SPICE Modeling Of Metal-Molecular Nanoelectronics Networks: An Exploration of Randomly Distributed Resistors & Diodes Modeling and Analysis

by

Kenil Sandipkumar Naik

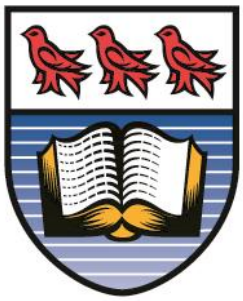
B Tech. Gujarat Technological University, 2021

A Project Report Submitted in Partial Fulfilment

of the requirements for the degree of

MASTER OF ENGINEERING

in the Department of Electrical and Computer Engineering at the University of Victoria, Victoria, British Columbia, Canada.



University of Victoria

Supervisory Committee

SPICE Modeling Of Metal-Molecular Nanoelectronics Networks: An Exploration of Randomly Distributed Resistors & Diodes Modeling and Analysis

by

Kenil Sandipkumar Naik

B Tech. Gujarat Technological University, 2021

Supervisory Committee:

Dr. Chris Papadopoulos, Department of Electrical and Computer Engineering

Supervisor

Dr. Tao Lu, Department of Electrical and Computer Engineering

Supervisory Committee Member

Abstract

An innovative approach to the development of metal-molecular nanoelectronic networks through LTSpice modeling is represented in this project, focusing on the simulation and analysis of randomly distributed resistor blocks and diodes in the network. In the digital era of miniaturization and increasing demand for secure electronic devices, this study incorporates a unique methodology for enhancing hardware security primitives and their performances. The approach proposed a novel methodology using a distinct resistor network circuit resembling that of the gold nanoparticle-molecular network configuration and their internal resistance and defects used for previous investigations regarding the same. A unique Mesh Resistor Network (MRN) with structured randomness based on the resistor network building blocks offers new insights into the correlation and electrical behaviors of nanoscale networks when examined. This novel procedure provides new opportunities to enhance the understanding of electronic transport in nanoparticles and evolves our development of robust hardware encryption keys for increased hardware security. To insert an additional tunable parameter, resistors in the formed MRN are replaced by the proportion of diodes. This adjustment introduces directional current flow and non-linear responses, aligning with the theoretical insights from the previous research. The integration of diodes, particularly in varied orientations, showcases the potential for creating complex, tunable electronic systems that leverage components' resistive and rectifying properties. Furthermore, this opens a broad spectrum of methods to design customized electronic devices with tunable properties for better security and performance, addressing the limitations of current network simulations. By systematically changing the position of the building blocks in the resistor network, the proportion of diodes and metal-gold particles in the Mesh Network provides tunable physical unclonable functions for the design of electronic devices with tunable electrical properties, paving a road for future advancements in molecular electronics and secure communication technologies.

Table of Contents

List of tables

List of Figures

Nomenclature

LTSpice: Linear Technology Simulation Program with Integrated Circuit Emphasis

PUF: Physical Unclonable Functions

MRN: Mesh Resistor Network.

NVM: Non-Volatile Memory

CRP: Challenge Response Pair

CMOS: Complementary Metal–Oxide–Semiconductor

PCM: Phase Change Memory

STT-MRAM: Spin-Transfer Torque Magnetic Random-Access Memory

CNFET: Carbon-Nanotube Field-Effect Transistors

NDR: Negative Differential Resistance

AFM: Atomic force microscopy

Acknowledgment

I am deeply thankful to my Guru Shree Sai for his countless blessings and for encouraging me to achieve my dreams.

I would like to express my greatest gratitude to my supervisor, Dr. Chris Papadopoulos, for his guidance and support throughout my program of study. Without his supervision and hard work, it would not be possible to achieve my maximum potential throughout the degree. Deeply thankful for his understanding and encouragement to lead my master's journey to a fruitful goal.

I am also thankful to Dr. Tao Lu for the time and effort spent being a member of my supervisory committee and for providing valuable suggestions.

Special thanks to Dr. Anusha Venkataraman for her immense help and guidance throughout this project work.

A special thanks to my amazing parents and my wife for their unwavering support and believing in me and encouraging me in every step of my life.

I am also grateful to all the professors, lab technicians, and staff in the Electrical & Computer Engineering Department at the University of Victoria for their support and assistance.

Lastly, I would like to thank my friends, colleagues, and the people in the beautiful city of Victoria for their positivity and kindness towards me.

Dedication

My amazing parents and my lovely wife

1. Introduction

1.1 Context

Nanotechnology and electronic miniaturization have had a prominent impact on the development of futuristic technologies, resulting in the creation of smaller, more efficient, and more powerful electronic devices year by year. Because of this, the field addresses the ongoing need for miniaturization while significantly enhancing security. Figure 1 shows the roadmap of nanotechnology use in global security, stating the development of nanotechnology and cybersecurity. The project comes hand in hand with the development of this transformative topic, which focuses on expanding the boundaries to enhance the understanding and utilization of nanoscale networks in security applications. By focusing on the innovative simulation of metal-molecular networks, this approach tackles the obstacles and potential advantages arising from the need for more significant downsizing and security enhancements [2].

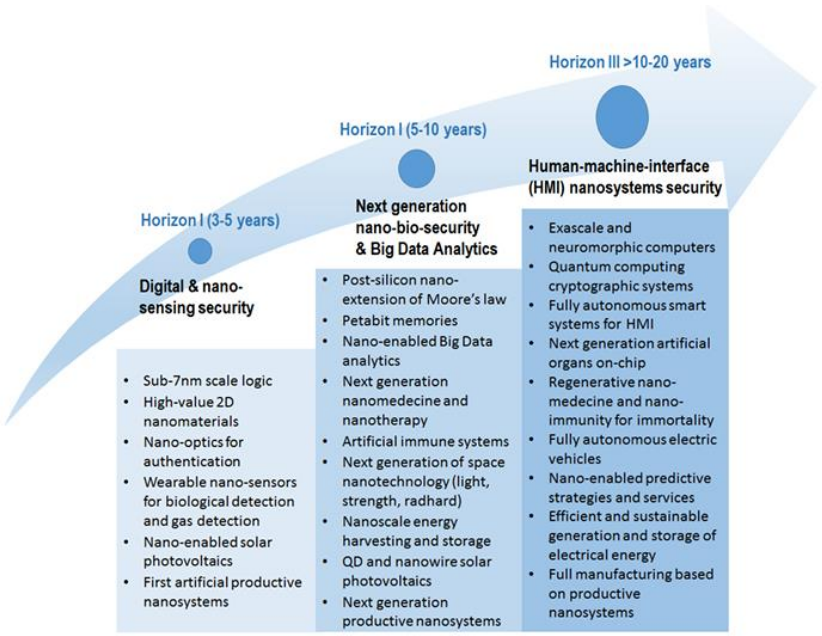


Figure 1: Roadmap of present and future major trends in nanotechnology in three-level horizon, with relevance for security [13].

Incorporating nanotechnology into cybersecurity also offers a revolutionary strategy for protecting both digital and physical assets of electronic devices. This report delves deep into the forefront of this amalgamation, investigating the possibilities presented by self-assembled nanoelectronic networks in terms of hardware encryption and enhancing security protocols. The genesis described here is rooted in a collection of groundbreaking research studies emphasizing the practicality and adaptability of nanomaterials and molecular-scale electronics in security applications. These studies specifically delve into the creation and attributes of nanoscale networks through self-assembly procedures, highlighting their potential to generate distinct, unclonable encryption keys, better known as Physical Unclonable Functions (PUFs) [1-8]. Each research contribution helps develop a comprehensive understanding of the electrical and physical properties that make these materials exceptional contenders for security applications.

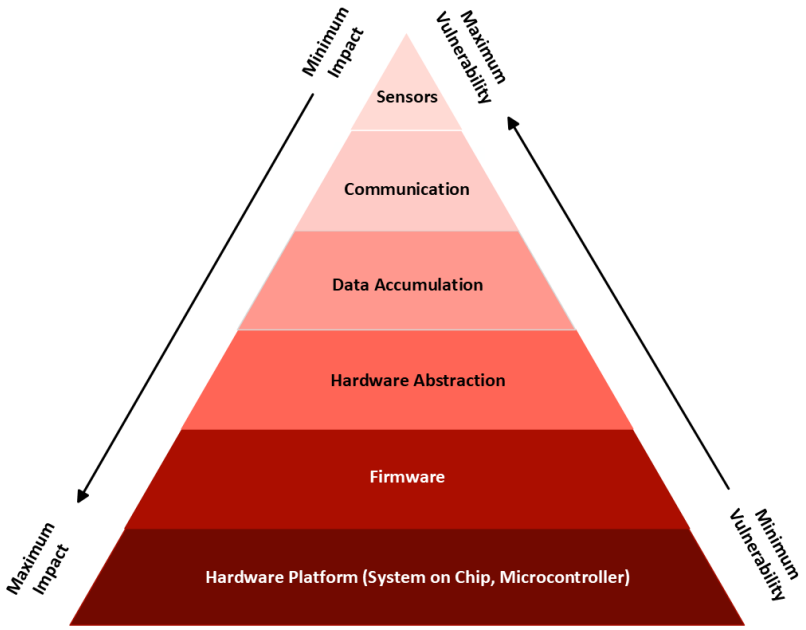


Figure 2: Vulnerability and Impact of attacks at different levels in electronic system [6].

Hardware devices and electronic systems, comprising various components, typically present a lower risk of successful internal attacks at electronic circuit levels. However, these risks cannot be overlooked with the advent of advanced artificial intelligence and increased computational capabilities. The vulnerability is particularly concerning for system-on-chip and memory cards, where valuable information is stored; an attack at this level can result in significant loss of sensitive data, surpassing the risks associated with other levels. Historical analyses of vulnerabilities and the impact of attacks highlight that the built-in hardware and electronic circuits are most severely affected by attacks on electronic devices, as illustrated in Figure 2 [6]. This scenario underscores the requirement to develop more secure and durable systems, which is the goal of this project, through the application of nanotechnology driven Physical Unclonable Functions (PUFs).

