VIA PUF Technology for Authentication and Key Exchange

Project-I (EC47003) report submitted to

Indian Institute of Technology Kharagpur

in partial fulfilment for the award of the degree of

Bachelor of Technology

in

Electronics and Electrical Communication Engineering

by

Posina Venkata Sai Nagesh

(20EC39023)

Under the supervision of

Prof. Indrajit Chakrabarti

Department of Electronics and Electrical Communication Engineering

Indian Institute of Technology Kharagpur

Autumn Semester, 2023-24

November 25, 2023

DECLARATION

I certify that

(a) The work contained in this report has been done by me under the guidance of my supervisor.

(b) The work has not been submitted to any other Institute for any degree or diploma.

(c) I have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.

(d) Whenever I have used materials (data, theoretical analysis, figures, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references. Further, I have taken permission from the copyright owners of the sources, whenever necessary.

Date: November 25, 2023 (Posina Venkata Sai Nagesh)
Place: Kharagpur (20EC39023)

DEPARTMENT OF ELECTRONICS AND ELECTRICAL COMMUNICATION ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

KHARAGPUR - 721302, INDIA

CERTIFICATE

This is to certify that the project report entitled "**VIA PUF Technology for Authentication and Key Exchange**" submitted by **Posina Venkata Sai Nagesh** (Roll No. 20EC39023) to Indian Institute of Technology Kharagpur towards partial fulfilment of requirements for the award of degree of Bachelor of Technology in Electronics and Electrical Communication Engineering is a record of bonafide work carried out by him under my supervision and guidance during Autumn Semester, 2023-24.

Date: November 25, 2023

Place: Kharagpur

Prof. Indrajit Chakrabarti
Department of Electronics and Electrical
Communication Engineering
Indian Institute of Technology Kharagpur
Kharagpur - 721302, India

Abstract

Name of the student: **Posina Venkata Sai Nagesh** Roll No: **20EC39023**

Degree for which submitted: **Bachelor of Technology**

Department: **Department of Electronics and Electrical Communication Engineering**

Thesis title: **VIA PUF Technology for Authentication and Key Exchange**

Thesis supervisor: **Prof. Indrajit Chakrabarti**

Month and year of thesis submission: **November 25, 2023**

Authentication is crucial for security, involving identity verification and cryptographic key establishment. Physical Unclonable Functions (PUFs) provide cost-effective and secure authentication through advanced hardware technology. The VIA PUF utilizes a distinctive method based on contact formation probability. By leveraging the stochastic nature of contact formation between metal and silicon in the chip's interconnect layer, the VIA PUF ensures reliability through intentional design choices. As we are measuring parasitic resistances of the circuit, VIA PUF is resilient to environmental variations. That leads in completely eradicating the error correction codes. Additionally, a novel application of via PUF technology is proposed by building a secure and mutually agreed key exchange protocol that enhances security within a IoT network. The VIA PUF is implemented and examined with the help of Cadence virtuoso tool using 180nm technology.

Keywords - VIA PUF, authentication, key exchange, IoT devices, parasitic resistance, Error Correction codes (ECC), Cadence virtuoso

Acknowledgements

I wish to express my heartfelt gratitude to my thesis advisor, Prof. Indrajit Chakrabarti, whose unwavering support and guidance have been instrumental in my reasearch. Professor Indrajit's expertise, mentorship, and willingness to engage in constructive discussions have greatly enriched my academic journey. His open door policy and willingness to offer guidance and insights, while still allowing me the autonomy to explore and learn independently have been invaluable. I would also like to extend my deepest appreciation for my mentor Sivappriya Manivannan. She was with me the whole time and provided constant and effective mentorship. She helped me debug my mistakes and make steady progress. I would also like to express my heartfelt gratitude to my parents for their constant support and encouragement throughout my years of education, as well as during the rigorous process of conducting research and writing this thesis.

