PUF Based Device Identification for Cryptographic Service Provision

By

Mubarak Mehdi
Fall 2016 - MS(IS) - 00000170596

Supervisor
Dr. Hasan Tahir

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Information Security (MS IS)

In

School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(June, 2020)

DEDICATION

Dedicated to Mama, Abu and my brother without their love support and prayers I would not have been what I am today

Online Printing Date & Time: Sunday, 21 June 2020 00:18:12

Approval

It is certified that the contents and form of the thesis entitled "PUF Based Device Identification for Cryptographic Service Provision" submitted by MUBARAK MEHDI have been found satisfactory for the requirement of the degree

Advisor : Dr. Hasan Tahir

Signature: ____________________

Date: 19-Jun-2020

Committee Member 1:Dr. Qaiser Riaz

Signature: ____________________

Date: 19-Jun-2020

Committee Member 2:Mehdi Hussain

Signature: ____________________

Date: 19-Jun-2020

Committee Member 3:Ms. Ayesha Kanwal

Signature: ____________________

Date: 20-Jun-2020

Publish Date & Time:

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "PUF Based Device Identification for Cryptographic Service Provision" written by MUBARAK MEHDI, (Registration No 00000170596), of SEECS has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: Hasan Tahir

Name of Advisor: Dr. Hasan Tahir

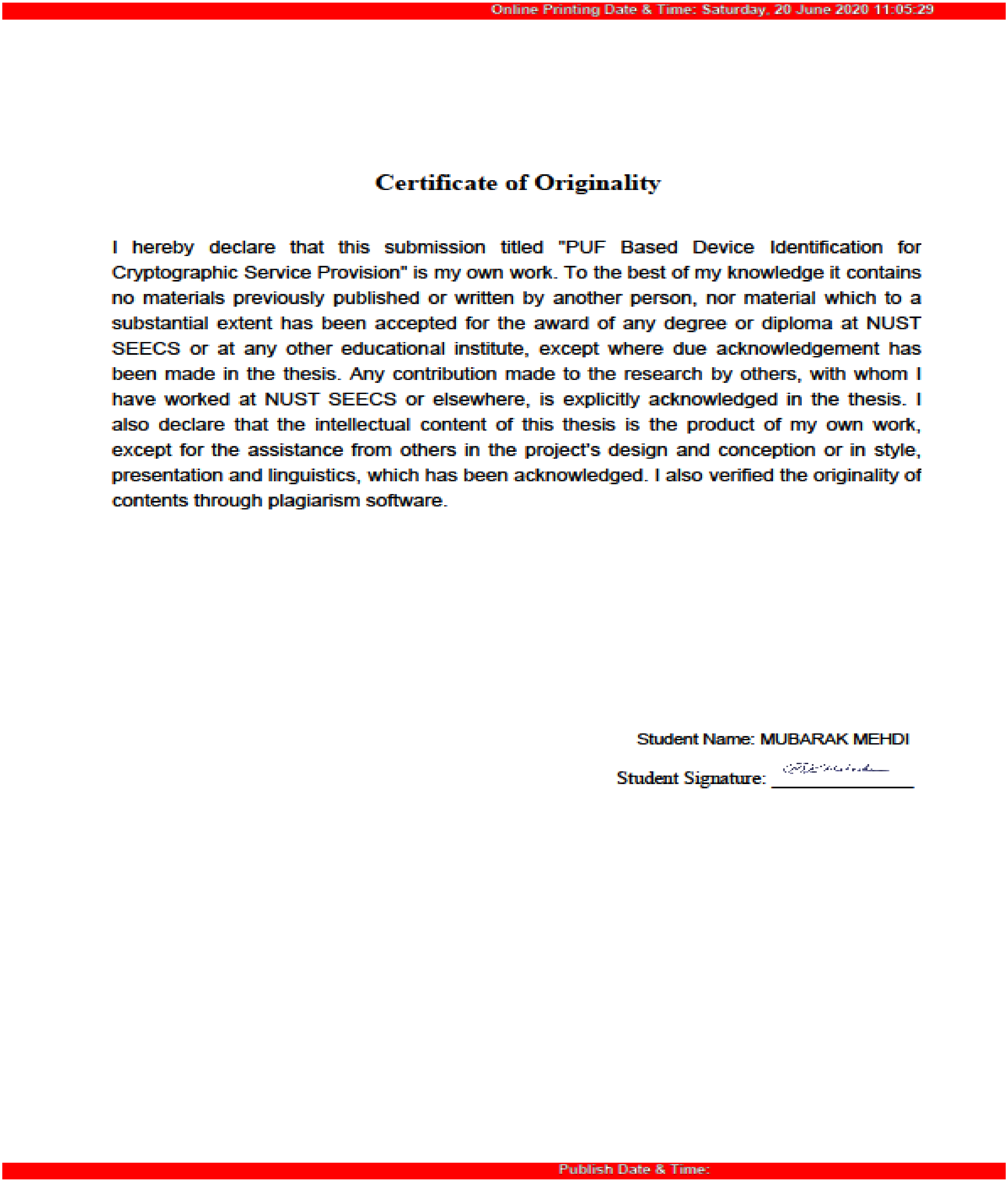
Date: 19-Jun-2020

Signature (HOD): ____________________

Date: ____________________

Signature (Dean/Principal): ____________________

Date: ____________________



Online Printing Date & Time: Saturday, 20 June 2020 11:05:29

Certificate of Originality

I hereby declare that this submission titled "PUF Based Device Identification for Cryptographic Service Provision" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: MUBARAK MEHDI

Student Signature: ______________

Publish Date & Time:

ACKNOWLEDGEMENT

I also declare first and foremost thanks, to Allah Almighty for His blessings throughout each and every step of my life and my research work.

I am thankful to my beloved family and friends, for their unconditional support and prayers. I am humbled by their unconditional trust and love for me.

I would like to express my deep gratitude to my research supervisor, Dr. Hasan Tahir, for giving me the opportunity to do research with him. Without his help, kind guidance and encouragement, I would not be able to complete me research successfully. His sincerity towards work has inspired me greatly. It was an honor to study under his guidance.

I would also like to thank all of my teachers who have ever taught me in my life. Their teachings and suggestions have always been a great help to me.

I am also very thankful to my committee members Dr. Qaiser Riaz, Dr. Mehdi Hussain and Ms. Ayesha Kanwal for their expert suggestions and contributions towards the research

ABSTRACT

Conventional cryptography relies on keys stored in the device. Whenever the key is needed for use in a cryptographic service, a stored key or template is used. The problem with stored keys is that they can be stolen; hence a novel root of trust is needed that can generate a key at run time and does not rely on storage of the key or template. To generate keys at run time physical root of trust can be considered in a Physically Unclonable Function (PUF). Using the concept of PUF a unique ID of the device can be created by using the device physical characteristics. Being rooted in the physical world means that extracting/ guessing the device identity requires considerable effort on part of the adversary, as physical access to the device may be required along with access to specialized hardware/ environment. Fundamentally, PUF is a challenge-response mechanism that is rooted in the physical realm. PUF receives a challenge and a corresponding response is generated. Once processed the generated response is provided to the PUF cannot be reproduced by any other device due to unique inherent physical features of the device. This unique response serves as the fingerprint of the device. In this study, physical features of MEMS sensors have been studied in detail that will generate a fingerprint which can serve as the identity of the device. The fingerprint of a device nor any associated PUF data is ever stored or maintained in a database. Thus only the correct device is able to generate the correct PUF identity of a device. This research makes major contributions towards creating a PUF identity that is entirely based on inherent device features. Firstly a range of device features have been identified that are either device encoded while other are extractable via device operational profile. The second major contribution of the thesis is that a statistical analysis of the data generated by MEMS sensors is considered to prove that the selected features are unpredictable, regeneratable and particularly stable for use in cryptographic operations. Lastly two authentication schemes are presented that can be used for the authentication of PUF_{ID} so devices can be authenticate and communicate with each other.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ASSOCIATED PUBLICATIONS

M. Mehdi, M.T. Ajani, H. Tahir, Z. Alizai, S. Tahir, F. Khan, Q. Riaz, M. Hussain, “PUF-based Key Generation Scheme For Secure Group Communication Using MEMS” *Submitted to Neural Computing and Applications. Springer*.

CHAPTER 1: INTRODUCTION

Secrecy of sensitive data is an important requirement in most modern systems. Whether the data is at rest, in motion or being processed; its integrity and confidentiality is paramount. With a rapid increase in the number of smart devices, group communication, IOT and cyber physical system (CPS) it is becoming difficult to ensure privacy and security of the data as the resources in possession of an adversary can no longer be considered limited. To make matters more complex the adversaries may choose a side channel to attack the system thus exposing it in its entirety. The attacks that are based on the weakness in the design of algorithm are difficult to correct as they require a complete redesign of the algorithm. Kerckhoff's Security Principle states that: "The security of a system should lie in keeping the key secret and not the algorithm"[1]. It is essential to know that increasing the size of the key makes it difficult for an attacker to guess the keys, but does not eliminate key theft. Any effort to increase the key size for increasing key deterrence is a fruitless effort.

1.1 Motivation

In recent years, heavy reliance on technology for the information communication has been noted. The need of secure communication has vastly increased due to the sensitive and private information being transferred and stored over the internet every second. The devices used for communication are still consider insecure despite the fact that there is tremendous amount of research in the field of information security. Every year there are many cyber security incidents reported that causes the loss of private information or financial loss [2]. Adversaries get stronger due to the availability of high computation power and connectivity of devices. . As capacity of the network increases it brings to light many new applications like teleconferencing, Real-time applications that can share information in blink of an eye, and collaborative environment to share the information in groups. In group communication one authorized sender sends the message to more than one authorized receivers. Many devices are being used as cyber physical system environment where they work collaboratively to share information and data. To an adversary this environment attracts where multiple devices are sharing data and working together using the communication links. Adversary can exploit the system and gain access to the devices and information by exploiting the weakness in the design of the system or by stealing the key from an unencrypted channel or physically stealing the keys from the system. If the theft of the keys can compromise the whole system then it raises serious questions and creates a strong case for new approach for key based authentication.

1.2 Statement

The algorithms and protocol for most common cryptographic schemes are publicly available while the only thing kept secret are the cryptographic keys. Hence it can be said that security of the system relies upon the keys and not on the protocol. If the keys get compromised or stolen at any point, then the security of the whole system is compromised. A way to secure passwords is its memorization thus defeating chances of it being known to any other person unwillingly. Keys on the other hand are hexadecimal and lengthy in size owing to which they are stored in the device. This makes them prone to many attacks which can be both external or internal. Cryptographers are increasing the size of the key making it harder for an attacker to brute force or guess the keys, but still that does nothing to eliminate key theft.

In this research a thorough study is presented that provides security to the keys that are stored in the device. The main purpose of this study is to analyze the concept of Physically Unclonable Function (PUF) and puts its theories into practice to generate to create a key at runtime. This research demonstrates the possibility of creating a unique id called PUF_{ID} for the device by using its own features. This PUF_{ID} can be used for the device identification and authentication for further provision of security in cyber physical systems.

To demonstrate this, many features and properties have been considered for creation of a device PUF_{ID}. In this research evidence for cryptographic provisions such as integrity, confidentiality and authentication is provided. Cryptographic keys can be generated using PUF technology thereby providing stronger guarantees which were previously not possible to provide.

This is assured on the basis that the generated keys are based on a novel root of trust. In this study PUF Technology is studied in two ways

1. PUF technology as a means of generating cryptographic keys
2. PUF technology as a means of preventing key theft

1.3 Contributions

In conventional cryptography security of the system is relies on keys that are often stored. Keys stored in a device are considered as vulnerability as an adversary can capture these keys using a variety of methods [3], [4]. Hence incorporating the PUF technology as a method of key theft deterrence can provide enhanced security as it can mitigate a big concern that is often faced by even the strongest cryptographic algorithms.

In this research unique features of device are studied which can be used to provide a unique identity specific to that device, then that unique ID can be used for cryptographic service provisions such as authentication, confidentiality and integrity. As the PUF identity is unique and a crucial element therefore it cannot be stored on the device or communicated insecurely. The first contribution this study makes is the identification of features that are suitable for the creation of a PUF identity specific to a device. Here the concern is to ensure that the PUF identity is regeneratable, unique and stable for repeated use.

The other major contribution of this research is the provision of a scheme that can be used to authenticate the devices. Two authentications scheme are presented and discussed that uses the PUF identity of the device for the cryptographic service provision such as authentication and identification. But the most noteworthy contribution is that it provides higher level of security to existing systems without making any major changes. Therefore, with minimal impact on existing infrastructure PUF can be integrated into any IT infrastructure. PUF was developed to integrate with traditional systems because it is designed as an additional layer that requires minimum intervention.

1.4 Aim of the Research

Fulfillment of security goals that needed to be achieved is the main aim when designing a cryptosystem and all the development activities revolve around these goals. Every goal must be in accordance with each other to ensure the complete security of the end system. The focal point of this study is the Security goals, because the choice of system primitives/ design is based to achieve three most important security goals: integrity, confidentiality and authentication. The project's security objectives and their explanation in light of the research are listed below.

