUT design. The characterization results show that the fabricated pLUT operates at 1 V. Furthermore, the usage cases of the proposed pLUT in the context of security countermeasures, yield, and performance improvements are discussed.

1.3 Outline

This chapter presents the problem statement, objective, and contributions of this thesis. The remainder of the thesis is organized into six chapters:

- Chapter 2 provides background information on Printed Electronics Technology, Physical Unclonable Functions, True Random Number Generators, and Reverse Engineering.
- Chapter 3 presents the first printed Physical Unclonable Function. The analysis framework for the printed PUF design is explained. The simulation-based analysis of the printed PUF using the framework is performed, and the fabrication-based analysis is presented as a proof-of-concept.
- Chapter 4 presents the first printed True Random Number Generator based on inkjet-printing technology and the additive printed resistor used in the TRNG design. The simulation-based analysis of the printed TRNG is conducted, and the fabrication-based analysis to prove the concept of the proposed TRNG design is demonstrated.
- Chapter 5 describes the need for a new reverse engineering methodology for PE circuits

and presents the proposed reverse engineering methodology for Printed Electronics circuits. The proposed RE methodology is applied to several PE circuits to demonstrate their vulnerabilities to the RE attack.

- Chapter 6 presents first printed LUT-based one-time programmable printed digital circuits and its fabrication and configuration flow. The simulation-based and fabrication-based analyses of the pLUT are reported. The utilization of the pLUT in PE applications for security, yield, and performance improvements is discussed.
- Chapter 7 finally concludes the thesis and provides an outlook for future research directions.

2 Background

This chapter presents the preliminary information required to understand the contributions of this thesis. In this context, we first provide an overview of Printed Electronics Technology. Moreover, the basics of Physical Unclonable Functions, True Random Number Generators, and Reverse Engineering are described.

2.1 Printed Electronics

Printed Electronics is drawing significant attention for contributing to applications where low-cost, mechanical flexibility, on-demand fabrication, lightweight, and/or large area play an important role [1, 2, 38]. It is likely to complement silicon-based electronics which shows limitations in fields of flexible electronics, disposable electronics, large-area applications, and highly customizable circuitry. Moreover, thanks to its feature of point-of-use manufacturing, it also addresses the ultra-low-cost applications where the transportation cost from the fabrication site to point-of-use might be unaffordable compared to product cost [37, 21].

The market driver applications of PE are radio frequency identification (RFID) tags [39, 40, 41, 42], sensor arrays [43, 44, 45], photo-voltaic cells [46], batteries [47, 48] and displays [49, 50]. In addition, some envisioned applications are internet of disposable things (IoDT), electronic skin (e-skin), dynamic newspapers, smart labels, smart sensors, smart cards, health care diagnosis devices, energy harvesters and smart clothing [21, 22, 27, 25, 26, 24, 51].

PE circuits and systems are manufactured by printing the functional materials additively on a flexible or rigid substrate. Figure 2.1 shows typical subtractive and additive processing steps to manufacture a structure. In subtractive manufacturing, masks, lithography and etching processes, and steps, which are complex, expensive, and environmentally hazardous, are used. Contrarily, additive manufacturing enables ultra-low-cost and simple fabrication of several materials to the point-of-interest on a substrate owing to the mask-less fabrication. This allows printing various materials easily in different shapes for several functionalities [27, 11].

Various printing methods are used to serve different application purposes. These additive printing processes are inkjet, aerosol jet, electrohydrodynamic jet, gravure, flexography, screen, and reverse offset printing. Some key parameters of these printing methods are given in Table 2.1. One of the prominent additive printing processes is inkjet printing, which receives great interest as a technique for printing electronic circuits. Its simplicity of applying custom changes and affordable tools make personalized and customizable fabrication possible even for end-users. Users can change the design, manufacture, and develop their components and circuitry according to their needs.

In the field of PE, various printed materials and processes have been developed to construct functional PE circuits. The organic material based transistors such as p-type organic-based thin-film transistors (OTFTs) [29, 52], organic field-effect transistors (OFETs) [30], are some

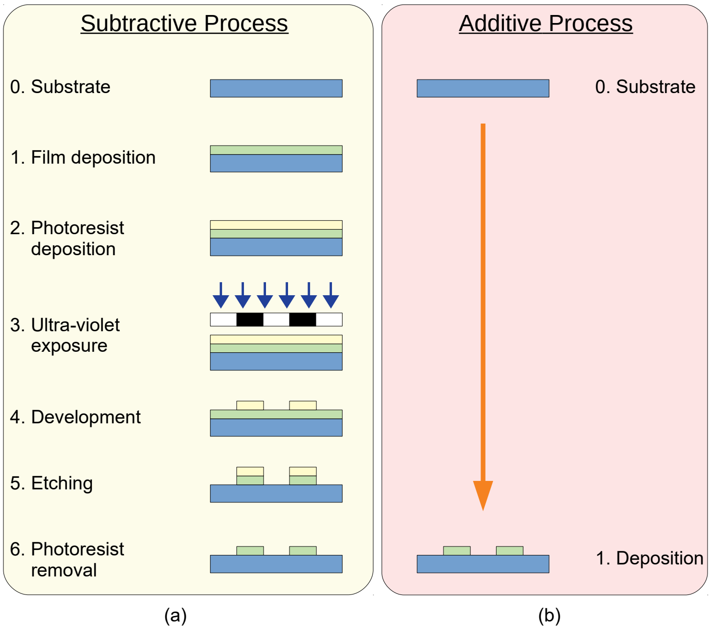


Figure 2.1: Processing steps to pattern a structure in a typical (a) subtractive process involving etching, (b) fully-additive process [11].

Table 2.1: Comparison of printing methods used in the manufacturing of PE [15].

Method/Feature	Resolution (μm)	Line width (μm)	Throughput (m^2s^-1)
Inkjet	2	2-8	≤ 1
Aerosol jet	10	10	≤ 0.01
Electrohydrodynamic jet	2	2	≤ 0.01
Gravure	2	35	≥ 1
Flexography	1	3	≥ 0.01
Screen	100	40	≥ 0.01
Reverse offset	1	2	0.01-1

of the early examples in this field. In addition, some n-type organic transistors are presented in literature [31, 32]. These transistors suffer from low mobility and high supply voltage requirement. To overcome these shortcomings, oxide-based semiconductors are used which together with electrolyte gating to provide high mobility and high gate capacitance, enabling low voltage operations, which fits the requirements of energy harvested and battery-backed low power applications [53, 54, 55, 12, 56, 57]. Therefore, we have used oxide-based n-type electrolyte-gated transistors (EGTs) in this work since EGTs enable the operation of circuits below 1 V [12, 13, 58, 37, 59]. However, due to the lack of well-performing p-type EGTs, the circuits are currently based on transistor-resistor logic designed with n-type EGTs in the pull-down network and a resistor as a replacement of p-type EGTs [12, 60, 61, 62].

In the fabrication process of EGTs, the channel material, indium oxide (In_2O_3) semiconductor, is inkjet printed to form the channel between drain and source electrodes which are made of lithographically structured indium tin oxide (ITO). Afterward, the electrolyte is inkjet printed on the top of the channel acting as the gate dielectric. Lastly, on top of the electrolyte, PEDOT:PSS is inkjet printed as a top gate in a way that it overlaps the channel area [63]. The cross-sectional view, top view, fabrication process, and the optical image of an EGT is shown in Figure 2.2 while Figure 2.3 shows the output curve measurement of a fabricated EGT with the dimensions of 100 μm width and 40 μm length. Although some passive structures, in the current development stage of this technology, are patterned, it still has the printing features of PE since the other parts are inkjet-printed.

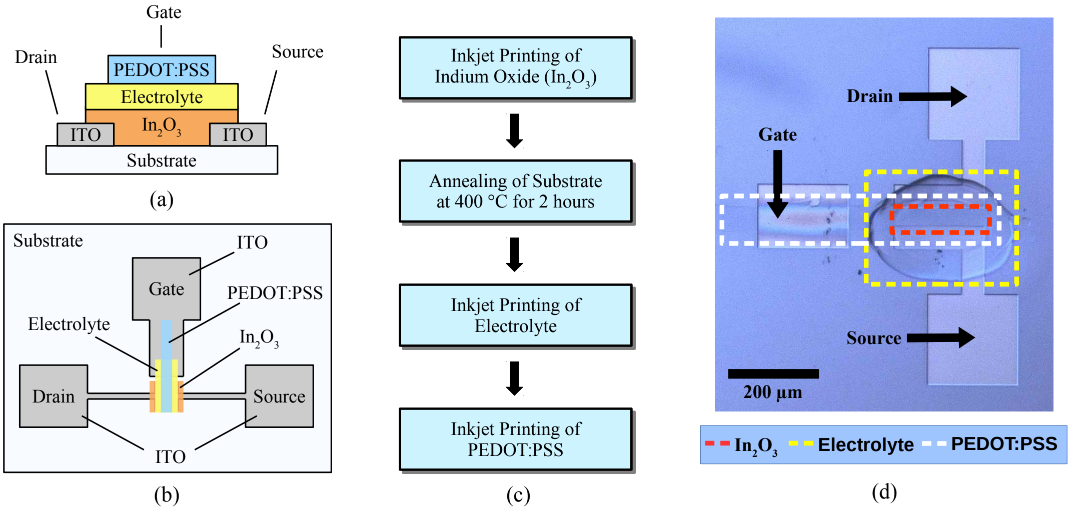

Gate
Drain
Source
PEDOT:PSS
Electrolyte
In_2O_3
ITO
ITO
Substrate
(a)
Substrate
ITO
Gate
PEDOT:PSS
Electrolyte
In_2O_3
Drain
Source
ITO
(b)
Inkjet Printing of Indium Oxide (In_2O_3)
Annealing of Substrate at 400 °C for 2 hours
Inkjet Printing of Electrolyte
Inkjet Printing of PEDOT:PSS
(c)
Drain
Gate
Source
200 µm
In_2O_3 Electrolyte PEDOT:PSS
(d)

Figure 2.2: Description of Electrolyte-gated transistor (EGT) technology. (a) Cross-sectional view of EGT. (b) Top view of EGT. (c) Fabrication process of EGT. (d) Optical image of a fabricated EGT device [12, 13].

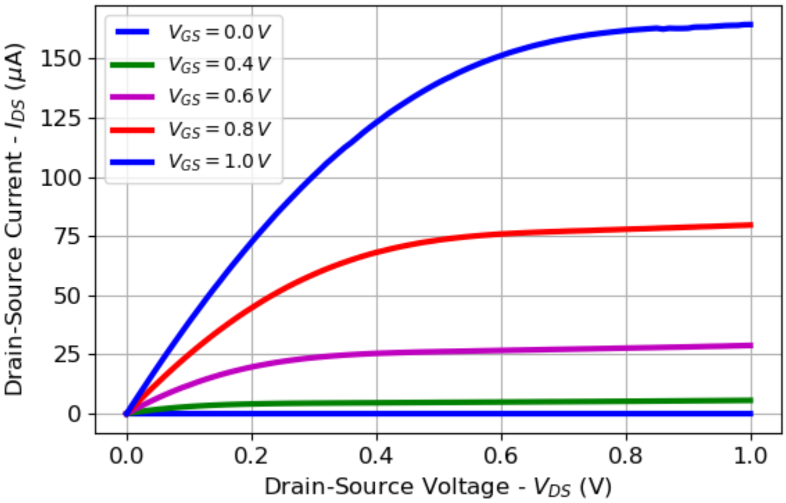
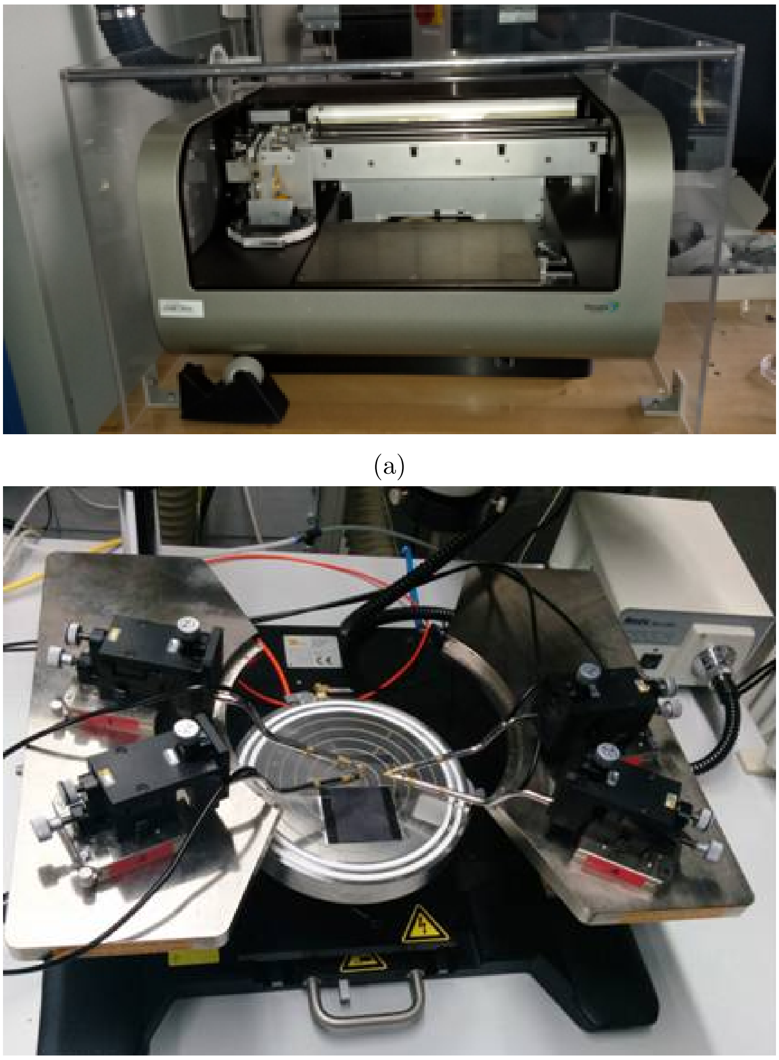


Figure 2.3: Measured output curves (I_{DS}-V_{DS}) at different Gate-Source Voltage (V_{GS}) of an EGT (width = 100 μm, length = 40 μm).

The research directions on PE circuits are focused on printed transistors as well as other circuit elements [29, 30, 12]. Moreover, there are some examples of printed circuits in literature such as inverters, latches, and ring oscillators (RO) contains limited numbers of elements

[64, 61, 62, 65, 66]. The large scale integration of printed transistors suffers from the high variation, low yield, and low performance of low-cost manufacturing printing processes such as inkjet printing. Moreover, to the best of our knowledge, the reported highest operation frequency of a printed RO in [64] is 1300 Hz. Although improving the performance of PE circuits is still investigated by researchers, the current performance can be sufficient for many PE applications.

The fabrication of printed structures in this thesis is performed using Dimatix DMP-283 inkjet-printer as shown in Figure 2.4a. Moreover, devices and circuits are contacted through a Süss Microtech probe station shown in Figure 2.4b. The fabrication and characterization setup of devices and circuits in the following chapters are elaborated in the corresponding chapter.



(a)

(b)

Figure 2.4: (a) Dimatix DMP-2831 Inkjet-Printer used for fabrication. (b) Süss Microtec Probe Station used for characterization.

2.2 Physical Unclonable Function

PUFs have been widely used to provide secret keys [67]. It derives digital signatures from intrinsic manufacturing process variations. The inherent variations make signatures unpredictable. Thus the signatures can be used as a key for security and authentication [68, 69].

A PUF is a function that produces a response corresponding to the challenge it receives [68]. Since the relation between challenges and responses is unpredictable, it is represented as a black box function with challenge-response pairs. PUFs are categorized as weak PUFs that provide few secret keys and are used for the key storage of cryptographic algorithms, and strong PUFs which provide numerous secret keys depending on their inputs and are used for authentication purposes [68].

The PUF metrics such as uniqueness and reliability are used to evaluate the performance of the PUFs. The uniqueness and reliability metrics are calculated using the definition of the Fractional Hamming Distance (FHD) which is given in Equation 2.1.

$$FHD(A,B) = \frac{1}{N}\sum_{i=1}^{N}|A_i - B_i| \tag{2.1}$$

where A and B denote two different bit arrays containing N bits while i denotes the bit index. Thus the FHD calculates the fraction of the bits which differs from A to B.

The uniqueness metric indicates how unique the responses of the PUFs are. It is obtained by calculating the FHD of every two PUF responses. The average of the uniqueness of an ideal PUF should be 50% [70]. The reliability metric explains the stability of the PUF response in the presence of different environmental and noise conditions. It is obtained by calculating the FHD between the reference PUF response and the PUF response in different environmental and noise conditions. In an ideal case, the reliability should be 100%.

PUFs enable applications that would be impossible to construct otherwise because of their unique properties as hardware primitives. Some of these applications that are made possible or improved by the use of PUFs are identification and entity authentication, anti-counterfeiting, key generation, key storage, and hardware-software binding.

Identification is being able to produce identifying information without any proof whether this information is valid, or even belongs to the entity presenting it while authentication requires the proof of the validity of the identifying information, and the entity presenting the proof at the time the proof was requested. Conventional electronic identification and authentication methods are based on presenting some form of the serial number as identifiers that are inherently clonable regardless of how well protected they are. Therefore, they only provide a reasonable level of authentication as long as it is guaranteed that the identifying information has not been stolen or copied. A PUF-based authentication system does not have this problem due to its unclonability feature. A set of challenge-response pairs for each PUF instance is pre-stored. Later, Each PUF can be authenticated by comparing its response to the pre-stored response for the same challenge [71].

Anti-counterfeiting is the same as authentication from a technology point of view, but, it is not an everyday application of cryptographic technology. Traditional non-electronic anti-counterfeiting methods rely on incorporating difficult to manufacture artifacts in a product such as embedding watermarks onto banknotes, which are naturally expensive [72]. Since a cheaper electronic method in many products is much more preferred, one of the first suggested applications for PUFs is anti-counterfeiting [73]. A manufacturer stores a set of challenge-response pairs for each product containing the PUF. To verify a product's genuineness, a challenge is applied, and the returned response is compared with the stored one. In this way, PUFs enhance the anti-counterfeiting of products by introducing the unclonability over a serial number.

Secret key generation and storage are necessary to store a secret key to perform encryption and decryption. According to Kerckhoff's principle, the secrecy of the key is fundamental for the security of the system. Conventionally, the key is stored in non-volatile memories (NVM) such as flash memory, EEPROM, anti-fuse, or battery-backed SRAM. The secret key generated using a true random number generator (TRNG) is stored in the NVM. The programming interface of the NVM also has to be disabled permanently to avoid possible attacks. The security of such a system depends on that the NVM is not accessible by an adversary. However, this is difficult to fulfill, since one can reverse engineer the chip and try to read-out the content electrically or apply different attack techniques on the NVM [74, 75]. PUFs can improve the key generation and storage because of its advantages. A remarkable advantage of PUFs is that the physical security of PUFs has better resilience against adversarial attacks since measuring the process variation is rather difficult.

2.3 True Random Number Generator

Cryptographic algorithms are the crucial points for securing systems and True Random Number Generators (TRNGs) are essential building blocks of embedded security systems. They provide secret keys, initialization vectors, random challenges, and data padding, masking against differential power analysis (DPA), and one-time password (OTP) [76, 35] to enable various cryptographic algorithms, protocols and secured implementations. The security of these applications depends on the unpredictability and uniformity of the utilized random numbers. The most common cause of failure in security systems results from a design flaw or an active attack on the used TRNG [27, 9] rather than to a broken cryptographic algorithm or an unprotected implementation [77, 78]. Because of their importance for security, TRNGs are strictly evaluated in the process of industrial certification.

All standards categorize Random Number Generators (RNGs) into two main types. TRNGs harness true randomness from unpredictable physical sources such as the timing jitter, the thermal noise, or the final state of a metastable element while PRNGs are deterministic algorithms that expand a short input sequence generated by TRNGs and produce a longer random-like sequence. Unlike TRNGs where physical phenomena such as noise in electronic devices are the source of true randomness for the unpredictable nature of TRNGs since PRNGs are purely deterministic, they do not produce any new true randomness.

The generic architecture of a TRNG consists of an entropy source and a digitization module and may include a post-processing module and an online tests module as illustrated in Figure 2.5. All true randomness is produced by the entropy source, in most cases in the form of analog signals. The digitization module converts these analog signals into digital bits. The produced outputs of the digitization module are called raw random numbers. The raw random

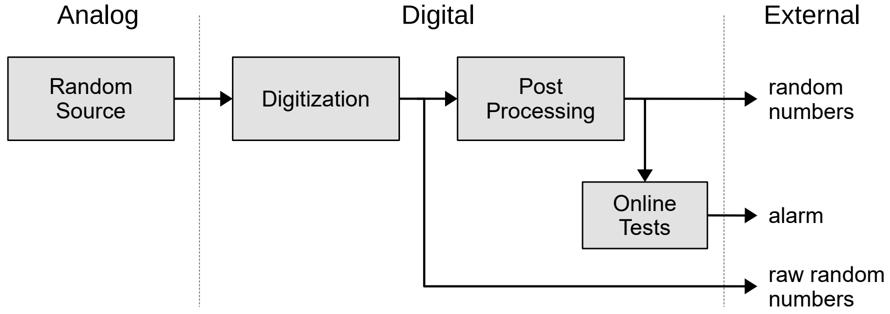


Figure 2.5: Generic architecture of True Random Number Generator (TRNG).

numbers usually contain statistical defects, such as the bias from an ideal probability of ones and the correlation between output bits. The post-processing module improves the statistical and security characteristics of the raw random numbers by extracting their densified randomness. The online tests detect failures simultaneously in the process of generating raw random numbers.

Several TRNGs have been proposed to generate the random seed which then can also be used for the initial vector of the Pseudo-Random Number Generators (PRNG) to generate longer keys [76, 35, 79]. Metastability based [80, 81] and ring oscillator (RO) based [82, 83] TRNGs are commonly used to convert a physical entropy source such as thermal noise and optical noise to binary numbers. The physical entropy source should be unpredictable so that the generated numbers satisfy the randomness tests. On the other hand, the TRNG circuit should harvest the entropy without or with minimum bias. The bias resulted from the entropy source, the process and run-time variation of the circuit, or the environmental changes can be determined using online tests. Furthermore, the remaining bias can be masked using post-processors to increase the entropy of TRNG output while reducing throughput [76, 79].

2.4 Reverse Engineering

Reverse engineering (RE) of integrated circuits (IC) is to determine the used technology, extract the circuit netlist, and infer the functionality. RE has been widely used for both honest and dishonest purposes in the integrated circuit market for the last few decades [84, 16, 85]. These purposes are summarized in Table 2.2.

Several RE works have been done for silicon-based ICs as they have been widely used in commercial products for decades [84, 89, 90, 91, 88, 92]. The RE process of a chip consists of three steps [16, 91].:

(1) Depackaging and Mechanical Preprocessing

(2) Delayering and Imaging

(3) Software Post-processing

In the first step (1), the chip is depackaged by using chemicals or mechanical tools. The next step (2) is to delayer the chip by using the combination of chemicals, plasma-etching, and mechanical polishing, and to image each layer by scanning electron microscope (SEM), transmission electron microscope (TEM) and scanning capacitance microscopy (SCM). It should be

Table 2.2: Purposes for Reverse Engineering [16].

”Honest” Intentions	**”Dishonest” Intentions**
Failure analysis and defect identification	Fault injection attacks
Detection of counterfeit products [86, 87]	Counterfeiting
Circuit analysis to recover manufacturing defects	Tampering
Confirmation of IP	IP piracy and theft
Hardware Trojan detection [88]	Hardware Trojan insertion
Analysis of a competitor’s product; Obsolete product analysis	Illegal cloning of a product
Education and research	Development of attacks

noted that delayering requires careful engineering to preserve important information since the transistor feature size has been shrunk dramatically. Also, environmental conditions, specifically brightness, affect imaging quality impacting the accuracy of the last step (3). In the last step (3), acquired images are stitched. Since (digital) ICs are composed of the cells of a standard cell library, every cell of the used cell library has to be identified manually. Then, the cells used inside the chip can be automatically detected using image processing methods. The wire connections between cells can also be detected, and the circuit netlist can be extracted automatically.

The extracted circuit netlist may have some errors because of the imperfection of the aforementioned steps. These errors can be mitigated by design rule checks and/or checking for any shorted input/output, floating nodes, or supplies and nets that have no input/output. Then, a reverse engineer can use the public information of the product such as the datasheet to analyze and/or organize the netlist [16, 91]. Then, several techniques can be used to infer the functionality of the circuit netlist [16, 93, 94, 95]. It should be noted that although there are tools to automate some parts of these steps, most of the process steps require expertise in various fields such as mechanics, imaging and circuit design, and manual effort to perform error-free RE [16, 89, 91].

3 Inkjet-Printed Physical Unclonable Function

The emerging applications of Printed Electronics (PE), particularly those in the context of smart sensors and IoT, require secure communication and/or authentication, for which secret keys are required [96, 97, 98, 99, 100, 101]. Physical Unclonable Functions (PUFs) have been proposed to provide such secret keys [68, 102], which derive unpredictable keys from uncontrolled physical feature disorders [103, 104, 105]. Recently, one study has presented a strong PUF using organic materials to provide secret keys in PE [106]. The organic PUF generates a key based on the frequency difference of ROs. However, the organic PUF suffers from a high circuit complexity rendering it very vulnerable to yield problems and high operation voltage, which are unsuitable features for the low-power applications.

In this chapter, we present the first weak printed PUF (pPUF) based on printed electrolyte-gated transistor (EGT) technology, which operates at low-voltage and has low circuit complexity, to be used in PE applications. The proposed pPUF is a memory-based circuit that benefits from positive feedback created by two cross-coupled inverters to provide the output (response) and includes a control transistor enabling the circuit by an input signal (challenge). Moreover, we propose a multi-bit pPUF design to reduce the area used for multiple bit key generation. We have developed a Monte Carlo (MC) based analysis framework including variation models based on the real EGT measurements to evaluate the proposed circuits. Furthermore, we fabricated and characterized the proposed single-bit pPUF circuits to validate its operation.

The results obtained from our analysis framework show that the proposed pPUF has near to ideal uniqueness (50.1%) and good enough reliability (89%). Furthermore, the proposed multi-bit pPUF saves 31.02% area for a 16-bit key with nearly ideal uniqueness (49.8%) and good reliability (92.6%). The experimental results show that the fabricated single-bit pPUFs can generate distinguishable outputs at the supply voltage of down to 0.5 V, and consume ~2.53 μW.

The summary of the contributions of the work is as follows:

- We present a printed PUF (pPUF) based on EGT technology.
- We have generated a variation model of the EGT calibrated using measurements from several fabricated EGTs.
- We develop an analysis framework that includes a Monte Carlo simulation flow for the evaluation of the pPUF.
- We propose a multi-bit pPUF which is optimized to reduce area usage for multiple bits.
- We fabricated and characterized the proposed single-bit pPUF to validate the operation of the pPUF at down to 0.5 V.

The rest of the chapter is organized as follows. Section 3.1 explains the proposed pPUF designs. In Section 3.2, the analysis framework for the pPUF is described. Section 3.3 and

3.4 shows the simulation and fabrication results respectively, and in Section 3.5, the chapter is concluded.

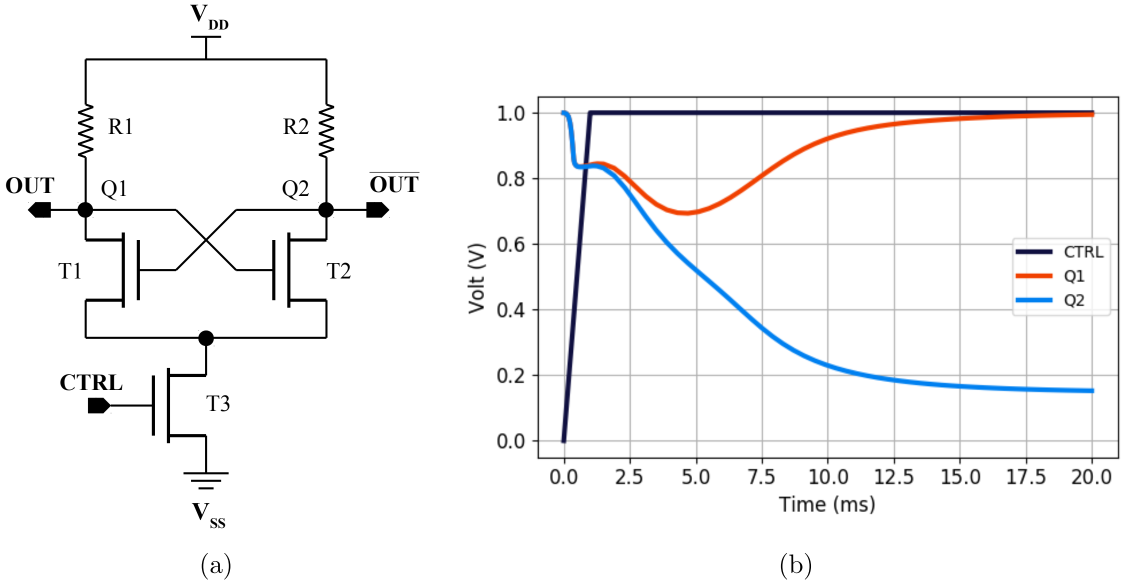


Figure 3.1: (a) Proposed single-bit pPUF circuit. (b) Simulated timing diagram of a single-bit pPUF circuit (A sample from Monte Carlo simulation using parameters: $R_1 {=} R_2 {=} 20\,k\Omega$, $W_1 {=} W_2 {=} 100\,\mu m$, $W_3 {=} 200\,\mu m$, $L_1 {=} L_2 {=} L_3 {=} 40\,\mu m$).

3.1 Proposed Printed PUF

Since the fabrication process of EGTs is based on inkjet printing, the EGTs have high intrinsic variation resulting from the random dispersion of the ink on the substrate, which is beneficial for PUF design. In the silicon technology, process variations are divided into local and global variations. Contrary to that, in inkjet Printed Electronics, all devices are printed individually by multiple additive process steps, where each step can vary on its own. These process and systematic variations originating from the ink, droplet forming, attachment of droplets on the substrate and manufacturing tools are random and cannot naturally be divided into local and global variations. Therefore, It should be noted that since transistors in inkjet printing are printed one by one, the spatial systematic correlation occurring in the lithographic fabrication of silicon circuits does not exist in inkjet printed EGTs. The high manufacturing variation of EGTs should be exploited to form stable PUF circuits. In addition, it is important to use as few number of circuit elements to have low-cost and low complexity PE products. At last, from this particular technology point of view, since the performance of p-type EGTs is orders of magnitude lower than n-type EGTs [61], resistors should be used for pull-up network as a substitute of p-type EGTs.

For this purpose, we have utilized a memory-based single-bit PUF circuit which exploits the high variation of the EGTs, uses few elements, and uses resistors for the pull-up network. Moreover, memory-based PUFs have nearly ideal average uniqueness results because of their working mechanism. Additionally, we have proposed a multi-bit PUF circuit which optimizes area usage through resource sharing. The details of the single-bit and multi-bit pPUF circuits are explained below.

3.1.1 Single-bit Printed PUF

The proposed memory-based pPUF is composed of two cross-coupled inverters and one control transistor which activates and deactivates the circuit. The schematic of the proposed pPUF is given in Figure 3.1a. The cross-coupled inverters create a positive feedback which forces the circuit to a stable state where the output is logic-0 or logic-1 depending on the manufacturing variation mismatch between inverter pairs. Figure 3.1b shows the timing diagram of a single-bit pPUF which uses $20\,k\Omega$ resistors and $100\,\mu m$ width and $40\,\mu m$ length for transistor pairs, $200\,\mu m$ width and $40\,\mu m$ length for CTRL transistor to illustrate its working mechanism.

When the control input (CTRL) is logic-0, the $Q1$ and $Q2$ nodes are equal to V_{DD}. While the $CTRL$ input is switching to logic-1, the feedback connections force the nodes, $Q1$ and $Q2$, to the stable states. Depending on the strength of the inverters, one node becomes logic-0 while the other becomes logic-1.

Figure 3.2 is the layout of the proposed pPUF circuit, which contains three EGTs, two resistors, and five input/output pads which are V_{DD}, V_{SS}, $CTRL$, OUT, and $\overline{OUT}$. Since the fabrication process of the technology supports only one layer for wiring, the inverters are connected in a way that wires are not crossed. Moreover, the delays of the wires are designed to be equal.