Contents

Chapter 1

Introduction

1.1 Background

Authentication is the process of verifying the identity of a user, system, or device. It ensures that the entity claiming an identity is legitimate and authorized to access the requested resources. Authentication acts as a primary defense mechanism against cyberattacks, reducing the risk of data breaches and identity theft. Presently, a common strategy involves storing cryptographic keys in non-volatile memory (like SRAM or EEPROM) and utilizing hardware cryptographic methods for encryption. However, this approach necessitates a substantial circuit area, is vulnerable to physical attacks leading to key extraction from memory, and is notably cost-prohibitive, making it impractical for deployment in low-cost devices.

An illustration of low-cost devices nowadays includes the Internet of Things (IoT) devices, which, in contemporary times, is susceptible to various security threats owing to vulnerabilities in the adopted authentication protocols. Ensuring a secure key exchange protocol among IoT devices is imperative, given their interconnected nature through the internet. This is crucial to establish a robust foundation for communication, safeguarding against unauthorized access and potential security breaches. Given the limited circuitry of many of the IoT devices, an effective solution demands a cost-effective and space-efficient approach.

1.2 Problem Statement and Research Question

The demand for affordable yet secure authentication solutions is on the rise. Ideal authentication circuits should occupy minimal space, be tamper-resistant, and exhibit low power consumption. Physically Unclonable Functions (PUFs) offer a promising solution, as they provide a primitive means of key storage without relying on volatile memory. PUFs generate a key on demand, leveraging the inherent physical characteristics of the circuit. Extracting the key from a PUF circuit without altering its physical properties is challenging.

This project specifically investigates a type of PUF known as VIA PUF or CONTACT PUF, which relies on contact formation probability. The contact occurs within the interconnecting layer between silicon and metal. Within a specific range of contact hole sizes, this process becomes stochastic, and the resulting randomness is utilized to generate the PUF output. The project delves into assessing the reliability and randomness of the PUF, along with the challenges encountered during its integration into device circuitry.

1.3 Objectives and Challenges

The project's goal is to design PUF circuitry and integrate it into device circuits. To achieve this, certain challenges must be addressed. First and foremost, the reliability of the PUF circuit is crucial. It should consistently produce the same output under varying environmental conditions, remaining unaffected by changes in temperature, pressure, or voltage fluctuations. Each PUF bitcell, responsible for a single-bit output, must be individually reliable.

Another key criterion for an effective PUF is its randomness. The output should be unpredictable and exhibit true randomness. The project specifically aims to design a via PUF circuit that fulfills both criteria of reliability and randomness. Determining the optimal number and range of contact hole sizes poses a challenge to ensure the randomness of the PUF output. Additionally, addressing the issue of unreliable bitcells, referred to as resistive contacts, is essential.

Once these challenges are overcome, the next task involves embedding these bitcells into logic gates within the device circuitry. This integration must be carefully executed to counteract potential reverse engineering attempts, enhancing the overall security of the PUF technology within the device.

1.4 Literature Review

What are Physically Unclonable Functions? [1]
As the name suggests a PUF is device whose design is hard to replicate physically. Therefore it is termed as the fingerprint of the device. PUFs are often based on the unique physical variations that occur during design and fabrication of chip. Since these variations are stochastic and hard to predict, it is not possible to clone a PUF that produces the same input-output response. There are many papers that discuss the different implementations of PUFs and their robustness. The papers I referred to while working on the project are decribed below.

Physically Unclonable Functions and Applications: A Tutorial [2]
This paper discusses the use of PUFs for low cost authentication and key generation purposes. A PUF is identified by its input output relationship known as challenge response pairs.