- Confidentiality is defined as concealment of information. Confidentiality means only authenticated and authorized personal can view the information. Encryption is the most common method to achieve confidentiality.
- Authentication is defined as the process of authenticating and identifying a personal, based on a unique information only known to the entity authenticating. Authentication make sure that the personal is who he claims to be.
- Integrity is defined as prevention of unauthorized changes. Integrity makes sure that the no malicious software or unauthorized persons has altered the data and the data stored on the device is correct Integrity ensures that no contributions and modifications are made in the communication and stop adversaries from making these dishonest contributions.

1.5 Physical Root of Trust

Attackers can now use powerful technology with sufficient resources to carry out powerful attacks. As a result, research has explored alternate support methods which could improve the security of traditional cryptographic implementations. Traditionally cryptosystems relies upon mathematical principles. The most important element is that the algorithm is based on the problems that are hard to solve by brute force. Mathematical difficulty is not enough to guarantee system security, because attackers will never behave as expected. Attackers often attack the system by not exploiting inherent mathematical weakness. Rather other ways such as cold boot attacks and side channel is used to attack the system. These methods of attack are particularly deadly because they are not related to the core design of the algorithm where the focus of all activities is while in the design phase. Furthermore, often the many possibilities of a side channel attack are overlooked by security engineers. Therefore, a new technologies and methods are required that uses physical reasoning [5]. Higher levels of security can be ensured by using a physical reasoning as the system primitives are rooted in the physical world. In this research Physically Unclonable Function (PUF) is studied as a novel physical root of trust due to its physical characteristics [6]. Fundamentally, a PUF is a challenge and response based function thus if a challenge x is queried to a PUF the function will provide a secret response y based on the device unique characteristics. Due to the unique characteristics and physical properties of a device, the output generated is unique. Owing to the strong qualities of PUF it can be used for high levels of random number generation (RNG), authentication and hardware entangled cryptography service provision. Perhaps the greatest quality of PUF is that it can be used as an alternative to stored keys. This quality makes it a suitable technology that can be used with both modern and traditional cryptographic schemes.

The breakdown of the contributions is arranged as follows:

- In chapter 2 previous research related to cyber physical system and physically unclonable function is discussed in detail. The chapter begins with describing how devices in cyber physical system communicate to create a corporative environment. The chapter also introduces PUF in detail, also addressed the security concerns when authenticating a device.
- Chapter 3 studies the imperfections of inertial MEMS sensors like accelerometer and gyroscope, the features of these MEMS sensors can be used as a response to a PUF.
- In chapter 4 statistical analysis for each MEMS sensor is carried out. Statistical analysis shows that PUF can be generated using MEMS sensor as there is significant bias in each sensor.
- Chapter 5 focuses on the authentication scheme that is can be used to establish authentication of a devices incorporating the PUF technology.
- Chapter 6 gives the conclusion of the research and provides future direction of this research.

CHAPTER 2: LITERATURE REVIEW

With the increase in interconnectivity of devices, extensive communication and data sharing it is compulsory to ensure that both the communication and data secured from an adversary. In this chapter a past work has been presented which shows attacks on the security key used for communication in field of cyber physical system and how PUF is being used to generate keys at run time that can be used for communication which makes it harder for adversary to attack on keys as they are not stored. This chapter shows how PUF is being used to generate finger print of a device using the physical characteristics of that device.

2.1 Cyber Physical System

In the field of computing extensive research has been carried out which resulted in the creation of sophisticated more sophisticated and intelligent devices Computing technology was initially used as a personal computer to facilitate people in homes, offices and labs. Recently the boundaries have disappeared as the internet has facilitated communication and sharing of data. The Internet is changing how people exchange data, the process of selling and buying is changing, from where they are accessing data and how they are communicating. The Cyber Physical System (CPS) is changing the way humans interact with physical world and how the environment can be controlled. Cyber Physical System can be described as devices that controls and monitors the entities in the physical world by combining the capabilities of data storage, communication and computing [1]. In general terms a CPS is not an embedded system, a PC or a sensor network. It is anticipated the CPS will increase the communication, computation, automation, and configuration in comparison to the existing systems. The purpose of this system is to make sure processes which involve physical elements and computation takes place more smoothly [2]. Some defining features of CPS are as follows.

- CPS should be closely integrated with physical and computation processes.
- Every resource and physical component should have the cyber capability so it can communicate with other devices. The system must have limited resources such as bandwidth and computing and software is embedded in a physical component or embedded system.
- CPSs must be easily to reconfigure as they are very complicated systems.
- CPSs must have automation and feedback technologies applied to the system.
- CPSs must be reliable and secure at large scale so they must be certified if necessary.
- The networks are geographically distributed through network technologies like WLAN, GSM, and Bluetooth but the system scales and categories of devices are highly variable.

Raj Rajkumar professor at Carnegie Mellon University USA used the term Cyber Physical Systems for the first time in 2006. Since then CPS is considered as an upcoming technology and . a lot of studies and research are presented in this field. Mainly research in this field is concentrated on these aspects.

2.1.1 Energy Control

CPS is a distributed system. Devices in CPS need limited energy but supplying energy to the device is still considered a challenge. Research [3] has studied a trade-off strategy between the energy requirement and user demand in the data centers. To achieve a maximum battery life research [4] has studied the design of a flexible and ideal discharge profile for square wave impulsive current. Similar research [5], [6] proposes an ideal lazy scheduler which uses services with the least amount of energy. To obtain energy efficiency [7] design a clustering architecture.

2.1.2 Communication and Management

Management and communication of the data produced by the sensors need to be maintained by CPS. An information-centric approach was proposed by [8] for real-time secure data services. Spatio temporal distribution was studied by [9] in CPS nodes. Another research [10] proposed a control mechanism in WSN monitoring application for estimation of spatio temporal.

2.1.3 Resource Allocation

The main focus of resource allocation has been on embedded and real-time device resource allocation. A study [11] of schemes has been presented that shows how bandwidth should be allocated in CPSs. Recent research [12] studies the properties of software in a dynamic model saying how resources should be allocated.

2.1.4 Security Control

Key management, identification and authentication has been researched to improve the security of CSP security controls. Many security controls have been proposed and challenges have been addressed for CSP. [13] present a signature scheme for mobile CSP which is certificateless. Research has also made effort to improve quality and security in WSN by exploiting message scheduling in critical CPS applications[14].

2.1.5 Applications of CPS

Major applications of CPSs are in driverless vehicles, traffic control and safety, medical devices, advanced automotive systems, environmental control avionics , assisted living, aviation software, energy conservation, process control, weapon and defense system, robotics, water and power grids, communication systems, advanced distributed command and control center manufacturing, smart structures, etc., [15]. Many test cases for application of CPS have been discussed and conducted. Some examples have been discussed in research and experiments have been conducted on healthcare systems, unmanned vehicles, and power grid [15].

2.1.5.1 Health Care Systems

CPS components in healthcare systems include patients record placed electronically in the database, operating rooms, health information network and home care etc. These devices are controlled by computers with many software and hardware components, majority of these systems are performing in real time which require safety and strict time constraints. In Figure 2.1 operating room is shown as an example of CPS.

Figure 2.1: Operation Room as an Example of CPS [15]

2.1.5.2 Critical Infrastructure/Electrical and Power Grid

Many critical infrastructures such as power stations, grid stations, software, and embedded control make a CPS. Many critical things such as security, economical aspects, fault tolerance, and decentralized control systems affect the design of CPS. Figure 2.2 shows a case study for the electrical power grids.

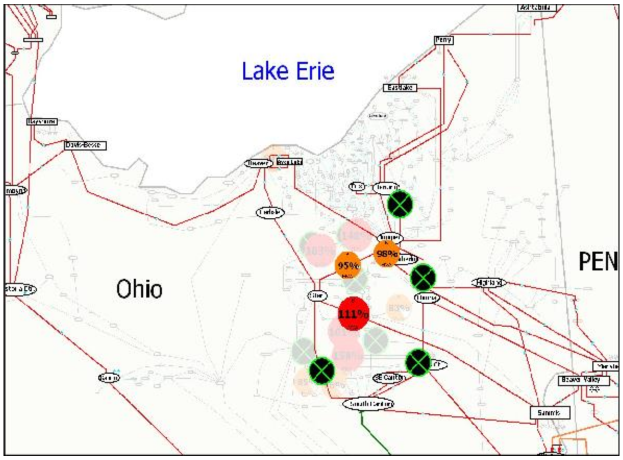


Figure 2.2: Electrical Power Grid Example of CPS [15]

2.1.5.3 Driverless Cars and Intelligent Roads System

As the driverless technology is increasing some new methods can be applied to driverless cars. A new system is being studied [16] that integrates driverless cars and intelligent road system to form a CPS as shown in Figure 2.3.

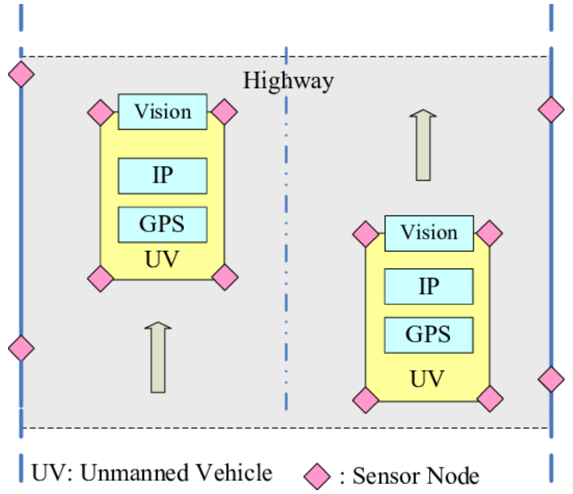


Figure 2.3: Unmanned Vehicle Example of CPS [16]

2.2 Security Concerns

Holistic security is difficult to achieve as vulnerabilities will always surface. Attackers find these vulnerabilities to exploit the system and gain access. Due to the excessive use of the internet and use of external resources, security threats are also increasing which can affect the availability, confidentially and integrity of the system. It cannot be denied that to achieve comprehensive security, the security of both software and hardware needs to be ensured. There are many attacks on the system some common attacks are discussed below.

2.2.1 Physical Attack

In the field of IT security, physical attack means penetrating into the perimeter physically, e.g., breaking into the server room. In the field of cryptography physical attack means an attack on cryptographic devices with physical means. Physical attack means unauthorized access or possession of the cryptographic physical device, e.g., RFID, key card. It can lead to the modification and tampering of the data such as password and security keys stored in a device.

Cryptographic boundary is defined as a boundary of cryptographic devices which have all security components software or hardware. The attacks that could happen on cryptographic boundary are as follows.

2.2.1.1 Penetration

Penetration is an active attack which means breaking into the device physically using vulnerability present in the devices. The aim of a penetration attack could be to read the memory to determine the security keys or password to get into cryptographic boundary.

2.2.1.2 Modification

Key Modification is also sophisticated attack on the stored keys. Adversary infer bits of keys stored on device in order to modify the keys so it can exploit the security of the system and communication.

2.2.2 Communication Attack

To gain illegitimate access to a network, communication attacks are used. Data flows from one device to another on network, if the adversary can exploit a network vulnerability thus causing unauthorize authentication and authorization. If an attacker gets into the network, he can steal security keys and also compromise other confidential credentials.

Eavesdropping is one of the most common attacks on communication. An adversary listens to the communication on the network and if keys are transmitted without encryption they can be stolen.

Another attack on the network is IP spoofing. IP is used as an address and if adversary successfully conducts a spoofing attack on the user IP then traffic can be redirected, captured, deleted, and modified. Mirai malware was used to carry out an attack on digital devices. The malware identifies devices using a default username and password. If a vulnerability is found, then that device is used as a bot to initiate a DDOS attack. [17]

2.2.3 Attack on Cryptography

In modern cryptography security of the device is based on the key. If keys are stolen the whole system can be compromised. In order to capture the key many attackers use a combination of communication attacks and physical attacks. Once captured, the adversary can make a duplicate of the key and use it without the original owner even knowing. An adversary can use the stolen key in any way and can go undetected.

An adversary can use many methods to steal the keys by exploiting vulnerabilities and weaknesses in the cryptographic algorithms and system. Some examples are given below[18], [19].

2.2.3.1 Brute Force

An adversary can find the key by using the brute force on cryptosystem. Rainbow tables, man in the middle and dictionary-based attacks, etc., are used to carry out brute force attacks. Brute force can be prevented by increasing the key size, using salts with keys and by not using vulnerable cryptographic algorithms.

2.2.3.2 Malware

An adversary can embed a virus into the user device and malware can send the stored key to the attacker. These type of attacks are much harder to detect, as user may not know about the presence of malware in the system. Such attacks can be prevented by using antivirus and by using regularly updated software.

2.2.3.3 Identity Theft

Identity theft is a scam and a crime whose consequent is lose in personal data such as banking information, passwords, health id, credit card information and social security number. It can be used to without the permission of owner to commit a crime. An example of identity theft in terms of cryptography is an adversary can use the public key of someone else and can claim it to be theirs. Certification authority has mistakenly issued certificates to forgers which can also lead to vulnerability [20].