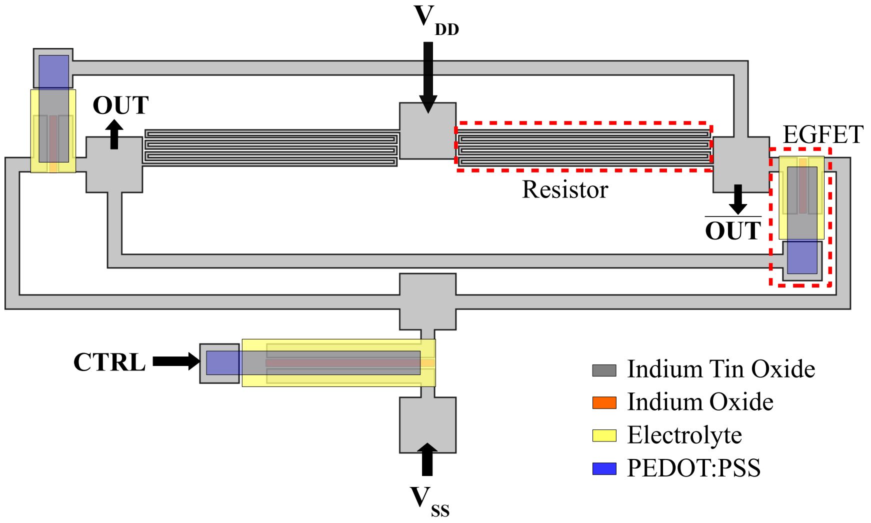


Figure 3.2: Layout of proposed single-bit printed PUF circuit.

3.1.2 Multi-bit Printed PUF

Since secret keys have multiple bits to be used in cryptographic algorithms and authentication, multiple single-bit PUF circuits can be used to generate multiple bit keys. However, a simple replication of single-bit pPUF circuits is inefficient as the increase of the area usage is proportional to the number of bits. For this reason, the resistors can be shared to reduce the area of the multi-bit PUF circuit. Figure 3.3 illustrates the proposed multi-bit pPUF design.

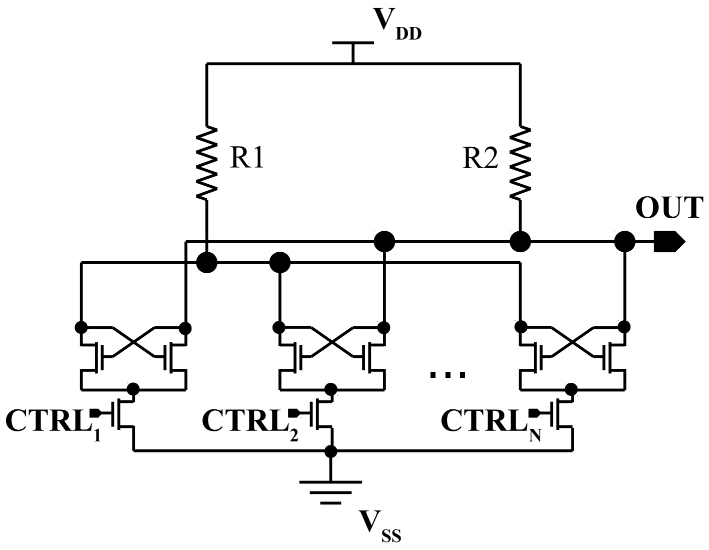


Figure 3.3: Proposed multi-bit printed PUF circuit.

As shown in Figure 3.3, the resistors are shared among transistor pairs. For an n bit array, n transistor pairs are required while the number of resistors is independent of the number of bits. Thus, the resistor usage for multiple bits is reduced. After power-up, the first control input ($CTRL_1$) is set to logic-1 to activate corresponding transistor pairs, then the output (OUT) is read, and the control input ($CTRL_1$) is reset to logic-0 to deactivate the transistor pairs. These steps are done sequentially for all transistor pairs to generate a multiple bit key. Since the resistors are shared among transistor pairs in multi-bit pPUF, the output (OUT) of transistor pairs are connected to each other, and if all CTRL signals are activated at the same time, only one bit can be generated based on all transistor pairs. The drawback of the multi-bit pPUF is that since bits are read sequentially, it requires more time to generate multiple bits than multiple single-bit pPUFs. However, since generating the key is done for one time, this drawback results in delay for once in the system.

Another possible optimization is to use one shared CTRL transistor for multiple single-bit PUF. However, since the current flowing through the EGT does not proportionally increase with the increase of the width according to Table 3.1 , the shared transistor should be designed larger in size than separated transistors, which finally result in similar area usages of shared and separated transistors. Therefore, the sharing of CTRL transistors is not taken into consideration.

Table 3.1: The mean saturated drain current of fabricated transistors with various widths

Width (Length = 40 μm)	200 μm	400 μm	600 μm	800 μm
Saturated Drain Current (μA)	276.37	369.27	380.72	437.78

3.2 Simulation-based Analysis Framework

In this section, the simulation framework created to analyse the proposed pPUF circuit is explained. The models required to analyse the pPUF such as variation, temperature, and noise models are explained.

3.2.1 Overall Printed PUF Analysis Flow

Because of the fact that the behaviour of a PUF circuit is based on manufacturing variations, it is critical to develop a variation aware simulation framework. For this reason, we have developed a MC simulation flow, allowing to simulate the variation due to manufacturing for EGT-based printed circuits, calibrated with actual EGT measurements, and integrated into a industry standard Electronic Design Automation (EDA) tool. In addition, an evaluation flow using MC simulation results to obtain the PUF metrics such as uniqueness and reliability is established. Figure 3.4 illustrates the overall analysis flow of the pPUF design.

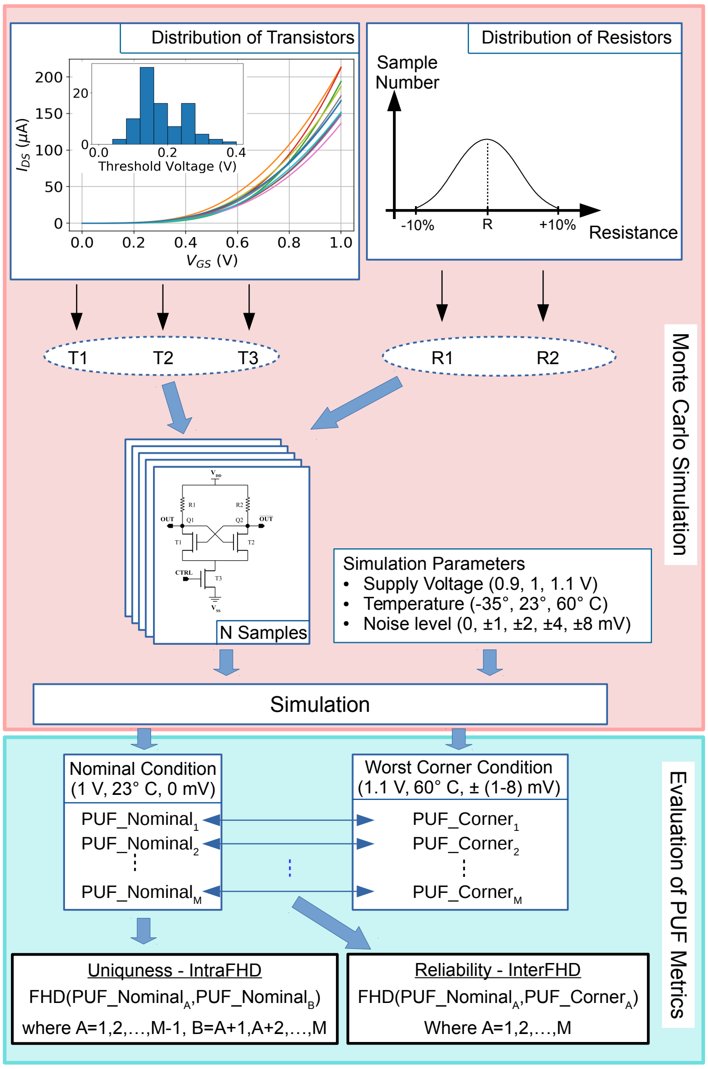


Figure 3.4: Analysis flow for proposed printed PUF that contains Monte Carlo simulation and evaluation of PUF metrics.

The analysis flow is composed of the MC simulation and the evaluation parts of the PUF metrics. In the MC simulation, first, a set of PUF instances are created by selecting transistors and resistors among possible variation range. Several transistors are fabricated and modelled, which is explained in detail later. These models based on measurements are selected uniformly, and define the variation range of the transistors. The variation range of the resistors is defined as ±10% which is obtained empirically. After that, PUF instances are simulated in nominal conditions and corner conditions, and the bits generated by instances are combined as keys.

The keys produced by the MC simulations are used to obtain the PUF metrics of the pPUF. The FHD between each key is calculated for the uniqueness. For reliability, the FHDs between the keys obtained in normal conditions and corner conditions are calculated.

3.2.2 Variation Modelling

Since our PUF circuit is based on manufacturing variations, it is vital to have a variation model of the circuit elements. However, since the EGT is an emerging transistor technology, the variation modelling of the EGT has not been studied yet. So, we aimed to create EGT variation model directly from the measurement data. Our approach is to create a binning model which includes the individual models of the numerous fabricated and measured EGTs, and the total variation effect can be simulated by making the individual models selectable. This approach not only allows us to develop a proper EGT empirical variation model, but also enables us to use measurement data for more realistic pPUF analysis.

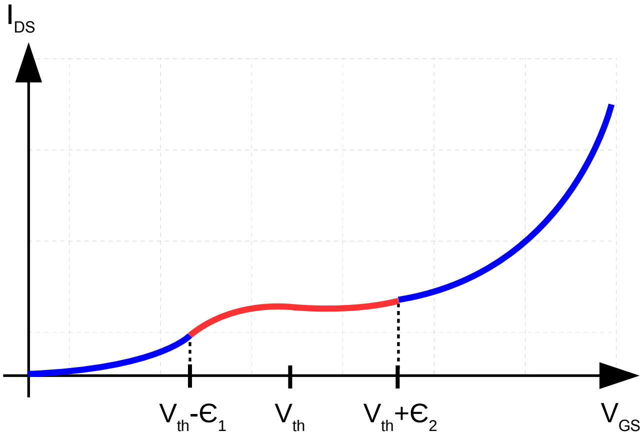


Figure 3.5: An example interpolation problem of fixed near threshold regime boundaries in transfer curve (I_{DS}-V_{GS}) of an EGT modeling.

The transistor model presented in [63] was extracted by using the mean values of the DC measurements of various fabricated EGTs. It includes three equations for three regimes of the EGT, namely below threshold, near threshold, and above threshold regimes. The below threshold regime is modelled by a modified sub-threshold swing model in Equation 3.1 [107]

$$I_{DS} = I_s.e^{\frac{V_{gs}-V_{th}}{nV_{therm}}} \tag{3.1}$$

where I_s is fitting parameter, n is the ideality factor, and V_{therm} is the thermal voltage while the above threshold regime is modelled by a modified Curtice model in Equation 3.2 [108]

$$I_{DS} = \beta.(V_{gs} - V_{th})^{\gamma} \tag{3.2}$$

where β is the transconductance parameter, and γ is the power-law parameter. The near threshold regime between the below and the above threshold regimes are interpolated by using third degree polynomial. The polynomial for the near threshold regime is given in Equation 3.3.

$$I_{DS} = aV_{gs}^3 + bV_{gs}^2 + cV_{gs} + d \tag{3.3}$$

where a, b, c and d denote the interpolation coefficients which are dependent on the boundaries of the near threshold regime.

The boundaries of the near threshold regime are fixed between $V_{th} - \epsilon_1$ and $V_{th} + \epsilon_2$ where epsilon values, ϵ_1 and ϵ_2, are chosen experimentally in [63]. However, when this modeling methodology is used to create individual models for various fabricated EGTs under process variation, the fixed boundaries of the near threshold regime cause problems, making it non-monotonic and causing convergence issues in simulation. Figure 3.5 illustrates an example transfer curve (I_{DS}-V_{GS}). In this example, interpolated polynomial is first increasing and then decreasing while providing continuity and smoothness. However, this causes convergence issues in simulation since multiple voltage levels have equal current values. The polynomial and its slope must be monotonically increasing to avoid this problem. To assure that, first and second derivatives of the polynomial which are given in Equation 3.4 and 3.5 must be positive.

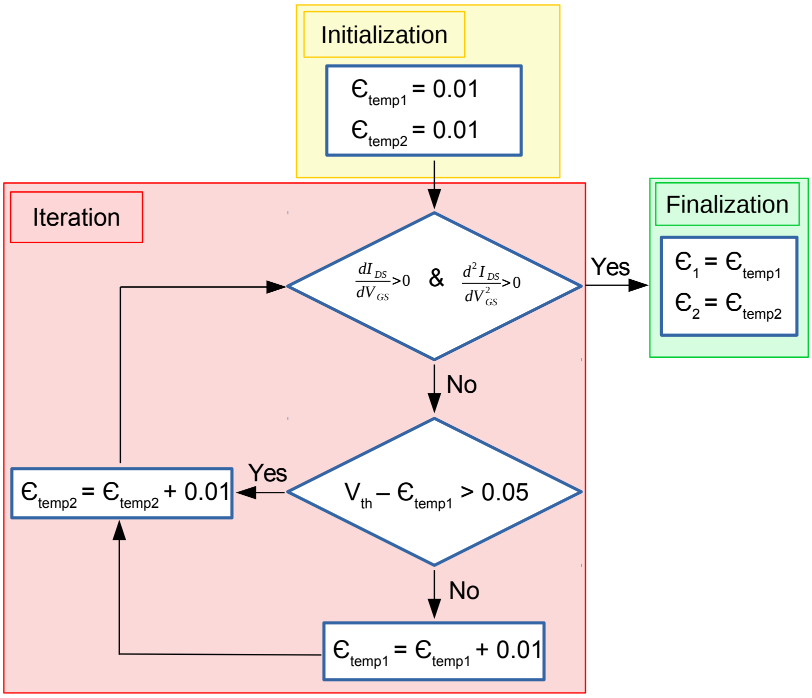

Initialization
$\epsilon_{temp1} = 0.01$
$\epsilon_{temp2} = 0.01$
Iteration
$\frac{dI_{DS}}{dV_{GS}} > 0$ & $\frac{d^2 I_{DS}}{dV_{GS}^2} > 0$
Yes
No
$V_{th} - \epsilon_{temp1} > 0.05$
Yes
$\epsilon_{temp2} = \epsilon_{temp2} + 0.01$
No
$\epsilon_{temp1} = \epsilon_{temp1} + 0.01$
Finalization
$\epsilon_1 = \epsilon_{temp1}$
$\epsilon_2 = \epsilon_{temp2}$

Figure 3.6: Flow for finding optimal epsilon values, ϵ_1 and ϵ_2.

$$\frac{\mathrm{d}I_{DS}}{\mathrm{d}V_{gs}} = 3aV_{gs}^2 + 2bV_{gs} + c \tag{3.4}$$

$$\frac{\mathrm{d}^2 I_{DS}}{\mathrm{d}V_{gs}^2} = 6aV_{gs} + 2b \tag{3.5}$$

To obviate the problem, we have developed a method which iteratively selects different boundaries for near threshold regimes for each transistor model to make sure that the first and second derivatives are positive. Figure 3.6 illustrates the flow of obtaining ϵ_1 and ϵ_2 for each transistors. At first, temporary boundary (ϵ_1-ϵ_2) values are defined around threshold voltage of corresponding EGT and the polynomial is interpolated according to these epsilon values. Unless the first and second derivatives of polynomial are greater than zero, these boundary values are increased until $V_{th} - \epsilon_1$ equals to 0.05 V since $V_{th} - \epsilon_1$, which defines where below threshold regime finishes and near threshold starts, should not be close to 0 V to obtain better below threshold regime modelling. After that point, only ϵ_2 is increased until the derivatives are greater than zero. At last, the obtained boundary values are used to define near threshold interval, and fabricated particular EGT is modelled. Figure 3.7 shows the $I_{DS} - V_{GS}$ curves of the measurements and the models of 9 sample instances out of total 88 fabricated EGTs. The models are implemented using Verilog-A and made it selectable. By changing model number, the variation of the EGT is simulated.

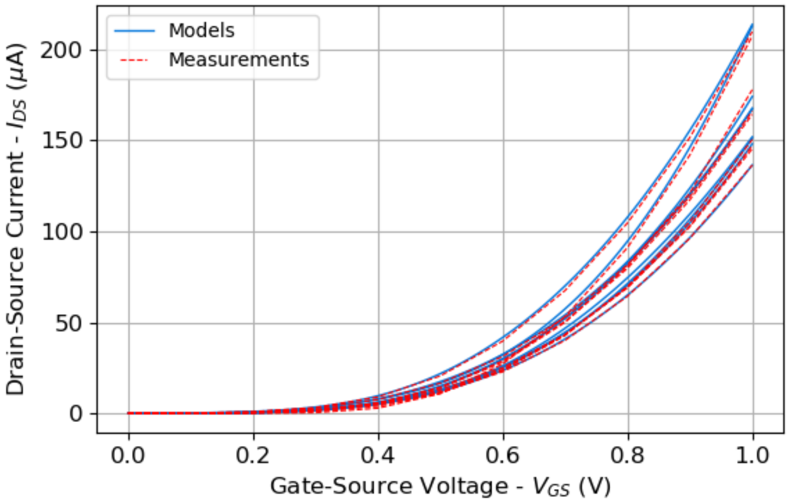


Figure 3.7: Transfer curves (I_{DS}-V_{GS}) of measurement and model of EGTs.

3.2.3 Temperature and Noise Modeling

The results presented in [17] on the impact of temperature on EGT characteristics are used to model the temperature effect. Since the saturated drain current $I_{d,sat}$ which is the combined result of other affected parameters is the circuit level parameter, we directly use the saturated drain current to model the temperature effect.

The saturated drain current increases while the temperature is increasing from $-35\,°C$ to $60\,°C$. To create the temperature model for corner cases, the highest ratios of the saturated drain current between $23\,°C$ and $-35\,°C$, and between $23\,°C$ and $60\,°C$ are calculated and given in Table 3.2.

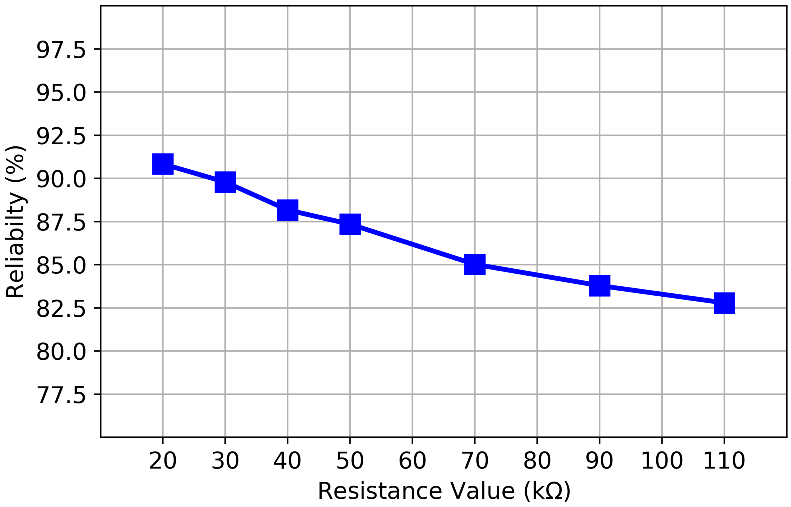


Figure 3.8: Reliability results where ±8 mV noise is introduced for various resistance values .

Table 3.2: Saturated drain current ratios extracted from [17] for corner temperatures

Reference Temperature	Corner Temperature	Saturated Drain Current Ratio
23 °C	60 °C	1.20
23 °C	-35 °C	0.83

To be able to simulate the temperature effect on the pPUF circuit and obtain the reliability of the pPUF circuit at corner temperature cases, a temperature constant (C_T) multiplying the drain-source current (I_{DS}) is added to the variation model. The temperature constant can be 0.83, 1, or 1.20 when temperature is -35 °C, 23 °C, or 60 °C respectively, using Table 3.2.

$$I_{DS}^{'} = C_T * I_{DS} \tag{3.6}$$

Since there is no experimental noise analysis done for the EGT yet, we used a method to mimic the noise effect on the circuit output. The method is to add a fixed amount of voltage (e.g., 8 mV) to one output (OUT) and subtract from the other output ($\overline{OUT}$), and vice versa, while the CTRL transistor is turning on. Therefore, the noise directly affects the response of the pPUF.

3.3 Simulation Results

3.3.1 Design Parameters

The PUF circuit is composed of three EGTs and two resistors. The width and length of T1 and T2 transistors and the resistance value of R1 and R2 resistors must be equal to have identical two inverters. The width and the length of the T1 and T2 EGTs are selected as 100μm and

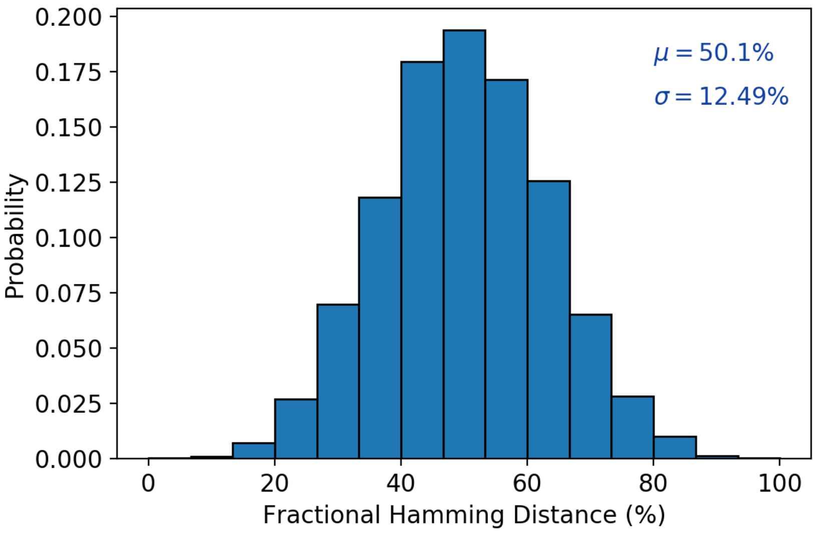


Figure 3.9: Uniqueness (inter-FHD) of the proposed printed PUF.

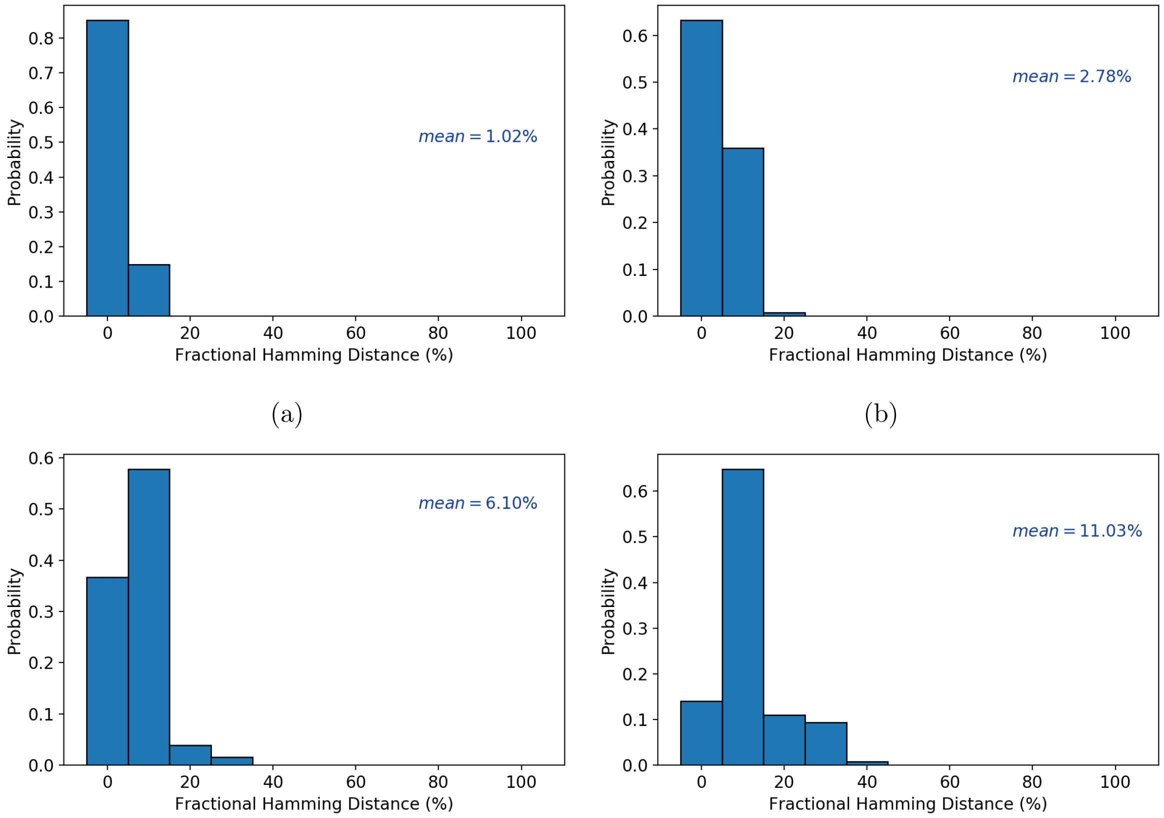
$40\mu m$ respectively since these values are the parameters of the smallest fabricated EGT. The width and the length of the T3 are $200\mu m$ and $40\mu m$ since T3 should be able to flow the sum of the current flowing through T1 and T2.

Since the resistance value of R1 and R2 affects reliability, the PUF circuits with various resistance values are simulated in nominal conditions and the conditions in which only $\pm 8\,mV$ noise is introduced to find out the resistance resulting in better reliability. The reliability results for various resistance values are given in Figure 3.8. The results show that the lower resistance values provide better reliability since the lower resistance allows higher current flow through circuit and this charges/discharges the noise on the outputs. Besides, the resistor area decreases while the resistance value is decreasing. However, while the resistance value decreases, the feedback strength of the inverters, which forces the PUF circuit to go to a stable state, also decreases. The low feedback strength of the inverters can bring unstable outputs. Therefore, the number of the unstable PUF outputs rapidly increases below $20\,\mathrm{k\Omega}$ according to simulation and experiments. For this reason, $20\,\mathrm{k\Omega}$ is selected as the resistance value of R1 and R2 to obtain better reliability, smaller area, and stable outputs.

3.3.2 PUF Metrics and Design Space Exploration

The analysis framework which is explained in Section 3.2 is utilized to obtain the PUF metrics. More than 20,000 MC simulations were executed to obtain uniqueness and reliability metrics. Since the single-bit PUF circuit generates one bit, 16 single-bit PUF circuits are used to obtain 16-bit keys.

For uniqueness, 128x16-bit keys, i.e. the digital response of the pPUFs, obtained in nominal condition, which denotes that the temperature is 23 °C, the supply voltage is 1 V, and the noise level is zero, are used. The histogram of the FHDs between the keys is shown in Figure 3.9. The mean of the histogram should be ideally 50%. In our work, the mean and the standard deviation are 50.1% and 12.49%, respectively. These results show that the uniqueness of our proposed pPUF is very close to the ideal uniqueness.



(a)

(b)

(c)

(d)

Figure 3.10: Reliability (intra-FHD) of the proposed printed PUF with different noise levels a) $\pm 1\,mV$ b) $\pm 2\,mV$ c) $\pm 4\,mV$ d) $\pm 8\,mV$

For reliability, the keys are obtained in nominal condition and corner condition, which denotes that the temperature is 60 °C, the supply voltage is 1.1 V, and the noise is introduced with various voltage levels since the worst reliability results are obtained for this corner condition. The FHDs between the keys are calculated for reliability at different noise voltage levels and the FHD distributions of each noise level are given in Figure 3.10. The results show that the mean of the worst reliability is around 89% where the noise level is $\pm 8\,mV$. According to the mean and standard deviation of the uniqueness histogram, the smallest FHD between two keys is 14.12% and the worst unreliability is around 40%. Since the unreliability of the majority of the keys is below 10%, and the smallest uniqueness is greater than that value, the majority of the keys are distinguishable. In addition, the unreliability can be mitigated by error correction codes [103],[109].

Although a multiple single-bit PUF circuit can be used to create multi-bit keys, a resource shared multi-bit pPUF circuit described earlier can be used to reduce the area usage. The area usage of the single-bit and the multi-bit PUF designs for various bit numbers, and the area reduction rates are given in Table 3.3. The results show that the area usage can be reduced by 31.02% for 16-bit by using multi-bit pPUF circuit which has the same PUF metrics results.

The PUF metrics of the multi-bit PUF are obtained for 16-bit multi-bit circuit. The uniqueness of the multi-bit pPUF is 49.8%, which is near to the single-bit pPUF, since the circuit behaviour of one pair is same as the single-bit pPUF. However, the reliability of the multi-bit

Table 3.3: Area usage of single-bit and multi-bit PE-PUF, and area improvements for various number of bits.

# of Bit	Area Usage ($10^3 * pm^2$)		Area Improvement (%)
	Single-bit	Multi-bit	
1	272	272	0
2	544	454	16.54
4	1088	818	24.82
8	2176	1546	28.95
16	4352	3002	31.02

pPUF for ±$8mV$ noise is around 92.6%, which is higher than the single-bit pPUF since the leakage currents of the deactivated pairs reduce the effect of noise.

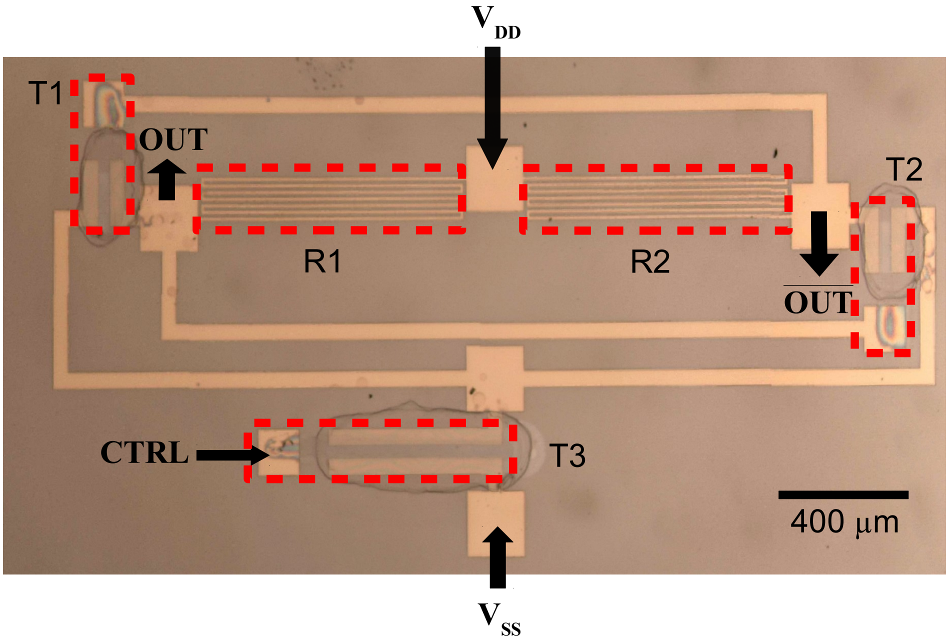


Figure 3.11: Optical image of a fabricated single-bit printed PUF circuit.

3.4 Fabrication Results

Fabricating the proposed pPUF is very important to validate the functionality of the design, find out the minimum operating voltage, and measure the power consumption. For this reason, we fabricated and characterized the proposed single-bit pPUF circuit. The detailed information of fabrication and experiments are explained in the following subsections.