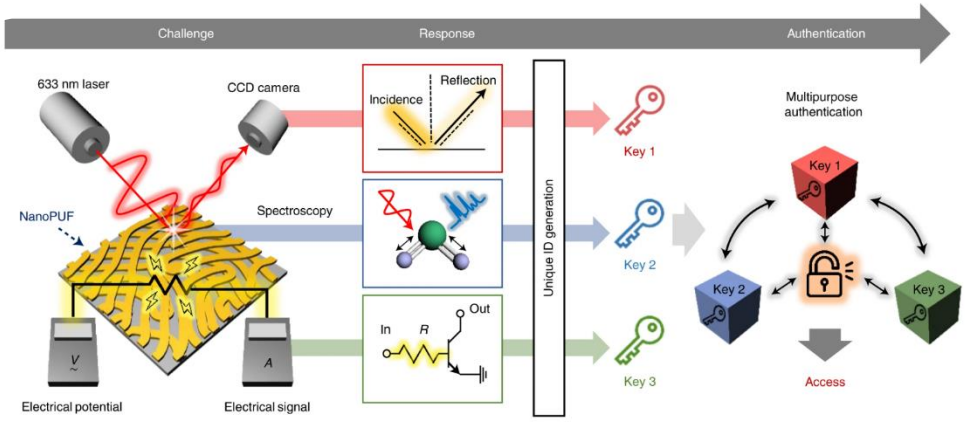


Figure 3: Multiple-nanoPUFs based authentication system [14].

Figure 3 illustrates an example of multiple key generation using nanoPUFs for authentication purposes. This figure utilizes responses from three different nanoPUFs to form unique challenges for each PUF. These include a light-scattering-based nanoPUF, a Light-Reflection and intensity-based PUF and an Electrical Network-based PUF. The responses from these PUFs are used to generate three distinct keys that are employed for system access and authentication [14].

Current research into nanoelectronics-based networks has concentrated on the electrical behaviours of assemblies comprising metals and molecules, highlighting their promising applications in nanoelectronics [1-5]. However, the prevalent methodologies for generating PUFs have posed significant obstacles to fully understanding the complexities of such networks used for it and the improvement of their parameters. To enhance the security against unauthorized duplication or tampering, this study introduces an element of uncertainty by randomly distributing building blocks with different resistor networks replicating molecular resistance, their intermolecular resistance, and defects formed during the self-assembly process across multiple iterations of the mesh network. This approach adds complexity and makes it significantly more challenging for unauthorized attempts to replicate or tamper with the system. This initiative aims to bridge these gaps by adopting an innovative simulation technique, which facilitates a more regulated investigation into the adjustable electrical properties of nanoparticle networks. This approach sets the stage for progress in molecular electronics and cybersecurity and heralds a new era of precision and innovation in studying nanoelectronic systems and their wide application.

The significance of this project goes beyond simply accomplishing the technical accomplishment of building these networks. It comprehends a wider perspective of utilizing the distinctive characteristics of materials at the nanoscale level to tackle some of the most urgent challenges in cybersecurity. With the rise in sophistication and large scale of digital risks, the requirement to advance the security of hardware is the topmost solution against the attacks to protect the sensitive information on hardware systems. This report aims to contribute to ongoing research on combining the field of nanotechnology and cybersecurity by providing valuable insights and simulation results through a unique methodology that potentially can pave the way for the next era of hardware security and data protection technologies.

1.2 Objectives

This project aims to develop a novel simulation methodology for nanoscale networks that uplifts and verifies the ongoing research by providing a more granular analysis of electrical properties through resistance-based building blocks and resistor-diode networks. This approach aims to enhance our understanding of metal-molecular networks, explicitly focusing on hardware security applications and developing advanced nanoelectronic devices with ongoing research. Through meticulous examination and comparison of different network topologies, the study aims to elucidate the factors influencing network efficiency, reliability, and security, thereby contributing valuable knowledge to designing and optimizing future mesh networks.

1.3 Report Outline

The report thoroughly examines SPICE Modeling for Metal-Molecular Nanoelectronics Networks, emphasizing networks comprising randomly arranged resistor blocks and diode substitution. It begins with an introductory [Chapter 1] that highlights the critical role of nanotechnology in improving both the security and efficiency of electronic devices, thus setting the stage for the stated research aims and methods. Chapter 2 delves into the transformative impact of nanotechnology, discussing the rise and importance of Physical Unclonable Functions (PUFs). It also incorporates the benefits of integrating PUFs with nanotechnology, including a method for self-assembling nanotechnology structures to create PUFs. This section also details the construction and electrical behavior of resistor-block and Mesh Networks based on prior research, establishing a foundation for the project's research and development of Mesh Networks.

The discussion progresses to creating Resistor-building blocks and their resistance values, which serve as the basis for randomly forming Mesh Networks for simulation and analysis in Chapter 3. This section provides an overview of three iterations of Mesh Network

construction from the building blocks and their in-depth analysis. Chapter 4 examines the electrical characteristics of modified Mesh Networks, achieved by adding a proportion of diodes to study non-linear responses and the impact of directional current flow. This analysis opens up new opportunities for using hardware security technologies. The considerable variances in the I-V curves simulated for all networks in LTSpice are also examined here. Through analysis and simulation, the report concludes by enhancing the understanding of nanoelectronic networks and showcasing their potential to enhance the security of future communication technologies and inform future research, laying the groundwork for further studies in this area.

This introduction establishes the foundation for thoroughly exploring the potential of self-assembled nanoelectronic networks in enhancing hardware security. It overcomes the limitations of existing research by providing a more granular analysis of electrical properties through resistance-based building blocks. The chapter dedicated to reviewing existing literature delves into the heart of past research that informs and supports the current investigation into self-assembled nanoelectronic networks for security applications and others. The scope of this report further includes the development of theories based on simulations and analyses to make significant contributions to the fields of molecular electronics and cybersecurity. Its goal is to establish a solid foundation for future research and technological advancements in these domains.

2. Background

2.1 Nanotechnology Characteristics

Nanotechnology represents a transformative theory within the scientific and engineering domains, emphasizing the art of manipulating matter on an atomic and molecular scale. This field is distinguished by its capacity to drive forward leaps in computational power, storage capabilities, and sensor precision by exploiting materials' distinctive attributes at the nanometer scale. Its contribution is pivotal in advancing the miniaturization of electronics, facilitating the development of significantly smaller, faster, and more energy-efficient devices than existing models, as shown in Figure 4 [9].

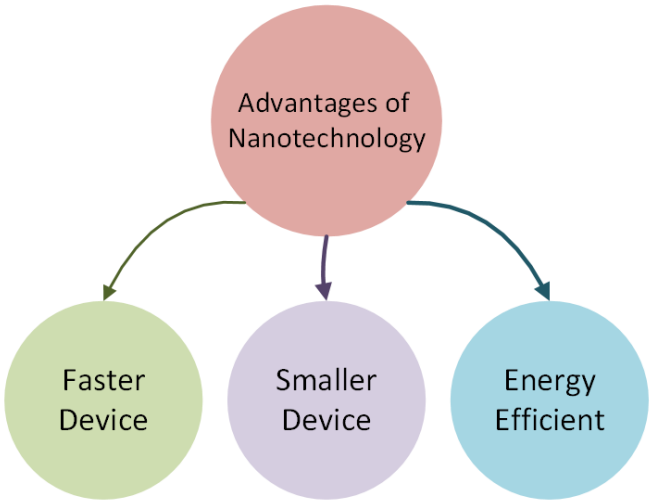


Figure 4: Advantages of Nanotechnology

At its core, nanotechnology involves the precise control and utilization of materials at atomic, molecular, and macromolecular dimensions. At these scales, materials exhibit novel phenomena that lead to groundbreaking applications, particularly in the convergence of nanotechnology with the exploration and deployment of nanoparticles. Nanoparticles, characterized by their unique physical, chemical, and optical properties that diverge from those of bulk materials, are integral to countless applications. These

range from nanoelectronics to cybersecurity, underscoring the transformative potential of nanotechnology in producing devices that are not only compact and energy-saving but also highly effective. This convergence of electronic innovation with nanoscale manipulation represents the project's groundbreaking nature, illustrating the vast possibilities that nanotechnology opens up for future advancements.

2.2 Physical Unclonable Functions

In traditional methods of encryption, digital keys or mathematical algorithms are used for encryption and data security, which uses Non-Volatile Memory (NVM) for cryptography. These methods have proven to be vulnerable to invasive physical attacks, such as cryptanalytic attacks [10]. Also, these methodologies increase device area and power overhead, which needs more than the general need to downsize them. Hence, Physical Unclonable Functions (PUFs) were used to encrypt electronic devices in hardware to overcome these vulnerabilities.

PUFs proposes a model security method that exploits the inherent physical properties and discrepancies in the material used to fabricate hardware components to strengthen its security. These discrepancies developed spontaneously during fabrication, making each device distinct and unpredictable[6-8]. Such uniqueness enables PUFs to function as a hardware device's fingerprint and facilitates applications in authentication, the generation of secure keys, and protection against counterfeiting [10-12]. The core principle of using PUF security primitives is that though they are easy to create, duplicating a device's precise physical attributes is impossible as it relies on uncontrollable physical parameters. This ensures that the PUF's output, or its response, acts as a unique and secure method for device identification.

PUFs are generally characterized based on their challenge (input) and their corresponding response (output), referred to as CRP (challenge Response Pair). This CRP is the primary fingerprint of each PUF, as shown in Figure 5 [8,12].

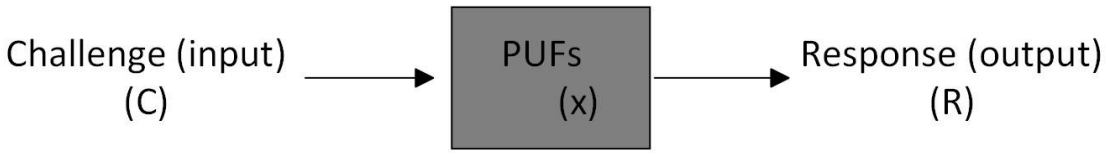


Figure 5: Characteristics of Physical Unclonable Functions [11].

The response of PUFs is characterized by its complex physical function, which is unique to each device or PUF instance. Figure 6 shows the typical characteristics of a good PUF [7]. The CRP of the PUFs can easily be varied to make numerous PUFs with unique characteristics based on thickness, cross-section area, and doping profile in the case of CMOS-based PUFs currently in the market [7-12]. Thus, a slight change in the degree of freedom changes the CRP of the PUFs.