2.2.3.4 Keys Generation Algorithm

Many cryptographic algorithms used factorization and prime numbers for a key generation because if weak keys are generated it is easier for an adversary to attack the keys. A third party can be used to generate keys/random number but make sure it is trusted as the adversary can act as a trusted party and generate a key/random number.

2.2.3.5 Social Engineering

The vulnerabilities of a system are not just limited to algorithms. Often the weakest link in s system is the user itself. Social engineering attacks can be used to manipulate a user to obtain a key from him.

2.3 Physically Unclonable Functions

Research [21] has shown that no two chips are manufactured alike. Whether they are from same lot or different wafer. Even if the manufacturing process and mask of the IC's are same no two chips will have the same physical characteristics. Variability in the IC's is at a molecular level. The variations in design can be due to the temperature or pressure variation in the different process of the manufacturing such as soldering or assembling of the IC's. These variations are unique characteristics of the device.

Physical Unclonable Function (PUF) is a one-way function that uses properties of variation of IC's as a unique response. PUF uses the physical characteristics of the device to generate a secret. As no two devices have the same physical characteristics the secret generated through these physical characteristics will be unique and unclonable. PUF is like a black-box and it is based on the process of challenge and response as shown in Figure 2.4. PUF receives a challenge x and a response y is generated. it can be simplified as $y = f(x)$ where $f(\,)$ is the PUF The response to a challenge provided to the PUF cannot be reproduced by any other device due to unique internal environment of the device [22]. Internal parameters are variability of the devices such as gate delay these variabilities are used to create secret output of the device which is harder to predict [21].

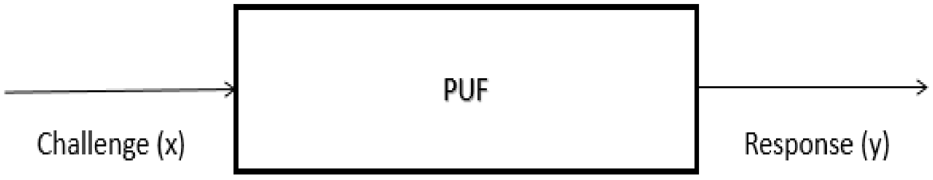


Figure 2.4: PUF Receives a Challenge(x) and Response(y) is Generated

Research has shown that PUF can be used for cryptographic provisions as the modern cryptographic schemes are under attack[22] [23]. Due to the properties of the PUF, it can be used for many cryptographic purposes such as to create random numbers, authentication, hardware-based cryptography, and device identification. Some properties of the PUF are defined below.

- Unclonable: No device can create an identical response to a challenge. It cannot be cloned.
- Robust: If queried with an identical challenge it must repeatedly generate a similar response and be able to resist tampering or external influences
- Unpredictable: It is impossible to predict the response of the PUF no matter how many responses are collected before.
- Reproducible: The responses must be reproducible and response can only be changed for the same challenge if the device is tampered with.

Two major applications of PUF are key generation and authentication. Secret keys can be generated using PUF as it provides secure storage and randomness, generated secret keys can be derived from the response generated by PUF.

2.3.1 Types of PUF

Many studies are presented that identify different characteristics which are used to generate PUF. Many types of PUF had been proposed which show different challenges and response to generate a PUF.

2.3.1.1 Optical PUF

Research [24] on creating a PUF by placing a scattering medium that can capture the scattered pattern of the beam in the path of the laser. In this scheme, an optical token is placed in between laser beam and a scattering medium as shown in Figure 2.5. Optical token contains refractive glass when the laser beam is passed through the refractive glass the refractive particles of the laser beam is scattered on the scattering medium which is observed by the camera. It is observed that a slight difference in the laser beam orientation can change the scattered pattern. The challenge in this application is the laser beam and response is the scattered pattern generated by that laser beam. To reproduce the PUF, exact orientation has to be known so scattered pattern from the beam can be regenerated..

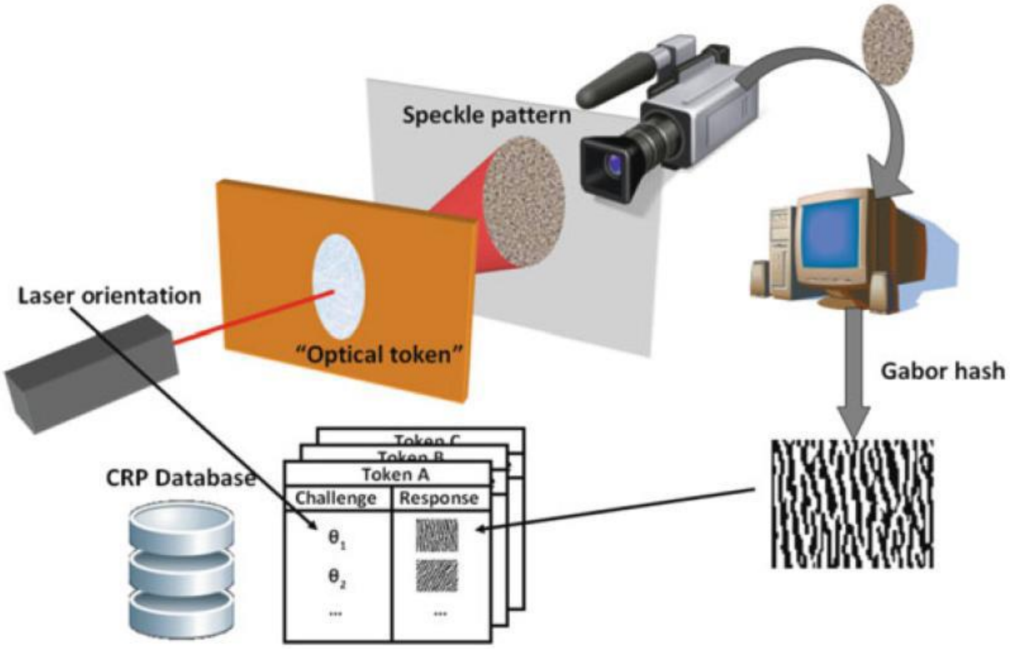


Figure 2.5: Optical PUF basic operation [24]

2.3.1.2 Coating PUF

In the top layer of IC's, a combed shaped structure of wire is laid out. The combed like structure is coated with chemically static and non-transparent dielectric particles as shown in Figure 2.6. Capacitance between the structures is measured and is used as PUF. due to the strength and randomness of the dielectric particles capacitance will be completely random [25].

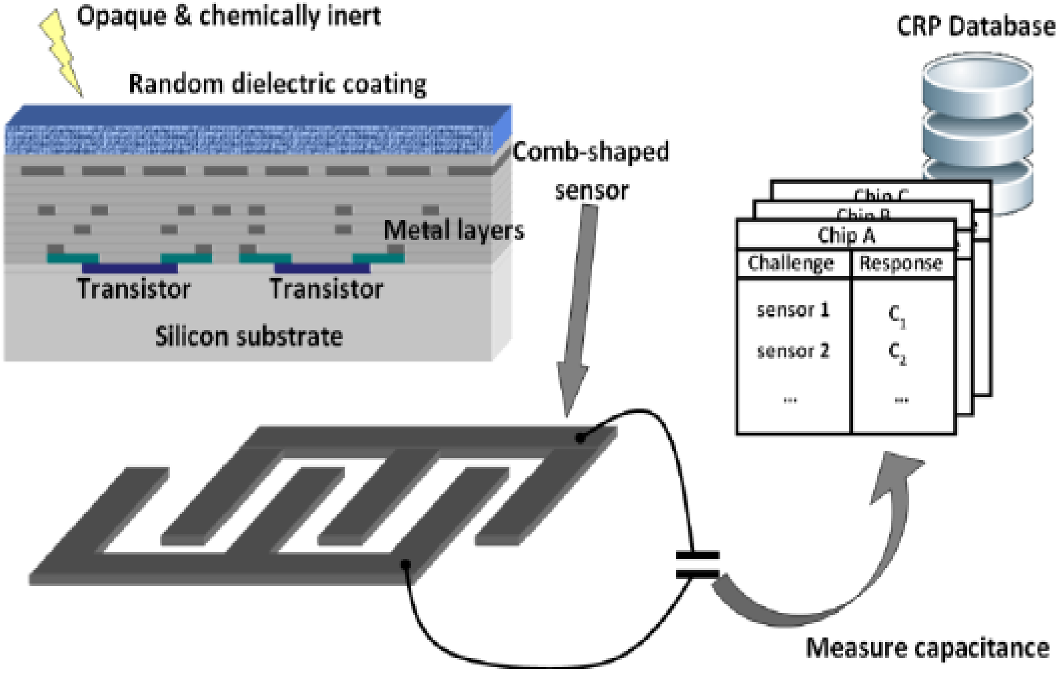


Figure 2.6: Coating PUF Basic Operation [24]

2.3.1.3 Arbiter PUF

Arbiter PUF was first introduced in [26],[27]. The concept of arbiter circuit is, in the symmetrical design circuit a race condition is created between two paths of the circuit and let arbiter circuit decide which path won the race. Due to the variations in the manufacturing process some parameters are affected which makes it difficult to know the exact delay of the circuit. Hence this delay can be used to create a randomness and can be used to create the PUF of the device. To create an arbiter circuit flip-flop and switch box is used as shown in Figure 2.7. Switch boxes are connected in series and each switch box has two inputs and two outputs and the input of one switch box is the output of the previous switch box. Switch boxes are connected either via straight or switched lines. These lines create a parametrize delay and all feed to arbiter circuit. The challenge, in this case, is switch box setting and output is the response generated by the arbiter circuit. Arbiter PUF security depends on the delay of gates as PUF cannot be generated because the delay of the circuit is unclonable due to the variability in the manufacturing process so no circuit will have the same delay.

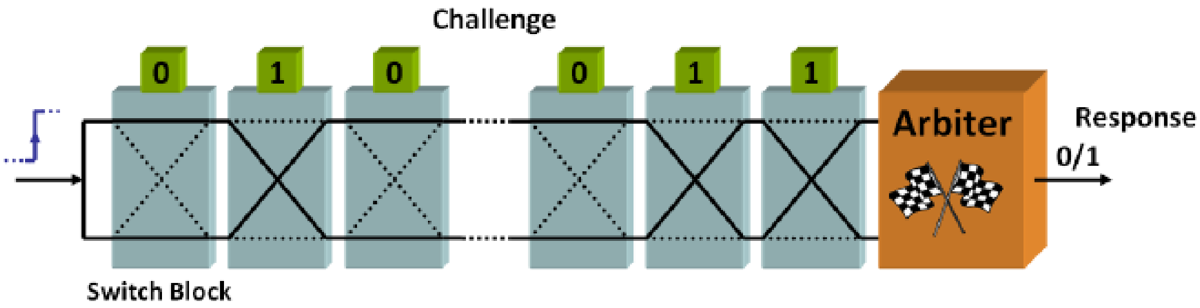


Figure 2.7: Basic Challenge and Response Operation of Arbiter Circuit [24]

2.3.1.4 Ring Oscillator PUF

Another way of using a delay of the circuit, to create PUF is Ring oscillator PUF [21], [28]. In-ring oscillator PUF an asynchronous loop is created by feeding the output of the delay line to the input. It will create an oscillating loop called ring oscillator. In order to generate the PUF frequency of this oscillator is measured by measuring the circuit delay in the delay line. Hence it can be said that measuring the delay of the circuit is equal to measuring frequency. So due to the device variability in manufacturing, frequency is based on the device and will differ from device to device and frequency measured is random. Due to the randomness, it can be used to create PUF. Frequency is measured using an edge detector it will detect the hikes/edges in the frequency and counter will count the number of edges over time. Figure 2.8 shows that the value generated by the counter is considered as response generated by PUF and the delay in the parametrized circuit is considered as a challenge.

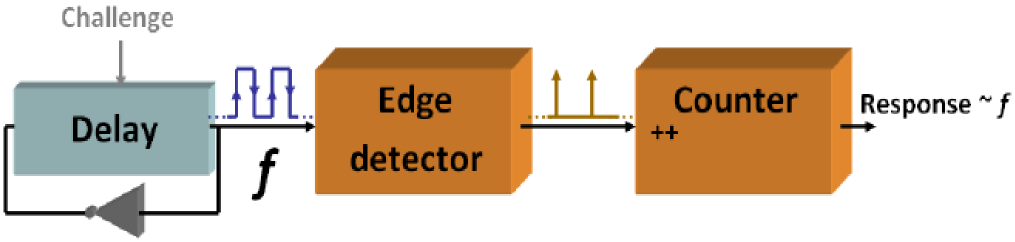


Figure 2.8: Basic Challenge and Response Operation of Ring Oscillator PUF [24]

Ring oscillator is considered as weak PUF as environmental factors such as supplied voltage, humid and temperature will have a great impact on the delay which generates an output error and create a wrong response.