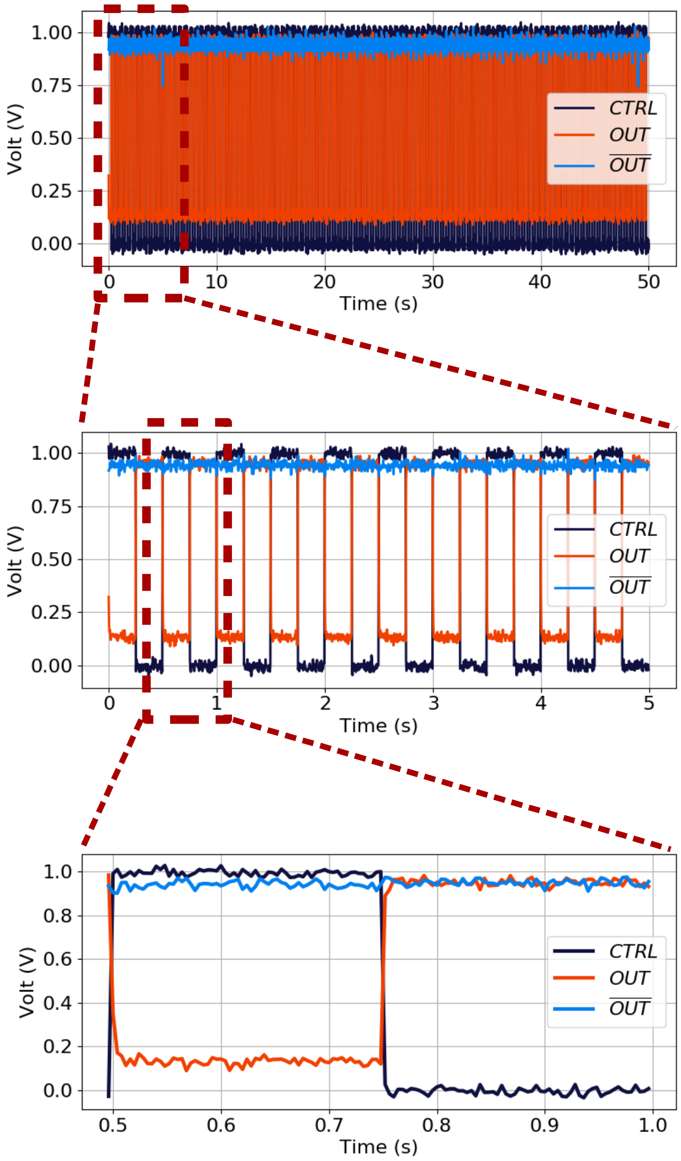


Figure 3.12: Timing diagram of fabricated single-bit printed PUF at 1 V.

3.4.1 Fabrication Parameters

The proposed single-bit pPUF circuit consists of three transistors and two resistors. The widths of the T1, T2 and T3 EGTs are selected as $200\,\mu m$, $200\,\mu m$ and $600\,\mu m$ respectively, and the length of EGTs are selected as $40\,\mu m$, to provide high current capacity. The resistance values of R1 and R2 are selected as $40\,k\Omega$ to provide sufficient amplification of the inverters. Figure 3.11 is the photo of the fabricated single-bit pPUF circuit.

Since this EGT-based PE technology is an emerging technology under development, it is probable to have yield problems. Therefore, to avoid any yield related problems, the width values of transistors and the resistance value of resistors are selected higher than the values used in simulation so that the fabricated pPUF has higher pull-up resistors providing more amplification and transistors providing higher current capabilities. These larger dimensions

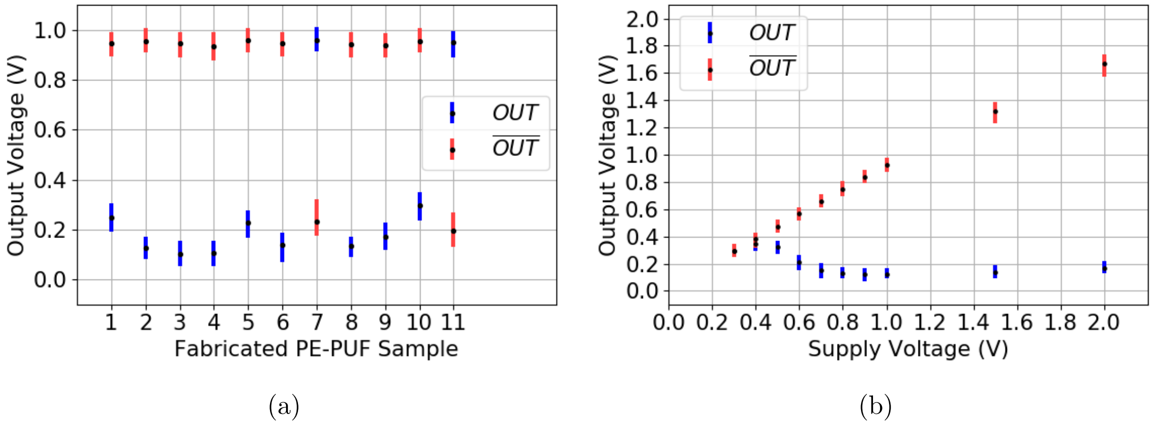


Figure 3.13: (a) Measured output voltage range of fabricated eleven single-bit printed PUFs at supply voltage of 1 V. (b) Measured output voltage range of fabricated single-bit printed PUF at supply voltage of 2 V down to 0.3 V.

help to have better yield in the printing process.

The fabrication process of the EGT is already explained in Section II. The fabricated single-bit pPUF also includes the resistors ($R1, R2$), wires and contacts other than EGTs. These are lithographically structured using indium tin oxide (ITO).

3.4.2 Measurement Setup

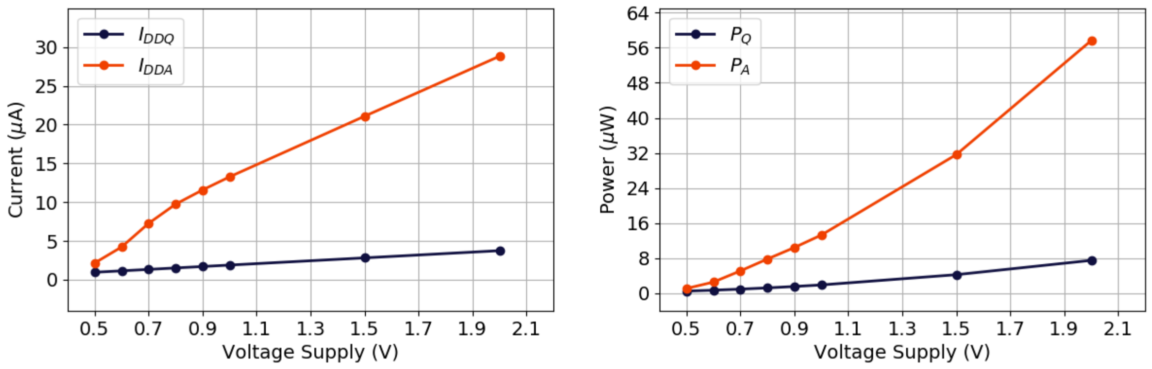
The fabricated single-bit pPUF circuits are contacted through a Süss Microtech probe station. As source for the supply voltage, Agilent 4156C precision semiconductor parameter analyzer is used. The enable signal ($CTRL$) is generated with a Keithley 3390 arbitrary waveform generator. The enable and the output (OUT, $\overline{OUT}$) signals are recorded with Yokogawa DL6104 digital oscilloscope. All measurements are performed at room temperature and 50% relative humidity.

3.4.3 Measurement Results

The fabricated single-bit pPUF circuits are supplied by 1 V voltage source and enabled by applying a 2 Hz, 50% duty cycle pulse signal to the $CTRL$ input. It is also noted that the high level of the $CTRL$ signal equals to the supply voltage for all measurements. After power-up, the circuits are enabled hundred times to examine the consistency of the outputs of the circuits.

Figure 3.12 is the measured timing diagram of a fabricated pPUF circuit. After enabling the circuit, one output (OUT) is logic-0 while the other output ($\overline{OUT}$) is logic-1, as it is expected. The outputs (OUT) of nine pPUFs among eleven fabricated pPUFs are logic-0 and the outputs (OUT) of other two pPUFs are logic-1 while the circuits are enabled by $CTRL$ signal.

The generated output bits by the single-bit pPUF circuits are stable while the circuits are enabled hundred times. Figure 3.13a illustrates the voltage level range of the outputs of the simulated and the fabricated pPUFs. The mean voltage level for logic-1 is above 0.9 V among



(a) (b)

Figure 3.14: (a) Quiescent and active currents (I_{DDQ}, I_{DDA}) of fabricated single-bit printed PUF at various supply voltages. (b) Quiescent and active power consumption (P_Q, P_A) of fabricated single-bit printed PUF at various supply voltages.

eleven fabricated pPUFs because of the leakage current of the EGT. The mean voltage level for logic-0 is below 0.3 V since resistors are used instead of low performance p-type EGTs. The output voltage level range of simulated pPUF is between 206 mV and 127 mV for logic-0, and between 1 V and 994 mV which are similar to the output voltage level ranges of fabricated pPUFs. The slight differences are mostly resulting from external conditions (*e.g.* noise) or minor modelling inaccuracies.

Since lower supply voltage is important for the PE applications, we measured the outputs of one pPUF at various supply voltages (from 2 V down to 0.3 V) to examine the lowest operating voltage of the pPUF. Figure 3.13b shows the voltage levels of the outputs at different supply voltages. The results show that the outputs are distinguishable as low as ∼0.5 V. In addition, we measured the quiescent (static) and active (dynamic) currents of the pPUF at various supply voltages to calculate the quiescent and active power consumption of the pPUF. Figure 3.14a shows the quiescent and active currents of the pPUF at various supply voltages.

Figure 3.14b shows the quiescent and active power consumption of the pPUF at various supply voltages. The active power consumption sinks from ∼57.64 μW to ∼2.53 μW when VDD is lowered from 2.0 V down to 0.5 V. Furthermore, active power consumption is always higher than quiescent power consumption because of the control transistor (T3). However, while the supply voltage is decreasing, the difference between active and quiescent power consumption is also decreasing since the control transistor limits the current (I_{DDA}) when a lower potential is applied to its gate.

3.5 Summary

Printed Electronics provides mechanical flexibility and low-cost fabrication which are crucial in many emerging applications, such as IoDT, smart sensors, and wearables. However, for secure communications and/or authentication, these applications may require secret keys. In this chapter, we have addressed the secret key requirement by proposing the printed PUF based on printed electrolyte-gated transistors. We evaluated the performance of the pPUF by using the analysis framework based on real measurements of several printed transistors. The analysis results show that the proposed pPUF has decent PUF metrics. Also, we have proposed the multi-bit design of the pPUF to optimize the area usage. The optimized multi-bit design saves 31.02% area usage for 16-bit compared to 16 times single-bit solution. Furthermore, we have presented the fabrication results of single-bit pPUFs. The measurement results show that the behaviour of the fabricated pPUFs are similar to the simulation, and the fabricated pPUFs operate at ∼0.5 V, and consume ∼2.53 μW, which is promising for low-power PE applications.

4 Compact True Random Number Generator based on Inkjet Printing Technology

The advances in Printed Electronics (PE) field give rise to security concerns, specifically authentication and cryptography, since the envisioned application areas are mostly interconnected, and contain sensitive data, which has to be secured. To that end, True Random Number Generators (TRNGs) are employed to generate unpredictable keys, the initial vector of Pseudo-Random Number Generators (PRNGs), padding values, and random challenge sequences [14].

TRNGs digitize an unpredictable natural phenomenon (entropy source) such as thermal noise to random bits while PRNGs use short initial random bits generated by a TRNG, and generate random-looking longer bitstreams [76]. The entropy source of the TRNG design is the most crucial component since it provides the unpredictability to the system, and the TRNG circuit should harvest the entropy without introducing bias. The bias caused by the entropy source, the process variation of the circuit, or the environmental changes can be masked using a post-processor, although it is not needed in all designs [76, 110].

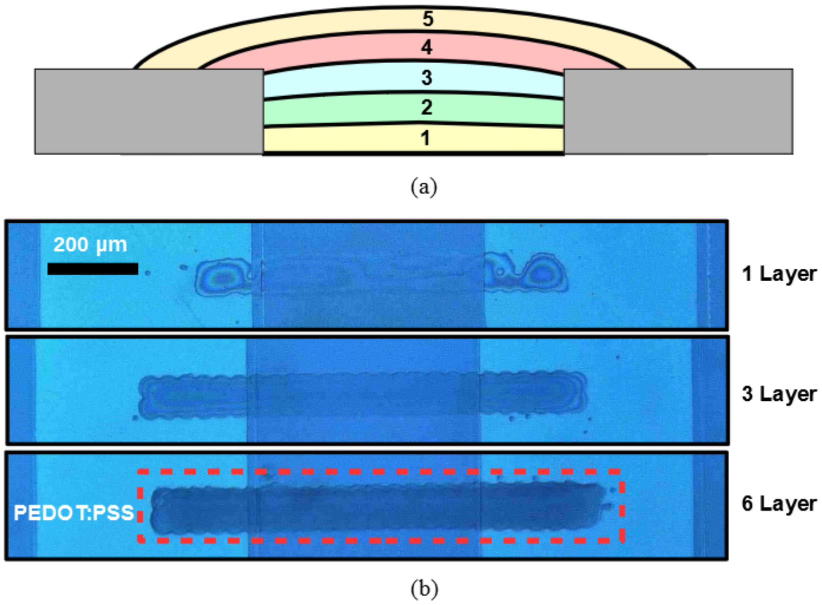
Additive printing processes including inkjet printing have high intrinsic process variation resulting from the dispersion of the ink printed in multiple steps, where each step varies on its own [111, 112, 113]. Since the high process variation can significantly introduce bias to the generated bits of TRNGs, designing an inkjet-printed TRNG, in other words mitigating the high variation, is very challenging. Nevertheless, inkjet printing enables the customization of each circuit individually, which can be exploited to mitigate the high process variation of the fabricated circuits in the post-fabrication phase [111, 114].

In this chapter, the first printed TRNG utilizing the customizable fabrication feature of the PE technology to compensate for the high intrinsic process variation is presented. A printed resistor that can be tuned by printing additional layers is presented and utilized in the proposed circuit to mitigate the overall process variation so that the power-up behaviour of the circuit is highly based on the noise. A resistor tuning flow is proposed to determine the point where the overall process variation of the circuit is mitigated, and the generated bits are random. Additionally, we optimize the resistor tuning flow to reduce the measurement and tuning efforts. Moreover, we fabricated, tuned, and characterized TRNG circuits to validate the functionality of the proposed TRNG.

The simulation results show that the mean of the overall process variation of TRNG instances is reduced by 110 times using the resistor tuning flow, and the optimized tuning flow decreases the tuning time by 10 times. The proposed TRNG passes National Institute of Standards and Technology - Statistical Test Suite (NIST-STS) showing that the proposed TRNG design can provide highly random bitstreams that pass the required tests. The experimental results show that the proposed tuning flow mitigates the process variation of the fabricated printed TRNGs, and they generate random bitstreams with near to 50% probability of ones.

The summary of the contributions of this work is as follows:

- We present the first printed TRNG using printed electrolyte-gated transistor (EGT) technology.
- We propose a method that exploits the additive manufacturing feature of PE utilizing presented printed resistors to efficiently mitigate the overall process variation of the proposed TRNG circuit.
- We validate the randomness of the tuned TRNGs using NIST-STS.
- We fabricate the proposed TRNG and apply resistor tuning flow to compensate for the overall process variation. We characterize the tuned TRNGs to validate their operation at below 1 V.



(a)

(b)

Figure 4.1: (a) Illustration of additively printed layers. (b) Top-view photos of fabricated printed resistors.

The rest of the chapter is organized as follows. Section 4.1 explains the resistor tuning using additive printing of resistors based on fabrication data. In Section 4.2, we present the proposed inkjet-printed TRNG design. Section 4.3 and 4.4 present and discuss the simulation and fabrication results, respectively. Lastly, Section 4.5 concludes the chapter.

4.1 Additive Printing of Resistors

Additive printing processes have several advantages over subtractive processes where sophisticated and/or expensive equipments and infrastructure are required. These advantages are low-cost, on-demand and customizable fabrication. The customizable fabrication can be used to modify/tune the circuits with very little effort, after the manufacturing.

We have examined an inkjet-printed resistor exploiting the customizable fabrication [115]. The resistance of the printed resistor which uses PEDOT:PSS as a material can be modified by printing more layers on top of existing layers. Each layer can be represented as a resistor,

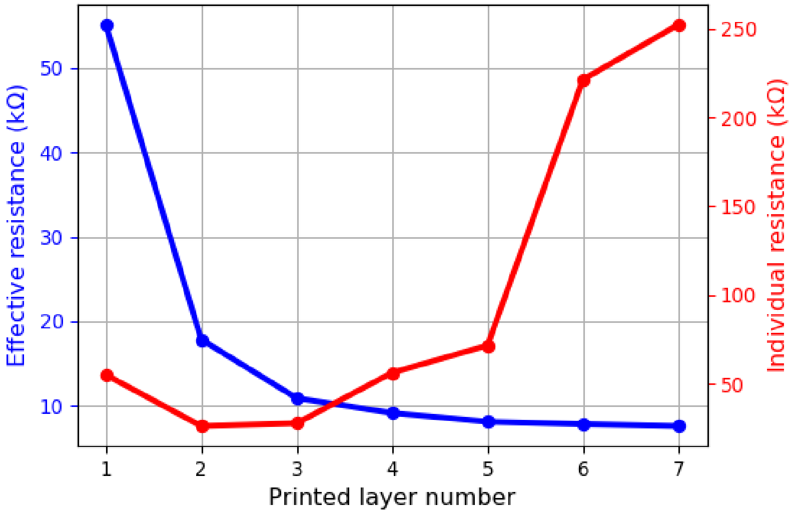


Figure 4.2: Effective and individual resistance of printed resistors with different layers.

and printing a layer on top of the other layers adds another resistor in parallel as illustrated in Figure 4.1.

The printed resistors containing various number of layers with the width of 50 μm are fabricated and characterized at room temperature. The measured effective resistance and the extracted individual resistance of the layers are given in Figure 4.2. Since the path of each successively printed layer is longer than the previous layers, as illustrated in Figure 4.1a, the resistance of each layer is larger than the previous layer.

The measurements show that the effective resistance decreases while the total number of layer is increasing, and the individual resistance of layers increases while the number of printed layers is increasing, except the first layer since it does not form a continuous line on the substrate, as shown in Figure 4.1b. Furthermore, to reduce the effective resistance even faster, additional layers can be printed next to other layers, which adds less resistance in parallel compared to the layer printed on top of other layers. Therefore, this feature of the resistor tuning can be used to compensate the process variation of the proposed TRNG circuit, as discussed in the next sections.

4.2 Proposed Inkjet-Printed TRNG Design

The proposed TRNG circuit should have few number of circuit elements to satisfy the low-cost requirement since most of the PE applications are expected to be low-cost. On the other hand, the inkjet printing of the EGTs causes high process variation which results from the random dispersion of the inks on the substrate [13]. The high process variation leads to the high degree of bias on the generated bits from the TRNG, reducing the entropy. The process variation of the TRNG must be low to provide high entropy. In existing TRNGs based on conventional technologies, the bias of TRNG is mitigated using an additional calibration circuitry which probes the generated bits, examines and calibrate the core TRNG circuit [116]. However, the calibration circuitry adds an overhead to TRNG core. Thus, we have proposed a compact

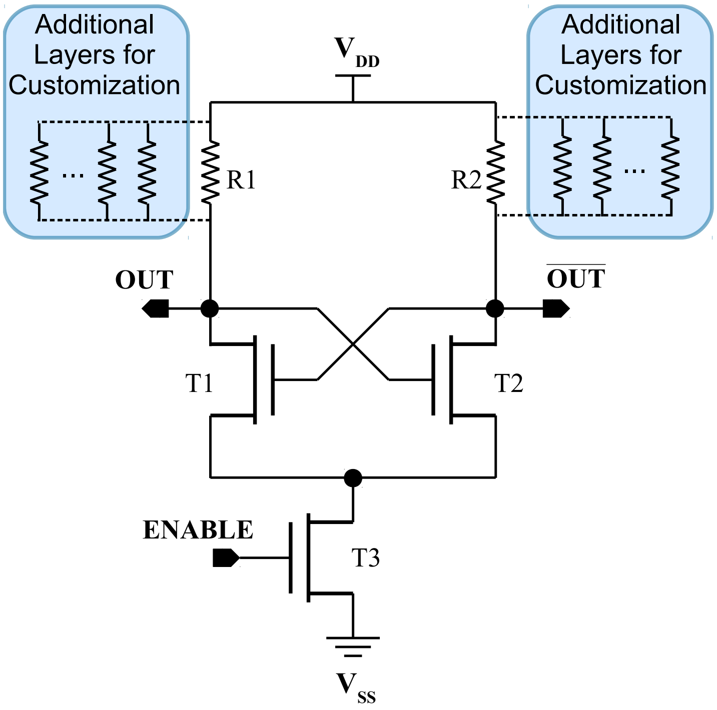

Additional Layers for Customization
Additional Layers for Customization
V_{DD}
R1
R2
OUT
$\overline{OUT}$
T1
T2
ENABLE
T3
V_{SS}

Figure 4.3: Proposed TRNG circuit with customizable resistors. Overall process variation of circuit is mitigated using additional layers for customization of printed resistors.

circuit which uses few elements, and instead of calibration circuitry, we have proposed a resistor tuning flow, which takes advantage of the additive manufacturing feature of the inkjet printing, to mitigate the high process variation without area overhead. The proposed TRNG circuit and the proposed resistor tuning flow is elaborated in the following subsections.

4.2.1 TRNG Circuit

The proposed TRNG circuit is a memory-based circuit that contains two cross-coupled inverters and an enable transistor enabling/disabling the circuit. The inverters are composed of an n-type EGT and a resistor. This is done for two reasons. Firstly, the use of resistors in the pull-up network allows to realize the additive tuning. Secondly, the p-type inorganic channel materials usually have very poor characteristics, hence effective p-type transistors are still under investigation. The circuit schematic of the TRNG is given in Figure 4.3.

The OUT and $\overline{OUT}$ nodes are equal to V_{DD} when the circuit is not enabled meaning that the $ENABLE$ input is zeros. Since the symmetrical inverters lead to a metastable state, the feedback amplifies the random noise (thermal noise, shot noise, etc.), and drives the OUT and $\overline{OUT}$ nodes to the stable states, either ones or zeros depending on the noise while the $ENABLE$ input is switching to ones. Therefore, the noise is digitized to generate true random bits. Figure 4.4 shows the waveform of the circuit generating the random bits based on the noise.

However, since the fabrication of the circuit is based on inkjet printing, it has high intrinsic process variation deriving from the random dispersion of the ink on the substrate. In addition, contrary to the silicon technology where the process variations are divided into local and global

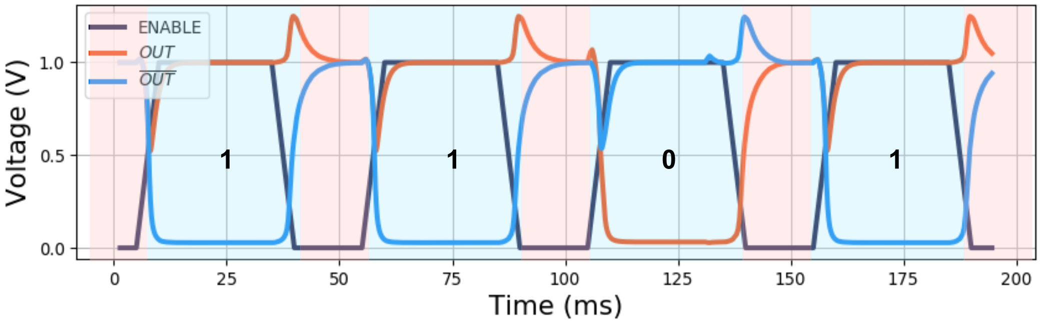


Figure 4.4: Example simulated timing diagram of output of an inkjet-printed TRNG circuit.

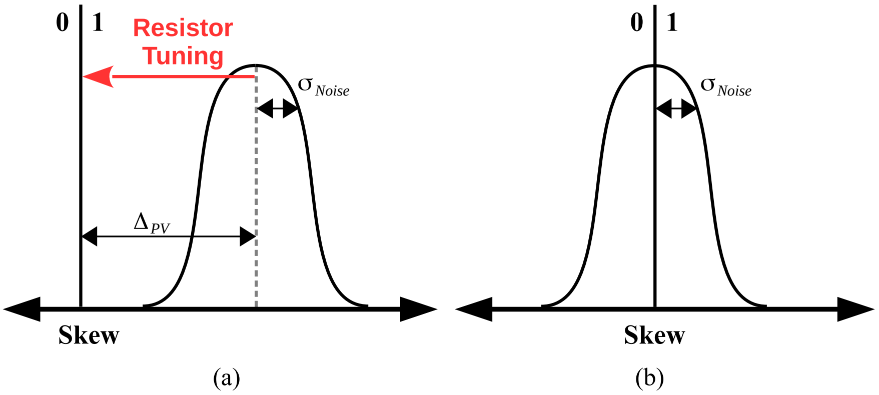


Figure 4.5: Illustration of behavior of (a) skewed, (b) non-skewed circuit (Δ_{PV}: skew because of process variation, σ_{Noise}: standard deviation of noise) [14].

variations, which result in low variation between two close devices, all devices are printed individually by multiple additive steps in inkjet printing, which cause higher variation, even for the two cross-coupled inverters in this circuit.

The process variation cause a skew that forces the circuit to one side which results in the bias at the generated bits. A skewed circuit whose behaviour is illustrated in Figure 4.5a is biased to ones because of the process variation (Δ_{PV}), while the non-skewed circuit whose behaviour is illustrated in Figure 4.5b is not biased and generates bits based on the random noise which is essential for a TRNG. Therefore, to construct an inkjet-printed TRNG, its high process variation should be mitigated. For this reason, we propose a resistor tuning flow explained in the following section.

4.2.2 Resistor Tuning Flow

It is vital to compensate the skew of the proposed TRNG circuit, which results from the overall process variation. The proposed resistor tuning flow as shown in Figure 4.6 utilizes the additively-printed resistor, as presented in Section III, to compensate the overall skew shown in Figure 4.5. The printed resistor tuning flow is as follows. After fabricating the circuit, the output has to be read N times, and the number of ones in N read is counted. If the number of ones is greater than $N/2$ (50%), which means that the tuned circuit is skewed to ones, printing one layer to the $R2$ shifts the skew towards neutral axis. If the number of ones is less than

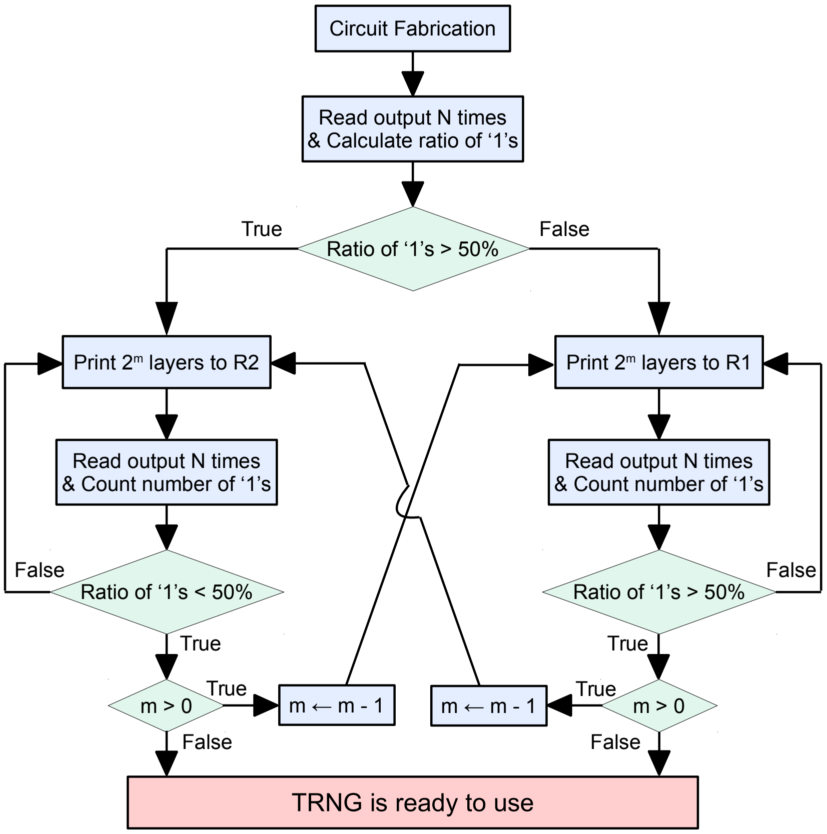
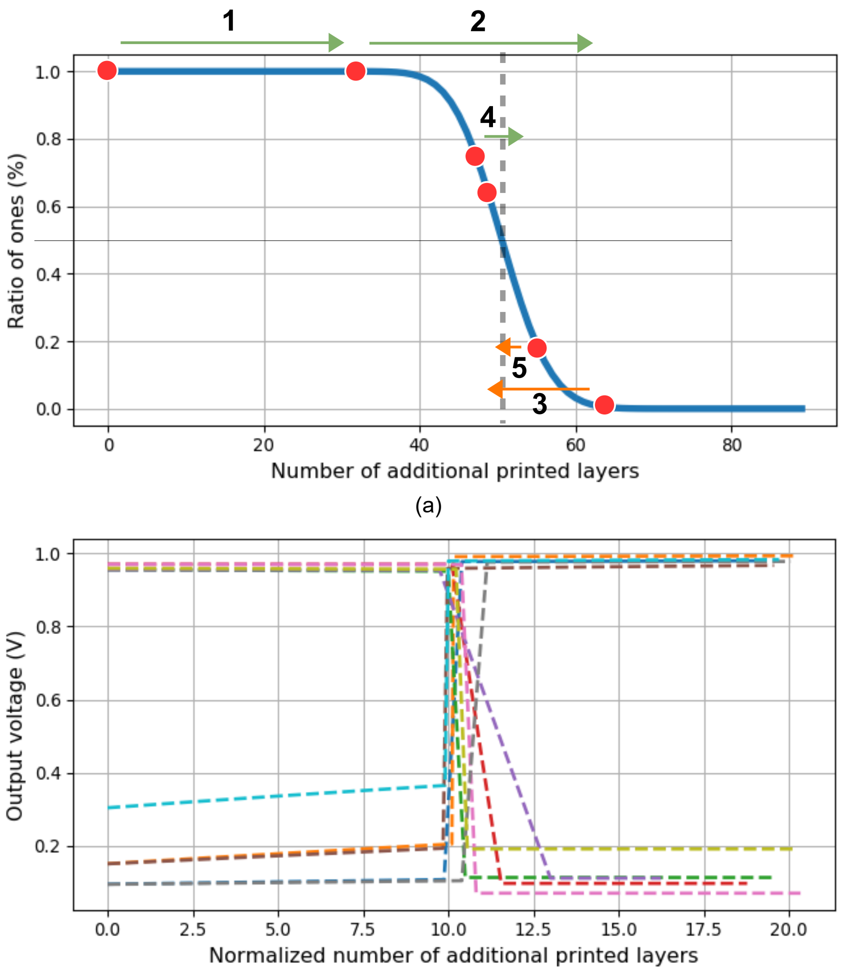


Figure 4.6: Optimized resistor tuning flow to mitigate process variation of proposed TRNG design. Resistors are additively tuned to converge ratio of ones to 50%. m and N are flow parameters.

$N/2$, printing one layer to the $R1$ shifts the skew from zeros towards neutral axis. Printing additional layers to the $R1$ or $R2$ is repeated until the number of ones reaches to $N/2$.

Figure 4.7a shows the ratio of ones in the generated bitstream of an inkjet-printed TRNG with respect to the number of additional layers. The simulation flow to obtain the generated bitstream is based on the Monte Carlo simulation of a TRNG instance, which uses the parameters given in Table 4.1 and ±10% variation for the resistors and the variation model presented in [113]. In addition, a normal distributed random noise source which has the mean (μ) and sigma (σ) of $0\,V$ and $3\,mV$ is used in simulation. Since the range near to 50% ratio of ones (non-skewed point) is too short, the additional layers of the resistor are printed one by one to not miss the non-skewed point. However, this leads to very long tuning time (including the number of iterative measurements and printing steps) since, in each step, the circuit output has to be read N times. For this reason, we optimize the resistor tuning flow to reduce the tuning time. In the improved flow as illustrated in Figure 4.6, if the ratio of ones is greater (smaller) than 50%, 2^m layers are printed on top of $R2$ ($R1$) in each step, and then the measurements are done, until the ratio of ones is less (greater) than 50%. When it is less (greater) than 50%, 2^{m-1} layers are printed on top of the resistor of the opposite branch, in this case $R1$ ($R2$) vice versa, and it continues until the number of printed layers reaches one. Therefore, the overall tuning time is significantly reduced.