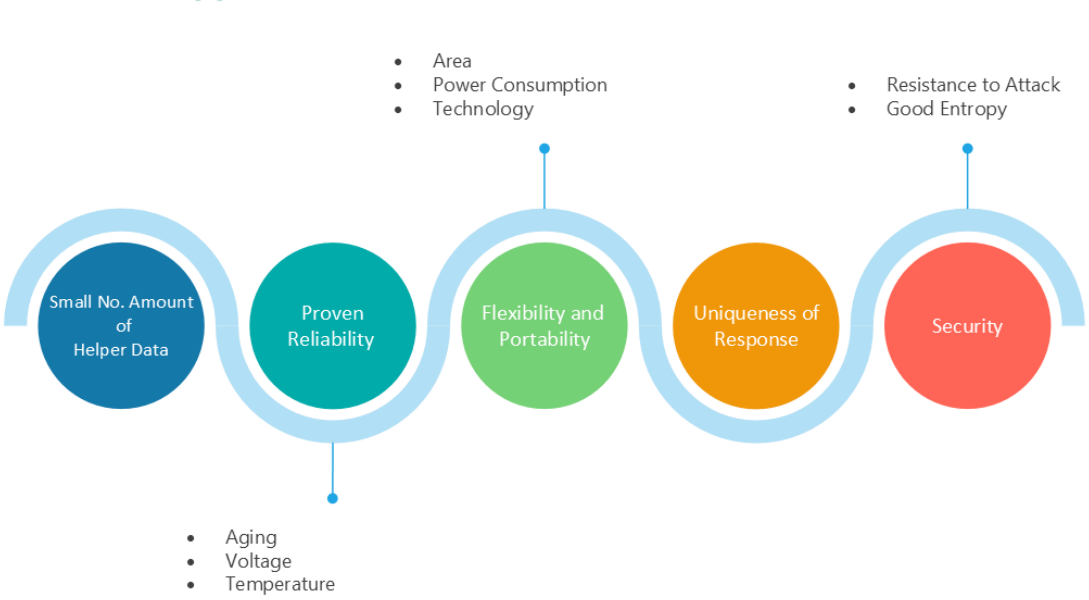


Figure 6: Typical Characteristics of Good PUF [7].

The main components to contribute the PUFs performance and strength is randomness, uniqueness and bit rate for encryption keys generation for hardware security. The randomness and uniqueness of generated bits can be assessed using several methods, including the NIST statistical randomness test suite and the Hamming distance metric. The Hamming distance, which measures the number of bit-by-bit changes needed to make two keys of equal length identical, is commonly used for shorter keys. Specifically, the Hamming intra-distance measures differences between two keys derived from the same set of electrode pairs tested repeatedly, indicating good repeatability and stability in our tests with very low intra-distances noted, ideally 0. Conversely, the Hamming inter-distance, ideal when averaging near 0.5, assesses keys from different samples, indicating they are random, uncorrelated, and unclonable. Figure 7, shows the current profile built by alternately combining four 16-bit keys from gold nanoparticle–nonanedithiol networked films with four 16-bit keys from a control sample (network without molecules). THe figure shows the 128-bit key generated by comparing adjacent currents from previous methodology for self-assembled Mesh Networks [5].

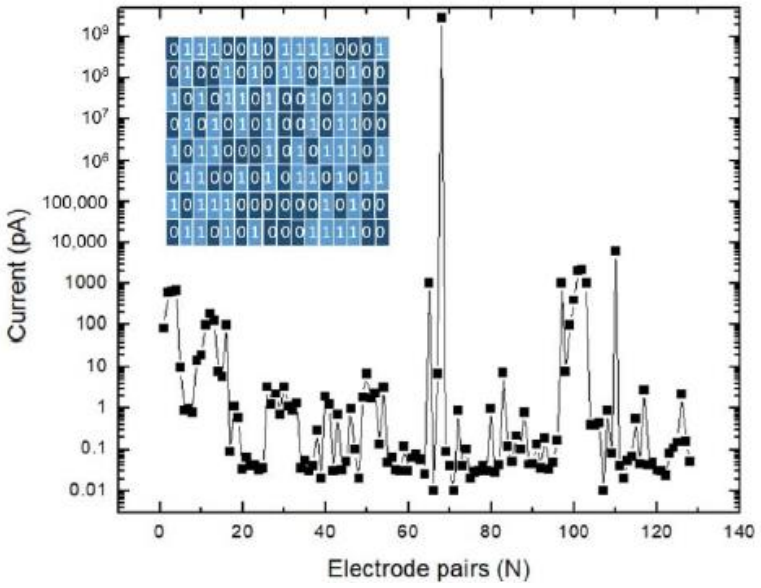


Figure 7: 128-bit Key Generation from current profile of gold-nonanedithiol network [5]

2.3 Rise of Nanomaterial based PUFs:

The use of nanomaterial-based Physical Unclonable Functions (PUFs) marks a significant evolution in the domain of security technologies, contrasting notably with their predecessors, including CMOS-based PUFs and other variants. This shift towards employing nanomaterials is driven by the need for more robust, scalable, and energy-efficient security mechanisms to meet the demands of modern applications, ranging from IoT devices to secure communications [6]. It also promotes the idea of miniaturization of devices and beyond.

Nanomaterial-based PUFs offer unparalleled advantages due to their inherent properties. For instance, the quantum effects and nanomaterials' unique electrical, chemical, and physical characteristics create more complex and unpredictable PUF responses, enhancing security against cloning and emulation attacks. It also helps to enhance the overall performance of electronic devices. Unlike CMOS-based PUFs, which rely on the macroscopic variability introduced during the manufacturing process, nanomaterial-based PUFs exploit the atomic or molecular scale irregularities, leading to a higher density of unique identifiers per unit area and, thus, a more compact and efficient design. Various applications of nano-PUFs are shown in Figure 8 below, resulting in their unique properties [7-9].

Moreover, nanomaterials open the door to novel PUF architectures by allowing for the integration of PUFs into a wider range of substrates and devices, including flexible and wearable electronics, where conventional CMOS technology may not be viable. This versatility underpins the growing preference for nanomaterial based PUFs in cutting-edge security applications, offering a promising avenue for future developments in authentication, anti-counterfeiting, and secure communications.

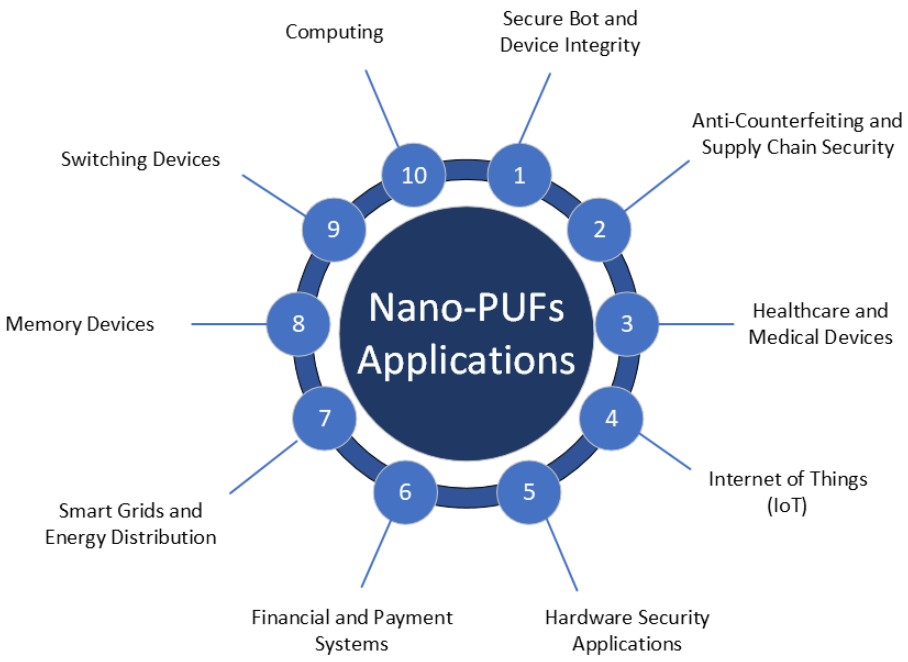


Figure 8: Nano-PUFs Applications [7].

Because of the unique and more robust characteristics of nano-PUFs, their application is widespread in almost every area. Nano-PUFs were fabricated using various manufacturing techniques and studied in past research. Distinct from the conventional PUFs that utilize manufacturing variances in silicon-based CMOS technologies, the nanotechnology-infused PUFs capitalize on more pronounced irregularities due to their nanoscale dimensions. These technological advances in nano-devices, including phase change memory (PCM), spin-transfer torque magnetic random-access memory (STT-MRAM), carbon-nanotube field-effect transistors (CNFETs), and memristors, not only pave the way for unique, intricate PUF configurations but also introduced pivotal attributes such as reconfigurability and multi-response capabilities showed in Figure 9 [7-11].

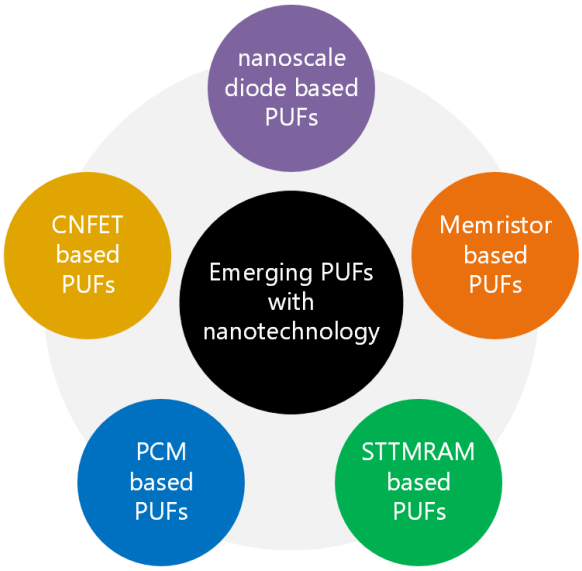


Figure 9: Emerging PUFs with Nanotechnology [11].

One such fascinating example of the emerging nanoPUFs is nanotube field Effect Transistors (CNFETs). CNFETs represent a novel category of transistors that overcome several limitations of traditional silicon MOSFETs by utilizing carbon nanotubes (CNTs) instead of silicon. This transition to CNTs has initiated considerable interest due to the potential for further technological scaling. The design of one such CNFET-(CNPUF-PE) is shown in Figure 10.