Based on the number of unique challenge response pairs possible the PUFs are classified as weak PUFs or strong PUFs. A weak PUF with limited number of challenge response pairs is used in the key derivation process.[9] The output of the PUF is used as key to encrypt/decrypt data on the device. A strong PUF can produce a large number of CRPs. So a strong PUF is directly authenticated based on these pairs without any need of additional cryptographic circuitry.[10]

The paper explores the deployment of various PUF implementations, each relying on the physical variations of active devices within a circuit. These implementations include Arbiter PUF[7], Optical PUF, SRAM PUF, and Ring Oscillator PUF. Although all these implementations generate challenge-response pairs based on the same principle, they differ in the underlying physical variations or electrical characteristics they leverage for output generation.

Ensuring the consistency of PUF output under diverse environmental conditions is crucial, and any deviation from the expected output is termed as the bit error rate. To enhance PUF reliability, one viable approach involves the use of error correction codes such as BCH, which can effectively increase the overall reliability of a PUF system.

A Physically Unclonable Function Based on Contact Formation Probability [3]

This paper introduces a novel PUF variant termed the contact PUF, diverging from previous implementations that heavily depend on environmental conditions. Unlike conventional PUFs, which are influenced by the temperature coefficients of MOSFET electrical characteristics, the contact PUF presents a distinctive approach.

In the contact PUF principle, the focus is on the formation of contacts between metal and silicon during the fabrication process. After depositing a dielectric material on the silicon substrate, a contact hole is created. In standard design processes, a minimum size for the contact hole is set to ensure formation. However, introducing uncertainty by drawing the contact hole smaller than the design rule allows exploits stochasticity to generate the PUF output.

A notable advantage of the contact PUF lies in its inherent stability. Once the contact is established, it remains unaffected by voltage fluctuations and environmental conditions. Consequently, this type of PUF demonstrates high reliability and obviates the need for post-processing error correction codes.

Yet, another critical property a PUF must satisfy is randomness. Although contact formation exhibits stochastic behavior within a specific size range, it falls short of achieving true randomness. Ideally, the contact formation probability should hover around 50% to ensure genuine randomness. Given the challenge of determining the size at which the process achieves randomness, and the inherent variability across cells, an alternative method is employed. This involves combining the outputs of multiple PUF bitcells through XOR operations. To enhance the randomness further, repeated XORing is conducted after the initial stage, acknowledging that the XORing operation alone may not be completely random. The uniqueness of these combined outputs is gauged by the interchip Hamming distance, providing a robust measure of their distinctiveness.

Research gaps

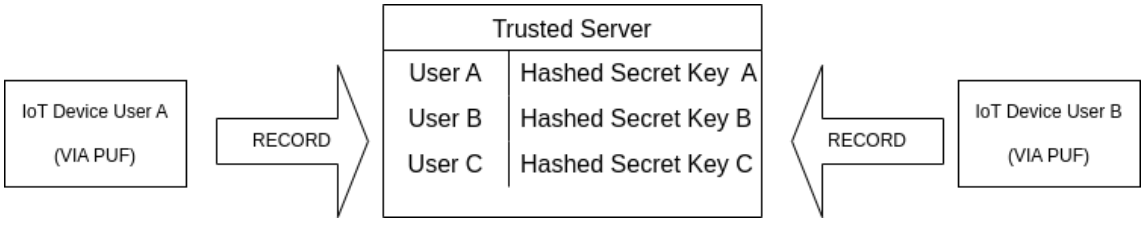
While many papers focus solely on PUF implementation, our project distinguishes itself by aiming to not only implement various PUFs but also design robust authentication protocols based on these implementations. Moreover, the crucial aspect of embedding PUF circuits into IoT device circuits is addressed. Additionally, the project seeks to leverage parasitic resistances as an entropy source, enhancing the reliability of PUF bitcells.