In addition to these improvements for the resistor tuning flow, the TRNG output voltage level can be used to further improve the tuning efforts. The change of the TRNG output

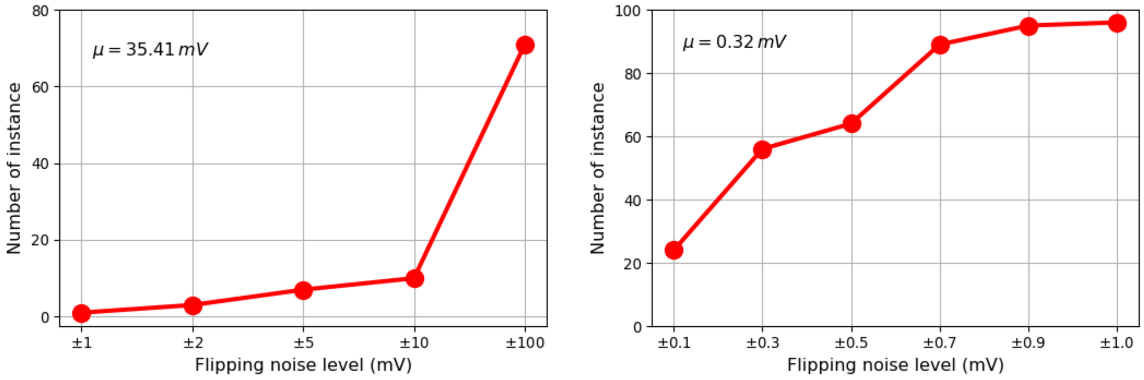


(a)

(b)

Figure 4.7: (a) Ratio of ones with respect to number of additionally printed layers of a TRNG instance under noise ($\mu = 0\,V, \sigma = 3\,mV$). Red dots indicate TRNG state and orange and green arrows represent change of TRNG state by printing additional layers to $R1$ and $R2$ respectively, based on the tuning flow presented in Figure 4.6. (b) Output voltage level vs. normalized number of additionally printed layers of 10 TRNG instances (layer numbers where output is flipped are normalized to 10.).

voltage level with each successive printed resistor layer can give an insight about the skewness of the TRNG so that the step size can be adjusted more effectively. Figure 4.7b shows the output voltage level of a TRNG circuit at different successive printing layers generated from the same setup described above. The more the circuit is skewed, the output voltage levels are closer to V_{DD} (or GND). As the skewness decreases, the output voltage level degrades more. This information could be used to further optimize the tuning flow. However, utilizing such information requires more precise, costly, and sophisticated measurements at the tuning steps, unlike the fast and low-cost binary readouts used in the proposed tuning flow.



(a)

(b)

Figure 4.8: Number of TRNG instances between various flipping noise levels (a) before resistor tuning, (b) after resistor tuning.

Table 4.1: Design parameters of transistors and resistors used in simulation of TRNG design. Resistance of resistors is initial value before resistor tuning.

	T1	T2	T3			R1	R2
Width	$200\,\mu m$		$400\,\mu m$		Resistance	$60\,k\Omega$	
Length	$40\,\mu m$						

4.3 Simulation-based Analysis

The proposed TRNG design and the impact of the resistor tuning flow is evaluated based on the simulation results in this section. The details of the simulation setup, the results of the resistor tuning flow, and the results of National Institute of Standards and Technology - Statistical Test Suite (NIST-STS) are explained in the following subsections.

4.3.1 Simulation Setup

The design parameter details are given in Table 4.1. We have assumed that the printed resistors are composed of one hundred layers resulting in $60\,k\Omega$ effective resistance, and we extrapolated the effective resistance for each additional printed layer. In addition, the process variation of the resistors is considered as ±10% of resistances based on the experiments. For EGTs, we have employed the variation model of EGT presented in [113]. We have used 100 Monte Carlo instances of printed TRNG, and a normal distributed noise source which has the mean (μ) and sigma (σ) of $0\,V$ and $3\,mV$ respectively, is introduced between inverters as an overall noise in the circuit to extract the results.

4.3.2 Resistor Tuning Flow Results

The minimum noise level to flip the output, which is called *flipping noise level* in this paper, is used to quantify the overall skewness of the TRNG instances. To extract the flipping noise level of the instances, instead of a normal distributed noise, a DC voltage was swept between $-100\,mV$ and $+100\,mV$. The number of TRNG instances based on their flipping noise levels,

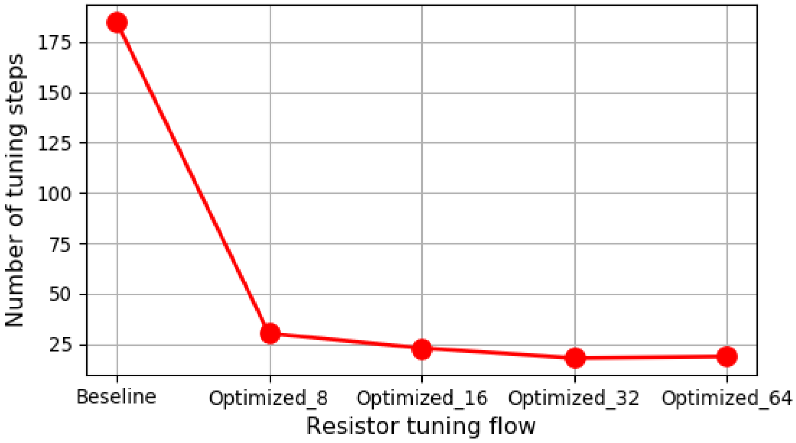


Figure 4.9: Mean number of tuning steps of 100 TRNG instances for baseline (one by one layer printing) and optimized tuning flows (2^m layer printing). Baseline denotes one by one additional layer printing flow. 8, 16, 32 and 64 denote initial 2^m value.

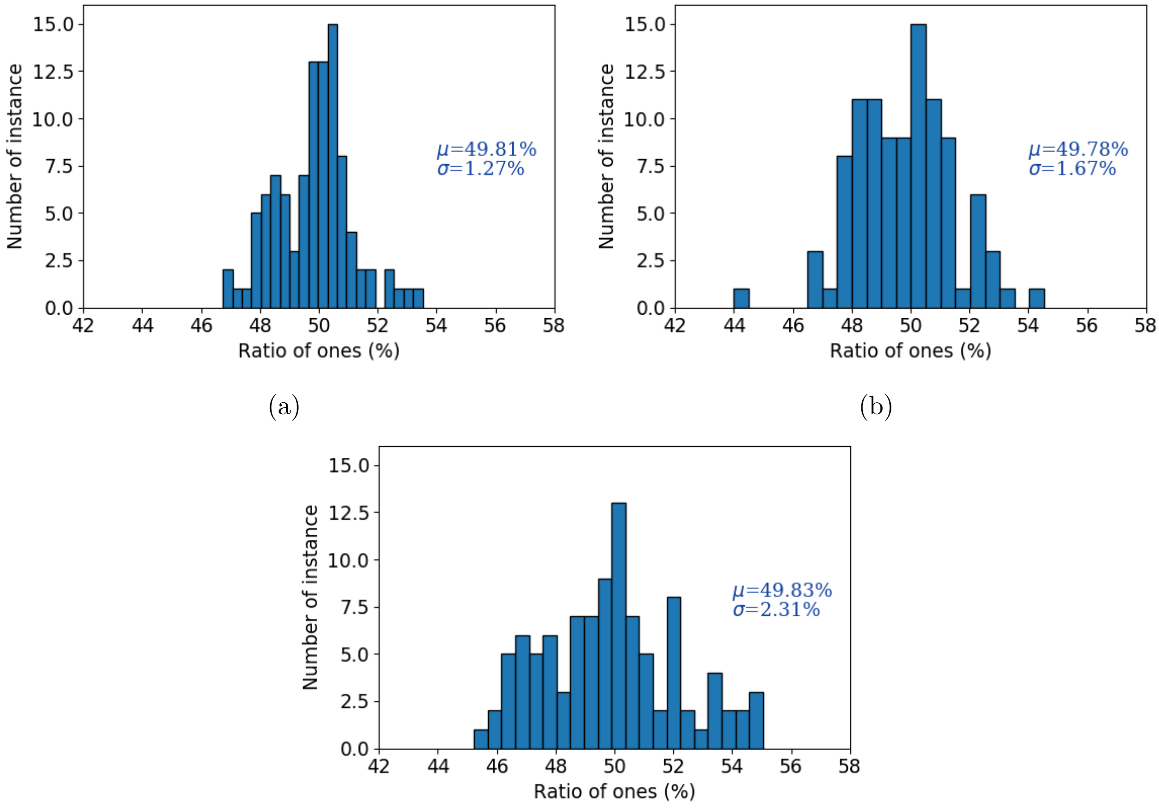
before and after the resistor tuning, is depicted in Figure 4.8. The mean values of the absolute flipping noise level before and after the tuning are 35.41 mV and 0.32 mV respectively, showing that the tuning flow reduces the mean variation by more than 110 times. In addition, the percentage of TRNG instances with the flipping noise level between ±1 mV, resulting in less bias at the generated bits, increases from 1% to 96% after the tuning.

As described in Section III, the resistors are tuned by printing additional layers in two ways which we name *Baseline* (one by one, printing only one resistor) and *Optimized_n* where n equals to 2^m, and is the step size (n steps and tuning both resistors) for convenience. The average trials to tune the instances are given in Figure 4.9. The average number of tuning steps for the baseline flow is 185.15 while with step size of 32 (m=5), the average number of tuning steps is minimized to 17.98. Therefore, the number of tuning steps is reduced by more than 10 times using our proposed method.

4.3.3 Analysis of Temperature Effect on Generated Bits

The generated bits of the circuits after the resistor tuning are slightly biased, compared to ideal true random bits because of the remained skewness of the process variation, due to the process variation of the additional printed resistor layers as well as the discrete nature of tuning.

The effect of the remained skewness on the bits can be quantified as the sigma (σ) of the distribution of the ones ratio in the generated bits, which is 1.27% while the mean is 49.81% at 25°C as shown in Figure 4.10a. To analyze temperature effect on the randomness of proposed TRNG, we utilized the EGT model with temperature effect described in [13], and implemented a temperature constant into printed resistor according to ratios given in [117]. The mean and standard deviation of the number of ones are 49.78% and 1.67% at 60°C, 49.83% and 2.31% at -35°C, as shown in Figure 4.10b and 4.10c, respectively. These results show that the effect of the temperature on the randomness of the tuned TRNGs is negligible.



(a)

(b)

(c)

Figure 4.10: Distribution of ratio of ones out of 100 bits for tuned 100 Monte Carlo TRNG samples at (a) 25°C, (b) 60°C, (c) -35°C. Sigma values are similar in distributions indicating that temperature effect on randomness is negligible.

4.3.4 NIST-STS Test Results

National Institute of Standards and Technology - Statistical Test Suite (NIST-STS) contains several tests explained in [118] to evaluate the randomness of the generated bits. We have used NIST-STS to evaluate the 10000 bits generated from each tuned TRNG instance. A P-value greater than 0.001 and a proportion greater than 96/100 are required to pass NIST tests. The results given in Table 4.2 show that the generated bits satisfy the requirements, and therefore, the proposed TRNG design passes the given NIST-STS tests.

4.4 Fabrication-based Analysis

We fabricated, tuned and characterized the proposed TRNG design to validate our approach. It should be noted that the inkjet-printed EGT technology used in the proposed TRNG is an emerging technology, and due to the lab setup which has limited yield and throughput, it requires a lot of effort to have functional circuits, and to tune these circuits at this stage of the technology. The details of fabrication and characterization are explained in the following subsections.

Table 4.2: NIST test results. Generated bitstream includes 10000 bits from 100 simulated TRNG instances. (A test requires the P-value greater than 0.001 and the proportion greater than 96/100 to pass.

Statistical Test	P-value	Proportion	Result
Frequency	0.202268	96/100	Pass
Block frequency	0.213309	100/100	Pass
Cumulative sums	0.428568	96/100	Pass
Runs	0.171867	99/100	Pass
Longest run of ones	0.437274	100/100	Pass
FFT	0.474986	98/100	Pass
Overlapping Template	0.055361	99/100	Pass
Serial	0.494555	100/100	Pass
Linear Complexity	0.249284	97/100	Pass

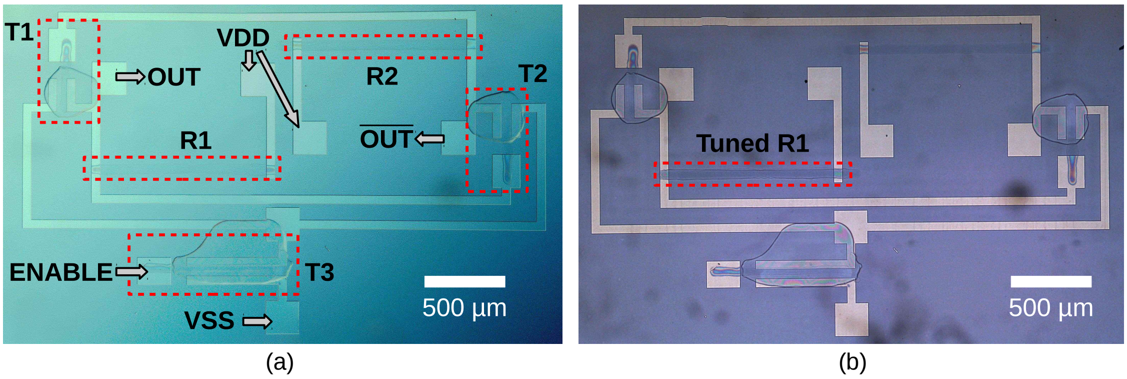


Figure 4.11: Images of a fabricated TRNG (a) Before resistor tuning. (b) After resistor tuning.

4.4.1 Fabrication and Characterization Setup

The proposed TRNG circuit contains three transistors and two resistors. The width and length of printed resistors are selected as 50 μm and 1 mm. The widths of T1, T2 and T3 are selected as 200 μm, 200 μm and 600 μm respectively, and the length of transistors is selected as 60 μm.

In the fabrication process of the EGTs, the channel material indium oxide (In_2O_3) semiconductor is inkjet-printed between drain and source electrodes which are lithographically structured indium tin oxide (ITO). Then, the substrates are annealed at 400 °C for two hours. After that, the electrolyte is inkjet-printed on top of the channel instead of a gate dielectric. Finally, poly(3,4-ethylenedioxythiophene)-polystyrenesulfonic acid ($PEDOT{:}PSS$) is inkjet-printed on top of the electrolyte as a top-gate [63, 119]. For printed resistors, PEDOT:PSS is inkjet-printed with the width of 50 μm and the length of 1 mm. The wiring and test pads are structured using a conducting material which is indium tin oxide (ITO).

The fabricated TRNG circuits are contacted through a Süss Microtech probe station. Agilent 4156C precision semiconductor parameter analyzer is used as source for the supply voltage. The enable signal ($ENABLE$) is generated with a Keithley 3390 arbitrary waveform generator. The enable and the output (OUT) signal are recorded with Yokogawa DL6104 digital oscilloscope. All measurements are performed at room temperature and 50% relative humidity.

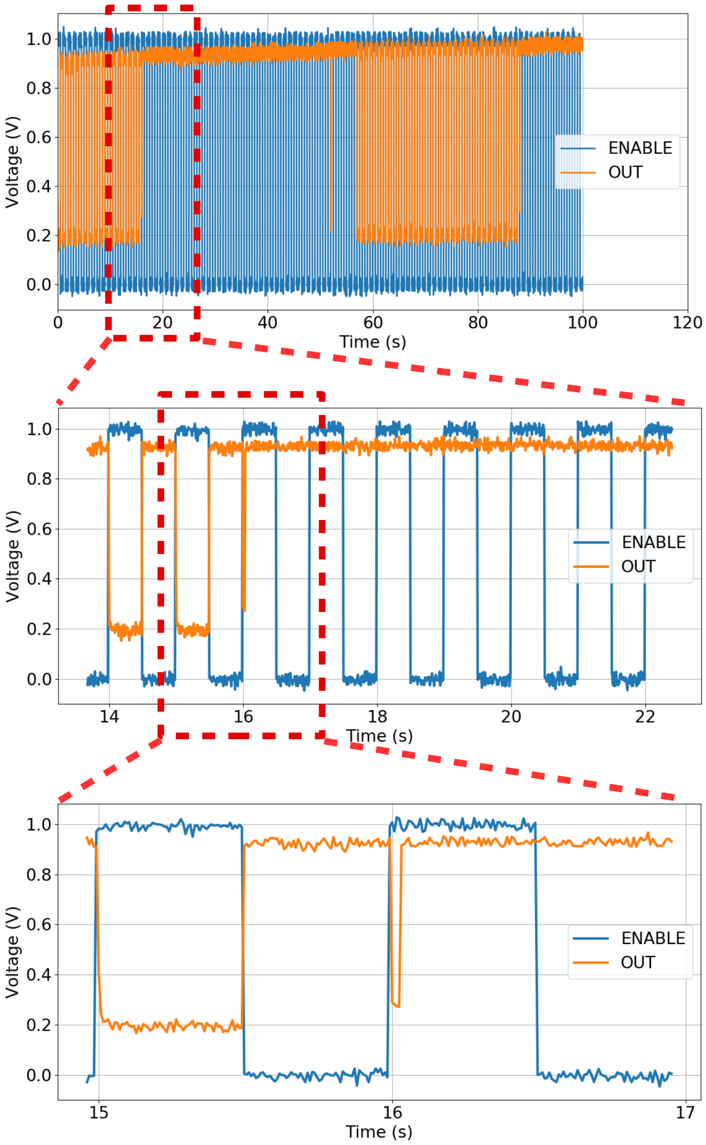
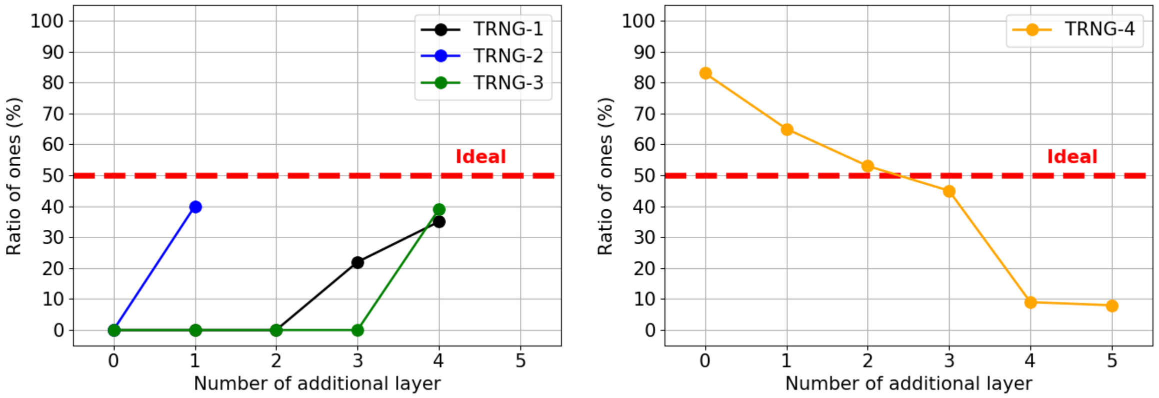


Figure 4.12: Timing waveform of a fabricated TRNG operating at 1 V after resistor tuning.

4.4.2 Results

The fabricated TRNGs are powered by 1 V supply voltage, and enabled by applying a 1 Hz, 50% duty cycle pulse signal to the *ENABLE* input. The high level of the enable signal is set to supply voltage. After each power-up, the circuits are enabled hundred times, and their outputs are measured to observe their functionality and calculate ratio of ones. Depending on the ratio of ones, an additional PEDOT:PSS layer is inkjet-printed on top of either $R1$ or $R2$ as discussed in Section 4.2.2.

Figure 4.12 is the measured timing waveform of a fabricated TRNG after resistor tuning. After enabling the circuit, the output (OUT) becomes ones or zeros depending on the mismatch of the inverter pair, which results from the process variation and the noise in the circuit. Since the additive resistor tuning alleviates the mismatch stemmed from the process variation, the output value relies on the random noise in each time the circuit is enabled. Figure 4.11 contains



(a)

(b)

Figure 4.13: Ratio of ones of out of 100 bits of fabricated TRNGs. (a) Ratio of ones for three TRNG converges to 50%. Bias due to process variation is mitigated by printing additional layer to corresponding printed resistor. (b) Ratio of ones for another TRNG converges to 50%. While more layers are printed to same resistor, it converges to 0%.

the annotated images of a fabricated TRNG before and after resistor tuning. The area usage of the fabricated TRNG is 4.59 mm^2.

The change in the ratio of the ones of the fabricated TRNGs with respect to the number of additional layers is given in Figure 4.13a. Fabricated TRNGs are annotated with a number (e.g., TRNG-1) for convenience. The measurements show that the resistor tuning mitigates the process variation of the circuit, and the ratio of ones for each TRNG converges to 50% which indicates that the output is highly dependant to random noise. Additionally, we have consistently printed additional layers on top of the R2 of TRNG-4 to examine its behaviour. As given in Figure 4.13b, after second and third additional layers are printed, its ratio of ones is reduced from 83% to 53% and 45%, respectively, meaning that the influence of the process variation is mostly reduced. Moreover, after fourth and fifth printed layers, the ratio of ones is decreased to 9% and 8%, respectively, since the tuning excesses the mismatch resulting from process variation.

We swept the supply voltage of the TRNG-3 from 0.6 V to 1.2 V to examine the susceptibility of its ratio of ones to supply voltage. The ratio of ones are 32%, 32%, 39% and 36% for the supply voltage of 0.6, 0.8, 1.0 and 1.2 V, respectively, which show that the change of the supply voltage does not bias the output to one value. Moreover, the slight change on the ratio of ones for different supply voltages demonstrates that the supply voltage susceptibility of the TRNG-3 is low.

Furthermore, we constantly measure the TRNG-3 for 12 weeks to check its functionality. During 12 weeks of measurements, the ratio of ones of TRNG-3 changed from 39% to 41%, and finally become 37%. This shows that the randomness of the tuned TRNG does not significantly change. Additionally, after 12 weeks, the maximum delays measured at different supply voltages are observed between 69 ms and 76 ms showing that it does not significantly vary at different supply voltages. Therefore, the throughput of the TRNG-3 is ~13.16 bit/s, which is sufficient for most of the PE applications.

Figure 4.14 shows the current and power consumption of the tuned TRNG-3 at various

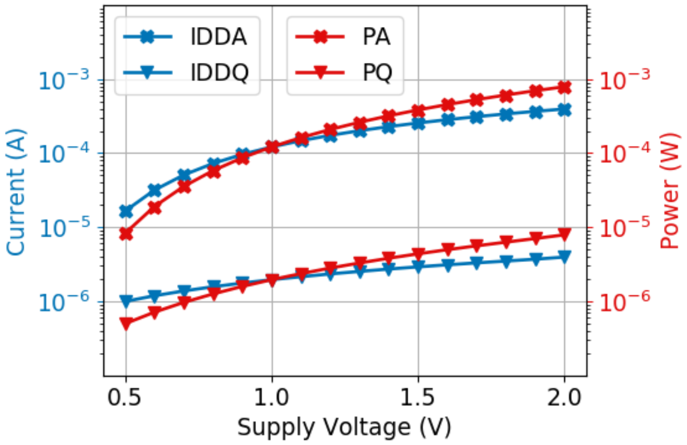


Figure 4.14: Current and power measurements of tuned TRNG-3 at various supply voltages. (left axis) Quiescent and active currents (IDDQ, IDDA), (right axis) quiescent and active power consumption (PQ, PA).

supply voltages. The quiescent and active currents decrease from ∼3.94 μA and ∼395.22 μA to ∼0.99 μA and ∼16.49 μA, respectively, when the supply voltage is lowered from 2.0 V down to 0.5 V. The quiescent and active power consumptions sink from ∼7.88 μW and ∼790.43 μW to ∼0.50 μW and ∼8.24 μW, respectively, when the supply voltage is reduced from 2.0 V down to 0.5 V. The active power consumption is always higher than the quiescent power consumption due to the enable transistor (T3) in the design.

4.4.3 Discussion on comparison with existing TRNGs

PE enables the applications where ultra low-cost is vital requirement. The ultra low-cost requirement constraints the complexity of PE circuits including security primitives such as Physical Unclonable Functions (PUFs) and TRNGs to secure interconnected applications of PE. The silicon-based TRNGs usually contains a calibration circuitry, which result in an additional cost, to mitigate the process variation. The complexity constraint of PE makes existing TRNGs infeasible in PE applications. The proposed circuit and its additive tuning method enable to realize a compact TRNG for ultra low-cost PE applications. The power-efficiency and the throughput of an existing silicon-based TRNG [116] and the proposed TRNG are incomparable since the feature sizes of the silicon-based TRNG and the printed TRNG are 14 nm and 10 μm respectively, and it is infeasible to extrapolate their power-efficiency and throughput. However, the area usage of two designs can be compared by extrapolating their reported area usage according to their feature size. The extrapolated area usage of the silicon-based TRNG is 555 mm^2 in 10 μm feature size while the reported area usage of the proposed TRNG is 4.59 mm^2 which is less than 1% of the silicon counterpart. So, the utilization of existing TRNGs in PE stem from high area usage resulting from their additional calibration circuitry.

4.4.4 Suitability of TRNG postprocessing techniques

The generated bitstream can be post-processed to compensate any bias and/or correlation. However, post-processing techniques introduce additional area and power overhead, which harm target low-cost and low-power applications [120]. Therefore, the post-processing technique should be selected according to the constraints of the target application. For instance, XOR function post-processing technique has high overhead, hence is inefficient for PE applications, since it calculates the odd parity of multiple TRNG instances to accumulate entropy from the TRNGs [76, 79]. On the other hand, the von Neumann corrector generates one bit from two bits, and removes consecutive ones/zeros increasing the entropy to one [121]. However, it reduces the throughput by at least 75% which is not harmful for most of PE applications where the operation requiring random bits is infrequent [27, 122]. Therefore, the von Neumann correct is a suitable post-processing technique since it has low overhead while providing sufficient throughput for the target applications.

4.5 Summary

Printed electronics is paving its way in many application domains. These applications may require random keys generated by TRNGs to secure their operations. Since PE circuits have high intrinsic process variation, designing a proper TRNG requires the mitigation of the process variation. In this chapter, we have presented a printed TRNG design that exploits the customizable fabrication feature of the PE to tune the circuit to mitigate the process variation impact. The proposed resistor tuning flow reduces the effect of the overall process variation by 110 times such that the tuned TRNGs can pass the NIST randomness test. Moreover, the proposed TRNG is fabricated and tuned using resistor tuning flow to validate our approach. The experimental results show that the fabricated TRNGs generate random bitstreams after tuning while operable at below 1 V and consuming down to ∼8.24 μW active power.

5 Reverse Engineering of Printed Electronics Circuits

The evolvement of Printed Electronics (PE) brings about security aspects, more specifically, the reverse engineering of PE circuits. However, the reverse engineering methodologies of silicon-ICs are unsuitable for PE circuits since PE circuit design and fabrication processes are fundamentally different from silicon-based chips. For instance, the custom fabrication feature of PE, thanks to its low-cost inkjet printing process, results in the use of miscellaneous circuit elements instead of the standard cell libraries used in silicon circuits, and non-structured layouts in the place of highly structured placement used in digital silicon chips. Besides, since the fabrication processes of PE circuits are additive and individual components such as transistors, resistors, and wires are printed individually and one by one, the variation of these circuits is higher than that of the silicon counterparts.

These differences imply that the existing reverse engineering (RE) methodologies for the circuits fabricated using wafer-scale silicon technologies, which contain standard elements with structured layouts and low variation, are inapplicable for RE of PE circuits. Therefore, a new RE methodology capable of dealing with these differences is required for honest (e.g. failure analysis and defect identification, yield learning and design improvement, detection of counterfeit products) and dishonest (e.g. counterfeiting, illegal cloning of a product) intentions.

In this chapter, we present the first RE methodology for PE circuits from image acquisition all the way to netlist extraction. We have defined the fundamental differences in PE design and fabrication that necessitate a new RE methodology. We have developed a robust, supervised learning-based RE methodology containing preprocessing, classification, and post-processing parts that can cope with the unique characteristics of PE design and fabrication. The results show that the proposed RE methodology extracts the netlist of various circuits without or with only minimal manual correction.

The contributions of this work are summarized as follow:

- We define the unique features of PE circuit design and fabrication, fundamentally different than the wafer-scale silicon-based circuits resulting in the necessity of a new RE methodology.
- We propose a robust RE methodology for PE circuits.
- We evaluate our RE methodology on several PE circuits.

The rest of the chapter is organized as follows: Section 5.1 explains the motivation of this work. The proposed RE methodology is described in Section 5.2, while the evaluation results are given and discussed in Section 5.3. Finally, Section 5.4 concludes the chapter.

5.1 Motivation of This Work

In PE circuit design and manufacturing, there are substantial differences compared to wafer-scale silicon-based ICs, leading to new security issues resulting in the rethinking of RE. The first difference is that circuit elements used in PE circuits vary in discordance with the silicon-based ICs where mostly CMOS is utilized. Some PE circuits based on organic technology use p-type transistors for the pull-up network and p-type transistors whose gates are shorted to its drain [123] while others use "pseudo-CMOS" logic [124]. In printed electrolyte-gated transistor (EGT) technology, n-type EGTs are used for the pull-down network while the resistor is used for the pull-up network because of the lack of p-type inorganic transistors [61]. Another difference which is derived from its customized fabrication feature is that the layouts of PE circuits are highly customizable. Since silicon-based circuits can only be fabricated in foundries with complex and extremely expensive manufacturing tools, and moreover due to complexity of such ICs, the layouts of these circuits are structured based on standard libraries, and the layout customization is limited in silicon-based ICs [69, 125]. In PE, personalized/customizable fabrication as well as the limited complexity of the circuits used for PE applications enables designers including non-expert users to customize the layout such that the layout is not structured well. Moreover, the shape of devices such as transistors, resistors and capacitors may change from one circuit to another since the efficient shape of devices are highly dependent on the capability of utilized printing processes and other limitations such as material types and consumption [27]. In addition, a generic layout designed and fabricated by experts can be mass printed but the fabricated layout can be customized in the field using low-cost printing schemes. In PE, the devices are individually spot printed. In addition, the number of printing layers is very limited, and may also be transparent. This is in contrast to wafer-scale silicon fabrication which has many complex processing steps and contains several fabrication layers, which are wafer coated and opaque. For instance, for wire crossing in silicon, there is an insulator layer in the entire wafer and vias are created to establish the connections through insulator layers. However, for PE, the wire crossings are fabricated on the spot and the insulator is droplet printed only at the crossing. The last difference is that PE circuits have higher inherent process variation than silicon counterparts since the PE fabrication methods are additive processes while silicon circuits are lithographically fabricated by using advanced subtractive processes. Since the circuit elements are printed one by one, there is no spatial correlation, as normally expected in the silicon processes [113, 13, 34]. These three group of differences can be summarized as follow:

- Non-standard circuit elements
- Customized layouts
- High variation

Since these differences are related to technology, design and fabrication, existing RE methodologies for silicon-based ICs are inapplicable for RE of PE, especially for the software post-processing part of RE. A new RE methodology considering these differences is required to cope with these unique characteristics of PE design, technology and fabrication.

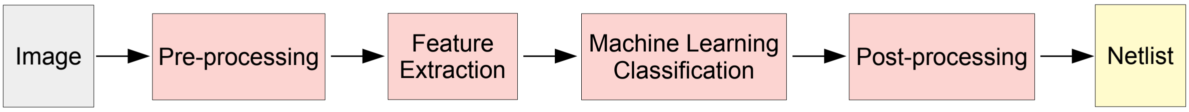


Figure 5.1: Overview of reverse engineering methodology of printed electronics circuits.

5.2 Reverse Engineering Methodology of Printed Electronics

This section explains the reverse engineering methodology starting from image acquisition to the netlist extraction. First, the image of a PE circuit is captured using an optical camera integrated to a microscope in contrast to the expensive tools such as scanning electron microscope (SEM) and focused ion beam (FIB) used in RE of silicon ICs. This image is preprocessed to remove any environmental effects such as noise and lighting problems. Then, a classifier based on supervised machine learning is utilized to classify circuit elements. At last, the classification results are post-processed to mitigate misclassified parts, such that the netlist can be extracted. After the transistors, resistors and their connections are fully detected, the circuit netlist can be extracted automatically as it is done in RE of silicon ICs [16, 90, 91]. The overview of the proposed RE methodology is illustrated in Figure 5.1. These steps are explained in detail in the following subsections.