The CNPUF-PE is comprised of multiple carbon nanotube field-effect transistors (CNFETs) connected in parallel across power sources. Each CNFET has a variable threshold voltage due to inherent process variations, particularly pronounced at the nanoscale. These variations contribute to the uniqueness and unpredictability of the PUF response. With the CNFETs connected in parallel, the current through each transistor is affected by its threshold voltage and the applied voltage (V_{DD}).

Since these threshold voltages vary, the currents flowing through each CNFET (I_{top} through I_{bot}) also vary. These currents are then input into a comparator, a device that compares two or more currents or voltages and outputs a binary signal based on this comparison. In the context of a PUF, this binary output (R) forms part of the unique CRP of the PUF [11].

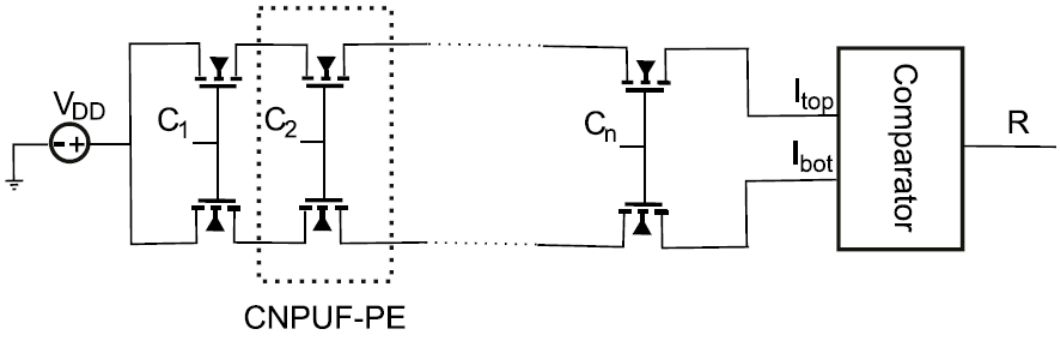


Figure 10: CNFET based PUF design [11].

The comparator might be designed to compare the top current (I_{top}) against the bottom current (I_{bot}) to produce a binary '1' or '0'. This unique combination of '1's and '0's across numerous CNPUF-PEs constitutes the PUF's unique identifier. These bits can be utilized for cryptographic purposes such as secure device authentication or key generation. However, it is essential that the CNFET manufacturing process is controlled to ensure that the variations in threshold voltage fall within a range that is detectable and reliable for PUF applications.

The primary disadvantage of Carbon-Nanotube Field-Effect Transistors (CNFETs) is the complexity of their fabrication. It is challenging to achieve precise control over carbon nanotubes' properties, such as chirality—which dictates whether they are metallic or semiconducting—and their diameter, alignment, and density. These factors lead to significant variability in CNFET performance. Additionally, the comparator in the design of CNFETs increases the area and power overhead of the device. The rigorous demands for

controlled assembly of CNTs increase manufacturing costs, area, power overhead, and complexity, potentially hindering the scalability of this technology for widespread nanoscale and economic applications.

Though Nano-PUFs offer significant benefits, they also face several challenges in traditional implementations. These include complex and expensive production processes that require precise material synthesis and nanoscale device fabrication. Scalability is also a problem, as moving from laboratory prototypes to widespread production without compromising performance and reliability is challenging. Each technology also has specific durability issues, such as resistance drift in PCM, magnetic stability in STT-MRAM, variability in CNFETs, and inconsistent memristor switching, affecting their long-term reliability and performance. Additionally, these devices are sensitive to environmental factors like temperature and radiation, which may hinder their functionality. While they are more energy-efficient than traditional technologies, their power consumption during certain operations is still a concern. Integrating these technologies with existing CMOS technology also presents challenges due to differing operational parameters and interfacing requirements. Although faster than traditional storage, they may be slower than volatile memories like DRAM or retain data and flash memory [7-11].

These limitations highlight the necessity for enhanced stability and security in PUF designs, which self-assembled nanoPUFs aim to address. This research advances self-assembled nanoPUFs due to their ability to achieve higher variability, scalability, cost-effectiveness, and stronger response patterns through the controlled assembly of nanostructures. This approach increases the unpredictability and security of PUFs, making them more resistant to cloning and predictive attacks.

2.4 Self-Assembled Nanostructures:

In scientific innovation, self-assembled nanostructures stand at the intersection of chemistry, physics, and materials science, emerging as microscopic entities that inherently arrange themselves from singular units into organized formations at the nanometer scale. This phenomenon of self-assembly results in the formation of nanoscale networks without external intervention through the self-organization of molecular constituents and nanoparticles. Such networks are intricately merged with nanoparticles—gold being a prime example—interlinked by organic molecules, including thiolate molecules, within particular solvents, driven by the synergy of chemical similarities and physical forces [1-5].

The utility of these nanoscale constructs extends across a broad spectrum of applications, from electronics and sensing technologies to medical diagnostics, attributed to their superior electrical, optical, and chemical characteristics. The self-assembly mechanism facilitates unparalleled precision in constructing the network architecture, laying the groundwork for creating sophisticated nanostructures destined for cutting-edge technological advancements.

At the forefront of scientific exploration, self-assembled nanostructures indicate a new era in the development of nanoelectronic devices. Originating from the meticulous assembly of molecules and nanoparticles, these formations exhibit unique electronic, optical, and mechanical properties. Such characteristics portray them as crucial across various applications, particularly in crafting highly efficient and secure nanoelectronic devices. The systematic organization of nanoscale components into functioning architectures via self-assembly presents a scalable, economically viable strategy for device manufacturing. This technique amplifies device performance and paves the way for innovative functionalities, which are pivotal for enhancing cybersecurity in today's digital landscape.

2.5 Hardware Encryption Using Self-Assembled Nanoelectronic Network

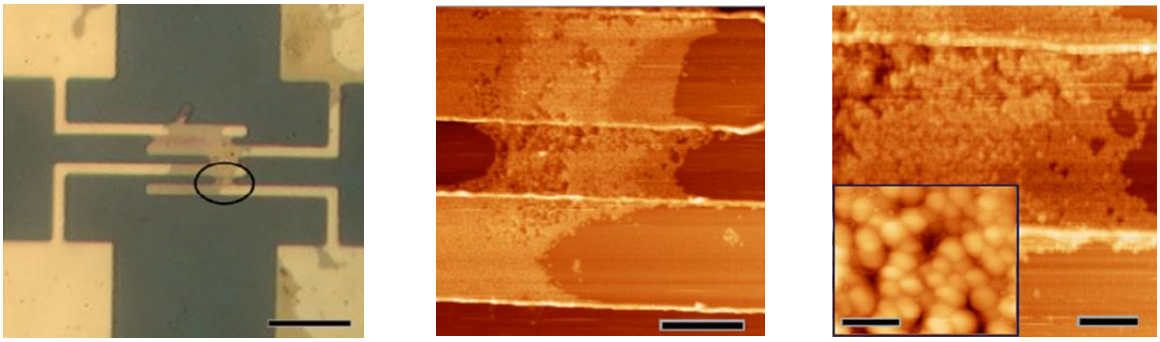
Research on self-assembled nanoscale networks, particularly those involving benzenedithiol–gold nanoparticle systems, showed great promise for hardware encryption and Physical Unclonable Functions (PUFs) creation. These networks possess Negative Differential Resistance (NDR) and hysteresis properties, essential for oscillators, amplifiers, and memory devices. Their inherent randomness and variability in the self-assembly process make them particularly valuable for developing unique, tamper-resistant cryptographic keys in hardware security [4].

A vital advantage of these networks is their ability to introduce high unpredictability in metal-molecular connections due to inherent mismatches and disorder. This unpredictability ensures the uniqueness of each network, making it nearly impossible to replicate or predict, thus significantly enhancing the security of cryptographic modules and PUFs. The resistance properties of these networks can be tuned by altering the molecule-to-nanoparticle ratios, allowing for the customization of electronic properties to meet specific security requirements, which provides flexibility and adaptability in security applications [1-5].

Moreover, the nonlinear electronic characteristics such as NDR and hysteresis, enabled by these self-assembled networks, are advantageous for developing more sophisticated encryption algorithms and security protocols [4]. These features allow the networks to function as passive security enhancers and active elements in dynamic encryption processes. The capacity to modify electronic properties through external stimuli, like electrical bias or light exposure, introduces an additional security layer, enabling real-time adjustments to cryptographic keys and security levels based on environmental or system changes. Overall, the distinctive combination of tunability, nonlinearity, and intrinsic variability makes self-assembled nanoscale networks especially suitable for advanced hardware security applications, heralding a new era of secure computing environments resistant to emerging threats.

2.6 Formation of PUFs from Self-Assembled Nanoelectronic Network:

Based on previous research, this study explains and uses the self-assembly process and formation of the PUFs. The self-assembly of gold nanoparticle-molecular networks using thiolated molecules, such as 1,6-hexanedithiol and benzenedithiol, proved to be a precise process where these molecules bind strongly to gold, enabling the formation of the network. The process of self-assembling gold nanoparticle-molecular networks involves a detailed method that leads to the preparation and organised interaction of citrate-stabilized gold nanoparticles and thiolated molecules, such as 1,4-benzenedithiol. Initially, ethanolic solutions of these molecules and colloidal gold are prepared separately, with the pH of the gold suspension being adjusted using dilute NaOH. These solutions are then mixed in equal volumes and incubated at 4°C for 24 hours, allowing the thiol groups to bind to the gold nanoparticles. This binding forms a self-assembled monolayer that connects the nanoparticles into a network [5].



(a) (b) (c)

Figure 11: Atomic Force Microscope Images of patterned gold electrodes with gold nanoparticles-benzenedithiol network.
(a) Optical microscope image of patterned gold electrodes after deposition of gold nanoparticle–benzenedithiol network from solution. (b) AFM image of encircled region in part (a) showing gold nanoparticle–benzenedithiol film bridging (c) Zoom-in AFM of networks [4].