Chapter 2

Methodology and Preliminary Results

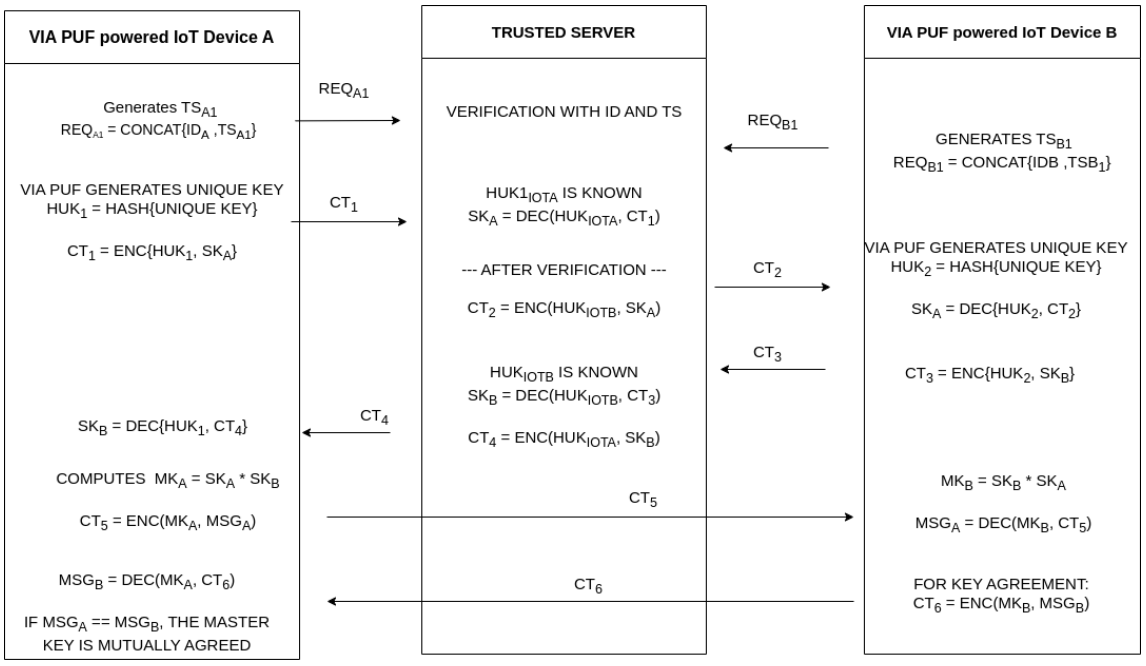
2.1 Secure and Mutually Agreed Key Exchange Protocol

2.1.1 Enrollment phase



The PUF enrollment is a standard, one-time (prior to deployment) and secure phase with no opportunity to "spy" for an adversary. Each user or the IoT device is registered to the server. The server stores the mapping of user to key generated by VIA PUF. Then the IoT device embedded with PUF is given to the client.

2.1.2 Key exchange protocol



Terminology

TS:Time-stamp , **REQ**:Request , **ID**:Unique ID of Device , **CT**:Cipher Text , **HUK**:Hashed Unique Key , **SK**:Secret Key , **MK**:Master Key , **ENC**:Encrypting operation , **DEC**:Decrypting operation , **MSG**:Message

Upon user registration with the server, communication between users is facilitated. The process begins with an IoT device sending a request that includes its unique ID and timestamp. The server, upon receiving the request, verifies the user's identity and acknowledges it. Subsequently, the secret key is encrypted using the hashed key generated by the VIA PUF and transmitted securely to a trusted server. The server, possessing the hashed key from the enrollment phase, decrypts the ciphertext. Then, the server encrypts the secret key of user A using the unique key of IoT device B and transmits it back to B. IoT device B decrypts the ciphertext and retrieves the secret key of user A.

This key exchange process is reciprocated, with IoT device B sharing its key with user A. Once the keys are exchanged, IoT device A combines its key with the key generated by B, creating a master key. Messages are then encrypted with this master key and directly sent from A to B. Similarly, IoT device B derives a master key using

the shared secret keys and decrypts the ciphertext to retrieve the message. The message is then encrypted with the master key of B and transmitted as ciphertext to A. IoT device A decrypts the message using its own master key. If the transmitted and received messages match, the mutual agreement of the master key is established.