As described before, through the involvement of fluids, and the less controlled production process of printed components, the resulting components show high variation, and the customizable fabrication results in non-standard cell layout design [11, 12, 126, 113]. Because of these differences, automated library-cell-based identification methods such as [92, 90, 89, 16, 91] is therefore inefficient. We thus resort to supervised machine learning techniques to eliminate the need for such expert-generated descriptions. The details of the classification, and the post-processing are illustrated in Figure 5.2.

5.2.1 Supervised Machine Learning

Supervised machine learning (ML) uses algorithms to generate a mapping (classifier) $m : X \to Y$ from a set of provided (explanatory) variables X, also referred to as features, which correlate with some other set of observed (response) variables of interest Y called labels. The classifier m is thereby developed by trying to map a set of observed tuples of instances $D = \{(x, y) \,|\, x \in X, y \in Y\}$ as well as possible, that is, assigning the correct y to a given x, while the details depend on the algorithm used. The evaluation of classifier m for a given x is also referred to as prediction.

Generally, not all available instances of D are utilized to develop the classifier (training), but only a subset $D_{train} \subset D$ (training set), while another subset $D_{test} = D \setminus D_{train}$ (test set) is held back to evaluate the quality of the classifier later on. The partitioning of the dataset is done to detect unwanted effects like the classifier being able to predict the training data very well but performing poorly on the test set. This would be an indicator that the classifier does not capture the general relationship between X and Y, which is desired, but overly adapted to D_{train}. This problem is also referred to as over-fitting.

In our use case, the data (x, y) will be generated by processing a set of (training) images of printed circuits, e.g. Figure 5.3a for a PUF circuit. The images will firstly be cut into multiple

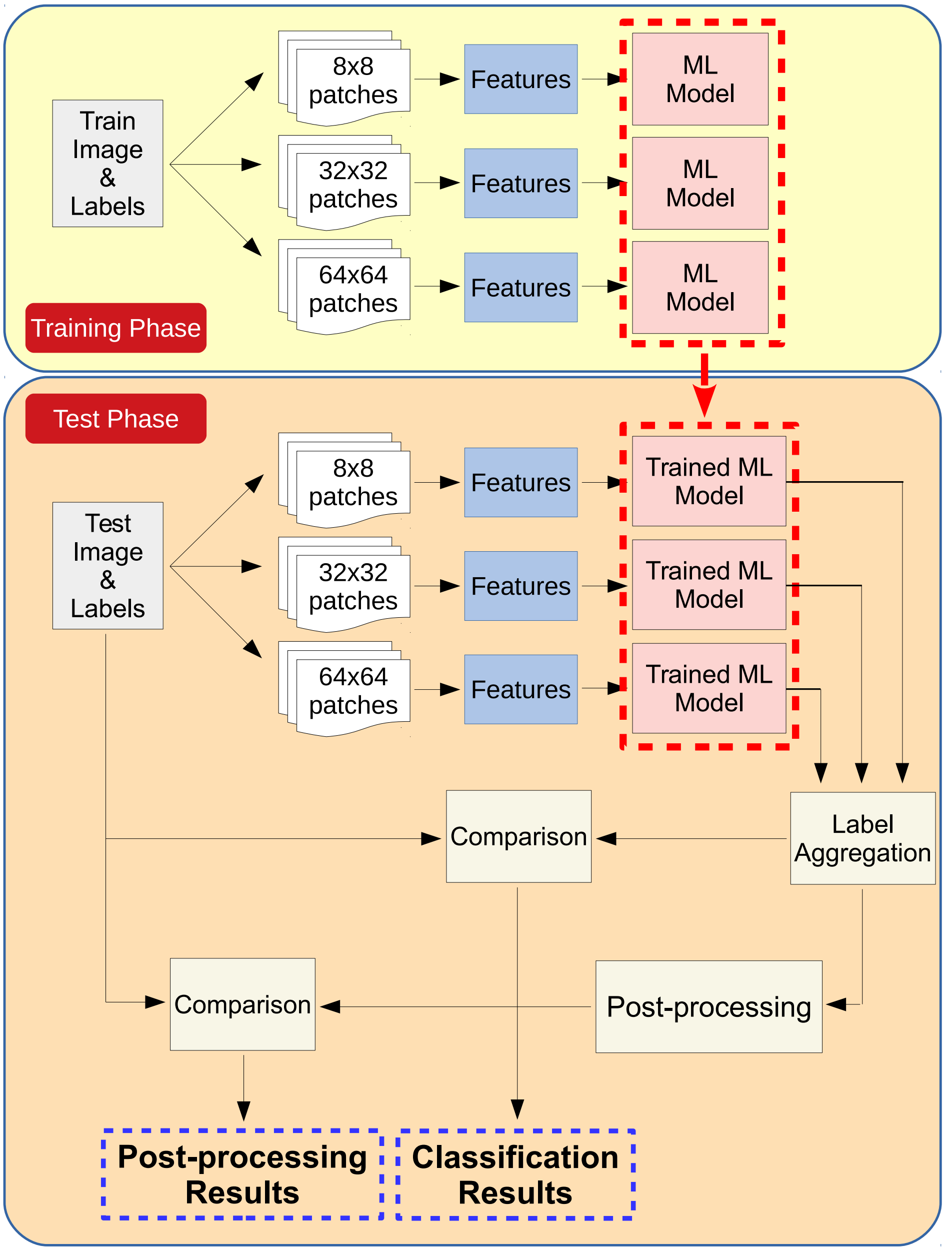


Figure 5.2: Training and test processes of proposed reverse engineering methodology of printed electronics circuits.

small images called patches. From these patches, we then extract vectors $x \in \mathbb{R}^n$, representing several calculated attributes (features), and labels $y \in \{T, R, W, B\}$ representing transistors (T), resistors (R), wires (W) and blank substrate (B).

In the following, we will describe the necessary steps to prepare the images of printed circuits in order to apply ML for the detection of individual components, namely transistors and resistors, as well as the wires connecting them.

5.2.2 Image Preprocessing and Training Label Preparation

Since the raw images show various properties, like non-homogeneous lighting and dust, which could influence the detection performance negatively, we apply the following image processing steps to mitigate them. See Figure 5.4 for the respective steps applied to the training image of a printed Physically Unclonable Function (PUF) circuit.

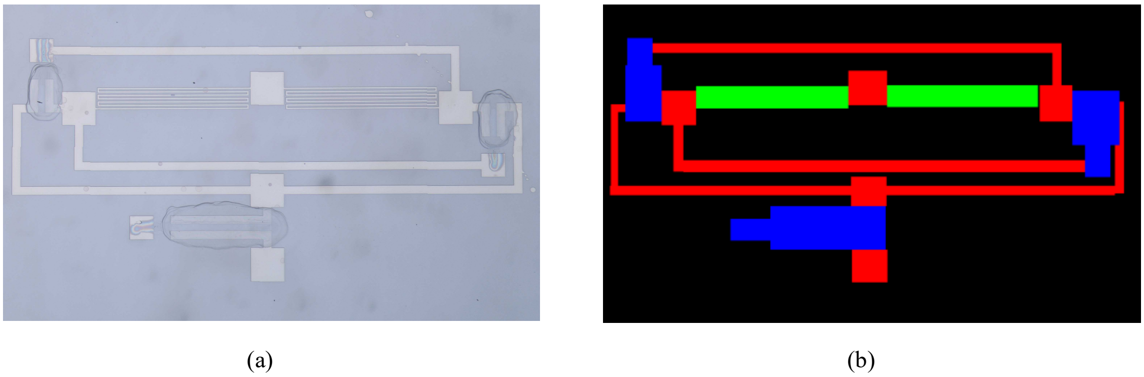
1. Conversion to grayscale
2. Image denoising
3. Image normalization
4. Edge detection
5. Adaptive Histogram Equalization
6. Image denoising
7. Adaptive Histogram Equalization

Firstly, the image is converted to a grayscale image to promote invariance to coloration. Even though the color channels might carry some information, the main coloration of the components is produced by different lighting or background.

The image denoising is done using bilateral filtering [127] which is an edge-preserving filter that averages pixels not just based on closeness in location, but also based on similarity in pixel values. After that, normalization is applied to scale all pixel values to the range of $[0, 1]$. This is mostly done to mitigate different lighting conditions between different pictures. Following the normalization, an edge detection step using Robers cross operator [128] is performed.

In the next step, Adaptive Histogram Equalization (e.g. see [129]) is employed, which should further increase the contrast of the detected edges by locally adapting the pixel intensity values for darker or lighter regions. Following this, the image is denoised again and Adaptive Histogram Equalization is used one more time which, in our experiments, improves the results further. All preprocessing steps can be performed in *python* using the $scikit - image$ library [130].

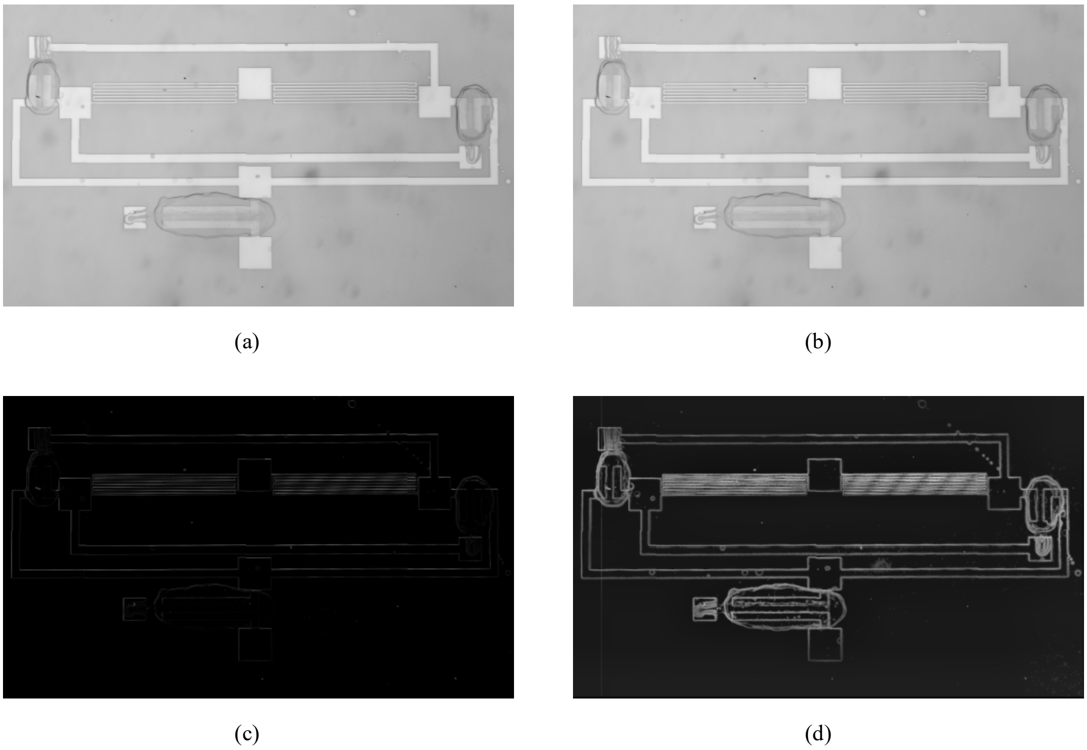
Furthermore, to have labels y for the ML algorithm later on, every pixel of the training image needs to be assigned one of the values of $\{T, R, W, B\}$ by the user. This can be done by approximately labeling whole regions of pixels at a time. See Figure 5.3b for the labeled training image.



(a)

(b)

Figure 5.3: (a) PUF_2 circuit image (b) Label of PUF_2 image; green: wire, blue: transistor, yellow: resistor, dark blue: blank.



(a)

(b)

(c)

(d)

Figure 5.4: Preprocessing of PUF_2 image, (a) Denoised PUF_2 image using bilateral filtering (b) Normalized PUF_2 (c) The Edges of PUF_2 extracted using Roberts cross operator (d) The result of Adaptive histogram equalization on PUF_2

5.2.3 Extracting and Labeling of Patches

To apply an ML Algorithm to the preprocessed image, we first need to generate our training data D_{train} consisting of tuples of (x, y) instances. For this, we divide the image into multiple patches p of $c \times c$ pixels. Those patches will later be used to calculate features $x \in \mathbb{R}^n$ and labels $y \in \{T, R, W, B\}$ for the training of the ML algorithm. A patch $p \in \mathbb{N}^{c \times c}_{\leq 255}$ can be thought of as a matrix of values containing natural numbers between 0 and 255. We denote the set $\mathbf{P}^{c \times c}$ as the set of patches p generated by partitioning the image into $c \times c$ pixels. Additional pixels at the edges, which can not form a full $c \times c$ patch, are omitted.

Since only one label y is assigned to a patch, the choice of c poses a trade-off. The higher c, the less patches are generated which will reduce the resolution of the classification. On the other hand, if c is taken to be too small, the features extracted from a patch might not contain enough information to distinguish the components. The value c should be chosen according to the resolution of acquired optical images and the feature sizes of the circuit elements. Since the feature sizes of the elements are mostly diverse, we have used three c values in the methodology. Specifically, the patches of used circuits in this work are extracted for $c \in \{8, 32, 64\}$ which result in the sets of patches $\mathbf{P}^{8 \times 8}$, $\mathbf{P}^{32 \times 32}$ and $\mathbf{P}^{64 \times 64}$.

5.2.4 Feature Engineering

In the following, we describe which features are extracted from a patch $p \in \mathbf{P}^{c \times c}$. A vector x, created by combining all extracted features of a given patch p into a list, and the label y can then be seen as an instance of (x, y) for training. The following methods are utilized to generate the features:

- Histogram of Oriented Gradients (HOG)
- Summary statistics of pixel values
- Histograms of pixel values
- Number of peaks
- Number of corners

Histograms of Oriented Gradients (HOG) [131] is an algorithm that generates features based on weighted counts of gradient orientations in an image. The HOG Algorithm is mainly defined by three parameters which are the *cell size* specifying the size of the regions for which histograms of gradients are created, the number of different *orientations* which correspond to the bins of the histogram, and the *block size*, which is used to normalize the histogram of multiple *cells* later. The steps performed by HOG usually include an optional normalization of the image, a computation of the gradients along the vertical and horizontal axis and the binning of the gradients based on their orientation, while their magnitude is used as a weight. The computation of the binning of the gradients is followed by a so called block-normalization step which selects multiple neighboring *cells* depending on the *blocksize* and normalizes them jointly. As HOG will generally produce many features, we calculate summary statistics from the results to strongly reduce the amount of features generated. For the summary statistics, we use the *mean*, *standard deviation*, *min* and *max*, this should not only decrease the amount of features, but also lead to increased invariance with respect to the specific position of patterns in the patch.

Furthermore, we apply several summary statistics to the pixel values of the preprocessed patches, namely mean, standard deviation, min, max and the counts from a histogram of the pixel values with eight bins, as well as the number of contrast peaks. We hope to capture generally lighter and darker areas with this feature, where the use of the summary statistics leads to position invariance within a patch. Additionally, we extract the number corner orientations [132] from the patch.

For the training images, we also need to select the label y of the patch. Since we are just allocating one label y to a patch $p \in \mathbf{P}^{c \times c}$, we need to apply an aggregation function to the labels of the pixels belonging to the patch. As the labels are categorical, taking the most frequent value (majority vote) is a natural choice. In case of a tie for the majority, the following label preference relation is used $B \succ T \succ W \succ R$, where $B \succ T$ indicates preference of B over T.

The feature calculation as well as label extraction steps will be applied to all patches $p \in \mathbf{P}^{c \times c}$ for $c \in \{8, 32, 64\}$, generating a different set of training data for each value of c.

5.2.5 Component Detection using Ensembles of Random Forests

A machine learning (ML) algorithm which has proven to work generally well in a lot of cases is Random Forest [133]. Random Forests use multiple Decision Trees trained on different subset of the training data and features to produce a prediction.

Decision Trees (CART) [134] are binary trees partitioning the feature space ($\mathbb{R}^n$ in our case) into different regions. These regions are chosen such that the training data points $D_{train} = \{(x, y) \,|\, x \in \mathbb{R}^n, y \in \{T, R, W, B\}\}$ populating them are as pure as possible with respect to their label y. The purity of a partition can be measured using any measure of purity, where generally the Gini-coefficient or the Shannon information entropy is used.

The partition is formed iteratively as follows. Starting from the root node, for all features, all values of the feature leading to different partitions are evaluated as possible splits. The split, consisting of a feature and a value tuple, producing the highest purity in the resulting partition is then selected and two child nodes representing the two regions separated by the split are added to the tree. This procedure is repeated for each child node, i.e. subregion, until some termination criterion is reached. While the trivial termination criterion is given by fully pure leaf nodes, additional criteria can be used, e.g. an upper bound on the depth of the tree, or a minimum number of data points in a region, to allow for a split to be performed. These additional criteria are often utilized to reduce the previously described over-fitting effect and increase the generalization properties of the prediction. After a tree is grown this way, a prediction for a data point $x \in \mathbb{R}^n$ can be obtained by returning the most frequent label value y in the region (leaf node) x belongs to. While this procedure, due to its greedy nature, might only reach a suboptimal partition with respect to the purity of the leaf nodes, it is computationally more viable than exhaustive search and produces good results in practice. To achieve sufficient generalization, i.e. prevent over-fitting and produce a classifier with a good test set performance, the termination criteria needs to be chosen carefully.

Another method which tries to generate a more robust classifier from trees uses so called Ensembles of multiple slightly different trees. One method to generate such an Ensemble is Bagging [135], which is short for bootstrap aggregation. In Bagging, k samples of size $|D_{train}|$

of the training data D_{train} are drawn with replacement (bootstrapping), and a Decision Tree is trained on each set using the aforementioned procedure. To obtain a prediction from an Ensemble of Decision Trees, an aggregation function is applied to the set of outputs of all Decision Trees of the Ensemble. In a classification setting usually the most frequent value is used. Ensembles of Decision Trees are generally less prone to over-fitting than individual Decision Trees since it is very unlikely that all trees were trained on the whole training data, which means they can not overfit it in the sense of memorizing training examples. Furthermore, this procedure simulates the effect of missing data on the models, while the aggregation of multiple of trees reflects the uncertainty of data points and leads to a more robust prediction where single instances have little influence.

Extending the idea of the Bagging procedure, Random Forests additionally select random subsets of features for each tree. This reflects uncertainty about the features used and can help to create a more robust representation that relies less on the presence of patterns in individual features.

All Random Forests described in the following are trained using the $scikit - learn$ [136] library, with a parametrization of 200 Decision Trees of depth 30 and the Gini-coefficient as label purity measure.

As we generate three sets of training data (see Section 5.2.3), one for each value of $c \in \{8, 32, 64\}$, we train a separate Random Forest on each training data set. We denote the Random Forest trained on the data generated by extracting (x, y) from $\mathbf{P}^{c \times c}$ as RF_c. Note that for each of the Random Forests a different number of predicted labels is obtained, e.g. RF_{32} will have four predictions for an area of 64×64 pixels, while RF_{64} will just have one.

To combine the predictions of the three Random Forests into a single predicted label for a 64×64 pixel patch, we first aggregate the predicted labels on the highest prediction resolution, i.e. 8×8 by RF_8 by majority voting. In case of a tie we utilize the preference relation used before, namely $B \succ T \succ W \succ R$. This will result in 64 labels for 8×8 patches in a region of 64×64 pixels.

After this step, the 64 aggregated 8×8 pixel predictions for the patches are combined to one label of a single 64×64 patch. The same majority voting methodology is used for this step but with one small adjustment regarding the B (blank) label. A 64×64 region is only assigned the label B if all of its 8×8 patches were assigned the label B, else, the second most frequent label is used. In case of a tie, we again use the same label preference relation as for the first step (excluding the relation for B). This way, the result of the combination of three Random Forest predictions will return one label for a 64×64 region. The final label of a 64×64 region is thus the result of an Ensemble of Random Forests trained on different resolutions. For a schematic illustration of the combination of the predictions of the three Random Forests see Figure 5.5.

Note that for this to work, unconnected wires need to be more than 64 pixels apart or they could be shortened. If such problems are observed, smaller $c \times c$ resolutions should be chosen. For an illustration of the individual predictions of the Random Forests on a real image see Figure 5.6.

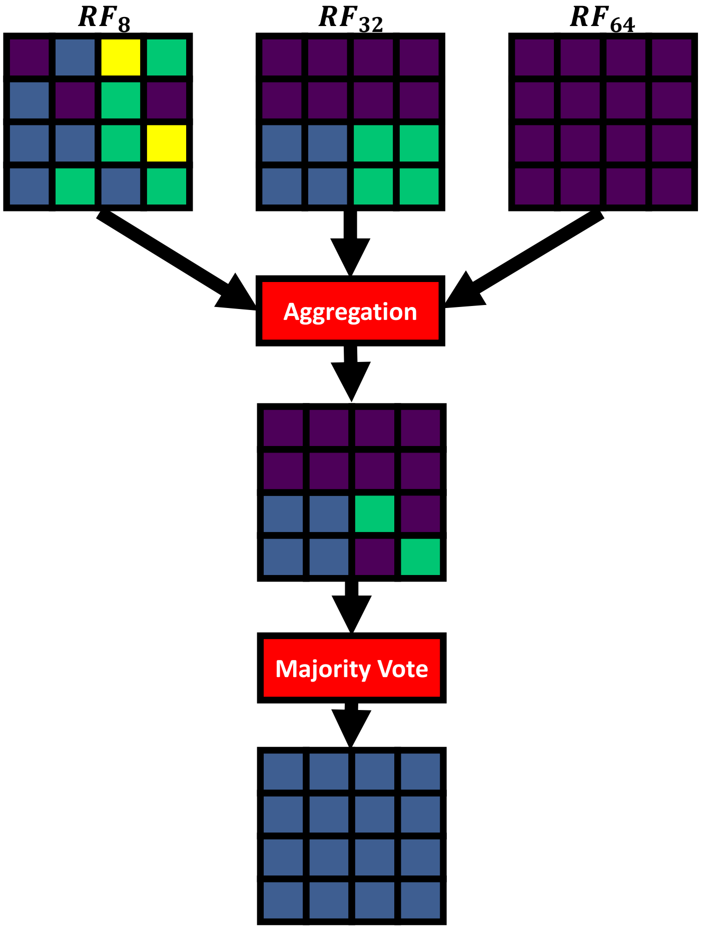


Figure 5.5: A schematic illustration of the procedure used to aggregate the predicted labels of the three Random Forest models into a single label. The labels of RF_8 where unified to 16×16 blocks for readability. Note that even though the majority of all smallest resolution patches are labeled B (blank) after the aggregation, the second most frequent label, namely T (transistor), is assigned after majority voting due to B being ignored in this step.

5.2.6 Post-processing

Due to the nature of the data we expect some wrong predictions. Even though small errors might not matter, as for example a single wrongly labeled patch on the substrate, other errors could lead to a false netlist. The most likely error leading to a false netlist is multiple misclassified patches causing a disconnected wire. We thus propose some post-processing steps to counteract these problems. Following the assumption that spatially close patches are highly probable to share the same label, we employ a post-processing step using a filter kernel for label correction.

A filter kernel on a patch uses aggregated information from a neighborhood of the patch to adjust its label. As such, it has two degrees of freedom. Firstly, the definition of the neighborhood and secondly the aggregation function. In our case, we will only consider directly adjoining patches in the horizontal and the vertical axis of the patch of interest. See Figure 5.7 for the filter kernel on the green patch.

This kernel will be applied two times, each time with a different aggregation function. The

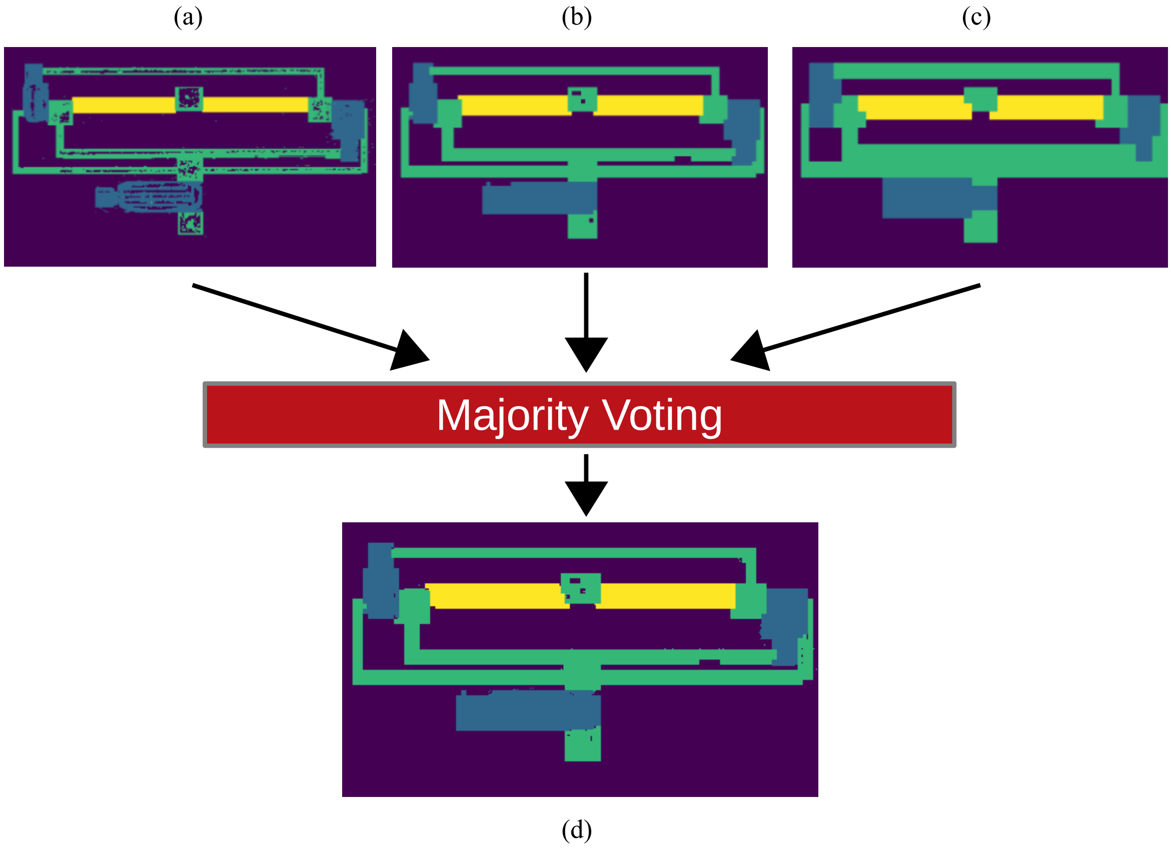


Figure 5.6: Random forest prediction results, (a) Prediction of RF_8 (b) Prediction of RF_{32} (c) Prediction of RF_{64} (d) Combination of three predictions by majority voting.

first time, the label correction is based on a majority vote, where in case of a tie for the most frequent label, again, the preference relation $B \succ T \succ W \succ R$ is used. The second time the aggregation is based only on a preference relation, namely $T \succ R \succ W \sim B$, where $W \sim B$ denotes indifference between W and B, such that not the most frequent label decides on the label adjustment i.e. majority voting, but the highest ranked label according to the preference relation.

The cross-shape of the kernel is mandatory to not loose the properties of for example a vertical wire surrounded by blank space. Given a wire size smaller than the patch resolution, the wires would always disappear if the diagonally adjoint patches would be included in the kernel, since six blank patches could overpower three wire patches. Note that, excluding the first, majority-vote based step and modifying the label dominance from $W \sim B$ to $W \succ B$ would also solve this problem but could in turn lead to connecting two wires separated by blank space which would shorten a connection. As can be seen in Figure 5.8, the kernel-based post-processing steps can drastically increase the quality of the detection of the components and the connections.

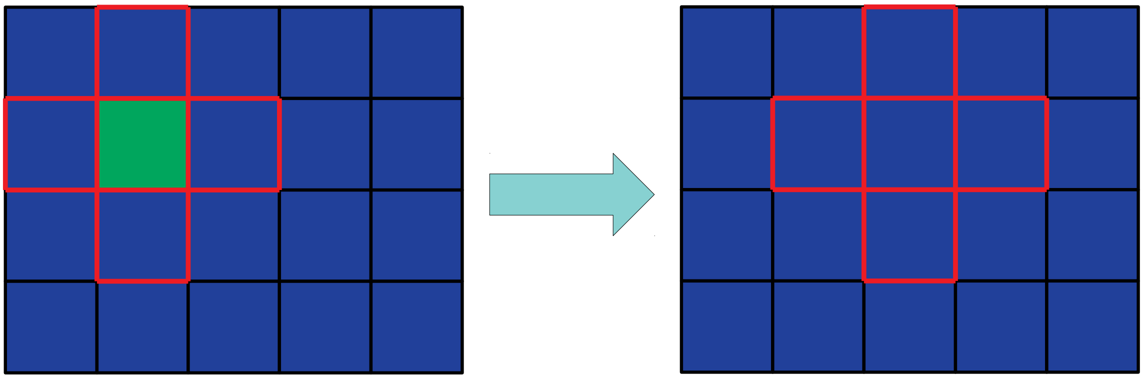


Figure 5.7: The filter kernel set up around the green patch. The label is adjusted based on its value and the labels of the four horizontally and vertically adjoint patches. This is done for every patch in the image.

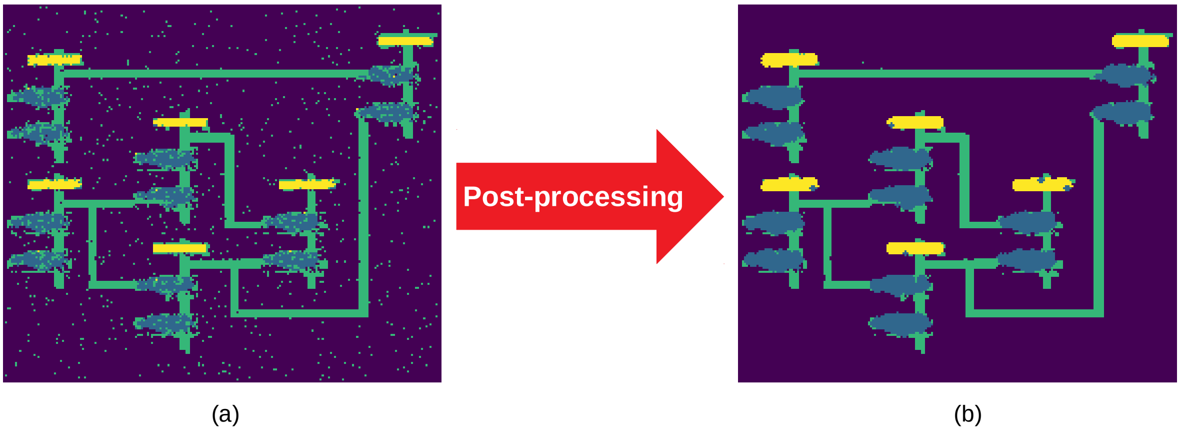


Figure 5.8: Illustration of classification and post-processing results of $C17_1$ circuit. (a) classification results, (b) post-processing results

5.2.7 Extraction of Netlist from Patches

After the detection of circuit components and their wires in terms of patches, this information has to be transformed into circuit netlist. For this reason, The connected component labeling (CCL) algorithm [137] is applied to classified patches in order to label each transistor, resistor and wire so that they are automatically annotated. A reverse engineer should manually annotate the power supply (V_{DD}) and ground (GND) to extract the netlist accurately. After the annotation, the method given in Algorithm 1 is used to extract the text-based netlist.