The resulting network is deposited onto silicon wafer substrates equipped with patterned electrodes and is left to dry under ambient conditions. The electrical properties of the network are then characterized through precise I-V measurements, and its structure is

confirmed using Atomic Force Microscopy. Adjusting the molecule-to-nanoparticle ratio allows the network's density and connectivity to be tuned, providing tailored control over its electrical and physical properties for applications such as hardware encryption and physically unclonable functions (PUFs). The ratio Nmolecule: Nparticle (where Nmolecule is the number of dithiol molecules and Nparticle is the number of colloidal gold particles) was varied to control the concentration and arrangement of molecule-to-gold interconnections in the resulting networks. This adds another degree of freedom for hardware primitives by varying the ratio of colloidal gold particles and dithiol molecules, which significantly increases hardware security, making it impossible to replicate the physical self-assembled nanoelectronic network used for encryption [1-5].

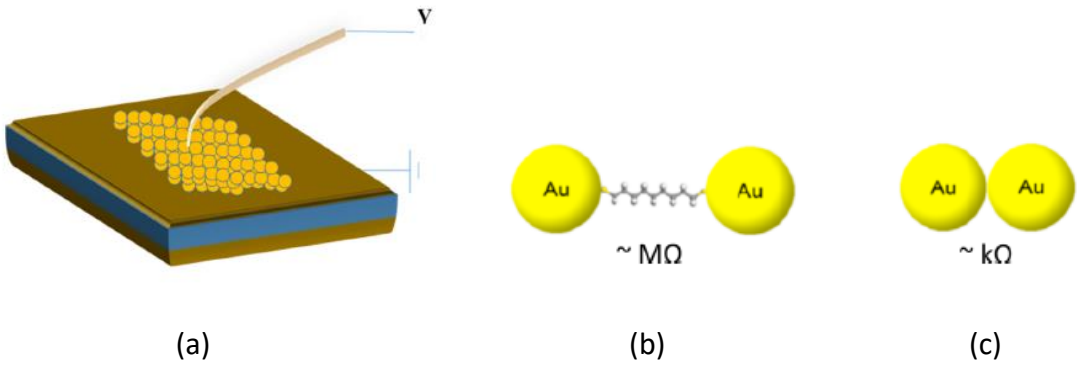


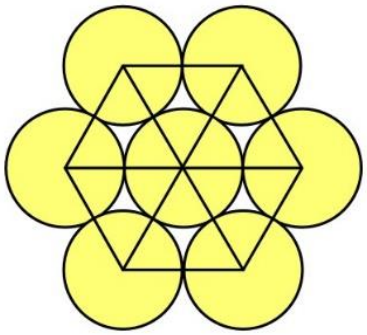
Figure 12: (a) Schematic of conducting-tip AFM measurement to measure conductive pathways. (b) Two Gold particle connections within the network bridged by molecule. (c) Gold-Gold direct connection [3].

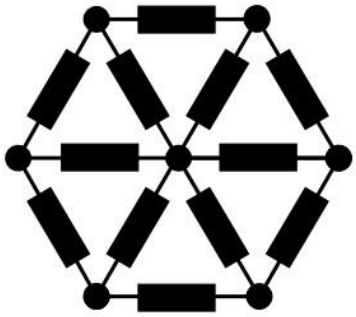
Atomic force microscopy (AFM) and optical microscopy are essential in visualizing these networks. AFM provides detailed images that illustrate dithiol molecules serving as connectors between gold nanoparticles, as shown in Figure 11 [5]. These visualizations confirmed the network's scale and arrangement and showed how changes in the molecule-to-nanoparticle ratio could influence network density and connectivity, thereby affecting electrical characteristics.

Additional evidence of network formation was provided by electrical measurements, such as two-terminal current-voltage (I-V) assessments, which confirm the different conductive paths within these networks and how they vary with the molecular structure and assembly ratios—with the help of the AFM images and proof of different current paths within the network pointed towards the presence of multiple particle and molecular connections within the self-assembled network. Hence, with further evidence, it was stated that the network consists of gold-molecule, gold-gold connections, and defects, which resulted in different conductive pathways and current values, Figure 12 [3].

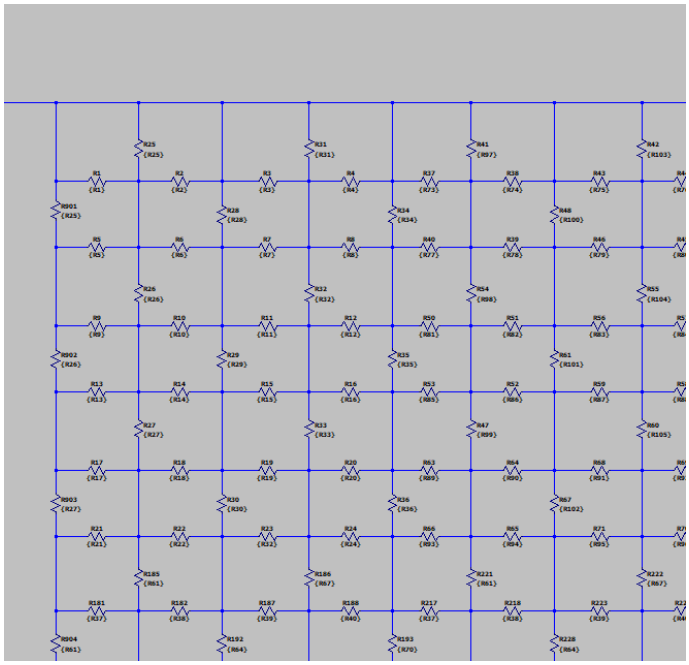
Conducting-tip AFM was used to probe the electrical conductivity specifically, differentiating between connections, gold-molecule versus gold-gold, highlighting variations in resistance associated with these connections. Defects noted in AFM analysis also reveal irregularities in the network that significantly affect electrical properties, leading to behaviors such as negative differential resistance (NDR) and hysteresis. These properties are crucial for molecular electronics applications [3-5].

The microscopic data through AFM confirmed the closed-packed lattice of each particle consisting of six nearest neighbors, which is converted into a lattice of resistors representing the metal-metal and metal-molecular electrical connections, as seen in Figure 13(b). This closed lattice resistor structure is then used to form building blocks in networks for simulation in LTSpice, Figure 13(c). This formation of self-assembly of gold nanoparticle-molecular networks using thiolated molecules and lattice arrangements from the AFM images was used as a reference to form the Mesh Network required for this study [3].





(a) (b)



(c)

s

Figure 13: (a) Molecular Network observed in AFM (Atomic Force Microscope [3]. (b) Formed Resistor Network at each closed-packed lattice of each particle. [3] (c) Network formed from amalgamating these resistor networks in LTSpice

3. Resistor-Blocks Mesh Networks and its Electrical Characteristics:

To find the electrical characteristics of the self-assembled nanostructures, the abstraction of particle networks is created and replicated with resistor networks. For the creation of the resistor network, all the molecular networks were considered for more accurate analysis of the network using LTSpice simulation software.

3.1 Creation of Resistor-Building Blocks and Mesh Networks

3.1.1 Designing Resistor-Building Blocks

Based on the molecular networks, the building blocks are formed. Past research stated that during the self-assembly of the metal-molecular structure, three different types of networks or bond connections are present in the self-assembled nanostructure. As the metal-molecular is the primary connection in the self-assembled nanostructures, the traces of metals-metal networks and defects during the self-assembly fabrication process were also found in the study. For analysis, the requirement for accumulating all three network connections into account is essential to accurately replicate the self-assembled nanoelectronic network formed by metal-molecular proportions to that of the resistor network. Each network connection, metal-metal, metal-molecule, and defect with its resistance can be used to create the resistor block for creating a Mesh Network.

As illustrated in Figure 13(b), the resistor electrical connections of a closed-packed lattice with six nearing neighbors and the building block with 36 resistors were formed, resembling mesh topology. From the study of previous research work on determining the electrical resistance value, the metal-metal (gold-gold nanoparticle) resistance was accepted to be the quantized value of 12907 Ohms. Similarly, the metal-molecular (gold nanoparticles-dithiol molecule) and defect resistance values were traced equal to 1M

Ohms and $1x10^{15}$ Ohms, respectively. For this study, the same values for resistance were used to form Mesh Networks from the blocks of resistors. These resistor blocks accumulating 36 resistors are called “building blocks,” which are used to form Mesh Networks, Figure 14 [3].

Under this study, the creation of the resistor block varied from the previous research to examine the electrical properties of the mesh network created differently. For this study, three building blocks were created instead of a singular resistor building block, each having 36 resistors. The resistors in these three building blocks were defined so that each building block has only one type of resistor value to all of its 36 resistors out of the three possible. The building blocks were named based on the resistor value that they comprise; “Low building block” with all 36 resistors having a value of 12907 Ohms; “Middle building block with all 36 resistors having a value that of metal-molecular connection, 1M Ohms; and at last, “High building block” with all 36 resistors values of 1x1015 Ohms as stated in Table 1. This study used These three building blocks to form Mesh Networks.

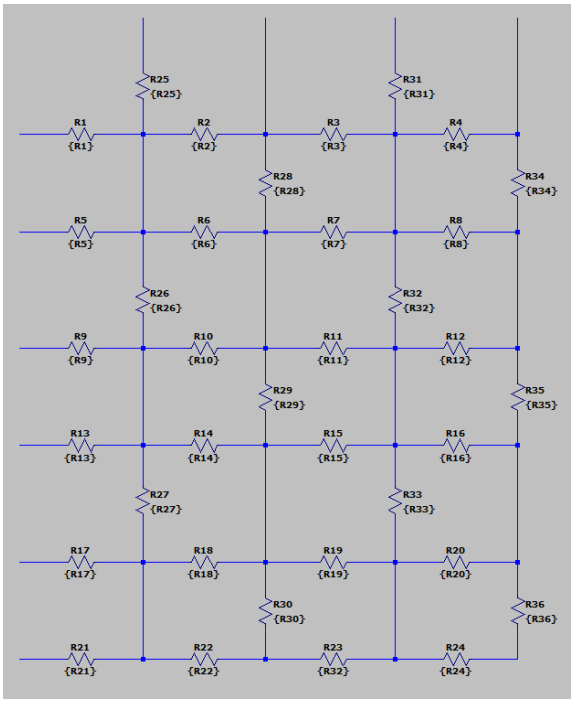


Figure 14: Basic Resistor Building Blocks example (shown High Building Block) in LTSpice

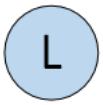
Building Block:	Resistor Values	Resistor No. Range	Number of Resistors	Denotation
Low Building Block	12907 Ohms	R72 : R108	36 Resistors	
Medium Building Block	1M Ohms	R37 : R72	36 Resistors	
High Building Block	$1x10^{15}$ Ohms	R1 : R36	36 Resistors	

Table 1: Resistor Building Blocks and their resistance values.