2.2 Reliability of the VIA PUF

We have seen that the reliability of a PUF is compromised in the presence of the active components. To address the issue one solution discussed is a PUF based on the contact formation probability. A new solution proposed is to use parasitic resistance as the entropy source for the PUF. The below circuit shows a basic contact PUF bitcell.

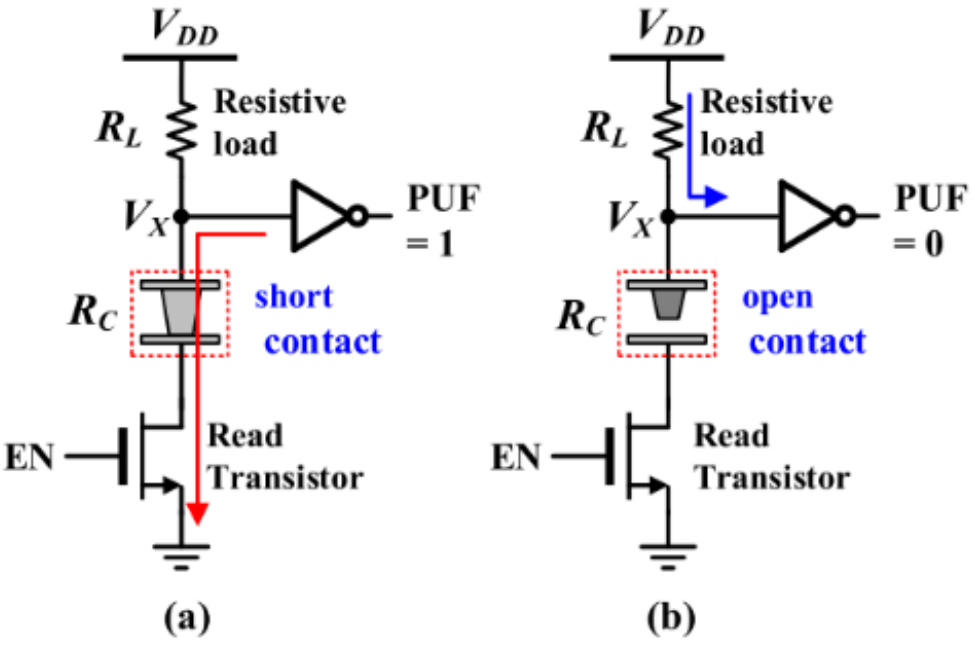


FIGURE 2.1: Basic contact PUF bitcell operation for (a) short and (b) open contacts[3]

In addition to the classification of contacts as open or short, there exists another category known as resistive contacts. These occur when the connection between the metal and silicon is only marginal. In such cases, it is possible to analyze the

circuit by representing the contact as a resistor with a designated value, denoted as Rc. However, resistive contacts are deemed unreliable due to their output variability under different environmental conditions.

In addressing this issue, the circuit can be effectively modeled as a voltage divider. Instead of utilizing contact holes, the parasitic resistance of the circuit can be conceptualized as contact resistance. When the parasitic resistance is sufficiently high, the voltage at Vx increases, resulting in an output of 0, akin to an open contact. Conversely, a low parasitic resistance leads to the opposite outcome. Achieving this requires adjusting the value of the load resistance accordingly. For a resistive contact, the output voltage of the inverter falls within the undefined region, neither reaching logic high nor logic low. It is crucial to ensure that the parasitic resistance remains outside the range associated with resistive contacts for optimal performance.

2.2.1 Simulation and Results

The tool is used to run design the circuit and perform the simulation is Cadence virtuoso in 180nm technology. The aim of the simulation is to observe how the PUF bitcell response varies with the parasitic resistance. To do this we have taken a resistance value Ro connected in place of parasitic resistance and DC Analysis is performed.