2.3.1.5 SRAM PUF

Another type of PUF is a memory based PUF. In digital memory, there are two stable states (0 or 1) and it stores information using these stable states. Whenever the memory goes to unstable it is not clear what may happen but it is clear some cells prefer a certain stable state over others. This phenomenon is caused by variation in the chip manufacturing process. The randomness of the memory stable states makes it a good option for the PUF. Static random-access memory SRAM is the memory cell which stores a binary digit. To differentiate between devices SRAM is available on every chip. Each time an SRAM is powered on it has a preferred stable state due to the threshold voltage differences. An uninitialized SRAM has a random startup value which will generate a completely randomized pattern of 1's and 0's. Generated random pattern is unique and will only be for that particular SRAM so it can be used as a fingerprint [29] [30]

2.3.1.6 Butterfly PUF

Butterfly PUF are introduced to overcome the shortcoming of the SRAM. As SRAM require the power up to get the response [31]. Butterfly PUF is similar to SRAM PUF. Butterfly PUF is made by cross coupling two latches as shown in Figure 2.9. It also consists of two stable states but the unstable state can be introduced due to the functionality of the latches. In comparison to SRAM, it doesn't require the actual power-up of the device. The state is determined by the latches and cross coupling in butterfly PUF. The variation in the manufacturing process is important if a mismatch of the latches needs to have an effect.

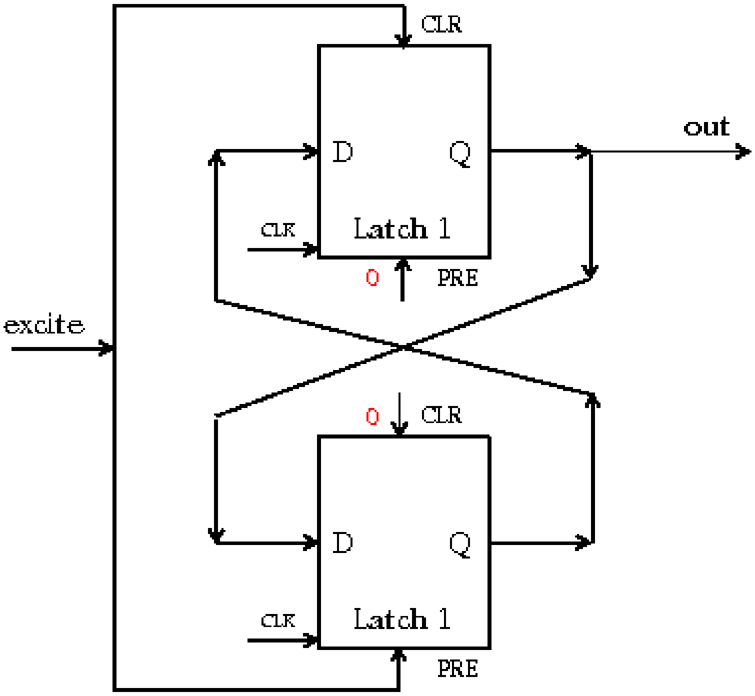


Figure 2.9: Basic Challenge and Resposne Operation of Butterfly PUF [24]

2.3.1.7 Magnetic PUF

One of the major uses of magnetic PUF is in the swipe cards which consist of magnetic a strip. Magnetic PUF uses the uniqueness of the particles in the magnetic structure to create the PUF. One application of the magnetic PUF is that it is used to detect credit cards fraud [24]

2.3.1.8 Paper PUF

Paper PUF are mainly based on scanning the paper fiber structure. Major application of paper PUF anti-counterfeiting of the currency notes. Study [32] creates a fingerprint of the document by hitting the laser beam and capturing the reflection of the paper fiber structure. As the fiber structure of the paper is unique reflection generated by it is also unique. Fingerprinting of paper can also be done by introducing ultraviolet fiber explicitly at the time of manufacturing in the paper. These changes can be measured easily. It can also be used to create a digital signature and to fingerprint a document [33].

It is studied that PUF can improve the functionality of cryptographic functions such as authentication, identification and provide reliability, flexibility, and security by removing key storage [34]. The increase in the security of cryptographic systems is delivered by removing the need for key storage by using PUF to create a cryptographic key. It uses gyroscope based MEMS sensors and calculates measurements on a wafer level. The unique physical and electrical properties of a device are used to generate the cryptographic key. This technique uses extensive hardware to gather measurements at the micro level which make it not feasible to generate keys at runtime.

2.4 Summary

This chapter takes the example of CPS communication and how keys are important for secure communication and authentication. It is studied that adversaries used weakness in cryptographic algorithms to exploit the system and often attack on the system to stole the keys stored in the system. In order to highlight the concerns with stored security keys attacks it is proven that stored keys can be stolen and can be used for malicious activities. In this chapter PUF based approach is studied and how it can be used to generate keys using the physical characteristics of the device. In upcoming chapters it’s discussed how PUF and MEMS sensors can be used to generate the fingerprint of the device that will be used for cryptographic services and device authentication.

CHAPTER 3: METHODOLOGY

Device finger printing is gaining a lot of attention these days, due to the increasing number of devices connected to the internet identification of these devices is a major issue and machine fingerprinting can help identification and authentication Problem with using fingerprinting for cryptography is that there are very few protocols, and algorithm that can provide higher levels of security. A device has many features that can be used for device identification and fingerprinting. Not all features of a device are suitable for the purpose hence research focuses on finding features that are truly unique, unpredictable and reproducible.

PUF technology is used for device identification and fingerprinting thus enabling cryptographic services such as authentication, integrity, confidentiality and key generation. Hence identification generated using device features can be used for many cryptographic services. This chapter studies the concept of hardware imperfection and their use for creating a device PUF identification. MMES sensors are embedded in almost every modern devices are which enable these devices to provide a range of services. This chapter shows how reading obtained from MEMS sensors like accelerometer and gyroscope can be used to create a PUF.

3.1 Hardware Imperfection in Sensors

Sensors are designed to read a stimulus by providing an output reading that is characteristic of the stimulus provided. These detections at times can be imperfect and it needs comprehensive research and analysis of both sensors and devices in which these sensors are embedded to deduce that readings by sensors are imperfect. Hardware identification is one major issue, as all sensors are not suitable for hardware identification. There could be many reasons for such issue as sensors embedded in the hardware lack adequate distinguishable features. Other reason can be an attacker making copy of readings by placing identical sensor in close vicinity to obtain similar readings even though distinguishable features exist.[35]. Hence implicit features such as device imperfection are needed which are difficult to spoof by an adversary.

There are many reasons behind imperfections in hardware. A prominent reason for the existence of device imperfections is the device fabrication process. MEMS sensors are mounted on a main board resulting in permanent bias due to applied stresses. The other reason could be damage caused during operation by mishandling. Results or reading can be imperfect due to even the operational temperature. Research [36][37][38] has previously studied MEMS sensors regarding their failure and reliability. These researches show that sensor bias can be caused by up to ten types of mechanical variability which can influence the readings making them imperfect as results generated by these sensors reflects these imperfections [39]. These influences maintain electrical integrity and bias varies from sensor to sensor. These imperfections can be compensated by incorporating linear values (calibration) in the imperfect results which are obtained from the MEMS sensors. Even in the presence of calibration the resulting readings are still imperfect. These imperfect values can be used to identify devices uniquely as per the research on the different sensors[40][41][42].

There are many features in computational devices which make them unique and make it possible to identify those devices. But only problem with unique features are that they are sometimes difficult to extract while other features might not be unique, so identifying devices becomes difficult in such cases.

Research [43] has shown the collection of implicit feature from MEMS sensors. When studying sensor bias in relation to statistics, sensor bias is defined as difference between the result expected and the actual test result. Which means bias shows one or more than one errors in the system of a measuring instrument.

It is commonly known that having readings at different instances will result in different readings while having same integrated device and the same sensor despite same stimulus is provided. Bias is present in every sensor which can be checked by verifying the output against the supplied stimulus. While choosing stimulus one should make sure that creation of stimulus is easy when required for that investigation. As PUF needs to be generated without user interaction so no special instruments or devices should be required. For example, magnetometer can be used to create a PUF but many appliances will highly effect the performance of the sensor as it is influenced by close vicinity electrical appliances such as speaker and television etc. So, to use magnetometer another device such as faraday cage need to be used which will prevent the interference of other appliances. Some common hardware components and their imperfections are shown in Table 3.1 that can be used to create PUF. It is worth pointing out here that not all sensors/ components in modern devices are suitable for collecting the bias.

Table 3.1: Imperfections of Some Components that can be Used to Create a PUF

Component	**Imperfection**
Touchscreen	Misalignment of touch screen
Magnetometer	Magnetic Bias
Camera	Noise pattern in camera
Flash Memory	Program disturbs[44]
GPS	Time skew between receivers
Accelerometer	Capacitance bias
Gyroscope	Rotational arms and drive arms biased

In this chapter hardware imperfection of accelerometer and gyroscope are studied in detail to generate a device identification.

3.2 Micro Electrical Mechanical System

The process of making very small sensors through a combination of electrical and mechanical components is called Micro Electrical Mechanical. This combination is used to sense physical characteristics which makes MEMS different from other sensors. MEMS do have special integrated components such as micro sensors, micro Structures, microelectronics and micro actuators which converts different phenomena’s such as magnetic, mechanical, thermal, optical into digital readings.

There are different types of MEMS sensors having wide range of applications but are most widely used MEMS sensors in applications like automobiles, laptops and smartphones are accelerometer and the gyroscope [45]. When studying smartphones these sensors are used to enable motion recognition and additionally these sensors also help in enabling tilt detection and rotation. To sense free-fall movement in laptops gyroscope and accelerometer are used which saves the head and surface of hard drives from any damage by pausing the hard drive when it sense the fall. These sensors have special usage in vehicles too where accelerometer provides the luxury of activating airbags at the time of collision by detecting spike in the acceleration. On the other hand, gyroscope helps to control and prevent rollovers by providing electronic stability features.

This chapter is based on possibility of generating PUF which is dependent on certain low level features of MEMS sensors. Generation of PUF requires particular experiments implemented through the device having MEMS sensor embedded such as MPU 6050. This particular sensor is composed of different components such as accelerometer and gyroscope. Before getting into details related to experiments, this chapter will focus on the working of accelerometer and gyroscope.

3.2.1 MEMS Accelerometer

The accelerometer is made up of fixed plates which are placed in a spring mounted movable mass called proof mass as shown in Figure 3.1. The accelerometer is a capacitance based displacement sensor which senses every movement in proof mass as a change in capacitance. These changes in capacitance are so minute that it needs special electronics to read the physical inputs.

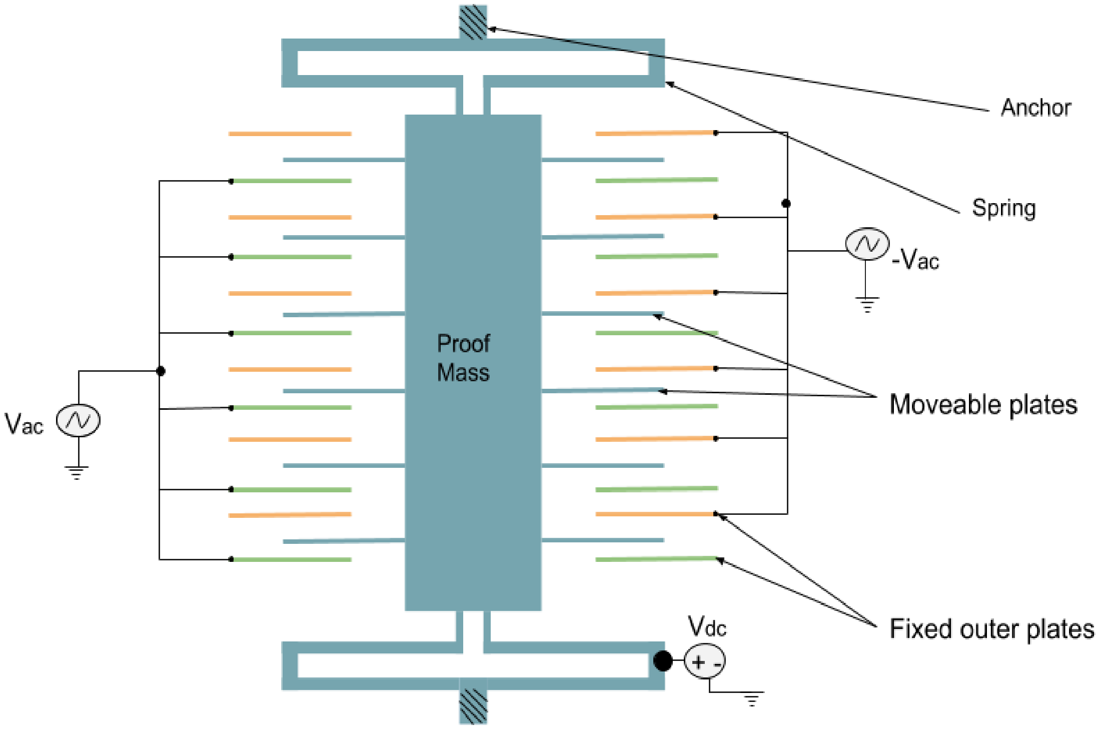


Figure 3.1: Accelerometer Structure

When an acceleration is applied it causes the mass to move in particular direction. The movement will cause change in capacitance produced between moveable plates and fixed plates. When device is in a stationary position capacitance between two plates will be equal.

$$C_1 = C_2$$

When force is applied to the sensor capacitance is produced between the fixed and moveable plates thus

$$C_1 \neq C_2$$

3.2.2 MEMS Gyroscope

When any object or body is exposed to velocity in rotation frame of reference Coriolis effect is experienced. Gyroscope is based upon the Coriolis effect. Gyroscope sensor is made up of drive arms which help to sense angular velocity whenever sensing arms are twisted and rotated as shown in Figure 3.2 (a). The structure of these arms is tall which produce movement according to the sensed rotation. After these arms experience any lateral moment or axial rotation acceleration or force is produced which is subjected by driving arms, this force or acceleration is known as Coriolis force or Coriolis acceleration as shown in Figure 3.2 (b) Gyroscope sensor is designed in such a way that this rotational acceleration is proportional to Coriolis force in this specific frame of reference which helps the sensor to measure the effect of a forced experience by the drive arm.