3.1.2 Formation of Mesh Networks

In previous research, the resistor-blocks Mesh Network was created using a standard building block consisting of 36 resistors. These building blocks were then used to populate the network to form the Mesh Network. The three values of the resistors were randomly assigned to the mesh network to observe the electrical properties of the network using various verification techniques [3,4].

In this project, three building blocks were used to form Mesh Networks. Three iterations of Mesh Networks were formed by randomly populating the three basic building blocks in a 5x5 network to form one iteration of a Mesh Network arranging building block from left to right direction from the voltage source. For simulation to analyze the electrical characteristics of the Mesh Networks, LTSpice simulation software was used to generate I-V graphs across resistors in each Mesh Networks to identify their properties and key differences which could be used to justify the previous research and

provide valuable insights. To generate the I-V graphs, a DC Voltage sweep was used across these Mesh Network resulting in the current values across the network.

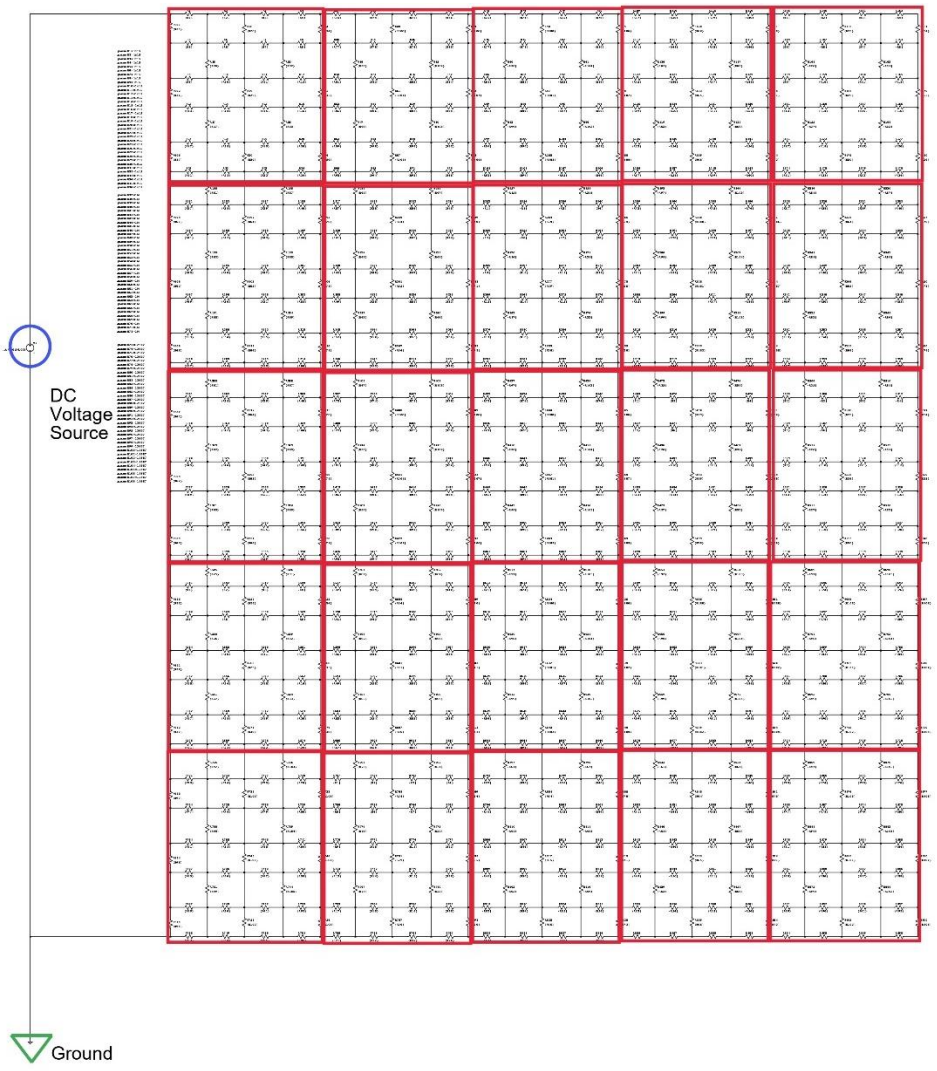
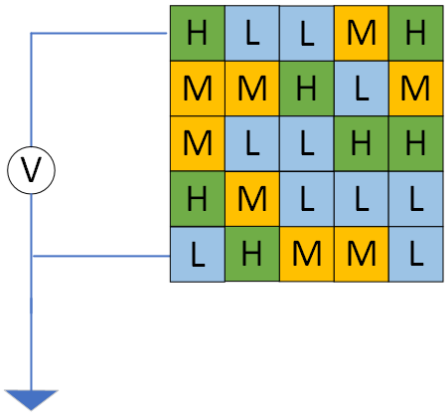


Figure 15: Mesh Network iteration constructed by randomly populating of three basic building blocks in 5x5 configuration with DC source.

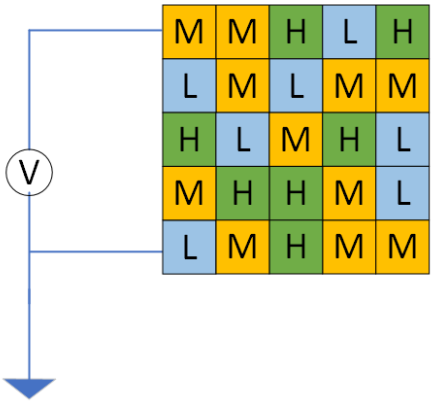
Figure 15 represents a Mesh Network iteration designed in LTSpice by randomly configuring the three basic building blocks in a 5x5 manner with a DC voltage source and ground. The rectangle outlined in the figures represents one of the three building blocks used in network construction. This same design process was used to construct all the Mesh Network iterations.

3.2 Resistor-Mesh Networks

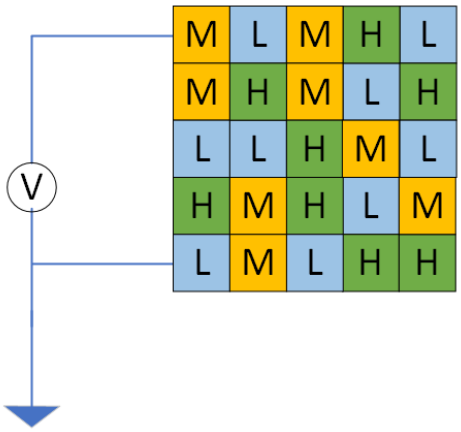
The study shows three iterations of Mesh Networks formed by random arrangements of the three building blocks (high, low, and medium) in such a way that it creates 5x5 Mesh Networks of building blocks. Below, Figures 16(a), 16(b), and 16(c) show three arrangements of each building block to form the three Mesh Network iterations in LTSpice, used for simulation and analysis of electrical characteristics in them.



(a)



(b)

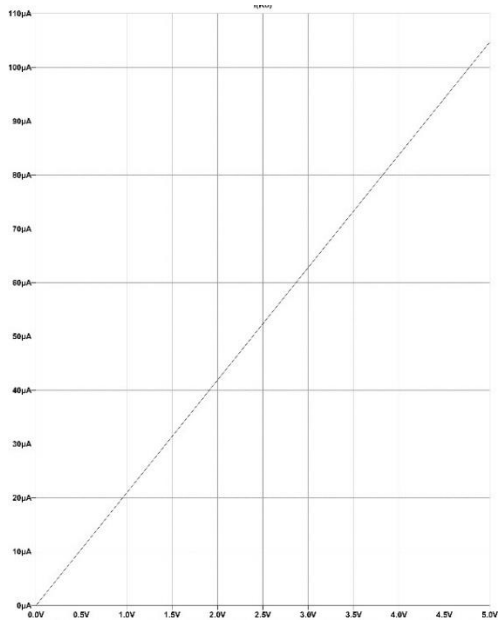


(c)

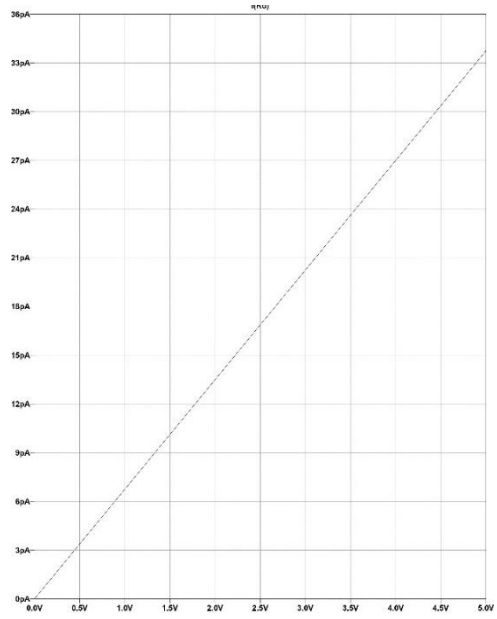
Figure 16: Arrangements of Building blocks in formation of (a) Mesh Network 1. (b) Mesh Network 2 (c) Mesh Network 3

I-V graphs for each of the overall mesh networks determined the resistive effects (linear characteristics) on the formation of Mesh Networks based on resistor-building blocks. The Mesh Networks were simulated and analyzed to understand the impact and key differences based on the arrangement and overall current values. A voltage source with DC sweep, which sweeps from 0 to 5V in LTSpice, was used for simulation.