The annotation step extracts the nets (wires) and their patches using CCL. The patches (or pixels) can be addressed via *n.patches* for a given net n. Every patch p has access to its horizontal and vertical neighbours through the attribute *p.neighbours*. Furthermore, p can access the component it belongs to, (through *p.component*) as well as its label *p.label*. The brackets [] indicate a list, while {} indicates a set (note the uniqueness property of the set). It should be noted that the netlist extraction algorithm extracts the connections without their input/output directions which have to be manually given by the reverse engineer. This

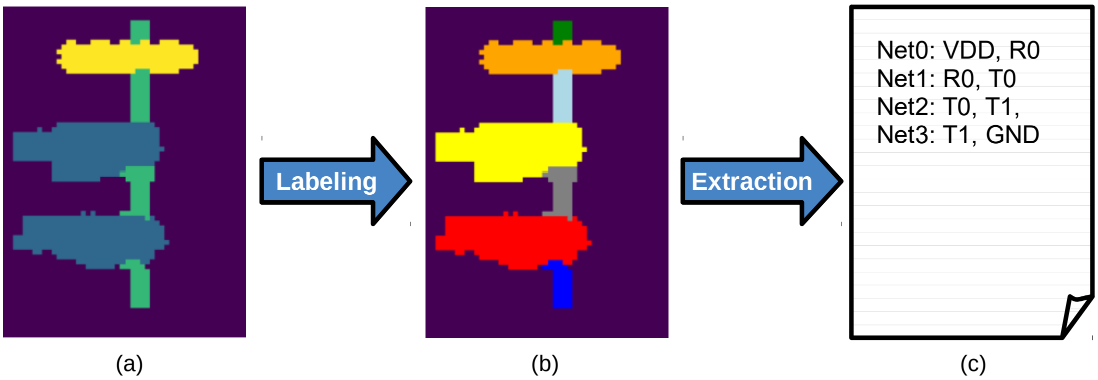


Figure 5.9: Netlist extraction from patches to netlist. (a) Classified patches, (b) Labeled patches for annotation, and (c) Netlist of NAND gate.

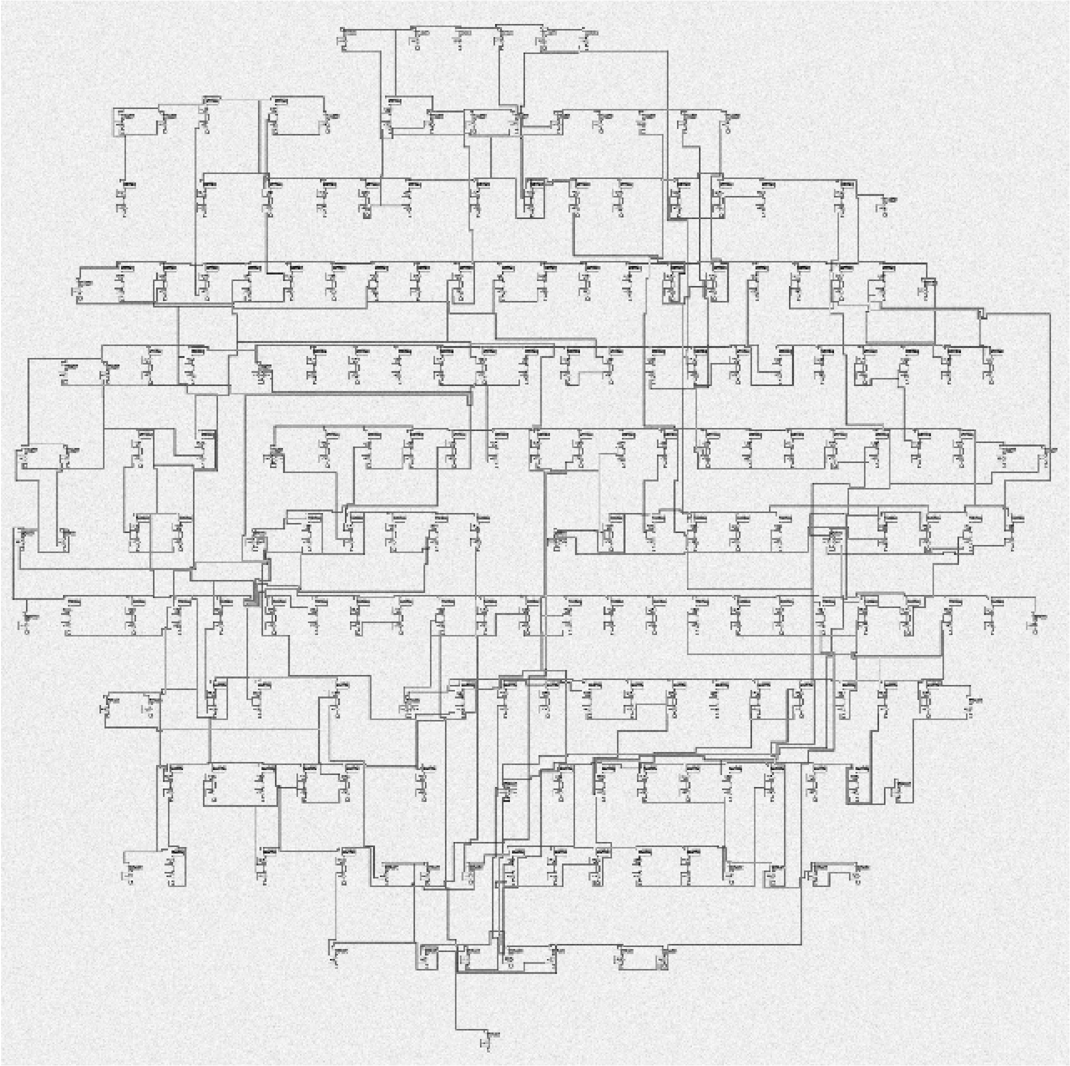


Figure 5.10: Negative semi-real image of a C432 circuit. Randomly selected the preprocessed images of circuit elements are placed to noisy blank image, and connected using wires.

Algorithm 1 Netlist Extraction

```
procedure NetlistExtraction(input nets)
    net_lists = []
    for n in nets:
        net = {}
        for patch in n.patches:
            for nb in patch.neighbours:
                if nb.label in ['T','R']:
                    net.append(nb.component)
        net_list.append(net)
    return net_list
```

is sufficient to construct a schematic and/or conduct further analysis such as inferring the functionality of the circuit [16, 90, 91]. An example netlist extraction of a NAND gate from patches to text-based netlist is shown in Figure 5.9.

5.3 Evaluation Results

In the following, we describe the test setup including the circuits and their images used to validate the methodology. We explain the evaluation metrics, and discuss the results obtained by applying the proposed methodology to real and semi-real images of various circuits.

5.3.1 Test Setup

Due to the infancy stage of the technology and the costs associated with the design and fabrication, we are currently only able to fabricate limited and small-size test structures. Because of these practical limitations, we used the images of several individually fabricated components (transistors, resistors and wires) to construct synthetic images, namely "semi-real image", of larger designs. Figure 5.10 is an example of a negative semi-real image of a C432 circuit. The images of fabricated components and circuits are acquired using an optical camera integrated to a microscope.

To generate semi-real images, first, Gaussian noise is added to a blank image to imitate the noise of camera and the imperfectness of the substrate (e.g. dust). Then, randomly selected preprocessed images of several transistors and resistors are placed and connected by the images of wires to form the pictures of our evaluation circuit. Furthermore, the images of the transistors and resistors are manipulated via scaling and flipping. Through this, a diverse set of transistor and resistor images can be achieved and it can be guaranteed that no exact copies of training set images are in the test set. We have generated the semi-real images of a NAND gate, a flip-flop and several ISCAS'85 circuits [138] which contains up to 644 gates using the method. In addition, we obtained two fabricated printed PUF images (PUF_1, PUF_2), which are based on EGT-based inorganic PE technology [13]. The images used in evaluation are summarized in Table 5.1. The image of PUF_1 circuit is used to train the ML model, which is subsequently used in the reverse engineering of PUF_2, NAND gate, $C17_1$ and $C17_2$ circuits, while other circuit images are reverse engineered with the ML model

Table 5.1: Circuit images used in evaluation, their explanations, and types

Circuit Name	Explanation	Image Type
PUF_1	Fabricated PE-PUF	Real
PUF_2	Fabricated PE-PUF	Real
NAND Gate	Generated NAND gate	Semi-real
Flip-flop	Generated Latch-based flip-flop circuit	Semi-real
$C17_1$	Generated ISCAS'85 C17 circuit containing 6 NAND gate	Semi-real
$C17_2$	Generated ISCAS'85 C17 circuit containing 6 NAND gate	Semi-real
$C17_3$	Synthesized ISCAS'85 C17 circuit containing 7 NAND gate	Semi-real
$C432$	Synthesized ISCAS'85 C432 circuit containing 148 NAND, 50 NOT and 7 NOR gate	Semi-real
$C499$	Synthesized ISCAS'85 C499 circuit containing 411 NAND, 227 NOT and 6 NOR gate	Semi-real
$C880$	Synthesized ISCAS'85 C880 circuit containing 301 NAND, 114 NOT and 13 NOR gate	Semi-real
$C1908$	Synthesized ISCAS'85 C1908 circuit containing 351 NAND, 154 NOT and 14 NOR gate	Semi-real

trained with 10% of themselves.

$$\text{Accuracy} = \frac{\text{\# correctly labeled instances}}{\text{\# all instances}} \tag{5.1}$$

$$\text{Precision of label } \bar{y} = \frac{\text{\# correctly labeled instances of } \bar{y}}{\text{\# all instances labeled as } \bar{y}} \tag{5.2}$$

$$\text{Recall of label } \bar{y} = \frac{\text{\# correctly labeled instances of } \bar{y}}{\text{\# all instances of } \bar{y}} \tag{5.3}$$

5.3.2 Evaluation Metrics

To judge the classification quality of the methodology, we report the Accuracy (see Equation 5.1) for the patches extracted from the circuit images. The Accuracy is the number of correctly predicted patch labels by the classifier. To further investigate the classification quality for individual labels, we additionally report Precision and Recall. The Precision of a prediction (see Equation 5.2) for a given label $\bar{y}$ (e.g. transistor, resistor, etc.) measures how many of the instances that were assigned the label $\bar{y}$ are truly of label $\bar{y}$, while Recall (Equation 5.3) is the ratio of true instances of $\bar{y}$ that were assigned $\bar{y}$. Generally, there is a trade-off between

Table 5.2: Accuracy of patch detection.
Classification indicates the accuracy before post-processing steps while post-processing indicates the accuracy after post-processing steps.

Training Data	Circuit	Accuracy (%)	
		Classification	Post-processing
PUF_1	PUF_2	80.86	86.51
PUF_1	Flip-flop	89.08	94.06
PUF_1	NAND Gate	85.75	93.15
PUF_1	$C17_1$	86.62	92.10
PUF_1	$C17_2$	91.38	94.94
10% of itself	$C17_3$	96.40	96.61
10% of itself	C432	92.66	91.88
10% of itself	C499	84.55	84.94
10% of itself	C880	84.84	85.17
10% of itself	C1908	86.75	87.15

Table 5.3: $C17_1$ circuit precision and recall results before (Classification) and after (Post-processing) post-processing steps.

Label	Precision		Recall		Number of patches
	Classification	Post-processing	Classification	Post-processing	
Blank	0.9052	0.9389	0.9741	0.9868	30968
Transistor	0.9806	0.9689	0.2947	0.5687	5096
Wire	0.5384	0.7356	0.8552	0.9106	2952
Resistor	0.9625	0.8740	0.5225	0.7414	1160
Avg / Total	0.8895	0.9259	0.8662	0.9210	40176

Precision and Recall and it is almost always possible to decrease either in favor of the other one, e.g. label everything as transistor to detect all transistors and maximize Recall while obtaining low Precision.

The aforementioned metrics provide insights about the patch-based detection of the machine learning and post-processing steps. However, since the main goal of our RE is to detect circuits elements and their connections (netlist), the focus of the evaluation should be on the number of correctly identified components and wires. Therefore, we report the number of detected transistors, resistors and connections.

5.3.3 Discussion of Results

The classification results for the accuracy before (*Classification*) and after the post-processing (*Post-processing*) for all circuits are given in Table 5.2. The results show that the classification and post-processing accuracies of all images are higher than 80.86% and 84.94% respectively. The average classification and post-processing accuracies are 87.89% and 90.65% respectively. Through post-processing, for most of the tested circuits, we considerably improve the other metrics for the individual components. For instance, for $C17_1$, it is evident from Table 5.3 that, while the *Precision* of the detection of transistors (98 %) and resistors (96%) is quite

Table 5.4: Number of detected and total transistors, resistors and connections.

Training Data	Target Circuit	# of Detected/Total Transistor	# of Detected/Total Resistor	# of Detected/Total Connection	Manual Correction from Reverse Engineer
PUF_1	PUF_2	3 / 3	2 / 2	6 / 9	Minor
PUF_1	NAND	2 / 2	1 / 1	4 / 4	No
PUF_1	Flip-flop	18 / 18	10 / 10	53 / 53	No
PUF_1	$C17_1$	12 / 12	6 / 6	31 / 31	No
PUF_1	$C17_2$	12 / 12	6 / 6	31 / 31	No
10% of itself	$C17_3$	14 / 14	7 / 7	37 / 37	No
10% of itself	$C432$	360 / 360	205 / 205	1101 / 1101	No
10% of itself	$C499$	1061 / 1061	644 / 644	3375 / 3375	No
10% of itself	$C880$	742 / 742	428 / 428	2293 / 2293	No
10% of itself	$C1908$	884 / 884	519 / 519	2787 / 2787	No

high, it suffers from low *Recall* with 29% and 52% respectively. As for wires, the *Precision* is only 53% while a *Recall* of 85% is achieved. The improvement of post-processing is especially noticeable in the increased *Recall* for transistors and resistors from 29% to 56% and 52% to 74%, while losing only 2% and 9% in *Precision* respectively. Also, the previously low *Precision* for wires with 53% is increased to 73% while also increasing the *Recall* from 85% to 91%. Both metrics are also improved slightly for blank. Therefore, through post-processing, the average *Precision* and *Recall* are improved from 88% to 92% and 86% to 92% respectively on the $C17_1$ semi-real test circuit.

While these metrics give insight about the performance of the ML model and the post-processing, the main goal of this work is to detect the circuit elements and their connections so that the circuit netlist can be extracted automatically. For this reason, the number of detected and total transistors, resistors and connections are given in Table 5.4. It can be seen that all transistors and resistors (100%) were identified, and 99.97% of the connections are detected successfully. Even though there are some misclassified patches resulting in erroneous netlists, most of them, such as floating wires, can be corrected automatically in the netlist with the help of commonly used design rule checks (DRC). However, very rare errors such as shorted wires cannot be mitigated by DRC. Therefore, a reverse engineer can automatically spot these errors by overlaying the target circuit image and the patch results, and correct them manually. Thus, the erroneously detected three connections in PUF_2 image due to the shortening of wires are corrected with comparably small manual effort. After all, the proposed RE methodology successfully extracts all circuit netlists in our dataset.

5.4 Summary and Future Work

Compared to silicon ICs, the customizable fabrication of PE leads to several differences such as non-standard circuit elements, customized layouts, and high variation. These differences leads to a new RE methodology requirement. In this chapter, we have defined these differences and proposed a new robust RE methodology for PE circuits. The proposed methodology contains a preprocessing step which mitigates noise, dust and other environmental conditions. Then, a robust supervised learning based classification is exploited which classifies patches. Finally, a post-processing step is utilized which mitigates erroneous classifications and perform netlist extraction. The results show that the proposed methodology can reverse engineer the given PE circuits with very limited manual effort.

As we have demonstrated that the given PE circuits can be reverse engineered, countermeasures have to be taken to prevent dishonest intentions. The investigation of such countermeasures against RE, such as camouflaging schemes, for PE should be investigated. The following chapter proposes a scheme that can be used for camouflaging, split manufacturing and hardware watermarking for various attacks including RE.

6 Printed Look-Up Table-based Programmable Printed Digital Circuit

The unique features of Printed Electronics (PE) such as large feature sizes and rather simple circuit structures bring security threats in the supply chain of PE applications [36]. These security threats are reverse engineering, counterfeiting, malicious modifications, IP piracy, and overbuilding which can lead to severe problems. For instance, inaccurate or erroneous functionality of a medical application may lead to false diagnosis [139, 140, 141]. Therefore, countermeasures against such threats must be considered in the design and fabrication flow of such applications. The countermeasure methods such as camouflaging, split manufacturing, and hardware watermarking can be realized with the help of a programmable printed circuit.

On the other hand, in many cases of PE applications, functional customization by end-users or other parties in the supply chain is needed. Therefore, enabling such customization through programmability is desired. Also, due to high intrinsic variations in this technology, manufacturing yield and performance metrics could be very low especially for low-cost printing processes [13, 61, 62]. A programmable circuit can improve the yield and performance metrics, and help to bypass defects to provide correct functionality despite the low manufacturing yield, performance and defects resulting from the low-cost printing processes.

For all these reasons, it is desired to have a (one-time) programmable building blocks for this technology to address security, yield, and performance challenges. The work in [142] presents a transistor level method utilizing functional transistors in a sea of transistors to improve the yield of printed circuits, but it requires a large amount of error-prone inkjet-printing and transistor characterization effort to provide large scale integration.

In this chapter, we propose the first one-time programmable printed Look-up Table (pLUT) design to implement virtually any printed digital circuits while addressing the aforementioned challenges. The pLUT can be fabricated using high throughput advanced techniques in a production center, then, the pLUT can be programmed using printing conductive inks to corresponding connections based on user requirements using an inkjet-printer. In this way, the programmable pLUT can be used to countermeasure against security attacks, and mitigate low performance and low yield. Besides, users can realize any on-demand printed circuits with minimum effort. Furthermore, the programmability feature of this approach can also be used to mitigate failures by bypassing defective components through re-routing. The suitability of the existing and the proposed LUT implementations to the proposed scheme is reviewed and compared in terms of area usage, worst-case delay, and power consumption. The proposed pLUT implementation is simulated and fabricated using inorganic electrolyte-gated printed transistors, and programmed with inkjet-printed conductive ink to implement XNOR, XOR, and AND gates to prove the programmability of the proposed design. The characterization results show that the fabricated pLUT operates at 1 V. Furthermore, the usage cases of the proposed pLUT in the context of security, yield, and performance improvement are discussed.

The summary of the contributions of the work is as follows:

- We propose the first one-time programmable printed Look-up Table (pLUT) design and compare it with existing LUTs in terms of area usage, worst-case delay, and power consumption,
- We present the efficient scaling of pLUT and chip architecture for complex circuit implementations,
- We synthesize several benchmark circuits with pLUT cells and standard cells, and present a comparison in terms of maximum frequency, area usage, and power consumption,
- We provide fabrication and characterization results of 2-input pLUT (pLUT2), configured as AND, XOR, and XNOR gates,
- We discuss the usage cases of the proposed design for security solutions, yield, and performance improvements in PE.

The rest of the chapter is organized as follows: Section 6.1 presents the design, architecture, and fabrication and configuration flow of the proposed pLUT while in Section 6.2, simulation and fabrication results are reported and discussed. Section 6.3 discusses the usage cases of proposed pLUT in PE applications, and Section 6.4 concludes the chapter.

6.1 Proposed Printed Look-up Table (pLUT)

This section explains the analysis of the existing look-up table (LUT) circuits in the context of printed electronics, and the proposed printed LUT (pLUT) design. Furthermore, the scaling of the design is elaborated to realize high volume production of printed digital circuits with minimum overhead.

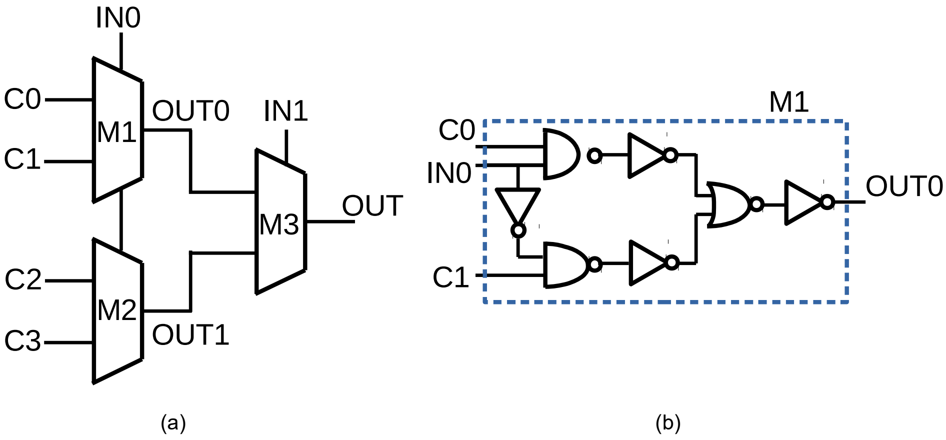


Figure 6.1: Logic Gate(LG)-based Look-up Table. (a) LUT2 implementation, (b) LG-based multiplexer implementation.

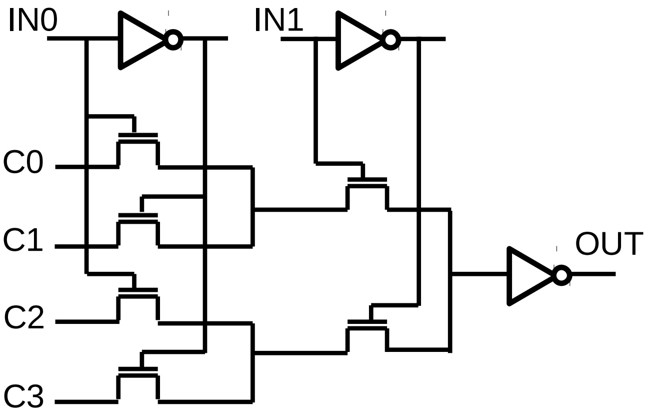
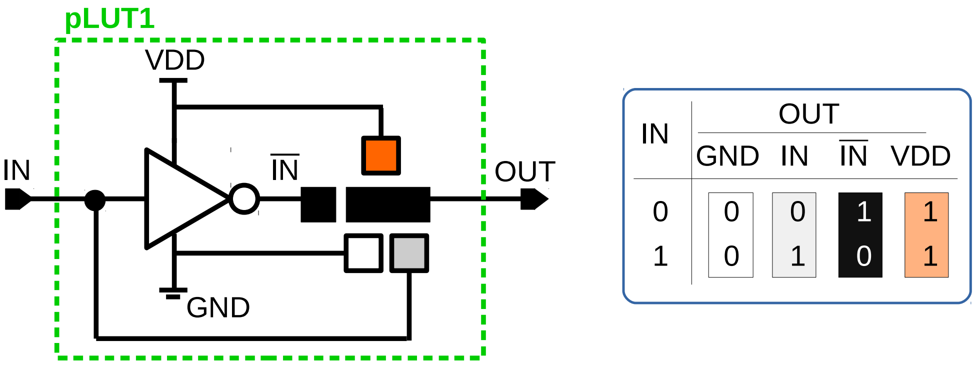


Figure 6.2: Pass Transistor(PT)-based Look-up Table.



IN	OUT			
	GND	IN	$\overline{\text{IN}}$	VDD
0	0	0	1	1
1	0	1	0	1

(a)

(b)

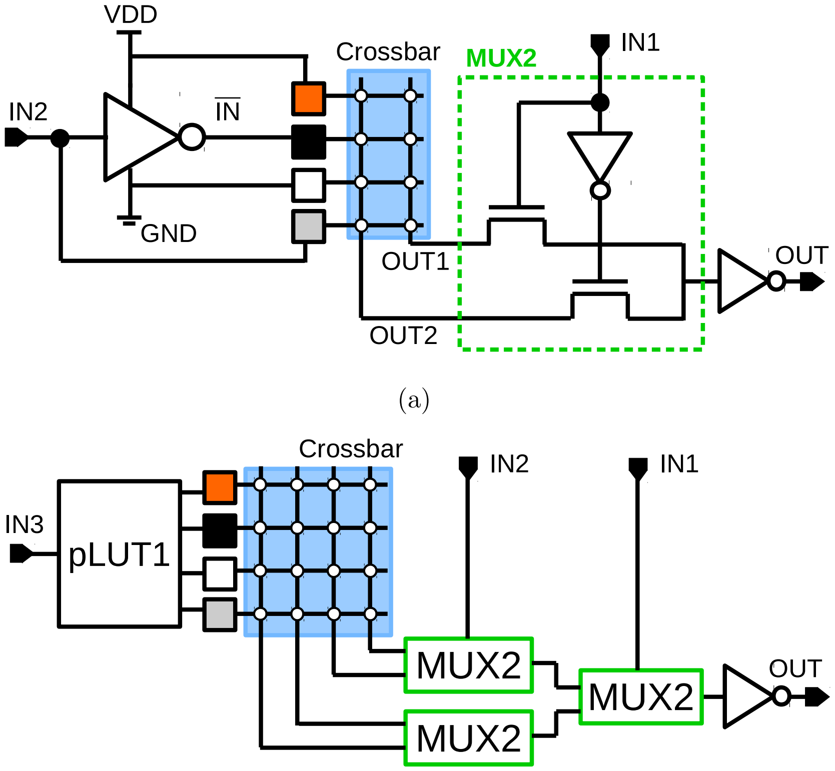
Figure 6.3: (a) Proposed 1-input printed look-up table (pLUT1) in which functionality is set using inkjet-printed conductive inks, (b) Illustration of pLUT1 programmability in table form. (pad colors indicate corresponding configuration in table.)

6.1.1 Existing LUT designs

In silicon technologies and for FPGAs, three different LUT designs have widely been used [143]. These LUT designs are revised according to one-time inkjet-printing programmability and resistor-transistor logic in printed electrolyte-gated transistor (EGT) technology. But, the circuits can be realized with any PE technology.

Logic Gate (LG)-based LUT: The baseline implementation of LUT is based on logic gates as shown in Figure 6.1. It has two inputs (IN0, IN1), four configurations (C0-C3) which can be connected to either VDD or GND to configure its functionality, and three 2-input multiplexers which contain two NAND, two INV and one NOR gates as shown in Figure 6.1b. The disadvantage of this design is the large area usage.

Pass Transistor (PT)-based LUT: This implementation, shown in Figure 6.2, consists of two inputs (IN0 and IN1), four configurations (C0-C3) which can be connected to either VDD or GND to configure its functionality, six pass transistors (NMOS) to form the multiplexer, and an inverter to strengthen the signal quality. The pass transistor implementation of multiplexer



(a)

(b)

Figure 6.4: (a) Proposed 2-input printed look-up table (pLUT2) containing multiplexer (MUX2). Crossbar is used to program LUT2 to desired functionality, (b) Proposed 3-input pLUT3

saves area greatly. However, the pass transistors degrade logic-1 signals. So, an inverter (or a half-latch) is required to improve the quality of logic-1 signals.

Transmission Gate (TG)-based LUT: This design replaces pass transistors with transmission gates to improve the signal quality at the expense of PMOS transistors. However, due to the high area usage and the constraint of resistor-transistor logic, this structure cannot be realized in EGT technology.

6.1.2 Proposed pLUT circuit

The core of the proposed LUT implementation is printed look-up table (pLUT1) which is shown in Figure 6.3a. The proposed pLUT1 contains an inverter and wires to realize any 1-input/1-output functionality by printing conducting inks between the corresponding node and the output. The pads of ground (GND), input (IN), the inverse of input ($\overline{IN}$) or power supply (VDD) are placed close to the output pad of pLUT1 so that the output of pLUT1 can easily be connected to either GND, IN, $\overline{IN}$ or VDD using inkjet-printed conductive inks to realize any functionality as illustrated in Figure 6.3b.

Using a pLUT1 and existing pass transistor based multiplexer (MUX2) consisting of an inverter and 2 pass transistors, N-input pLUT (pLUTN) can be constructed. Figure 6.4a shows an LUT2 which is composed of a pLUT1, a MUX2 and an output inverter which improves the voltage level quality. A crossbar is used to connect pLUT1 signals to multiple intermediate

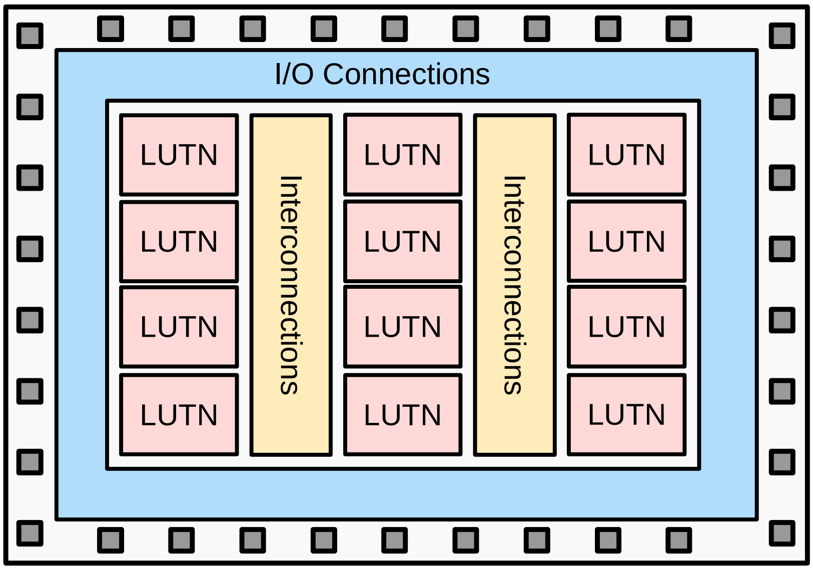


Figure 6.5: Illustration of a programmable printed chip using N-input Look-up Tables (LUTNs). Number of input, N, can be chosen based on requirements. Interconnections and I/O connections contains crossbars that are programmable and connects LUTNs and I/Os.

outputs. As shown in Figure 6.4a, a pLUT1 and two intermediate outputs (OUT1 and OUT2) are used in the crossbar for LUT2 while for N-input pLUTN, a pLUT1 and N intermediate outputs are used. Moreover, with this way, larger LUTs can be efficiently implemented as shown in Figure 6.4b. Therefore, the number of pLUT1 is constant for any input size LUT, which reduces complexity.

6.1.3 Overall system Architecture

The proposed pLUT implementation can be scaled to construct any LUT with N-input (pLUTN). Figure 6.5 shows the system architecture of a programmable printed digital chip which is fabricated at the high-throughput fabrication center. I/O connections are to connect input/output pad to pLUTNs and interconnections while pLUTNs are connected to each other through interconnections. I/O connections and interconnections are constructed using a crossbar so that the connectivity among pLUTNs, and between pLUTNs and I/Os are programmed by inkjet-printed conductive inks. Based on the placement and routing (P&R) of the HDL design, the crossbars of I/O connections and interconnections are configured using inkjet-printed conducting material inks (such as PEDOT:PSS) at the user-site. It should be noted that the programmable circuit can be utilized in two ways. It can be some parts of a bigger PE design, or complete programmable chip based on the usage scenario (see Section 6.3).