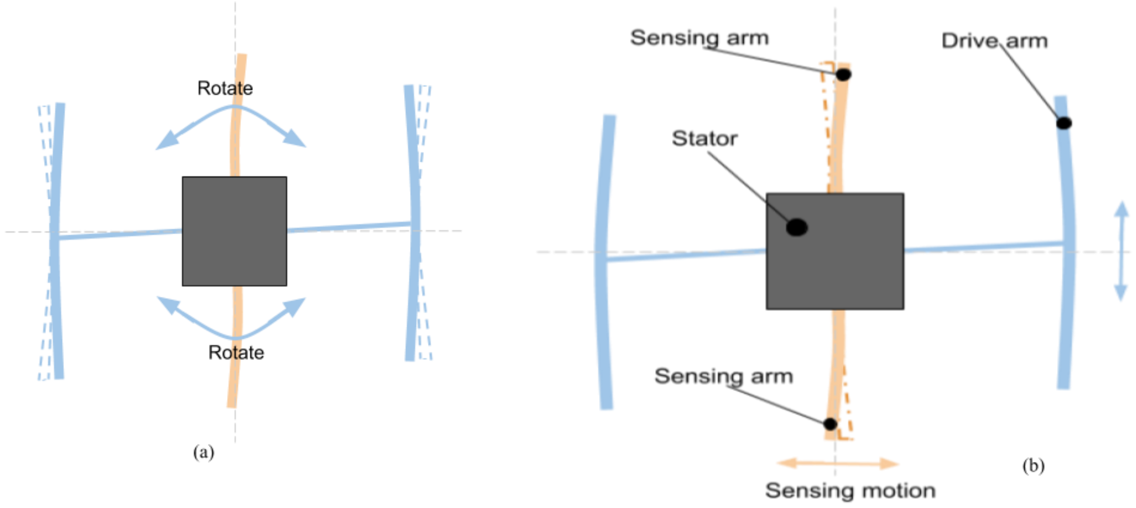


Figure 3.2: MEMS Gyroscope Working Principle (a) Direction of Rotation (b) Sensing Vibration in Drive Arm Whenever Sensing Arm Moved

Imperfections in gyroscope is reflected in readings collected and can be used as a suitable input to create a device PUF.

3.3 Experimental Setup

Throughout the experiments in this work, the PUF ID is created by using the MPU-6050. This is a MEMS sensor containing gyroscope and accelerometer. It has 16 bit analog to digital converter which make it accurate and all three axis values which can be captured at the same time. It also has user-programmable scale of ±2g, ±4g, ±8g, ±16g for precise tracking. To connect with Arduino, it uses I2C. I2C is a protocol involving two line to send and receive the data between components of the motherboards and other embedded electronics components. To collect the MPU-6050 axis values an external Arduino UNO was used which makes it easier to program and give full control over sensor as shown in Figure 3.3. In total 3 setups were created as show in Figure 3.3 so PUF ID generation can be tested. To test the existence of the PUF ID, the accelerometer sensors are subjected to vibration free and motion free surface. To test for reproducibility, the sensor is subjected to this standard stimulus and the experiments are repeated under strict conditions.

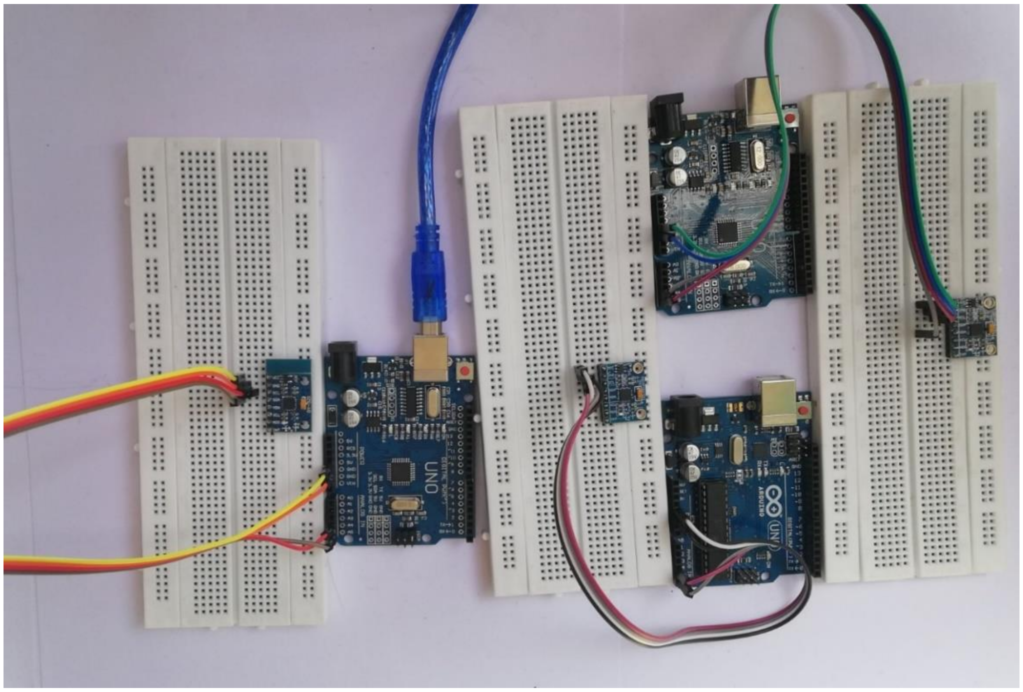


Figure 3.3: Testbed of 3 MPU-6050 Sensors with 3 Arduino

3.4 Methodology

The proposed method for the creation of a device PUF ID is through the determination of sensor bias. For this purpose, X-axis, Y-axis and Z-axis readings were extracted from all the sensors. The readings extracted further were used to create frequency distribution which exhibits uni-modal distribution using histograms, which means a single modality being developed through asymmetric statistical distribution. It is not necessary that unimodal distribution is normal distribution but on the other hand every normal distribution is uni-modal distribution [46].

The number of readings is dependent upon couple of important factors such as the accuracy of the sensors and sampling rate. To judge the correct behavior of sensor, the number of readings matter a lot. Taking too many readings and too little leads to serious concerns as so many readings causes insignificant events to become significant. While talking fewer readings, causes adequacy problem. So to create stability in the mean an accurate number of readings must be taken to achieve target mean value and also to attain stability in statistical credentials.

It is also important to find the number of individual classes needed for frequency distribution and to find this number Sturges rule is applied. The formula to calculate the individual classes is:

$$K = 1 + 3.3 * (\log_{10}(N))$$

$$where\ N = sample\ size$$

According to Sturges rule if the sample size is N, then K gives the number of classes in the frequency distribution. The next step is to perform statistical analysis of histograms to prove that there is a unique bias in each sensor. The histogram is uni-modal which requires statistical indicators like standard deviation, mean, standard deviation and Interquartile range. To ensure that the sensor readings don't follow normal curves and have uni-modal distribution the Shapiro-Wilk normality test is conducted. Through statistical analysis unique bias of sensor is identified.

As for the experiment three sensor are used further named Device A, Device B and Device C. Each device was run for 30 seconds and data of X, Y and Z axis is collected. For each device first and last 10 seconds of the data is removed as it is not representative of the correct sensor functioning. Hence only 10 second of data is used for final calculations. For each device; values are calculated 10 times to look for the consistency in the generated values. Root Sum Square (RSS) of axis values is calculated. RSS is a tolerance analysis method which assumes the normal distribution describes variation of dimensions. RSS is calculated by taking a square of adding the square of all 3-axis at a single instant and then taking its square root, it is repeated for every single instant of axis values. Now the statistical analysis on these RSS values of every sample is presented.

$$RSS_i = \sqrt{(x_i)^2 + \ (y_i)^2 + (Z_i)^2}$$

3.4.1 Accelerometer

For the bias analysis of accelerometer, the MEMS sensor MPU- 6050 is used. This device is embedded with a tri-axial accelerometer that has a sensitivity from $\pm 2g$ to$\pm 16g$.

In order to collect the values MPU- 6050 is placed on the surface which is free from any movements and vibrations. Surface should also be flat. To ensure the values collected are not corrupted or affected by vibrations it was made sure that the sensor is not placed near any electrical appliance. Experiments shows that values can be regenerated by placing the device on stable surface and collecting the values to generate ID. Experiments also shows that the sensor is sufficiently bias and this bias can be used to create the device fingerprint.

The values calculated for each device in 10 second run is different for each device. For device A, 503 values are calculated in each run. For device B, 439 values are calculated in each run and for device C, 478 values are calculated in each run. Each Device is run for 10 times.

RSS is calculated for each run and that RSS is used to create the histograms of the devices. It is noted that there is a significant variance in the histograms of the sensors which shows the bias of the sensor. Figure 3.4, Figure 3.5 and Figure 3.6 shows the histograms of the calibrated accelerometer of device A, device B and device C each have a different bias and there is no correlation and similarity between the devices.