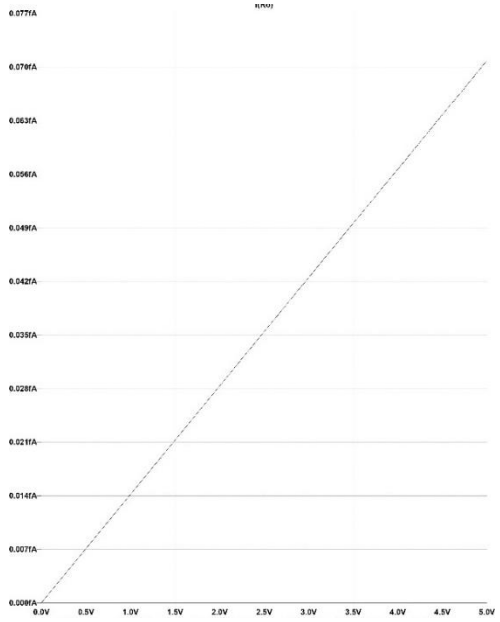
3.2.1 Simulation Results and Analysis of Mesh Network Iterations



(a)



(b)



(c)

Figure 17: LTSpice simulation result across (a) Mesh Network 1, (b) Mesh Network 2 and (c) Mesh Network 3

Figure 17(a) shows the simulation results for the overall current values of Mesh Network 1 across the resistor. Upon analyzing Figure 16(a) for building blocks used in Mesh Network 1, it is evident that Low Building Blocks were significantly populated in this Mesh Network. The large presence of low blocks indicated that the resistance between metal-metal connections was predominant in this network. The result is justified in the I-V graphs, as the overall current value across the network was higher than those of other networks. Hence, the current values increased linearly with the increase in metal-metal connections in the Mesh Network 1.

Similarly, the electrical characteristics of this network at various resistors resulted in a linear function to voltage. All the current values at each simulated resistor linearly increased with the increase in voltage from 0-5V. The over-current across the resistor was high in microamperes, verifying the influence of majorly populated Low Building Blocks in this network.

For the use of this Mesh Network in security applications, as the low resistance was dominating in the network, it created large low-resistance paths for current to flow easily through the network, resulting in easier current paths to flow in the network. Such networks can be used in applications where network speed and efficiency are important and of high importance rather than security.

Figure 17(b) shows the simulation overall results across Mesh Network 2. The Medium Building Blocks ruled Mesh Network 2 over other building blocks during random allocation on observing building block arrangement for this network in Figure 16(b). Hence, the metal-molecular connections and their resistance in the networks were more significant than others. As a result, the simulation of Mesh Network 2's current value was comparatively less than that of Mesh Network 1. The overall current value decreased as the increased metal-molecular network resistance across the network. Similar to Mesh Network 1, the I-V characteristics of Mesh Network 2 resulted in a linear pattern. The current value across all tested resistors in the network increased linearly with that of voltage from 0-5V.

As Mesh Network 2 was a balanced distribution of the building blocks, it was expected to yield a network with moderate resistance and less variability than the first iteration, which the simulation results proved. Hence, this configuration could be beneficial for security applications where a balance between robustness and predictability is desired.

The I-V graphs in Figure 17(c) show the current values across Mesh Network 3. Focusing on random building block arrangements for Mesh Network 3 using Figure 16(c), the High Building Block guides this network more than the other two building blocks. Hence, it was expected that the current values across the resistors of the overall network would be much lower compared to the other two Mesh Networks discussed previously. The presence of defect resistances is higher than that of other connection resistances, which results in a decrease in overall current value across this network compared to the other two networks, which was again evident from the simulation results.

This network distinctly showed the linear characteristics of the I-V graphs when applied across a DC voltage sweep from 0 to 5V, which leads to a linear increase in current values across the resistors with an increase in voltage.

As stated, the higher significance of the High Resistance block in this network was evident; the network was anticipated to exhibit high resistance and hence fewer overall current values, which makes it more suitable for applications where high security and resistance to tampering are paramount.

To find the influence of the neighbouring building blocks on current values, the current value simulated across resistors with the same resistance but surrounding different neighbouring blocks were inspected in all three iterations. The current values of resistors neighbouring adjacent High and Middle Building Blocks were found relatively lower than those across other resistors neighbouring Low Building Blocks in each network. Hence, the current values across any circuit resistor and the Mesh Network depend on the neighbouring building blocks and majorly populated building blocks.

3.2.2 Mesh Network Results Conclusion:

While comparing the electrical characteristics for each Mesh Network formed in LTSpice, it was found that each resistor-block network exhibits linear characteristics when applied across DC voltage sweep from 0-5V. The current values of each network across the resistor increase linearly with an increase in voltage applied across it. This aligns seamlessly with the previous research on the Mesh Network formed from self-assembly, where the Mesh Network was formed with just one building block and randomly assigned the three resistor values in the network. Hence, the results meet hands-in-hand with previous work using Mesh Network formed for hardware primitives from self-assembly, even with different approaches in methodology in their formation. [1-5]

The influence of neighbouring blocks on the current values across the resistor in the Mesh network can also be used as a degree of freedom along with the random arrangement of building blocks when using the network for security applications. A network with different electrical characteristics could be formed by changing the neighbouring blocks in the same network for the resistor of interest.

4. Diode Influenced Resistor-Mesh Networks and their Electrical Characteristics

In this study, diodes were integrated into previously established Mesh Networks as a novel parameter for characterization. Introducing diodes aims to result in a non-linear response within these networks, with identical diodes replacing resistors throughout. Two variations of the network were constructed to assess the impact of diodes on the network's electrical behavior. The two networks involved substituting diodes for 25% and 35% of the resistors, selected randomly within the existing Mesh Network formed previously. By examining the current-voltage (I-V) characteristics of these modified networks, the study aims to illustrate the effects of diode inclusion on the electrical properties of the Mesh Networks. To ensure the network's variability, diodes were randomly inserted in the forward and reverse directions in place of resistors, adding a layer of complexity and unpredictability to the study's findings.

By including diodes in different arrangements, we open the door to complex, customizable electronic systems that utilize these elements' blocking and conducting abilities. This strategy builds on previous research, introducing ways to control the flow of electricity in one direction and produce responses that change in non-linear ways. It emphasizes the value of being able to adjust and complicate electronic networks on a small scale, indicating a vital demand for the future of electronics at the molecular level. Furthermore, it highlights the opportunity to improve electronic hardware security by thoughtfully adding semiconductor components, building on, and extending the knowledge base of existing scientific theories.

4.1 Diode Characteristics

The diode used to replace the resistor in both newly designed Mesh Networks was selected based on its low power characteristics. For the design purpose in the network, the 1N4148 diode, which is available in LTSpice component libraries, was used. Table 2 below lists all the electrical characteristics of this diode, which was used to model and simulate the I-V characteristics of the resistor-diode network designed.

Diode Characteristics	**Definition**	**Value**
Is	Saturation current: the current that flows through the diode when it is reverse-biased	2.52 nA
Rs	Series resistance: the ohmic resistance of the diode	568 Ω
N	Emission coefficient: a dimensionless parameter that affects the forward voltage drop across the diode	1.752
Cjo	Junction capacitance: when the diode is reverse-biased	4 pF
M	Grading coefficient: a parameter that affects the voltage dependence of the junction capacitance	0.4
tt	Transit time: the average time it takes for a carrier to cross the junction	20 ns
Iave	Average current: the maximum current the diode can conduct continuously	200 mA
Vpk	Peak voltage: the maximum reverse voltage the diode can withstand without breaking down	75 V
mfg	Manufacturer of the diode	ON Semiconductor
type	The semiconductor material used in the diode	Silicon

Table 2: Diode Characteristics and their corresponding values.

4.2 Diode-Resistor Network with 25% and 35% Diodes

This section will discuss the electrical characteristics of Diode-Resistor Networks with diodes with characteristics as discussed above. Previously designed Mesh Network 3 was used to replace 25% of random resistors to design the Diode-Resistor network with 25% Diodes. The I-V graphs of this network were simulated in LTSpice to compare the influence of the diode in this network.

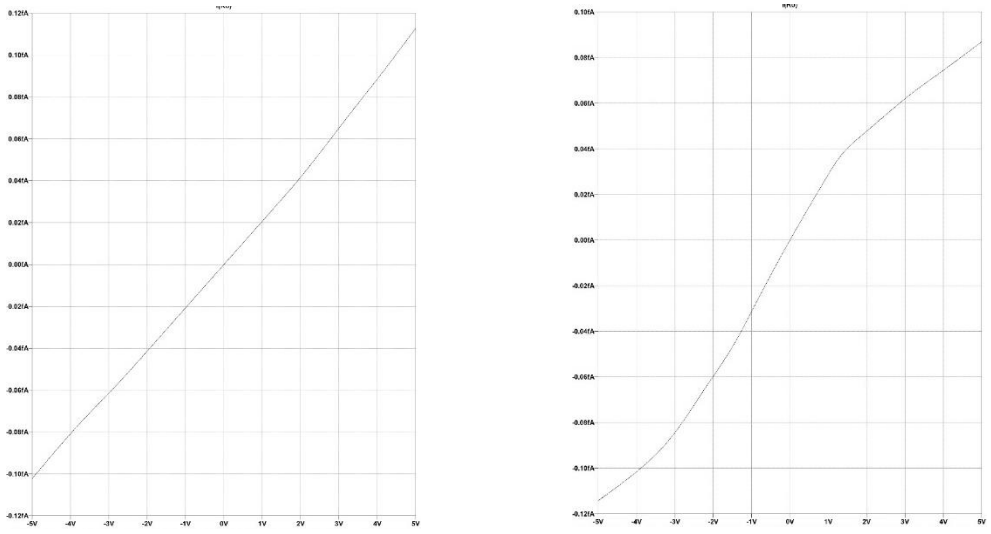
Moreover, to understand the relation of the current values to the proportion of the diode replaced in the network, another Mesh Network with 35% diode proportion was formed. Similar to 25% Diode Mesh Network, Resistor Mesh Network 3 was used to replace 35% of the diodes randomly used to replace resistors for this network design. This comparison helps to observe the electrical behavior of the networks with more diodes, noticing the effect of the increase in diodes on the network's performance and comparing it with linear resistor-building block networks previously discussed.

4.2.1 Simulations Results and Analysis Across Diodes-Resistor Networks

Figure 18(a) highlights the examination of I-V characteristics across the diode-resistor network, which has a 25% diode proportion. Diodes constitute 25% of the network components.

The resulting I-V graph across the network linearly increased under a voltage range from -5V to 2V. Beyond that window, the current rapidly increases with the increase in voltage. Introducing diodes enhances the network's non-linear characteristics, affecting the current flow across resistors after a certain voltage threshold. The linearity of the network still exceeds the non-linear components because of the smaller proportion of diodes in the network. A similar pattern was observed in I-V graphs of diodes and resistors simulated across the network. The current values resulted in a linear graph under the same fixed voltage range and shot off beyond the region.