6.1.4 Fabrication and Configuration Flow

The fabrication and configuration flow of pLUT based programmable printed chip, to realize high volume and high throughput fabrication of PE circuits without sacrificing on-demand and point-of-use fabrication features, is illustrated in Figure 6.6 . In this flow, a programmable printed chip is fabricated using advanced high-throughput and high-yield fabrication tech-

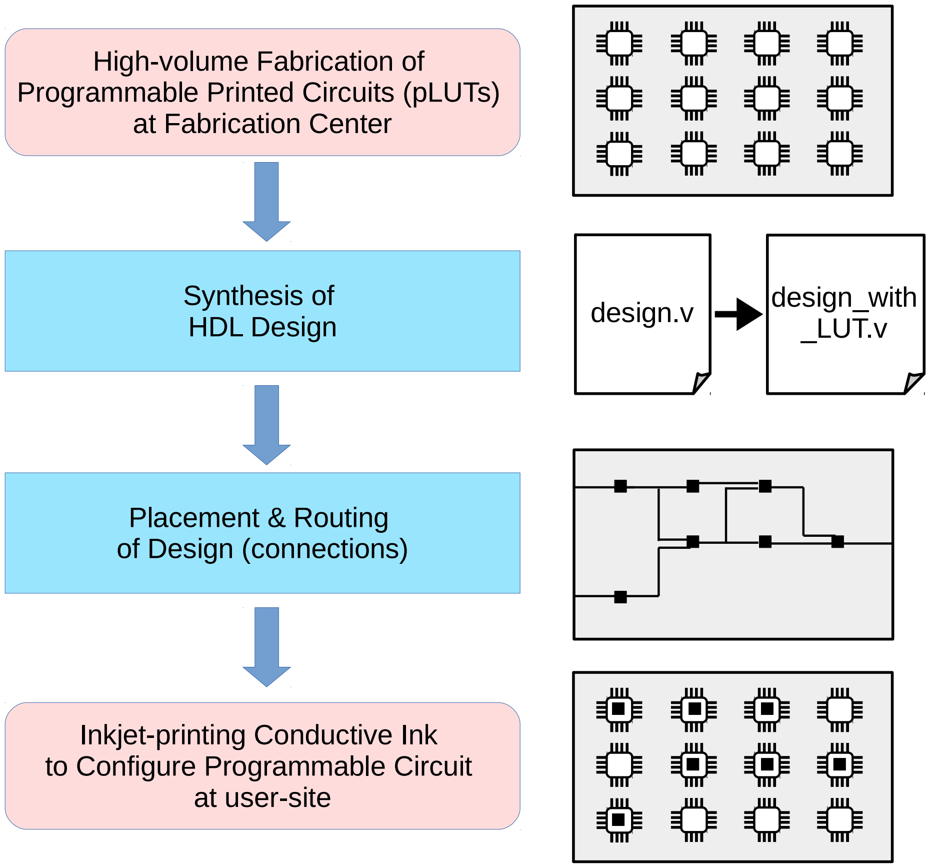
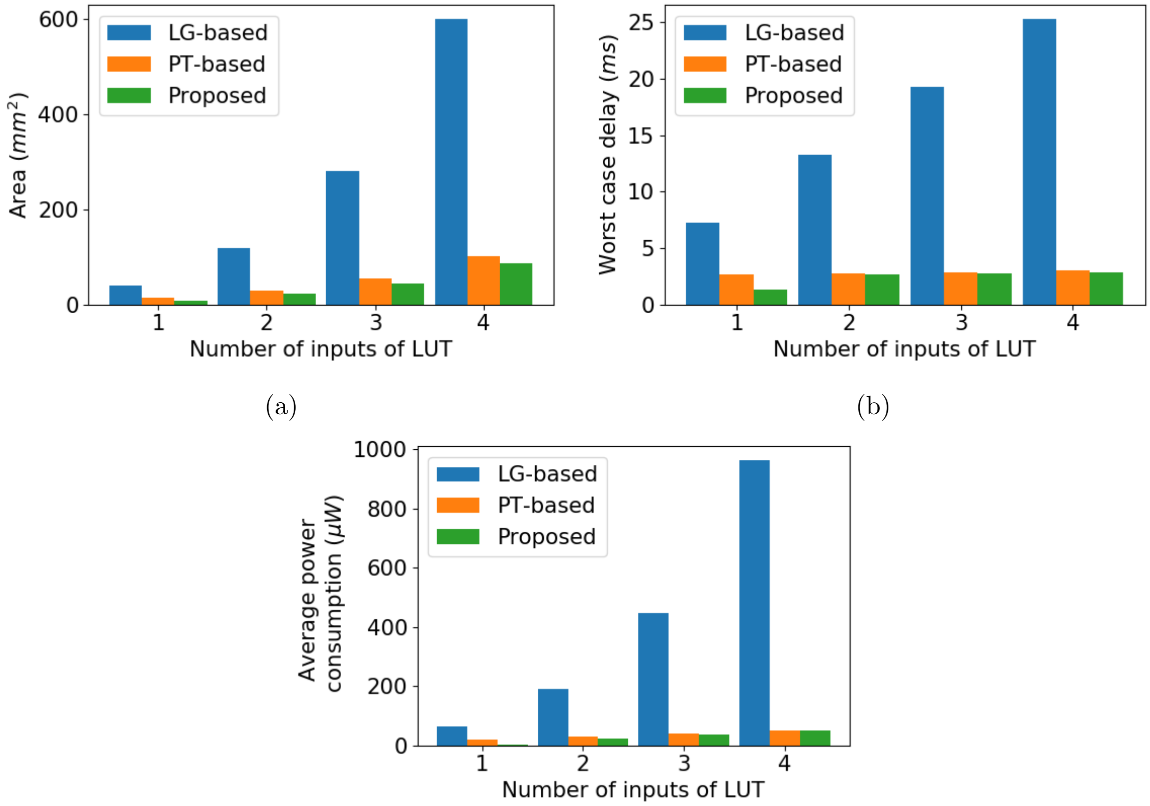

High-volume Fabrication of Programmable Printed Circuits (pLUTs) at Fabrication Center
Synthesis of HDL Design
design.v
design_with_LUT.v
Placement & Routing of Design (connections)
Inkjet-printing Conductive Ink to Configure Programmable Circuit at user-site

Figure 6.6: Fabrication and configuration flow of pLUT based programmable printed chip. A programmable printed chip is fabricated in high-volume at fabrication center. At the user site, the target design HDL is synthesized, and then placed and routed (P&R) according to programmable chip. Finally, the programmable chip is configured using inkjet printing at point-of-use.

niques, which due to high-costs, are only economical for high-volume production. In a subsequent step, end-users are able to program it according to their specifications using low-cost processes such as inkjet printing. This way, the best of two worlds, high-throughput and high-yield fabrication as well as on-demand point-of-use customization, are achieved.

As illustrated in Figure 6.6, the programmable printed chip is fabricated with advanced fabrication processes resulting in higher yield and better performance compared to low-cost fabrication processes (inkjet-printing). At the point-of-use, the HDL (design.v) of the target design is synthesized using the standard cells used in the programmable printed chip (pLUT). The synthesized netlist (design_with_LUT.v) is converted into placement and routing file (P&R file) that contains the configuration information (configuration of LUTs and interconnections). Finally, the customization of programmable printed chip is configured into desired functionality by inkjet-printing conductive inks according to the P&R file. Therefore, the complex circuits can easily be implemented without dealing with the yield and performance issues.



(a)

(b)

(c)

Figure 6.7: Comparison of various LUT implementations with different number of inputs in terms of (a) area, (b) worst-case delay, and (c) power consumption.

6.2 Experimental Results

In this section we first provide a simulation-based analysis of the proposed pLUT and compare it with EGT-based implementations of existing LUT designs. Afterwards, we provide fabrication-based evaluation of proposed pLUT.

6.2.1 Simulation, Fabrication and Characterization Setup

The simulation and measurement results presented in this section are based on the EGTs which have the channel geometry of 200 μm width and 80 μm length, and the 100 $k\Omega$ resistors. We have employed the variation model of EGT and Process Developmennt Kit (PDK) presented in [113, 144].

After the resistors, wires and transistor electrodes are structured using laser ablation on a float glass substrate with 150 nm coated indium tin oxide (ITO), the substrates are cleaned with 2-propanol and acetone. The channel semiconductor material, indium oxide (In_2O_3) precursor, is inkjet-printed with Dimatix 2831 inkjet printer between drain and source electrodes. Then, the substrates are annealed at 400° C for 2 hours. In the next step, composite solid polymer electrolyte (CSPE) is inkjet-printed on top of channel to cover it. After the CSPE is dried at room temperature, PEDOT:PSS is inkjet-printed on top of electrolyte to

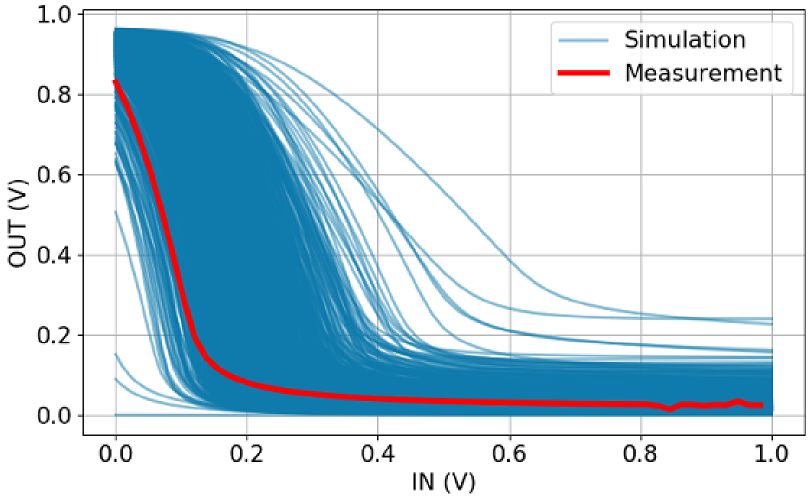


Figure 6.8: Monte Carlo simulation and measurement of CLUT1 programmed as inverter ($\overline{IN}$).

Table 6.1: Comparison of various LUT2 implementations in EGT technology in terms of area, delay, power and voltage level quality at 1 V.

	LG-based	PT-based	pLUT
Area (mm^2)	120	28.2	17.4
Worst case delay (ms)	13.3	2.8	2.7
Average power consumption (μW)	192.561	29.661	24.717
Logic-1 level at output (V)	1	0.6	0.8

form top-gate structure. In order to program circuits, PEDOT:PSS is inkjet-printed between corresponding nodes. It should be noted that the inkjet-printed EGT technology used in the fabrication of proposed method is an emerging technology in which there are many challenges to be resolved for large scale circuit fabrication. Moreover, due to our lab setup, we can only reliably fabricate and experimentally validate small scale circuits. For this reason, we have only fabricated pLUT1 and pLUT2 to prove the concept.

The fabricated circuits are characterized and powered with Agilent 4156C semiconductor parameter analyzer and Yokogawa DL6104 digital oscilloscope. The input signals are generated with Keithley 3390 arbitrary waveform generator. The measurements were carried out at room temperature and 70% relative humiditiy.

6.2.2 Simulation-based Comparison of LUT Circuits

We have compared the EGT-mapped LG-based, the PT-based and the proposed pLUT implementations in terms of area, worst case delay and average power consumption to provide the strengthens of different implementations. The comparison given in Table 6.1 is based on 2-input LUT (LUT2) implementation since it is the basic building block of the LUTs with more inputs. Moreover, the area, worst case delay and average power consumption of various input-length LUTs (LUT1-LUT4) are given in Figure 6.7.

Table 6.2: Comparison of synthesis results of several ISCAS'85 and EPFL benchmark circuits with standard cells (NOT, NOR and NAND gates) and proposed pLUT2 cell.

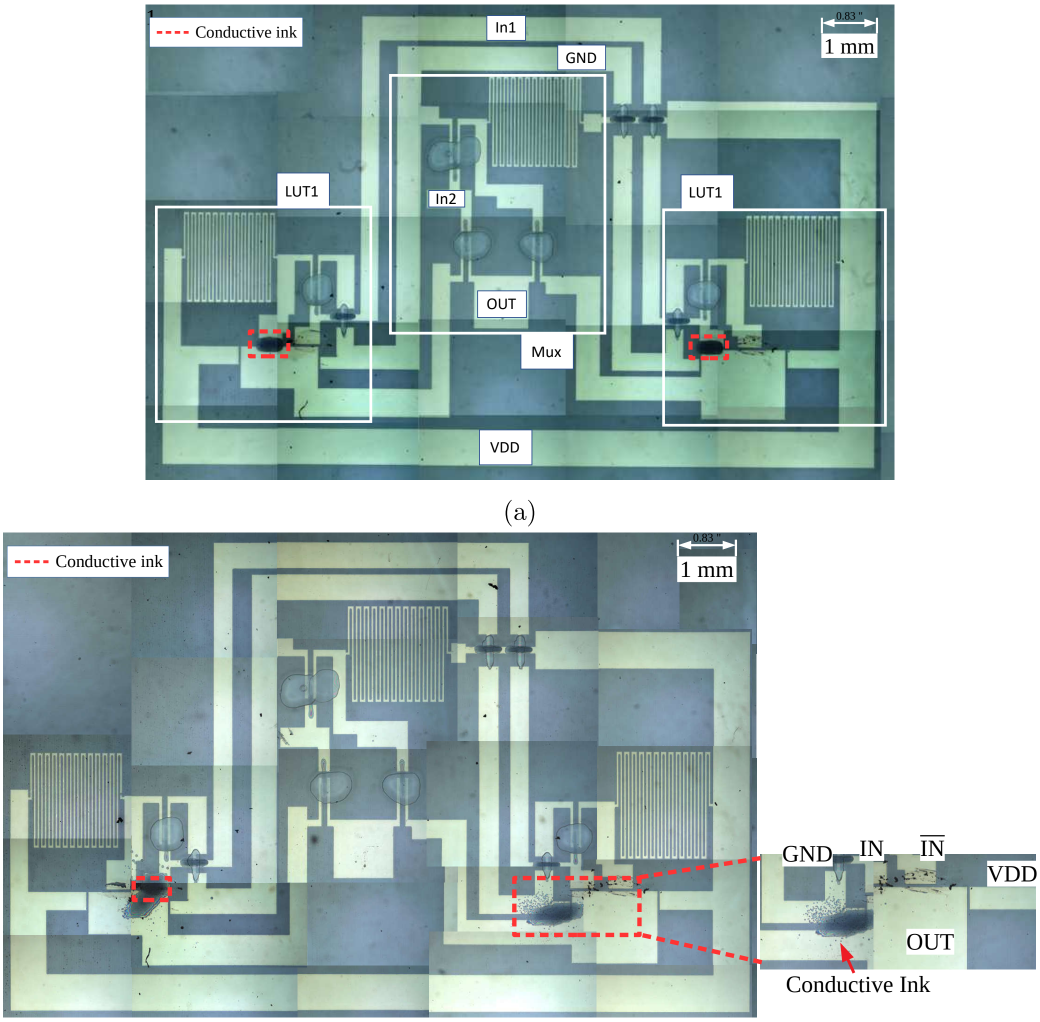
	F_{max} [Hz]			Area [cm^2]		
Circuit	Gates	LUT2	Diff	Gates	LUT2	Diff
c17	336.01	336.23	0.07%	0.55	1.26	129.14%
c432	43.19	39.84	-7.76%	11.07	21.94	98.10%
c499	39.38	79.64	102.24%	33.06	32.66	-1.21%
c1908	28.98	55.27	90.72%	29.02	37.32	28.60%
c2670	32.40	41.83	29.10%	47.594	77.96	63.82%
c7552	20.52	21.96	7.04%	107.01	175.69	64.18%
adder	4.48	4.41	-1.57%	78.47	191.81	144.43%
barrel shifter	87.99	73.35	-16.63%	250.40	649.90	159.54%
max	2.07	1.87	-9.67%	222.35	504.91	127.08%
sine	5.60	7.71	37.68%	420.95	752.458	78.75%
Average			23.12%			89.25%

	Total Power [W]			Total Cells		
Circuit	Gates	LUT2	Diff	Gates	LUT2	Diff
c17	0.00067	0.000368306	-45.03%	9	8	-11.11%
c432	0.003674	0.003936444	7.15%	183	133	-27.32%
c499	0.016668	0.006743485	-59.54%	547	190	-65.27%
c1908	0.0110684	0.0012733049	-88.50%	475	216	-54.53%
c2670	0.0142332	0.004219984	-70.35%	824	609	-26.09%
c7552	0.02973	0.033540835	12.82%	1762	1146	-34.96%
adder	0.015054	0.032469592	115.68%	1274	1194	-6.28%
barrel shifter	0.117369	0.149192	27.11%	3741	3742	0.03%
max	0.033004	0.078386967	137.51%	3643	3102	-14.85%
sine	0.086911	0.0237784098	-72.64%	6845	4651	-32.05%
Average			3.58%			-27.24%

The results show that LG-based LUTs have much larger area usage, delay and power consumption although it has high reliability as it has no signal degradation effect. The proposed pLUTs are better than PT-based LUTs in terms of area and delay since it reduces the number of pass transistor levels using pLUT1 in the first level. Moreover, since the number of pLUT1 used in the pLUTs remains one as explained before, the average power consumption and the area usage of the pLUTs are increasing slower than the PT-based LUTs resulting in lower power consumption and less area usage while the number of inputs of pLUTs increases. The area usage of the proposed pLUT is 27%, 61%, 60% and 53% of the area usage of PT-based LUT for the number of input of 1, 2, 3, and 4, respectively.

6.2.3 Circuit Synthesis Results with pLUT2

We synthesized various combinational circuits from ISCAS'85 [138] and EPFL [145] benchmarks using the proposed pLUT2 cells, and have compared with custom synthesis using EGT standard cells (NOT, NAND and NOR gates). The results are given in Table 6.2. Since the



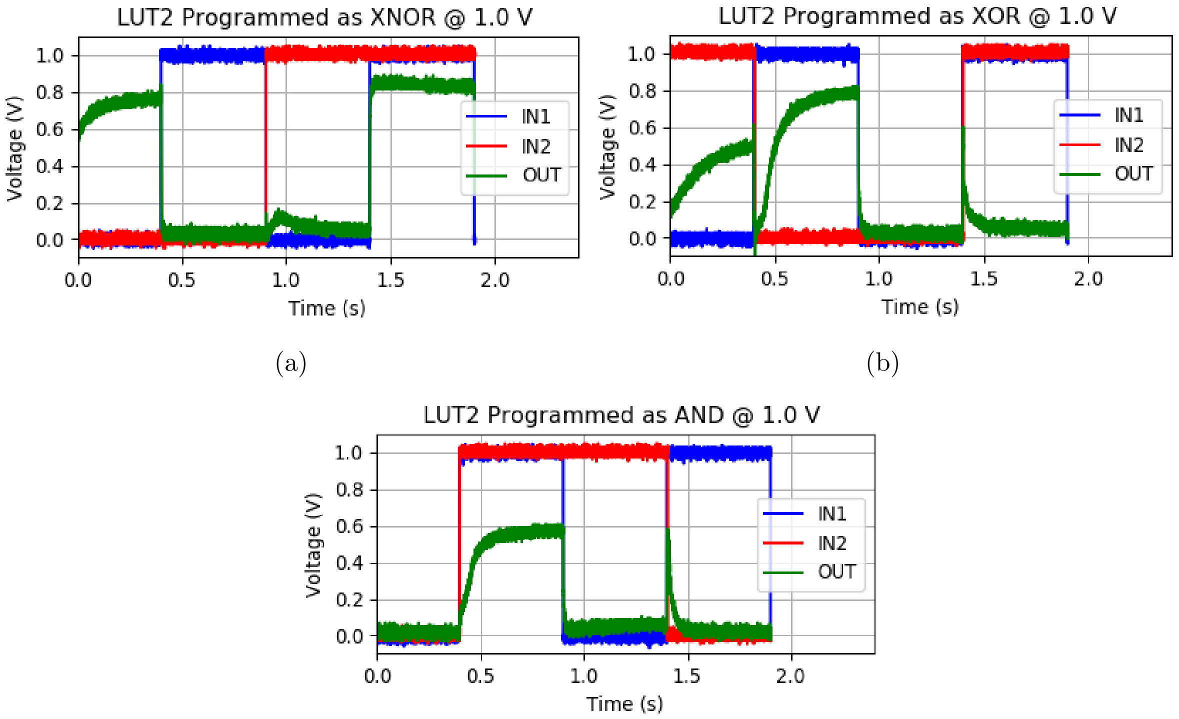
(a)

(b)

Figure 6.9: LUT2s programmed with inkjet-printed conductive inks as (a) XOR gate, (b) AND gate.

pLUT2 has more area usage, latency and power consumption than standard gates, it is expected that the synthesis results are worse than custom implementation using standard cells. However, such overheads are justified due to programmability features. This is the same in silicon-based technologies where FPGA-based implementations have higher area, delay and power consumptions compared to full-custom ASIC implementations.Typically, for the implementation of complex boolean functions such as XOR and XNOR, the pLUT2 is more efficient since only one pLUT2 cell is sufficient to realize these functions. For instance, c499, which is an XOR intensive circuit, has higher maximum operating frequency (F_{max}), less area usage and less power consumption compared to custom synthesis.

The average improvement of the maximum frequency is 10.53% resulting from the efficient implementation of complex gates with the pLUT2 and the less delay overhead of the pLUT2. The average overhead of the area usage and the power consumption are 103.04% and 27.96% caused from the high area and power overhead of the pLUT2 compared to standard gates. Since the pLUT2 can implement complex boolean functions with less number of cells, the average reduction of the number of cells is 22.82%.



(a)

(b)

(c)

Figure 6.10: Timing diagram of fabricated programmable LUT2s programmed as (a) XNOR, (b) XOR, (c) AND at 1 V.

6.2.4 Fabrication Results of Proposed pLUT

We have fabricated four pLUT1 and programmed them for four different configuration which are all-0 (GND), buffer (IN), inverter ($\overline{IN}$) and all-1 (VDD) as in Figure 6.3a-6.3b. Figure 6.8 shows that the DC measurement of a pLUT1 programmed for inverter functionality matches with the range of simulation results extracted from 100 Monte Carlo samples using the EGT variation model [113]. The other three functionality measurements of pLUT1 are also as expected.

We have also fabricated multiple pLUT2s to demonstrate the preliminary results of the programmability of the proposed design. One of the pLUT2 is programmed as XNOR gate while others are programmed as XOR and AND gates to construct half-adder. The images of pLUT2 programmed as XOR and AND are shown in Figure 6.9. The programmed pLUT2s are characterized to prove their functionality at 1 V. Figure 6.10 shows the behaviour of three programmed pLUT2s in all input conditions at the supply voltages of 1 V. The level of logic-1 at the output does not reach to VDD due to the pass transistors and resistor-transistor logic, as the pass transistors reduce the voltage level by threshold voltage (Vth), and the logic-0 for the inverters controlling the pass transistors is slightly more than 0 V (GND) resulting in higher leakage current in disabled pass transistors. For instance, as shown in the waveform of pLUT2 programmed as XOR, the output levels for '01' and '10' input values are 0.55 V and 0.8 V. For '01', the pass transistor transmitting the signal reduces 1 V (VDD) by Vth, whose mean value for EGTs is 0.2 V, and the other pass transistor disabled by above 0 V signal leaks more current resulting in low logic-1 (0.55 V). To solve this problem, an inverter or a half-latch can be used to improve logic-1 voltage level. Please note that the fabrication results of the pLUT2 do not contain inverter/half-latch at the output.

Moreover, the average power consumption of the fabricated pLUT2 is 25.12 μW while the worst case delay is 73.28 ms. Additionally, the area usage of a pLUT2 is $60\,mm^2$ which is higher than the area usage value given in Table 6.1 due to the test pads and exaggerated wire widths for the prototype.

6.3 Programmable Components in PE Applications

The proposed programmable circuit can be utilized for different purposes. As explained before, since the yield of PE circuits fabricated with low-cost fabrication processes is low, the chip can be fabricated in an advanced production center resulting in high yield, and programmed using a low-cost and on-demand processes (e.g., inkjet-printing). Additionally, the failures can be mitigated bypassing defective part of the circuit through rerouting. For instance, after the initial configuration is done, the defective parts are identified using digital testing methods. Then, these part of the design are rerouted and configured into functional elements left in the neighbourhood for this purpose. In this way, the yield can be improved while maintaining point-of-use functionality customization. This concept is similar to what has been done in the research direction of the defect and fault tolerance in FPGAs and reconfigurable computing in which several methods and defect-aware P&R have been proposed [146, 147, 148]. Moreover, in the context of high volume fabrication, this enables high throughput fabrication, which lowers the overall fabrication cost. Therefore, the proposed LUT-based printed digital circuit can be used to improve yield, performance and fabrication throughput.

Another usage scenario of the proposed programmable circuit is that the end-customers of the programmable circuit buy soft IPs (RTL level) from a central IP provider, follow the fabrication and configuration flow in Figure 6.6, to convert the IP into the configuration information of the chip, and then print the connections of programmable circuits in the point-of-use (user site). This allows the decentralized manufacturing of printed circuits. However, this scheme is vulnerable to IP piracy where one end-customer share the IP with other unauthorized end-customers. The countermeasure against IP piracy is hardware watermarking where IP owners introduce a watermark into their design at different levels to claim their ownership [149, 150]. In this scenario, the IP owner can constraint the IP at placement & routing level such that it uses different certain pLUTs in the chip for different end-customer as a watermark, which allows tracing the source of IP piracy [69].

Last but not least, in the scenario where the entire design is manufactured in a fabrication center, the attacker can overproduce the circuit and sell it on the market or reverse engineer the design [36, 69]. To prevent this, the designer can use the programmable circuit to prevent this security threat using two separated manufacturing steps. At the fabrication center, programmable circuit is fabricated, and the configuration is implemented at point-of-use. Therefore, the fabrication center cannot overproduce or reverse engineer the design since there is no functionality implemented at this step, which will be performed by the designer at the point-of-use [69].

The above mentioned security countermeasure is resulted from the intrinsic feature of programmable printed circuit, and targets the attack performed at production center. However, after the connections of the circuit are fabricated, one can buy the product, reverse engineer the design, and counterfeit it [36, 69]. Since the connections are optically visible, it is comparably easy to automatically reverse engineer design. To conceal the connections, a simple countermeasure is to fabricate a non-conductive ink, which looks optically similar to the conductive one, to other nodes. In this way, the connectivity information is optically camouflaged, which dramatically increases the reverse engineering effort of the attacker.

6.4 Summary

In this chapter, we have presented a printed Look-up Table (pLUT) which is suitable to combine advanced high-throughput and high-yield fabrication processes and low-cost inkjet-printing for on-demand customization to realize high volume printed circuits while improving performance and yield without sacrificing on-demand point-of-use customization. The proposed pLUT has been fabricated, programmed with inkjet-printing, and characterized. The results show that the proposed circuit is programmable to realize any digital functionality, and operates at 1 V. Moreover, we have discussed the pLUT utilization for security countermeasures, yield and performance improvements.

7 Conclusions and Outlook

Printed Electronics (PE), as a complementary solution to conventional technologies, has demonstrated exponential market growth in recent years. PE combines printing techniques and electronic functionality to enable the usage of numerous materials in the fabrication of electronic components on a wide range of rigid and flexible substrates. The unique features of PE enable emerging applications that can be flexible, stretchable, lightweight, large-area, and implantable, and manufactured using cost-effective, customizable, and environmentally friendly processes. Hence, several applications such as e-skin, smart packaging, healthcare patches can be realized using promising features of PE technology.

Since PE is an emerging technology, experts from different scientific fields have been intensively addressing the fundamental challenges such as yield, performance, cost, and reliability to advance the technology. The security aspects of PE were disregarded as in the early phase of existing technologies. However, numerous destructive hardware-based attacks have recently proved that securing hardware platforms is as important as other aspects of technology development. So, security aspects of PE and its applications should be primarily investigated to offer trusted and secure applications.

7.1 Conclusions

This thesis provides a technology-specific assessment of hardware-level attacks and their countermeasures in the form of compact circuits to secure the supply-chain and functionalities of PE applications at the hardware level. In this regard, we have proposed a printed Physical Unclonable Function (pPUF) and a printed True Random Number Generator (pTRNG) that generates unclonable and random keys to utilize in several countermeasures against hardware-based attacks and provide secure communication and authentication to PE applications. Moreover, we have proposed a reverse engineering method for PE circuits and demonstrated their vulnerability. Furthermore, we have proposed a printed Look-up Table based programmable circuit (pLUT) to thwart hardware-level attacks including reverse engineering, IP piracy, and overbuilding in the supply-chain. The main property of proposed hardware primitives is their low-overhead designs achieved by exploiting the technology-specific features of PE.

Chapter 3 presents the pPUF to produce secure keys and analysis framework to evaluate the proposed pPUF. The simulation-based analysis shows that the pPUF has adequate uniqueness and reliability. Moreover, a multi-bit pPUF design is presented to optimize the area usage. The multi-bit pPUF reduces the area usage by 31.02% for the 16-bit key generation. Furthermore, the fabrication-based results prove that the functionalities of the fabricated pPUFs are similar to the simulation, and they can operate at 0.5 V.

Chapter 4 presents compact pTRNG enabled by the customizable fabrication feature of the inkjet-printing to tune the circuit to mitigate the bias resulted from high process variation, and additive resistor tuning flow to efficiently perform the mitigation of the process variation. The simulation-based analysis shows that the tuning flow reduces the overall process variation of the TRNGs by 110 times, and the generated bitstream of tuned pTRNGs pass the National Institute of Standards and Technology Statistical Test Suite. Moreover, the fabrication-based analysis demonstrates that the tuned pTRNGs generate random bitstreams, and can operate at 0.5 V.

Chapter 5 describes the differences between conventional circuits and PE circuits to assess the vulnerability level of PE circuits to reverse engineering (RE) attacks and presents a RE methodology based on supervised machine learning that starts from image acquisition until netlist extraction of PE circuits. The results prove that the proposed RE methodology can reverse engineer various PE circuits without complex and expensive tools, thus, PE circuits are highly vulnerable to RE attacks, and countermeasures against such attacks have to be taken.

Chapter 6 presents a one-time programmable pLUT that implements any printed digital circuits and can be used for camouflaging, split manufacturing and IP watermarking to thwart hardware attacks including RE in the supply-chain of PE. The simulation and fabrication-based analyses prove that the proposed pLUT outperforms the existing LUT designs in terms of area, power, and delay while it is operable at 1 V. Furthermore, the usage scenarios of the pLUT in the context of security countermeasures, yield, and performance improvements are discussed.

7.2 Outlook

This thesis provides the assessment of potential hardware-level attacks of PE applications and countermeasures in the form of resource-constrained hardware primitives for the first time. Therefore, it highlights the importance of security aspects of PE applications and provides a basis for future investigations to secure PE applications. Therefore, several research directions are foreseen to improve the security of such applications. The investigation of different hardware primitive designs, the attack-resistance assessment of the primitives, and the optimization of the primitives in terms of attack-resistance, reliability, and performance are paramount research directions that should be taken to further advance the countermeasures against threats. Moreover, new types of countermeasures at different levels should be examined to secure the decentralized manufacturing of PE applications which is a unique concept for this technology. Furthermore, more compact countermeasure solutions considering application-specific features such as communication interface, type of functionalities, and usage scenario should be investigated to lower the overhead of security measures.

Bibliography

[1] Raghu Das, K Ghaffarzadeh, and X He. Printed, organic & flexible electronics forecasts, players & opportunities 2020-2030. https://www.idtechex.com/de/research-report/printed-organic-and-flexible-electronics-2020-2030-forecasts-technologies-markets/687, 2020. Accessed: 2020-05-08.

[2] The oe-a roadmap for organic and printed electronics: creating a guidepost to complex interlinked technologies, applications and markets. https://oe-a.org/viewer/-/v2article/render/26785800. Accessed: 2020-05-08.

[3] Printed electronics examples. https://www.printedelectronics.com/electronics/examples/. Accessed: 2020-05-08.

[4] Anusha Withana, Daniel Groeger, and Jürgen Steimle. Tacttoo: A thin and feel-through tattoo for on-skin tactile output. In *Proceedings of the 31st Annual ACM Symposium on User Interface Software and Technology*, pages 365–378, 2018.

[5] Bryant Chu, William Burnett, Jong Won Chung, and Zhenan Bao. Bring on the bodynet. *Nature*, 549(7672):328–330, 2017.

[6] Nan-Wei Gong, Jürgen Steimle, Simon Olberding, Steve Hodges, Nicholas Edward Gillian, Yoshihiro Kawahara, and Joseph A Paradiso. Printsense: a versatile sensing technique to support multimodal flexible surface interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1407–1410, 2014.

[7] Imec and tno launch comfortable, disposable health patch with long battery life to measure vital signs. https://www.imec-int.com/en/articles/imec-and-tno-launch-comfortable-disposable-health-patch-with-long-battery-life-to-measure-vital-signs. Accessed: 2020-05-09.

[8] Imec, tno and cartamundi develop flexible tags that communicate with standard touch screens. https://www.imec-int.com/en/articles/imec-tno-and-cartamundi-develop-flexible-tags-that-communicate-with-standard-touch-screens. Accessed: 2020-05-09.

[9] Nikolaos Papadopoulos, Weiming Qiu, Marc Ameys, Steve Smout, Myriam Willegems, Filip Deroo, Jan-Laurens van der Steen, Auke Jisk Kronemeijer, Marco Dehouwer, Alexander Mityashin, et al. Touchscreen tags based on thin-film electronics for the internet of everything. *Nature Electronics*, pages 1–6, 2019.

[10] A smart shoe for athletes and diabetics. https://www.imec-int.com/en/imec-magazine/imec-magazine-july-2018/a-smart-shoe-for-athletes-and-diabetics. Accessed: 2020-05-09.

[11] 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*, 7(1):7–26, March 2017.

[12] Gabriel Cadilha Marques, Dennis Weller, Ahmet Turan Erozan, Xiaowei Feng, Mehdi Tahoori, and Jasmin Aghassi-Hagmann. Progress report on “from printed electrolyte-gated metal-oxide devices to circuits”. *Advanced Materials*, page 1806483, 2019.

[13] Ahmet Turan Erozan, Gabriel Cadilha Marques, Mohammad Saber Golanbari, Rajendra Bishnoi, Simone Dehm, Jasmin Aghassi-Hagmann, and Mehdi B Tahoori. Inkjet-printed egfet-based physical unclonable function—design, evaluation, and fabrication. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 26(12):2935–2946, 2018.

[14] Daniel E Holcomb, Wayne P Burleson, and Kevin Fu. Power-up sram state as an identifying fingerprint and source of true random numbers. *IEEE Transactions on Computers*, 58(9):1198–1210, 2008.