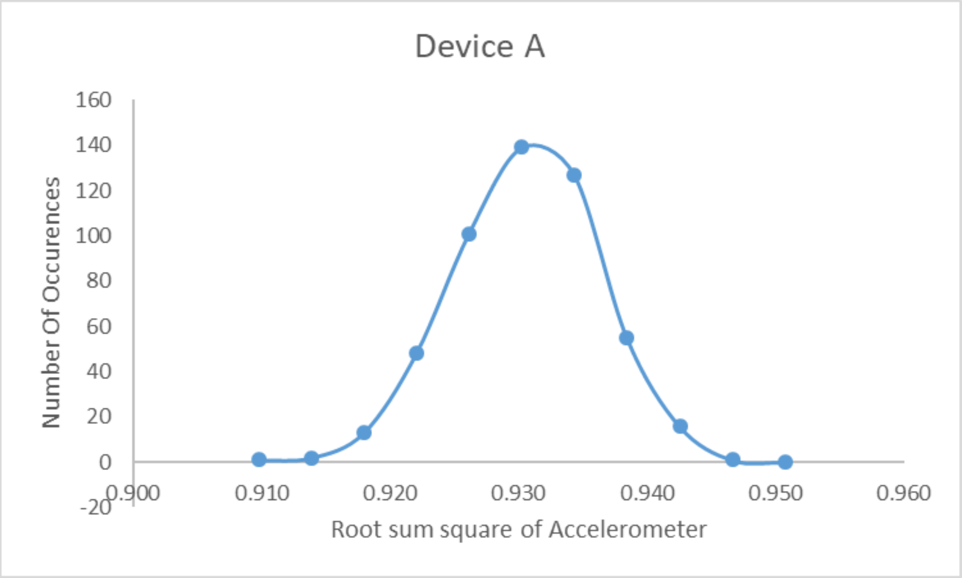


Figure 3.4: Acceleration Histogram for Device A Root Sum Square

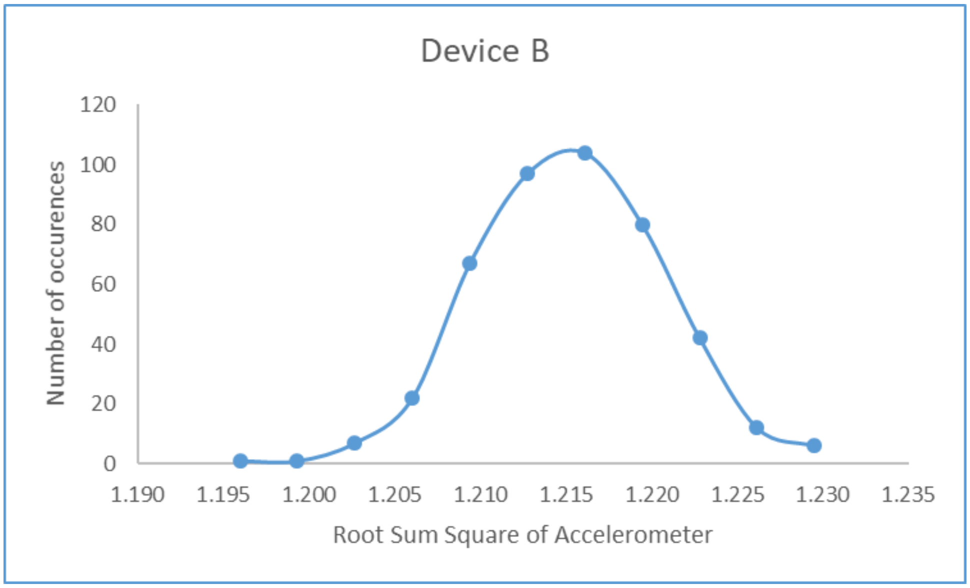


Figure 3.5: Acceleration Histogram for Device B Root Sum Square

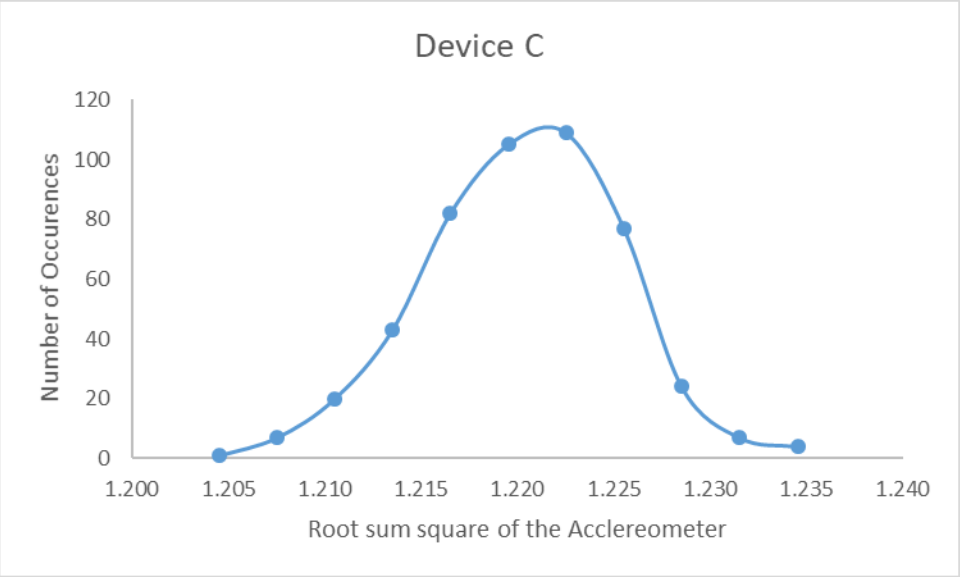
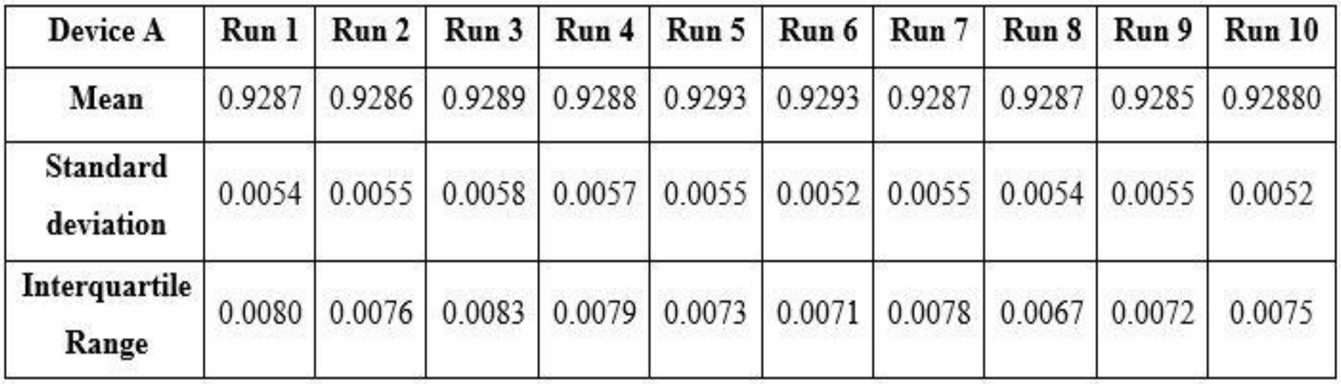


Figure 3.6: Acceleration Histogram for Device C Root Sum Square

On performing the statistical analysis on the initial values such as mean, standard deviation and interquartile range it is shown that there is a similarity in each run for the single device. But no two devices have identical values. Significant difference can be seen in the reading obtained from the accelerometer and there is significant similarity in the values obtained from the sensor when the experiment is repeated (details in the next chapter). Given below Table

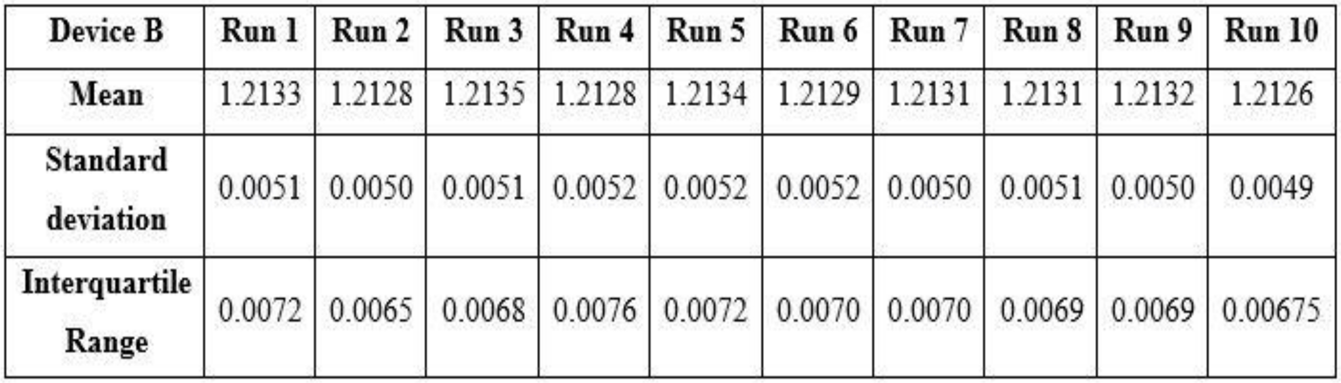
3.2, Table 3.3 and Table 3.4 shows the analysis of values obtained from MPU-6050 accelerometer.

Table 3.2: Statistical Analysis of Device A Accelerometer for 10 Runs



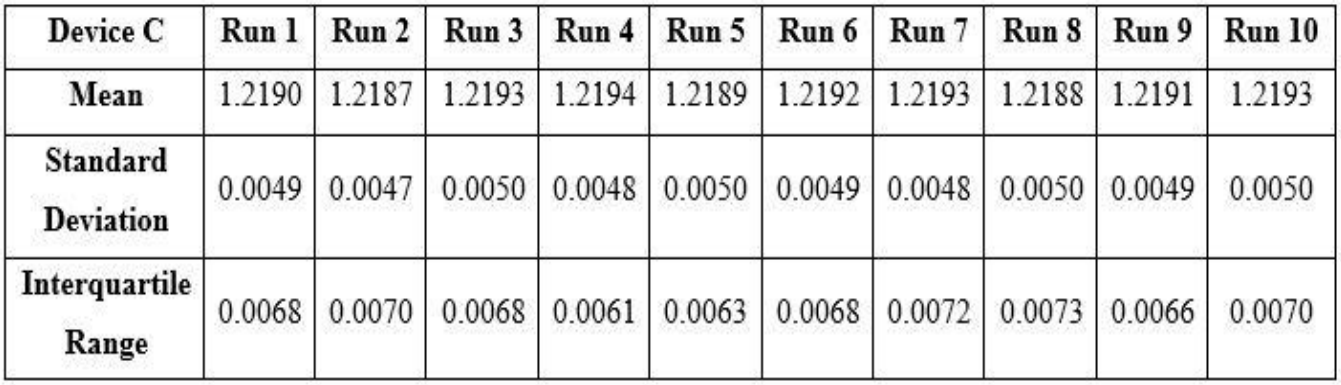
Device A	Run 1	Run 2	Run 3	Run 4	Run 5	Run 6	Run 7	Run 8	Run 9	Run 10
Mean	0.9287	0.9286	0.9289	0.9288	0.9293	0.9293	0.9287	0.9287	0.9285	0.92880
Standard deviation	0.0054	0.0055	0.0058	0.0057	0.0055	0.0052	0.0055	0.0054	0.0055	0.0052
Interquartile Range	0.0080	0.0076	0.0083	0.0079	0.0073	0.0071	0.0078	0.0067	0.0072	0.0075

Table 3.3: Statistical Analysis of Device B Accelerometer for 10 Runs



Device B	Run 1	Run 2	Run 3	Run 4	Run 5	Run 6	Run 7	Run 8	Run 9	Run 10
Mean	1.2133	1.2128	1.2135	1.2128	1.2134	1.2129	1.2131	1.2131	1.2132	1.2126
Standard deviation	0.0051	0.0050	0.0051	0.0052	0.0052	0.0052	0.0050	0.0051	0.0050	0.0049
Interquartile Range	0.0072	0.0065	0.0068	0.0076	0.0072	0.0070	0.0070	0.0069	0.0069	0.00675

Table 3.4: Statistical Analysis of Device C Accelerometer for 10 Runs



Device C	Run 1	Run 2	Run 3	Run 4	Run 5	Run 6	Run 7	Run 8	Run 9	Run 10
Mean	1.2190	1.2187	1.2193	1.2194	1.2189	1.2192	1.2193	1.2188	1.2191	1.2193
Standard Deviation	0.0049	0.0047	0.0050	0.0048	0.0050	0.0049	0.0048	0.0050	0.0049	0.0050
Interquartile Range	0.0068	0.0070	0.0068	0.0061	0.0063	0.0068	0.0072	0.0073	0.0066	0.0070

3.4.2 Gyroscope

Gyroscope is embedded in MPU-6050. Gyroscope measures rotation per seconds. Similar to accelerometer, MPU-6050 is places on a flat and stable surface to measure the gyroscope values. To make sure the values collected are not corrupted or affected due to vibrations, it was ensured that the sensor is not to be placed near any electrical appliance. Experiments shows that values can be generated again by placing the device on stable surface and collecting the values to generate ID. Experiments also shows that the sensor is sufficiently bias and this bias can be used to create the device fingerprint.

For each device values are calculated hence for device A, 481 values are calculated. For device B, 556 values are calculated and for device C, 530 values are calculated. RSS is calculated for each run and that RSS is used to create the histograms of the devices. It is noted that there is a significant variance in the histograms of the sensors which shows the bias of the sensor. Figure 3.7 - Figure 3.9 shows the histograms of the calibrated accelerometer of three devices A, B and C each have a different bias and there is no correlation and similarity between the devices.