The overall current value across the network was significantly low compared to all the other networks designed for simulation. This diode-resistor network, which has 25% diode, was designed from Mesh Network 3, which consists of most High building blocks. Additionally, with the diode replacement in the network, the resistance of the overall network resulted in a lower value of the overall current.



(a) *(b)*

Figure 18: LTSpice simulation results across (a) 25% Diode-Resistor Mesh Network
(b) 35% Diode-Resistor Mesh Network

With a smaller increase in the proportion of the diode addition to form a 35% diode-resistor Mesh Network by substituting more resistors from existing 25% diode-resistor Mesh Network, the non-linear characteristics became more distinct. The I-V graph across the network of 35% diode-resistor network in Figure 18(b), simulated through DC voltage sweep from -5V to +5V supported the increase in non-linearity. Unlike the previous 25% diode network showing linearity throughout the majority of the voltage across the network, this network resulted in a linear increase pattern through a certain voltage band, from -1V to +1V. Beyond this voltage range, the non-linear characteristics because of the increase in diodes resulted in a small increasing curve with an increase in voltage. The

increased directional property of the diodes also affected the current value across the network, which is evident from the uneven rate of increase in either polarity of voltage beyond the linearity range.

4.2.2 Comparing Resistor Mesh Networks and Diode-Resistor Mesh Networks

In this research, the electrical characteristics of five distinct Mesh Networks were explored through the simulation of I-V graphs in LTSpice. Initially, when comparing networks formed primarily from resistor building blocks, it was observed that the current response across the resistors to DC voltage remains linear across these configurations. The differences in current values among these resistor-based networks reflected the predominant building block forming the network and the adjacent blocks, which played a crucial role in modulating current values.

The anticipated deviation from linearity due to diode incorporation was validated upon examining networks that integrate diodes with resistors. For the network with a lower diode content (25%), there was a noticeable linear current behavior within a specific voltage range across the network, attributed to most components being linear (i.e., resistors). Outside this voltage domain, a sharp increase in current was noted, emphasizing the influence of the non-linear diodes and the spatial arrangement of the components. A slight increase in the proportion of the diodes resulted in a significant increase in the nonlinearity of the network. However, the small linear current value across the 35% diode network was found within a small voltage window. The nonlinear characteristics within the network were evident from the major non-linear curves beyond the small linear voltage range. Hence, the results for all the networks justify the previous research in this field but with different methodologies, giving a broader understanding of the electrical properties of the networks [3-5].

Type of Mesh Network and iteration:	Majorly influenced building block	Current Value at -3V	Current Value at 3V	Current Value at 5V
Resistor Mesh Network 1	Low Building Block	-	≈ +15 µA	≈ +25 µA
Resistor Mesh Network 2	Middle Building Block	-	≈ +150 nA	≈ +255 nA
Resistor Mesh Network 3	High Building Block	-	≈ +0.042 fA	≈ +0.070 fA
25% Diode-Resistor Mesh Network	High Building Block	≈ -0.18 fA	≈ +0.18 fA	≈ +0.33 fA
35% Diode-Resistor Mesh Network	High Building Block	≈ -0.32 fA	≈ +0.27 fA	≈ +0.45 fA

Table 3: Comparing Resistor and Diode-Resistor Mesh Networks overall current values at selected voltage.

5. Conclusion and Future Scope:

The study outlined the formation and analysis of Mesh Networks using resistor-based building blocks and integrated diodes to simulate the electrical properties of self-assembled nanoelectronic networks. The simulation results of these Mesh Networks using LTSpice proved the linear current flow for resistor-block Mesh Networks. This provides easy scalability of PUFs formed using this approach by merely changing the arrangement of building blocks and rearranging a few neighbouring blocks, resulting in a new PUF with a unique CRP. Through organized simulation, the study revealed that the proportionate replacement of resistors with diodes, representing directional current flow and non-linear responses, introduces a new degree of freedom for tunability in the electrical properties of nanoscale networks.

Examining the effects of varying the proportion of diodes within these networks highlighted the potential for creating complex, tunable electronic systems that influence both resistive (linear) and complex non-linear properties of components for enhanced security and performance. This work underlines the capability of using these tunable networks to develop robust hardware encryption keys and physically unclonable functions (PUFs), which are cost-effective, easily scalable, and advanced, paving the way for secure communication technologies.

For future advancements, this research opens various opportunities for scalability of the proposed Mesh Network models while exploring their applications and results in different nanoelectronic configurations and environments to verify their physical security. Progress could be made by deriving the encryption keys using the current values across fixed component pairs (electrodes). The encryption keys can be derived using the Hamming inter and intra distance [5]. This study can be elaborated to find each network's characteristics and resulting CRP acting as a PUF and its application in hardware security [11]. Observed from the study and faced challenges, the clear indication for the requirement of more sophisticated simulation models that can capture the dynamic

complexity of the components and their inter-relations within these networks, including quantum effects and other nanoscale phenomena, more accurately.

Figure 19 shows a method for generating binary keys from the I-V characteristic curve of a nonlinear Mesh Network, applicable in designing Physical Unclonable Functions (PUFs). The methodology determines resistance vaules at selected voltages in I-V graphs comparing it with certain threshold resistances. If the measured resistance exceeds threshold, it is assigned a binary '1', otherwise a '0'. This results in each threshold resistance creating a unique 8-bit key that reflects the nonlinear curve at that specific threshold.

This process enables the generation of multiple binary keys from a single I-V curve simply by adjusting the resistance thresholds. Each key can act as a distinct identifier or encryption key in hardware security applications, offering a flexible and scalable method to boost security. The use of various resistance thresholds provides additional customization for the PUF generation, accommodating specific security needs.

Figure 19: Three 8bit keys sampled from non-linear I-V graph across the Mesh Network

Furthermore, advancing towards quantum modeling could provide deeper insights into electron transport mechanisms and simulations at the nanoscale level, potentially transforming our methods in cybersecurity and hardware encryption. These developments could facilitate the practical use of nanoscale devices in daily technology, improving their efficiency and security. Another aspect to further investigate would be

time delay observed while simulating I-V curves for different proportion of linear and non-linear Mesh Networks. Research into the timing characteristics of Mesh Networks would provide valuable insights into the interactions between components and the transmission of signals through resistor and diode configurations, which are essential for both network performance and stability.

Further research on nanoelectronic networks for hardware security could be done focusing on integration and strategic configuration of nonlinear elements such as diodes, in addition with other multi-terminal devices. These studies can particularly emphasize on the optimal placement, arrangement, and orientation of these components within the networks to improve unpredictability and resistance against security threats. Additionally, varying the ratios of these nonlinear elements in relation to other network components can be considered as a critical area of research. This can be explored through experimental testing and advanced simulations to refine the network's electrical characteristics and response, aiming to optimize security outcomes in physically unclonable functions (PUFs) and other cryptographic applications.

In conclusion, while this study has established a solid foundation for understanding and applying metal-molecular networks in hardware security, it represents just the beginning. The future involves enhancing these models and merging them with new technologies, ensuring that the security and efficiency of nanoelectronic networks advance alongside the swift progress of digital and communication technologies. This ongoing journey of exploration and innovation holds the promise of exciting breakthroughs in nanotechnology and cybersecurity.

6. Bibliography

[1] Venkataraman, E. V. Amadi and C. Papadopoulos, "Hardware security using self-assembled nanoelectronic networks," *Small,* 2021.

[2] A. Venkataraman, E. V. Amadi and C. Papadopoulos, "Nanoscale self-assembly : concepts, applications, and challenges," *IOP Publishing,* 2021.

[3] P. Zhang, A. Venkataraman, and C. Papadopoulos, "Self-assembled gold nanoparticle–molecular electronic networks," *physica status solidi (b),* vol. 254, p. 1700061, 2017.

[4] T. Zhang, D. Guérin, F. Alibart, D. Vuillaume, K. Lmimouni, S. Lenfant, A. Yassin, M. Oçafrain, P. Blanchard and J. Roncali, "Negative Differential Resistance, Memory, and Reconfigurable Logic Functions Based on Monolayer Devices Derived from Gold Nanoparticles Functionalized with Electropolymerizable TEDOT Units," *The Journal of Physical Chemistry C,* vol. 121, pp. 10131-10139, 2017.

[5] Anusha Venkataraman , Eberechukwu Amadi and Chris Papadopoulos, “Molecular-Scale Hardware Encryption Using Tunable Self-Assembled Nanoelectronic Networks,” *Micro* 2022, 2, 361–368.

[6] Alireza Shamsoshoara, Ashwija Korenda, Fatemeh Afghah, Sherali Zeadally, “A survey on physical unclonable function (PUF)-based security solutions for Internet of Things,” *Computer Networks* 183 (2020) 107593

[7] Kusum Lata 1 and Linga Reddy Cenkeramaddi, “FPGA-Based PUF Designs: A Comprehensive Review and Comparative Analysis” *Cryptography* 2023, 7, 55

[8] Shital Joshi, Saraju P. Mohanty, and Elias Kougianos, “Everything You Wanted To Know About PUFs “ *IEEE Potentials · November* 2017

[9] Amadi, E.V.; Venkataraman, A.; Zaborniak, T.; Papadopoulos, C., “Nanoelectronic circuit elements based on nanoscale metal–molecular networks*.” J. Comput. Electron.* 2021, 21, 319–333.

[10] LuckyStep48/Alamy Stock Vector, “Fighting counterfeiting at the nanoscale,” *Nature Nanotechnology* | VOL 14 | JUNE 2019 | 497.

[11] Yansong Gao, Damith C. Ranasinghe, Said F. Al-Sarawi, Omid Kavehei, And Derek Abbott, “Emerging Physical Unclonable Functions With Nanotechnology,” *IEEE Access Volume* 4, 2016

[12] A. Maiti, I. Kim, and P. Schaumont, “A robust physical unclonable function with enhanced challenge-response set," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 333_345, Feb. 2012

[13] Adrian M. Ionescu, “Nanotechnology and Global Security,” *Connections QJ* 15, no. 2 (2016): 31-47

[14] Kim, J.H., Jeon, S., In, J.H. *et al.* “Nanoscale physical unclonable function labels based on block copolymer self-assembly.,” *Nat Electron* 5, 433–442 (2022).