[15] Suresh Kumar Garlapati, Mitta Divya, Ben Breitung, Robert Kruk, Horst Hahn, and Subho Dasgupta. Printed electronics based on inorganic semiconductors: from processes and materials to devices. *Advanced Materials*, 30(40):1707600, 2018.

[16] Shahed E Quadir, Junlin Chen, Domenic Forte, Navid Asadizanjani, Sina Shahbazmohamadi, Lei Wang, John Chandy, and Mark Tehranipoor. A survey on chip to system reverse engineering. *ACM journal on emerging technologies in computing systems (JETC)*, 13(1):6, 2016.

[17] Falk von Seggern, Inna Keskin, Erin Koos, Robert Kruk, Horst Hahn, and Subho Dasgupta. Temperature-dependent performance of printed field-effect transistors with solid polymer electrolyte gating. *ACS Applied Materials & Interfaces*, 8(46):31757–31763, 2016. PMID: 27802016.

[18] Gordon E Moore. Cramming more components onto integrated circuits. *Proceedings of the IEEE*, 86(1):82–85, 1998.

[19] Robert R Schaller. Moore’s law: past, present and future. *IEEE spectrum*, 34(6):52–59, 1997.

[20] Bob Schaller and R Stough. The origin, nature, and implications of moore’s law. *PUBP801*, 1996.

[21] AM Fitzgerald. The internet of disposable things will be made of paper and plastic sensors-for disposable sensors, silicon will never be the right fit—but cheaper tech is nearly here. *IEEE Spectrum*, 2018.

[22] Jun Chang Yang, Jaewan Mun, Se Young Kwon, Seongjun Park, Zhenan Bao, and Steve Park. Electronic skin: Recent progress and future prospects for skin-attachable devices for health monitoring, robotics, and prosthetics. *Advanced Materials*, 31(48):1904765, 2019.

[23] Hwiwon Kang, Hyejin Park, Yongsu Park, Minhoon Jung, Byung Chul Kim, Gordon Wallace, and Gyoujin Cho. Fully roll-to-roll gravure printable wireless (13.56 mhz) sensor-signage tags for smart packaging. *Scientific reports*, 4:5387, 2014.

[24] Benjamin Stassen Cook, Atif Shamim, and MM Tentzeris. Passive low-cost inkjet-printed smart skin sensor for structural health monitoring. *IET Microwaves, Antennas & Propagation*, 6(14):1536–1541, 2012.

[25] Joao Marques, Barbara Pahl, and Christine Kallmayer. Thermoplastic packaging and embedding technology for id-cards. In *Microelectronics Packaging Conference (EMPC), 2013 European*, pages 1–5. IEEE, 2013.

[26] Leonardo Weiss Ferreira Chaves and Christian Decker. A survey on organic smart labels for the internet-of-things. In *Networked Sensing Systems (INSS), 2010 Seventh International Conference on*, pages 161–164. IEEE, 2010.

[27] Paulo Rosa, António Câmara, and Cristina Gouveia. The potential of printed electronics and personal fabrication in driving the internet of things. *Open Journal of Internet Of Things (OJIOT)*, 1(1):16–36, 2015.

[28] Vivek Subramanian, Josephine B Chang, Alejandro de la Fuente Vornbrock, Daniel C Huang, Lakshmi Jagannathan, Frank Liao, Brian Mattis, Steven Molesa, David R Redinger, Daniel Soltman, et al. Printed electronics for low-cost electronic systems: Technology status and application development. In *Solid-State Device Research Conference, 2008. ESSDERC 2008. 38th European*, pages 17–24. IEEE, 2008.

[29] Christos D Dimitrakopoulos and Patrick RL Malenfant. Organic thin film transistors for large area electronics. *Advanced materials*, 14(2):99–117, 2002.

[30] Henning Sirringhaus. 25th anniversary article: Organic field-effect transistors: the path beyond amorphous silicon. *Advanced materials*, 26(9):1319–1335, 2014.

[31] Lay-Lay Chua, Jana Zaumseil, Jui-Fen Chang, Eric C-W Ou, Peter K-H Ho, Henning Sirringhaus, and Richard H Friend. General observation of n-type field-effect behaviour in organic semiconductors. *Nature*, 434(7030):194, 2005.

[32] Sujeong Kyung, Jimin Kwon, Yun-Hi Kim, and Sungjune Jung. Low-temperature, solution-processed, 3-d complementary organic fets on flexible substrate. *IEEE Transactions on Electron Devices*, 64(5):1955–1959, 2017.

[33] Ahmet Turan Erozan, Mohammad Saber Golanbari, Rajendra Bishnoi, Jasmin Aghassi-Hagmann, and Mehdi B Tahoori. Design and evaluation of physical unclonable function for inorganic printed electronics. In *2018 19th International Symposium on Quality Electronic Design (ISQED)*, pages 419–424. IEEE, 2018.

[34] Ahmet Turan Erozan, Rajendra Bishnoi, Jasmin Aghassi-Hagmann, and Mehdi B Tahoori. Inkjet-printed true random number generator based on additive resistor tuning. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1361–1366. IEEE, 2019.

[35] Kyungroul Lee, Sun-Young Lee, Changho Seo, and Kangbin Yim. Trng (true random number generator) method using visible spectrum for secure communication on 5g network. *IEEE Access*, 6:12838–12847, 2018.

[36] Ahmet Turan Erozan, Michael Hefenbrock, Michael Beigl, Jasmin Aghassi-Hagmann, and Mehdi B Tahoori. Reverse engineering of printed electronics circuits: From imaging to netlist extraction. *IEEE Transactions on Information Forensics and Security*, 15:475–486, 2019.

[37] Ahmet Turan Erozan, Dennis D Weller, Farhan Rasheed, Rajendra Bishnoi, Jasmin Aghassi-Hagmann, and Mehdi B Tahoori. A novel printed look-up table-based programmable printed digital circuit. *IEEE Transactions on Very Large Scale Integration*

(VLSI) Systems, 2020.

[38] Robert A Street, TN Ng, David E Schwartz, Gregory L Whiting, JP Lu, RD Bringans, and Janos Veres. From printed transistors to printed smart systems. *Proceedings of the IEEE*, 103(4):607–618, 2015.

[39] YJ Chan, CP Kung, and Z Pei. Printed rfid: technology and application. In *Radio-Frequency Integration Technology: Integrated Circuits for Wideband Communication and Wireless Sensor Networks, 2005. Proceedings. 2005 IEEE International Workshop on*, pages 139–141. IEEE, 2005.

[40] Vivek Subramanian, Paul C Chang, Daniel Huang, Josephine B Lee, Steven E Molesa, David R Redinger, and Steven K Volkman. All-printed rfid tags: materials, devices, and circuit implications. In *VLSI Design, 2006. Held jointly with 5th International Conference on Embedded Systems and Design., 19th International Conference on*, pages 6–pp. IEEE, 2006.

[41] Vivek Subramanian, Paul C Chang, Josephine B Lee, Steven E Molesa, and Steven K Volkman. Printed organic transistors for ultra-low-cost rfid applications. *IEEE transactions on components and packaging technologies*, 28(4):742–747, 2005.

[42] Li Yang and Manos M Tentzeris. Design and characterization of novel paper-based inkjet-printed rfid and microwave structures for telecommunication and sensing applications. In *Microwave Symposium, 2007. IEEE/MTT-S International*, pages 1633–1636. IEEE, 2007.

[43] Kevin C Honeychurch and John P Hart. Screen-printed electrochemical sensors for monitoring metal pollutants. *TrAC Trends in Analytical Chemistry*, 22(7):456–469, 2003.

[44] Serena Laschi, Ilaria Palchetti, and Marco Mascini. Gold-based screen-printed sensor for detection of trace lead. *Sensors and Actuators B: Chemical*, 114(1):460–465, 2006.

[45] Bo Li, Suresh Santhanam, Lawrence Schultz, Malika Jeffries-El, Mihaela C Iovu, Genevieve Sauvé, Jessica Cooper, Rui Zhang, Joseph C Revelli, Aaron G Kusne, et al. Inkjet printed chemical sensor array based on polythiophene conductive polymers. *Sensors and Actuators B: Chemical*, 123(2):651–660, 2007.

[46] Frederik C Krebs. Fabrication and processing of polymer solar cells: a review of printing and coating techniques. *Solar energy materials and solar cells*, 93(4):394–412, 2009.

[47] Robert Hahn and Herbert Reichl. Batteries and power supplies for wearable and ubiquitous computing. In *Wearable Computers, 1999. Digest of Papers. The Third International Symposium on*, pages 168–169. IEEE, 1999.

[48] M Hilder, B Winther-Jensen, and NB Clark. Paper-based, printed zinc–air battery. *Journal of power Sources*, 194(2):1135–1141, 2009.

[49] André C Arsenault, Daniel P Puzzo, Ian Manners, and Geoffrey A Ozin. Photonic-crystal full-colour displays. *Nature Photonics*, 1(8):468, 2007.

[50] Jason Heikenfeld, Paul Drzaic, Jong-Souk Yeo, and Tim Koch. A critical review of the present and future prospects for electronic paper. *Journal of the Society for Information Display*, 19(2):129–156, 2011.

[51] B Huber, PB Popp, M Kaiser, A Ruediger, and C Schindler. Fully inkjet printed flexible

resistive memory. *Applied Physics Letters*, 110(14):143503, 2017.

[52] S. Ogawa. *Organic Electronics Materials and Devices*. Springer Japan, 2015.

[53] Se Hyun Kim, Kihyon Hong, Wei Xie, Keun Hyung Lee, Sipei Zhang, Timothy P Lodge, and C Daniel Frisbie. Electrolyte-gated transistors for organic and printed electronics. *Advanced Materials*, 25(13):1822–1846, 2013.

[54] Kihyon Hong, Se Hyun Kim, Keun Hyung Lee, and C Daniel Frisbie. Printed, sub-2v zno electrolyte gated transistors and inverters on plastic. *Advanced Materials*, 25(25):3413–3418, 2013.

[55] Suresh Kumar Garlapati, Nilesha Mishra, Simone Dehm, Ramona Hahn, Robert Kruk, Horst Hahn, and Subho Dasgupta. Electrolyte-gated, high mobility inorganic oxide transistors from printed metal halides. *ACS Applied Materials & Interfaces*, 5(22):11498–11502, 2013. PMID: 24224773.

[56] Xiaowei Feng, Christian Punckt, Gabriel Cadilha Marques, Michael Hefenbrock, Mehdi B Tahoori, and Jasmin Aghassi-Hagmann. Impact of intrinsic capacitances on the dynamic performance of printed electrolyte-gated inorganic field effect transistors. *IEEE Transactions on Electron Devices*, 66(8):3365–3370, 2019.

[57] Xiaowei Feng, Gabriel Cadilha Marques, Farhan Rasheed, Mehdi B Tahoori, and Jasmin Aghassi-Hagmann. Nonquasi-static capacitance modeling and characterization for printed inorganic electrolyte-gated transistors in logic gates. *IEEE Transactions on Electron Devices*, 66(12):5272–5277, 2019.

[58] Ahmet Turan Erozan, Guan Ying Wang, Rajendra Bishnoi, Jasmin Aghassi-Hagmann, and Mehdi B Tahoori. A compact low-voltage true random number generator based on inkjet printing technology. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2020.

[59] Nathaniel Bleier, Muhammad Husnain Mubarik, Farhan Rasheed, Jasmin Aghassi-Hagmann, Mehdi B. Tahoori, and Rakesh Kumar. Printed microprocessors. In *Proceedings of the 47th Annual International Symposium on Computer Architecture (ISCA)*. ACM, 2020.

[60] Gabriel Cadilha Marques, Farhan Rasheed, Jasmin Aghassi-Hagmann, and Mehdi B Tahoori. From silicon to printed electronics: a coherent modeling and design flow approach based on printed electrolyte gated fets. In *Proceedings of the 23rd Asia and South Pacific Design Automation Conference*, pages 658–663. IEEE Press, 2018.

[61] Gabriel Cadilha Marques, Suresh Kumar Garlapati, Simone Dehm, Subho Dasgupta, Horst Hahn, Mehdi Tahoori, and Jasmin Aghassi-Hagmann. Digital power and performance analysis of inkjet printed ring oscillators based on electrolyte-gated oxide electronics. *Applied Physics Letters*, 111(10):102103, 2017.

[62] Dennis Weller, Gabriel Cadilha Marques, Jasmin Aghassi-Hagmann, and Mehdi B Tahoori. An inkjet-printed low-voltage latch based on inorganic electrolyte-gated transistors. *IEEE Electron Device Letters*, 39(6):831–834, 2018.

[63] 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*, 64(1):279–285, Jan 2017.

[64] Fazel Zare Bidoky, Boxin Tang, Rui Ma, Krystopher S Jochem, Woo Jin Hyun, Donghoon Song, Steven J Koester, Timothy P Lodge, and C Daniel Frisbie. Sub-3 v zno electrolyte-gated transistors and circuits with screen-printed and photo-crosslinked ion gel gate dielectrics: New routes to improved performance. *Advanced Functional Materials*, page 1902028, 2019.

[65] Florian De Roose, Hikmet Çeliker, Jan Genoe, Wim Dehaene, and Kris Myny. Dual-gate self-aligned a-ingazno transistor model for flexible circuit applications. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 25–29. IEEE, 2019.

[66] M Fattori, IA Fijn, L Hu, Eugenio Cantatore, Fabrizio Torricelli, and M Charbonneau. Circuit design and design automation for printed electronics. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 42–47. IEEE, 2019.

[67] Masoud Rostami, James B Wendt, Miodrag Potkonjak, and Farinaz Koushanfar. Quo vadis, puf?: trends and challenges of emerging physical-disorder based security. In *Proceedings of the conference on Design, Automation & Test in Europe*, page 352. European Design and Automation Association, 2014.

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

[69] M. Rostami, F. Koushanfar, and R. Karri. A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE*, 102(8):1283–1295, Aug 2014.

[70] A. Maiti, J. Casarona, L. McHale, and P. Schaumont. A large scale characterization of ro-puf. In *International Symposium on Hardware-Oriented Security and Trust*, pages 94–99, June 2010.

[71] Alfred J Menezes, Jonathan Katz, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography.* CRC press, 1996.

[72] Richard D Warner, Dr Richard M Adams, Diana Varma, Elaine Leung, and Shanley Maguire. *Introduction to security printing.* Printing Industries Press, 2016.

[73] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026–2030, 2002.

[74] Dilip SV Kumar, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede. An in-depth and black-box characterization of the effects of laser pulses on atmega328p. In *International Conference on Smart Card Research and Advanced Applications*, pages 156–170. Springer, 2018.

[75] Sergei Skorobogatov. Flash memory 'bumping'attacks. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 158–172. Springer, 2010.

[76] Berk Sunar, William J Martin, and Douglas R Stinson. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Transactions on computers*, 56(1):109–119, 2006.

[77] Daniel J Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, and Nicko Van Someren. Factoring rsa keys from certified smart cards: Coppersmith in the wild. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 341–360. Springer, 2013.

[78] Markus Dichtl. How to predict the output of a hardware random number generator. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 181–188. Springer, 2003.

[79] John S Liberty, Adrian Barrera, David W Boerstler, Thomas B Chadwick, Scott R Cottier, H Peter Hofstee, Julie A Rosser, and Marty L Tsai. True hardware random number generation implemented in the 32-nm soi power7+ processor. *IBM Journal of Research and Development*, 57(6):4–1, 2013.

[80] Carlos Tokunaga, David Blaauw, and Trevor Mudge. True random number generator with a metastability-based quality control. *IEEE Journal of Solid-State Circuits*, 43(1):78–85, 2008.

[81] Jeremy Holleman, Seth Bridges, Brian P Otis, and Chris Diorio. A 3μw cmos true random number generator with adaptive floating-gate offset cancellation. *IEEE Journal of Solid-State Circuits*, 43(5):1324–1336, 2008.

[82] Kaiyuan Yang, David Blaauw, and Dennis Sylvester. An all-digital edge racing true random number generator robust against pvt variations. *IEEE Journal of Solid-State Circuits*, 51(4):1022–1031, 2016.

[83] Ülkühan Güler and Günhan Dündar. Modeling cmos ring oscillator performance as a randomness source. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 61(3):712–724, 2013.

[84] Randy Torrance and Dick James. The state-of-the-art in semiconductor reverse engineering. In *Design Automation Conference (DAC), 2011 48th ACM/EDAC/IEEE*, pages 333–338. IEEE, 2011.

[85] Jason Abt and Chris Pawlowicz. Circuit analysis techniques: Delayering and circuit vision, 2012.

[86] Ujjwal Guin, Daniel DiMase, and Mohammad Tehranipoor. Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. *Journal of Electronic Testing*, 30(1):9–23, 2014.

[87] Ujjwal Guin, Ke Huang, Daniel DiMase, John M Carulli, Mohammad Tehranipoor, and Yiorgos Makris. Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. *Proceedings of the IEEE*, 102(8):1207–1228, 2014.

[88] Chongxi Bao, Domenic Forte, and Ankur Srivastava. On application of one-class svm to reverse engineering-based hardware trojan detection. In *Quality Electronic Design (ISQED), 2014 15th International Symposium on*, pages 47–54. IEEE, 2014.

[89] Karsten Nohl, David Evans, Starbug Starbug, and Henryk Plötz. Reverse-engineering a cryptographic rfid tag. In *USENIX security symposium*, volume 28, 2008.

[90] Dmitry Lagunovsky, Sergey Ablameyko, and M Kutas. Recognition of integrated circuit images in reverse engineering. In *Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on*, volume 2, pages 1640–1642. IEEE, 1998.

[91] Marc Fyrbiak, Sebastian Strauß, Christian Kison, Sebastian Wallat, Malte Elson, Nikol Rummel, and Christof Paar. Hardware reverse engineering: Overview and open challenges. In *Verification and Security Workshop (IVSW), 2017 IEEE 2nd International*, pages 88–94. IEEE, 2017.

[92] Randy Torrance and Dick James. The state-of-the-art in ic reverse engineering. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009*, pages 363–381, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[93] Mark C Hansen, Hakan Yalcin, and John P Hayes. Unveiling the iscas-85 benchmarks: A case study in reverse engineering. *IEEE Design & Test of Computers*, 16(3):72–80, 1999.

[94] Wenchao Li, Zach Wasson, and Sanjit A Seshia. Reverse engineering circuits using behavioral pattern mining. In *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*, pages 83–88. IEEE, 2012.

[95] Pramod Subramanyan, Nestan Tsiskaridze, Kanika Pasricha, Dillon Reisman, Adriana Susnea, and Sharad Malik. Reverse engineering digital circuits using functional analysis. In *Proceedings of the Conference on Design, Automation and Test in Europe*, pages 1277–1280. EDA Consortium, 2013.

[96] Jae W Lee, Daihyun Lim, Blaise Gassend, G Edward Suh, Marten Van Dijk, and Srinivas Devadas. A technique to build a secret key in integrated circuits for identification and authentication applications. In *VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on*, pages 176–179. IEEE, 2004.

[97] Pier Francesco Cortese, Francesco Gemmiti, Bernardo Palazzi, Maurizio Pizzonia, and Massimo Rimondini. Efficient and practical authentication of puf-based rfid tags in supply chains. In *RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on*, pages 182–188. IEEE, 2010.

[98] A. Mosenia and N. K. Jha. A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, 5(4):586–602, Oct 2017.

[99] A. O. Akmandor and N. K. Jha. Smart health care: An edge-side computing perspective. *IEEE Consumer Electronics Magazine*, 7(1):29–37, Jan 2018.

[100] Mehran Mozaffari Kermani, Meng Zhang, Anand Raghunathan, and Niraj K Jha. Emerging frontiers in embedded security. In *VLSI Design and 2013 12th International Conference on Embedded Systems (VLSID), 2013 26th International Conference on*, pages 203–208. IEEE, 2013.

[101] M. Zhang, A. Raghunathan, and N. K. Jha. Trustworthiness of medical devices and body area networks. *Proceedings of the IEEE*, 102(8):1174–1188, Aug 2014.

[102] G Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th annual design automation conference*, pages 9–14. ACM, 2007.

[103] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 148–160. ACM, 2002.

[104] Ulrich Rührmair, Srinivas Devadas, and Farinaz Koushanfar. Security based on physical unclonability and disorder. In *Introduction to Hardware Security and Trust*, pages 65–102. Springer, 2012.

[105] Vinay C Patil, Arunkumar Vijayakumar, Daniel E Holcomb, and Sandip Kundu. Improving reliability of weak pufs via circuit techniques to enhance mismatch. In *Hardware*

Oriented Security and Trust (HOST), 2017 IEEE International Symposium on, pages 146–150. IEEE, 2017.

[106] Kazunori Kuribara, Yohei Hori, Toshihiro Katashita, Kazuaki Kakita, Yasuhiro Tanaka, and Manabu Yoshida. Organic physically unclonable function on flexible substrate operable at 2 v for iot/ioe security applications. *Organic Electronics*, 51:137–141, 2017.

[107] S.M. Sze and K.K. Ng. *Physics of Semiconductor Devices*. Wiley, 2006.

[108] W. R. Curtice. A mesfet model for use in the design of gaas integrated circuits. *IEEE Transactions on Microwave Theory and Techniques*, 28(5):448–456, May 1980.

[109] M. D. Yu and S. Devadas. Secure and robust error correction for physical unclonable functions. *IEEE Design Test of Computers*, 27(1):48–65, Jan 2010.

[110] Benjamin Jun and Paul Kocher. The intel random number generator. *Cryptography Research Inc. white paper*, 27:1–8, 1999.

[111] Madhusudan Singh, Hanna M Haverinen, Parul Dhagat, and Ghassan E Jabbour. Inkjet printing—process and its applications. *Advanced materials*, 22(6):673–685, 2010.

[112] Farhan Rasheed, Mohammad Saber Golanbari, Gabriel Cadilha Marques, Mehdi B Tahoori, and Jasmin Aghassi-Hagmann. A smooth ekv-based dc model for accurate simulation of printed transistors and their process variations. *IEEE Transactions on Electron Devices*, 65(2):667–673, 2018.

[113] Farhan Rasheed, Michael Hefenbrock, Michael Beigl, Mehdi B Tahoori, and Jasmin Aghassi-Hagmann. Variability modeling for printed inorganic electrolyte-gated transistors and circuits. *IEEE Transactions on Electron Devices*, 66(1):146–152, 2018.

[114] Malte Brettel, Niklas Friederichsen, Michael Keller, and Marius Rosenberg. How virtualization, decentralization and network building change the manufacturing landscape: An industry 4.0 perspective. *International journal of mechanical, industrial science and engineering*, 8(1):37–44, 2014.

[115] SKM Jönsson, Jonas Birgerson, Xavier Crispin, Grzegorz Greczynski, Wojciech Osikowicz, AW Denier Van Der Gon, William R Salaneck, and Mats Fahlman. The effects of solvents on the morphology and sheet resistance in poly (3, 4-ethylenedioxythiophene)–polystyrenesulfonic acid (pedot–pss) films. *Synthetic metals*, 139(1):1–10, 2003.

[116] Sanu Mathew, Sudhir Satpathy, Vikram Suresh, and Ram Krishnamurthy. Ultra-low energy circuit building blocks for security technologies. In *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 391–394. IEEE, 2018.

[117] C Ionescu, P Svasta, A Vasile, and D Bonfert. Investigations on organic printed resistors based on pedot: Pss. In *2012 IEEE 18th International Symposium for Design and Technology in Electronic Packaging (SIITME)*, pages 85–89. IEEE, 2012.

[118] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-Allen and Hamilton Inc Mclean Va, 2001.

[119] Gabriel Cadilha Marques, Falk von Seggern, Simone Dehm, Ben Breitung, Horst Hahn, Subho Dasgupta, Mehdi B Tahoori, and Jasmin Aghassi-Hagmann. Influence of humidity on the performance of composite polymer electrolyte-gated field-effect transistors and

circuits. *IEEE Transactions on Electron Devices*, 66(5):2202–2207, 2019.

[120] Vikram B Suresh and Wayne P Burleson. Entropy and energy bounds for metastability based trng with lightweight post-processing. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 62(7):1785–1793, 2015.

[121] John von Neumann. Various techniques used in connection with random digits. *John von Neumann, Collected Works*, 5:768–770, 1963.

[122] HF Castro, E Sowade, JG Rocha, P Alpuim, AV Machado, RR Baumann, and S Lanceros-Méndez. Degradation of all-inkjet-printed organic thin-film transistors with tips-pentacene under processes applied in textile manufacturing. *Organic Electronics*, 22:12–19, 2015.

[123] Seungjun Chung, Seul Ong Kim, Soon-Ki Kwon, Changhee Lee, and Yongtaek Hong. All-inkjet-printed organic thin-film transistor inverter on flexible plastic substrate. *IEEE electron device letters*, 32(8):1134–1136, 2011.

[124] Tsung-Ching Huang, Kenjiro Fukuda, Chun-Ming Lo, Yung-Hui Yeh, Tsuyoshi Sekitani, Takao Someya, and Kwang-Ting Cheng. Pseudo-cmos: A design style for low-cost and robust flexible electronics. *IEEE Transactions on Electron Devices*, 58(1):141–150, 2011.

[125] Jeyavijayan Rajendran, Michael Sam, Ozgur Sinanoglu, and Ramesh Karri. Security analysis of integrated circuit camouflaging. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 709–720. ACM, 2013.

[126] Xi Zhang, Tong Ge, and Joseph S Chang. Fully-additive printed electronics: Transistor model, process variation and fundamental circuit designs. *Organic Electronics*, 26:371–379, 2015.

[127] Carlo Tomasi and Roberto Manduchi. Bilateral filtering for gray and color images. In *Computer Vision, 1998. Sixth International Conference on*, pages 839–846. IEEE, 1998.

[128] Lawrence G Roberts. *Machine perception of three-dimensional solids.* PhD thesis, Massachusetts Institute of Technology, 1963.

[129] Stephen M Pizer, E Philip Amburn, John D Austin, Robert Cromartie, Ari Geselowitz, Trey Greer, Bart ter Haar Romeny, John B Zimmerman, and Karel Zuiderveld. Adaptive histogram equalization and its variations. *Computer vision, graphics, and image processing*, 39(3):355–368, 1987.

[130] Stéfan van der Walt, Johannes L. Schönberger, Juan Nunez-Iglesias, François Boulogne, Joshua D. Warner, Neil Yager, Emmanuelle Gouillart, Tony Yu, and the scikit-image contributors. scikit-image: image processing in Python. *PeerJ*, 2:e453, 6 2014.

[131] Navneet Dalal and Bill Triggs. Histograms of oriented gradients for human detection. In *Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on*, volume 1, pages 886–893. IEEE, 2005.

[132] Paul L Rosin. Measuring corner properties. *Computer Vision and Image Understanding*, 73(2):291–307, 1999.

[133] Leo Breiman. Random forests. *Machine learning*, 45(1):5–32, 2001.

[134] Leo Breiman, Jerome Friedman, RA Olshen, and Charles J Stone. Classification and regression trees. 1984.

[135] Leo Breiman. Bagging predictors. *Machine learning*, 24(2):123–140, 1996.

[136] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12:2825–2830, 2011.

[137] Kesheng Wu, Ekow Otoo, and Arie Shoshani. Optimizing connected component labeling algorithms. In *Medical Imaging 2005: Image Processing*, volume 5747, pages 1965–1977. International Society for Optics and Photonics, 2005.

[138] F. Brglez and H. Fujiwara. A neutral netlist of 10 combinational benchmark circuits. In *Proceedings of the IEEE International Symposium on Circuits and Systems*, pages 695–698, 1985.

[139] Gang Cui, Sang Jin Kim, Sung Hyuk Choi, Hakhyun Nam, Geun Sig Cha, and Ki-Jung Paeng. A disposable amperometric sensor screen printed on a nitrocellulose strip: A glucose biosensor employing lead oxide as an interference-removing agent. *Analytical Chemistry*, 72(8):1925–1929, 2000. PMID: 10784163.

[140] Dae Y Kang, Yun-Soung Kim, Gladys Ornelas, Mridu Sinha, Keerthiga Naidu, and Todd P Coleman. Scalable microfabrication procedures for adhesive-integrated flexible and stretchable electronic sensors. *Sensors*, 15(9):23459–23476, 2015.

[141] Christoph Steiger, Alex Abramson, Phillip Nadeau, Anantha P Chandrakasan, Robert Langer, and Giovanni Traverso. Ingestible electronics for diagnostics and therapy. *Nature Reviews Materials*, 4(2):83–98, 2019.

[142] Jordi Carrabina, Mohammad Mashayekhi, Jofre PallarÈs, and Lluis TerÉs. Inkjet-configurable gate arrays (iga). *IEEE Transactions on Emerging Topics in Computing*, 5(2):238–246, 2016.

[143] Saman Kiamehr, Abdulazim Amouri, and Mehdi B Tahoori. Investigation of nbti and pbti induced aging in different lut implementations. In *2011 International Conference on Field-Programmable Technology*, pages 1–8. IEEE, 2011.

[144] Farhan Rasheed, Michael Hefenbrock, Rajendra Bishnoi, Michael BeigI, Jasmin Aghassi-Hagmann, and Mehdi B Tahoori. Predictive modeling and design automation of inorganic printed electronics. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 30–35. IEEE, 2019.

[145] Luca Amarù, Pierre-Emmanuel Gaillardon, and Giovanni De Micheli. The epfl combinational benchmark suite. *Proceedings of the 24th International Workshop on Logic & Synthesis (IWLS)*, 2015.

[146] G. H. Chapman and B. Dufort. Using laser defect avoidance to build large-area fpgas. *IEEE Design Test of Computers*, 15(4):75–81, Oct 1998.

[147] N. J. Howard, A. M. Tyrrell, and N. M. Allinson. The yield enhancement of field-programmable gate arrays. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2(1):115–123, March 1994.

[148] J. Narasimham, K. Nakajima, C. S. Rim, and A. T. Dahbura. Yield enhancement of programmable asic arrays by reconfiguration of circuit placements. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 13(8):976–986, Aug 1994.

[149] Amr T Abdel-Hamid, Sofiéne Tahar, and El Mostapha Aboulhamid. A survey on ip watermarking techniques. *Design Automation for Embedded Systems*, 9(3):211–227, 2004.

[150] F. Koushanfar and G. Qu. Hardware metering. In *Proceedings of the 38th Design Automation Conference (IEEE Cat. No.01CH37232)*, pages 490–493, June 2001.

List of Publications

Journals

- **A. T. Erozan**, D. Weller, F. Rasheed, R. Bishnoi, J. Aghassi-Hagmann and M.B. Tahoori, "Split Manufacturing for Printed Electronics: Programmable Printed Circuits", in IEEE Transactions on Very Large-Scale Integration Systems (TVLSI), 2020.

- **A. T. Erozan**, G. Y. Wang, R. Bishnoi, J. Aghassi-Hagmann, M. B. Tahoori, "A Compact Low-Voltage True Random Number Generator based on Inkjet Printing Technology", in IEEE Transactions on Very Large-Scale Integration Systems (TVLSI), 2020.

- **A. T. Erozan**, M. Hefenbrock, M. Beigl, J. Aghassi-Hagmann and M.B. Tahoori, "Reverse Engineering of Printed Electronics Circuits: From Imaging to Netlist Extraction", in IEEE Transactions on Information Forensics and Security (TIFS), vol. 15, pp. 475-486, 2020.

- G.C. Marques, D. Weller, **A. T. Erozan**, X. Feng, M. Tahoori, and J. Aghassi-Hagmann, "Progress Report on 'From printed electrolyte-gated metal-oxide devices to circuits'", in Advanced Materials, vol. 31, no. 26, pp. 1806483, 2019.

- **A. T. Erozan**, G.C. Marques, M. S. Golanbari, R. Bishnoi, S. Dehm, J. Aghassi-Hagmann, M. B. Tahoori, "Inkjet-Printed EGFET-based Physical Unclonable Function - Design, Evaluation, and Fabrication", in IEEE Transactions on Very Large-Scale Integration Systems (TVLSI), vol. 26, no. 12, pp. 2935-2946, 2018.

Conferences

- **A. T. Erozan**, R. Bishnoi, J. Aghassi-Hagmann and M.B. Tahoori, "Inkjet Printed True Random Number Generator based on Additive Resistor Tuning", in proceedings of Design, Automation & Test in Europe (DATE), pp. 1361-1366, 2019.

- **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 proceedings of International Symposium on Quality Electronic Design (ISQED), pp. 419-424, 2018.