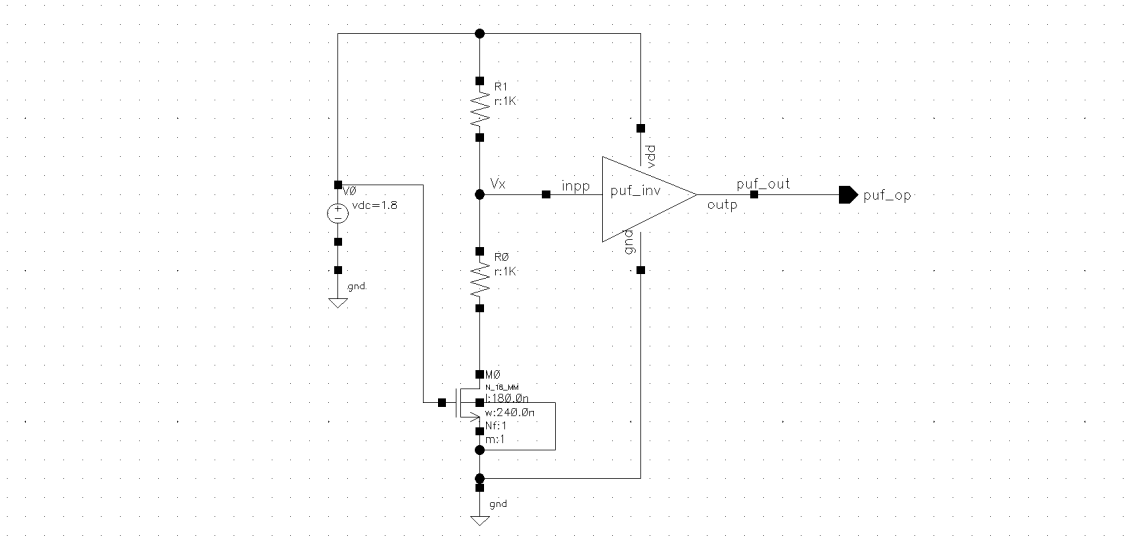


FIGURE 2.2: PUF BITCELL Circuit

In the above circuit the value of Ro i.e., contact resistance is varied. Ro is set as the sweep value in DC Analysis. The PUF output for each of the contact resistance is plotted. Other specifications of the circuit are -
VDD = 1.8V, **RL** = $1K\Omega$, **NMOS** : l = 180nm, w = 240nm.

The values of resistance Ro are varied between $Ro = 1\Omega$ to $Ro = 1000k\Omega$.