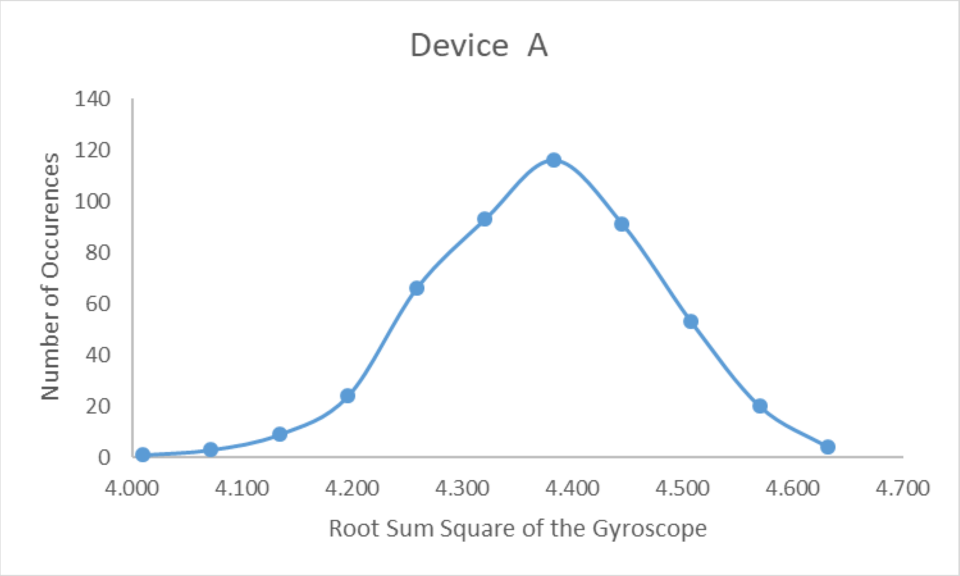


Figure 3.7: Gyroscope Histogram for Device A Root Sum Square

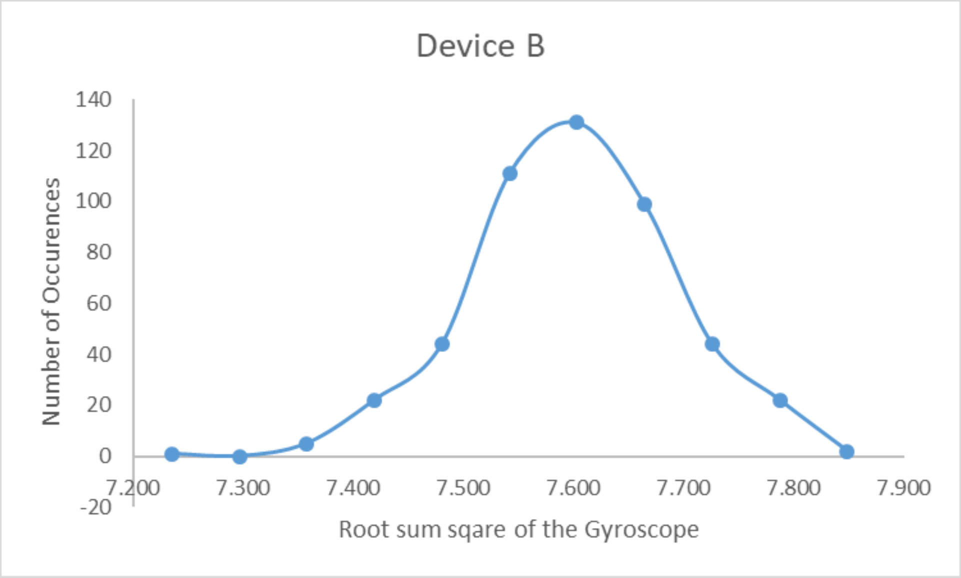


Figure 3.8: Gyroscope Histogram for Device B Root Sum Square

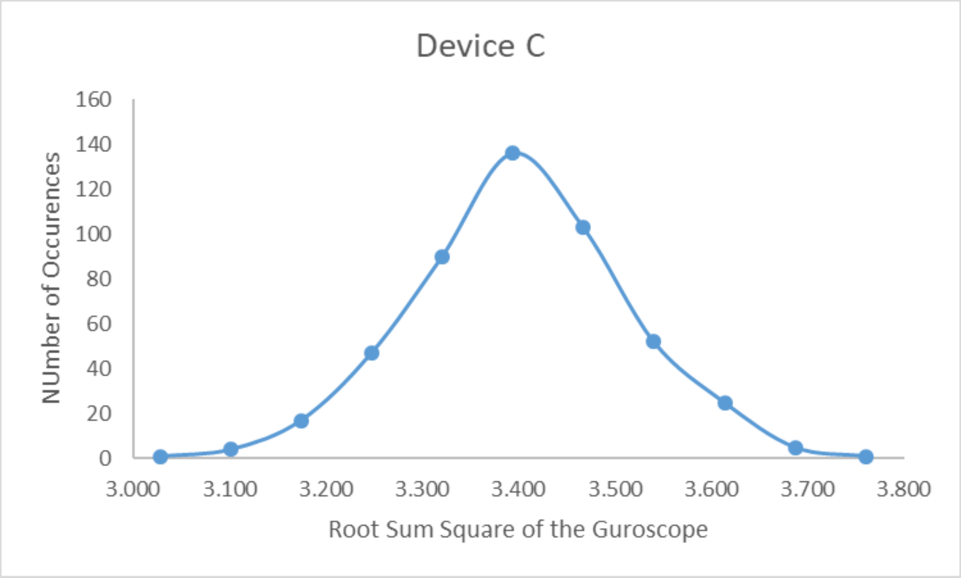
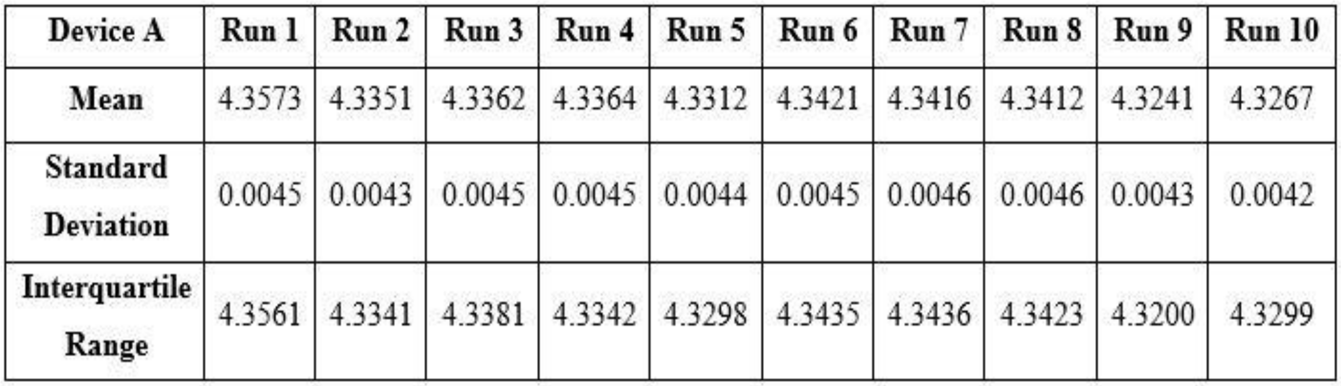


Figure 3.9: Gyroscope Histogram for Device C Root Sum Square

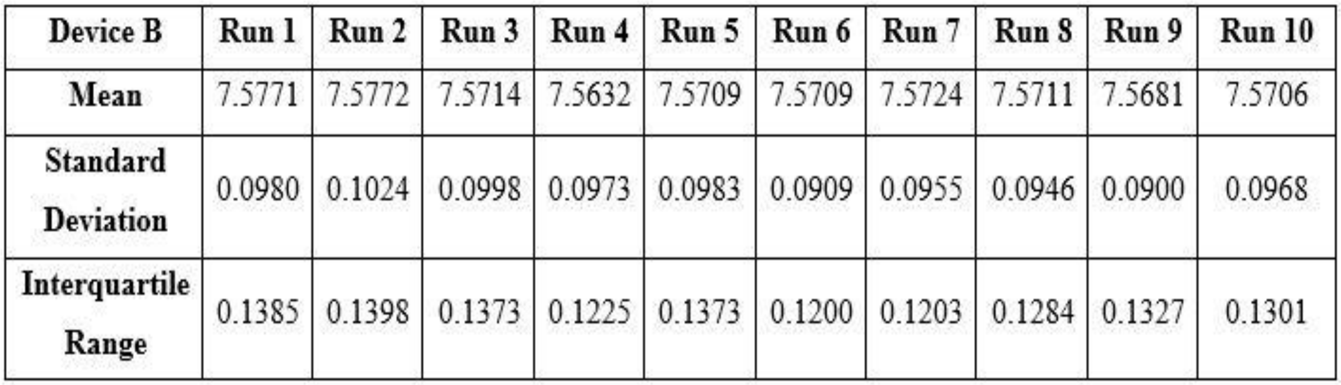
On performing the statistical analysis on the initial values obtained from gyroscope such as mean, standard deviation and interquartile range it is shown that there is a similarity in each run for the single device. But no two devices have the same values. Significant difference can be seen in the reading obtained from the gyroscope and there is significant similarity in the values obtained from the sensor when the experiment is repeated (details in the next chapter). Given below Table 3.5,Table 3.6 and Table 3.7 shows the values obtained from MPU-6050 gyroscope.

Table 3.5: Statistical Analysis of Device A Gyroscope for 10 Runs



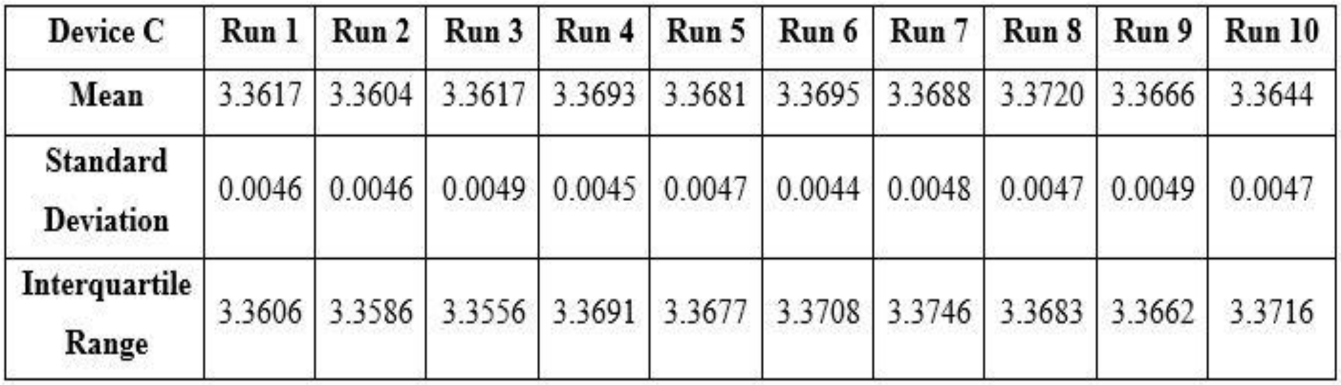
Device A	Run 1	Run 2	Run 3	Run 4	Run 5	Run 6	Run 7	Run 8	Run 9	Run 10
Mean	4.3573	4.3351	4.3362	4.3364	4.3312	4.3421	4.3416	4.3412	4.3241	4.3267
Standard Deviation	0.0045	0.0043	0.0045	0.0045	0.0044	0.0045	0.0046	0.0046	0.0043	0.0042
Interquartile Range	4.3561	4.3341	4.3381	4.3342	4.3298	4.3435	4.3436	4.3423	4.3200	4.3299

Table 3.6: Statistical Analysis of Device B Gyroscope for 10 Runs



Device B	Run 1	Run 2	Run 3	Run 4	Run 5	Run 6	Run 7	Run 8	Run 9	Run 10
Mean	7.5771	7.5772	7.5714	7.5632	7.5709	7.5709	7.5724	7.5711	7.5681	7.5706
Standard Deviation	0.0980	0.1024	0.0998	0.0973	0.0983	0.0909	0.0955	0.0946	0.0900	0.0968
Interquartile Range	0.1385	0.1398	0.1373	0.1225	0.1373	0.1200	0.1203	0.1284	0.1327	0.1301

Table 3.7: Statistical Analysis of Device C Gyroscope for 10 Runs



Device C	Run 1	Run 2	Run 3	Run 4	Run 5	Run 6	Run 7	Run 8	Run 9	Run 10
Mean	3.3617	3.3604	3.3617	3.3693	3.3681	3.3695	3.3688	3.3720	3.3666	3.3644
Standard Deviation	0.0046	0.0046	0.0049	0.0045	0.0047	0.0044	0.0048	0.0047	0.0049	0.0047
Interquartile Range	3.3606	3.3586	3.3556	3.3691	3.3677	3.3708	3.3746	3.3683	3.3662	3.3716

3.5 Summary

PUF uses internal environment of the device to create a key at run time. Thus by using a PUF based system key theft can be prevented and the PUF based generated key can also be used for many cryptographic services such as identification, authentication and group key generation.

This chapter has studied various features suitable for the creation of a PUF ID. Embedded sensors are by design delicate components and are influenced by the fabrication process. This influence is seen as a sensor bias in the system. In this chapter the accelerometer and gyroscope sensors have been analyzed by studying their sensor bias to determine if it is a sufficient characteristic for the establishment of a PUF ID. Detailed analysis in the chapter has shown that there is sufficient bias in the sensor and that the sensors readings have uni-modular characteristics. This quality indicates that the readings from a sensor are unpredictable as a single sensor will provide an output within a particular range as long as the stimulus remains the same.

CHAPTER 4: ANALYSIS

To show there is significant similarity in the population generated by sensors, analysis of variance (ANOVA) is used [47]. ANOVA is a statistical technique that is used for the comparison between datasets. ANOVA was invented by a statistician R.A. Fisher that why this method is also known as Fisher's ANOVA. It is much similar to z-test and t-test in technique, because it also compares relative variance and means between datasets. When 2 or more than 2 datasets need to be compared ANOVA is used. ANOVA proves that the population/samples calculated are equal and there is no significant difference in the mean. To perform ANOVA, some assumptions need to be made. All the assumptions needed to be satisfied before ANOVA can be applied. These assumptions are as follows [48]:

1. **Independence of case**: Independence of case assumption means that the case of the dependent variable should be independent or the sample should be selected randomly. There should not be any pattern in the selection of the sample.
2. **Normality:** Distribution of each group should be normal. The Kolmogorov-Smirnov or the Shapiro-Wilk test may be used to confirm normality of the group.
3. **Homogeneity**: Homogeneity i.e. variance between the groups should be the same. Levene's test may be used to test the homogeneity between groups.

If particular data follows the above assumptions, then the analysis of variance (ANOVA) is the best technique to compare the means of two, or more, populations.

ANOVA is distributed in to three types.

1. **One way analysis**: One way ANOVA is used when three or more groups are compared based on the single factor.

2. **Two way analysis**: This analysis is used when two or more groups are compared based on the more than two factors.
3. **K-way analysis**: This analysis is used when the factor variables are K in number.

In this case one-way analysis was used as number of groups are 10 and variable factor is one which is root sum square (RSS) values generated in each run.

To analyze statistical significance most important indicator is p-value. The p-value determines whether the null hypothesis is accepted or rejected. In ANOVA null hypothesis is that there is a significant similarity in all groups or the mean is same for all groups, that's one hypothesis. Alternate hypothesis is that for all groups mean is not the same. p-value plays important part in the acceptance or rejection of null hypothesis. If p-value is less than significant value which is 0.05 $(p < 0.05)$ than it can b said that null hypothesis is rejected and there is a significant difference between means or not all means are equal. If $p > 0.05$ it can be said that there is a significant similarity in the datasets or mean is same for all groups so null hypothesis is accepted.

The important point or question for statistician is about the location of mean in the population that is based on certain levels of confidence. When curves don't follow normal distribution these level of confidence gains particular importance as it determines the population mean and its location. The confidence interval (CI) is used to determine in which interval mean is lying most commonly used CI are 99%, 95% and 90% To prove the bias in the sensors the confidence interval of 95% is used.