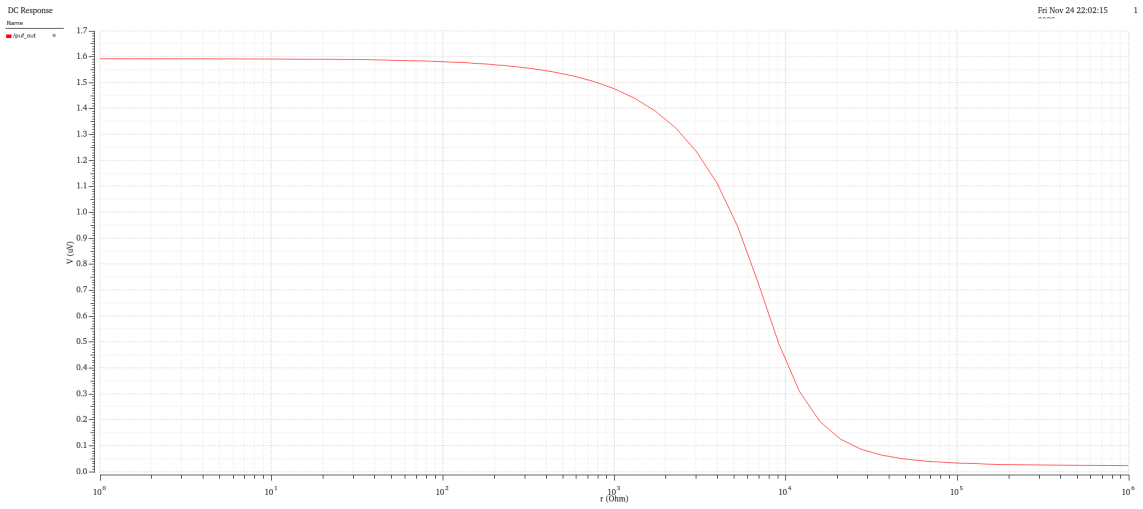


FIGURE 2.3: VIA PUF output v/s the contact resistance

The x-axis represents the contact resistance and the y-axis is the output of the puf bitcell.

2.3 Conclusion and Future work

The findings indicate that the output of the VIA PUF varies between logic 0 and logic 1 based on the parasitic resistance value. Within the transition range depicted in the plot, neither logic 0 nor logic 1 is clearly defined. It is imperative to eliminate PUF bitcells with parasitic resistance falling within this region to ensure the reliability of the PUF.

- Conducting post-layout simulations in Cadence Virtuoso is essential for determining parasitic resistances. Subsequently, based on these values, the assignment of logic 0 or logic 1 to each contact becomes possible.

- After categorizing PUF cells as either short or open contacts, the next step involves incorporating them into the circuitry of the IoT device. A thorough examination of the specific IoT device circuitry is crucial for the seamless integration of the VIA PUF.

Bibliography

[1] Pappu, Ravikanth, et al. "Physical one-way functions." Science 297.5589 (2002): 2026-2030.

[2] C. Herder, M. -D. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1126-1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516.

[3] D. Jeon, J. H. Baek, Y. -D. Kim, J. Lee, D. K. Kim and B. -D. Choi, "A Physical Unclonable Function With Bit Error Rate ¡ 2.3 × 108 Based on Contact Formation Probability Without Error Correction Code," in IEEE Journal of Solid-State Circuits, vol. 55, no. 3, pp. 805-816, March 2020, doi: 10.1109/JSSC.2019.2951415.

[4] B. Park, D. Forte, M. M. Tehranipoor and N. Maghari, "A Metal-Via Resistance Based Physically Unclonable Function With Backend Incremental ADC," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 68, no. 11, pp. 4700-4709, Nov. 2021, doi: 10.1109/TCSI.2021.3105907.

[5] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," 2007 44th ACM/IEEE Design Automation Conference, San Diego, CA, USA, 2007, pp. 9-14.

[6] Teddy Kyung Lee, CTO, ICTK, "Via PUF Technology as a Root of Trust in IoT Supply Chain", Global Semiconductor Alliance (GSM).

[7] S. Hemavathy and V. S. K. Bhaaskaran, "Arbiter PUF—A Review of Design, Composition, and Security Aspects," in IEEE Access, vol. 11, pp. 33979-34004, 2023, doi: 10.1109/ACCESS.2023.3264016.

[8] D. Jeon and B. -D. Choi, "Circuit design of physical unclonable function for security applications in standard CMOS technology," 2016 IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC), Hong Kong, China, 2016, pp. 86-90, doi: 10.1109/EDSSC.2016.7785216.

[9] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh and S. Lee, "8.7 Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45nm smart-card chips," 2016 IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, USA, 2016, pp. 158-160, doi: 10.1109/ISSCC.2016.7417955.

[10] L. Kraleva, M. Mahzoun, R. Posteuca, D. Toprakhisar, T. Ashur and I. Verbauwhede, "Cryptanalysis of Strong Physically Unclonable Functions," in IEEE Open Journal of the Solid-State Circuits Society, vol. 3, pp. 32-40, 2023, doi: 10.1109/OJSSCS.2022.3227009.