4.1 Accelerometer

To generate fingerprint of a device it needs to be statistically proven that values generated by single sensors are similar. So ANOVA is applied to all three devices lets apply all three assumptions on the Accelerometer values first.

4.1.1 Device A

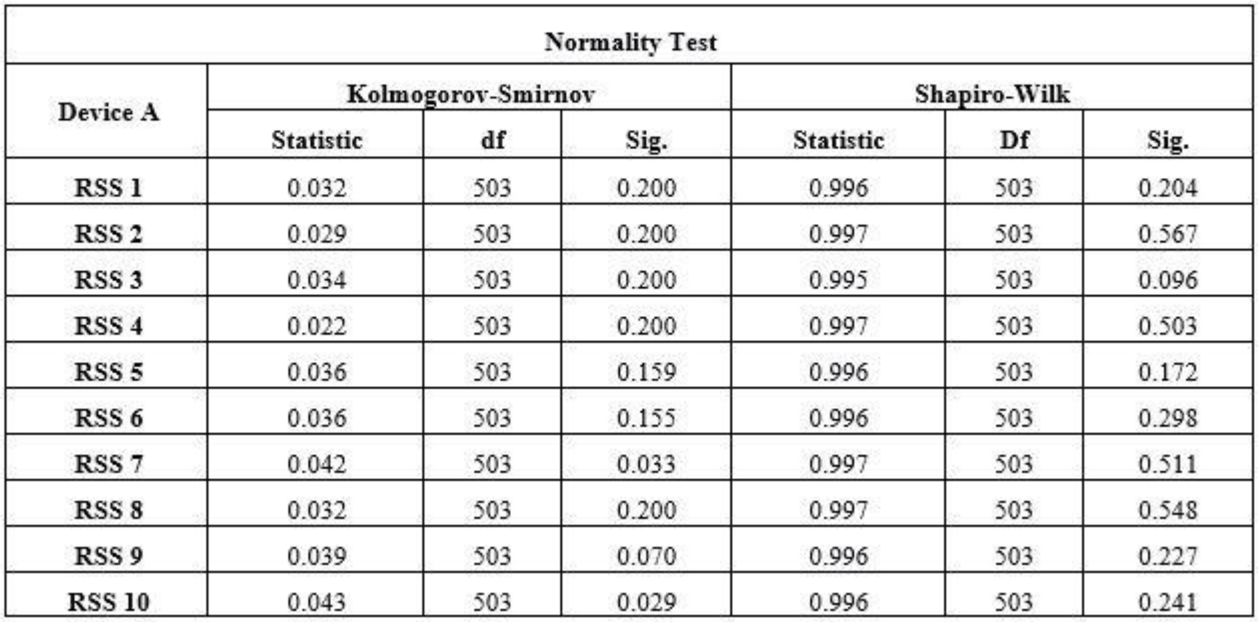
4.1.1.1 Assumption 1

All the offsets values collected for every round are independent of each other and are random.

4.1.1.2 Assumption 2

To perform ANOVA on the calculated RSS of samples it needs to be confirmed that data collected is normalized as it is the pre requisite for ANOVA. Normality of the data is checked by running two tests, Shapiro-Wilk and Kolmogorov-Smirnov. These tests are performed on root sum square of every run using IBM SPSS tool. According to Shapiro-Wilk Test if p-value is greater than significance value (p-value $>$ α-value) then the data is normalized. As confidence interval is set to 95% so α-value is 0.05. Results shown in Table 4.1, Kolmogorov-Smirnov p-value/sig of RSS 1 is 0.200 which is more than 0.05 similarly p-value is 0.204 when Shapiro-Wilk test is performed and even in Shapiro-Wilk test p-value is greater than 0.05 thus according to both test RSS 1 is normalized. Similarly, both tests are applied on every other RSS, in RSS 7 and RSS 10 p-value is 0.033 and 0.029 which is less than 0.05 thus sample is not normalized but in Shapiro-Wilk test p-values are 0.511 in RSS 7 and 0.241in RSS 10 which is greater than the α-value. 0.05 In case there is contradiction in both the test result Shapiro-Wilk test is preferred [49]. By analyzing the Shapiro-Wilk it is clear all the RSS are normalized.

Table 4.1: Results for the Normality Test When Tests are Applied on Device A

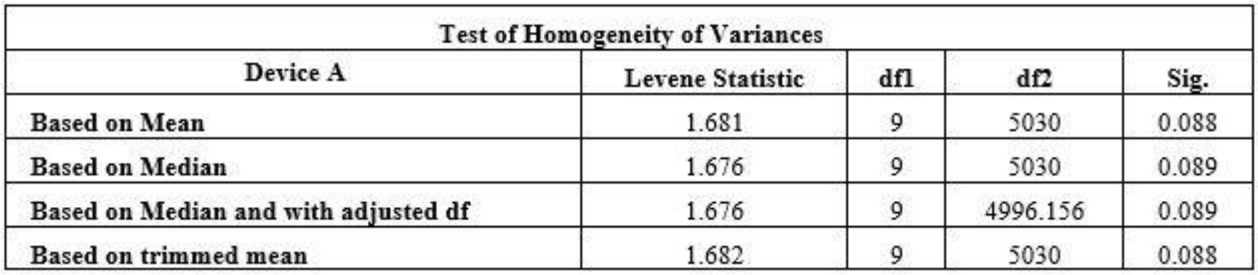


Normality Test						
Device A	Kolmogorov-Smirnov			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	Df	Sig.
RSS 1	0.032	503	0.200	0.996	503	0.204
RSS 2	0.029	503	0.200	0.997	503	0.567
RSS 3	0.034	503	0.200	0.995	503	0.096
RSS 4	0.022	503	0.200	0.997	503	0.503
RSS 5	0.036	503	0.159	0.996	503	0.172
RSS 6	0.036	503	0.155	0.996	503	0.298
RSS 7	0.042	503	0.033	0.997	503	0.511
RSS 8	0.032	503	0.200	0.997	503	0.548
RSS 9	0.039	503	0.070	0.996	503	0.227
RSS 10	0.043	503	0.029	0.996	503	0.241

4.1.1.3 Assumption 3

For third assumption it needed to be proved that variance of the data is homogenous. IBM SPSS was used to perform the Homogeneity of Variances test. Table 4.2 shows the result based on mean it can be seen that p-value 0.088 is higher than α-value 0.05 which proves the hypothesis that all variances are homogenous. Similarly, for others it is also clear that p-value is higher so assumptions is satisfied.

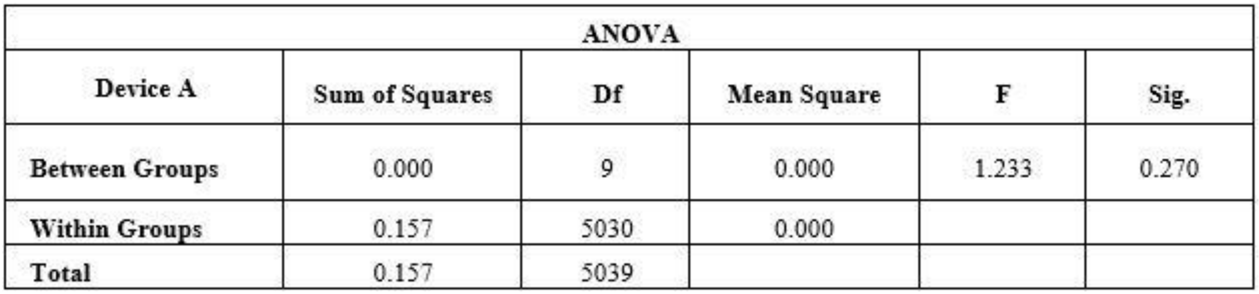
Table 4.2: Results for the Homogeneity Test When Tests are Applied on Device A



Test of Homogeneity of Variances				
Device A	**Levene Statistic**	**df1**	**df2**	**Sig.**
Based on Mean	1.681	9	5030	0.088
Based on Median	1.676	9	5030	0.089
Based on Median and with adjusted df	1.676	9	4996.156	0.089
Based on trimmed mean	1.682	9	5030	0.088

As all three assumptions are satisfied now one-way ANOVA can be applied on the samples to compare the means of population. By analyzing the results in Table 4.3 generated by ANOVA it can be seen that p-value is 0.270. As $0.270 > 0.05$ (p-value $> \alpha$-value) null hypothesis is accepted and proved that the collected mean contain a significant similarity. As mean is similar statically it can also be said that population are similar.

Table 4.3: ANOVA for Accelerometer of Device A



ANOVA					
Device A	**Sum of Squares**	**Df**	**Mean Square**	**F**	**Sig.**
Between Groups	0.000	9	0.000	1.233	0.270
Within Groups	0.157	5030	0.000		
Total	0.157	5039			

4.1.2 Device B

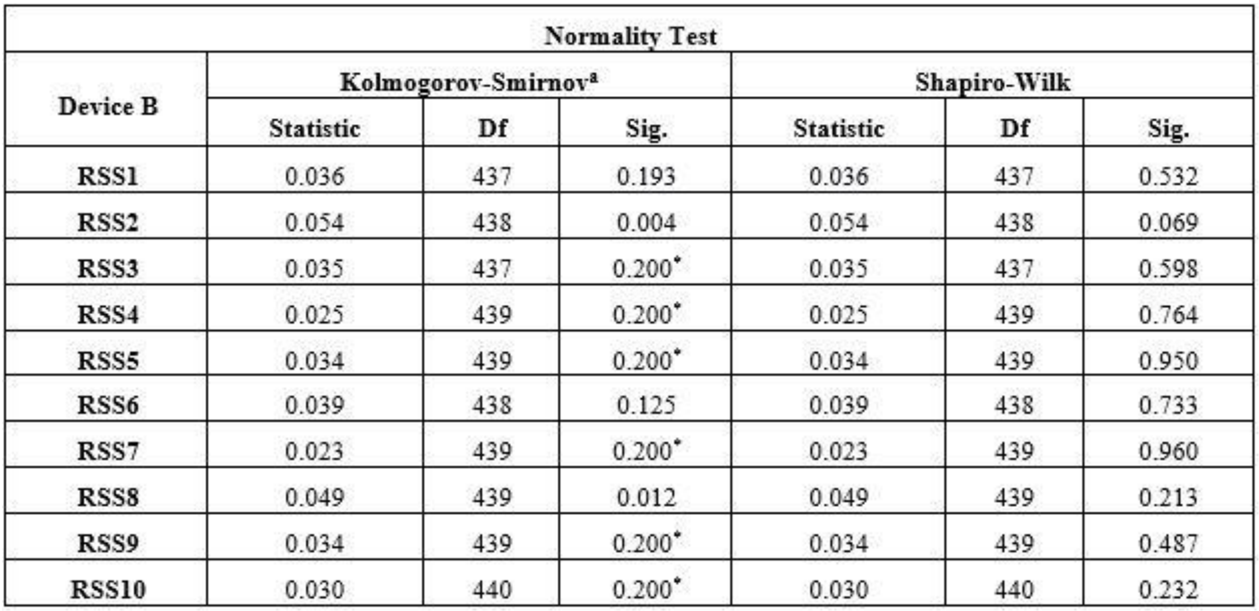
4.1.2.1 Assumption 1

For device B it is also ensured that data collected is random and independent of each other in every group.

4.1.2.2 Assumption 2

Shapiro-Wilk and Kolmogorov-Smirnov tests are performed using IBM SPSS tool on the data collected from Device B to prove the normality. Analysis of results generated by SPSS shows that data is normalized in both Kolmogorov-Smirnov and Shapiro-Wilk as shown in Table 4.4 with the exception of run 2 and run 8 in which (p-value < α-value) . It can be seen that p-value is 0.004 in Run 2 and in Run 8 p-value is 0.012. Both 0.004 & 0.012 are considerably less than the target α-value . In both runs for Shapiro-Wilk p-value is greater than 0.05 hence Shapiro-Wilk is considered [49].

Table 4.4: Results for the Normality Test When Tests are Applied on Device B

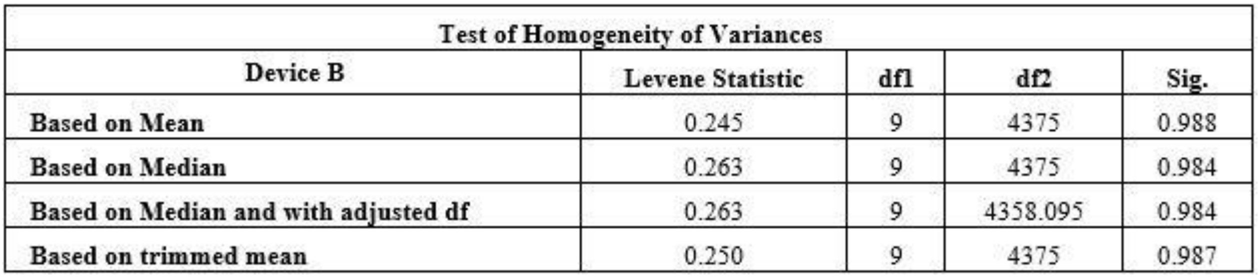


Normality Test						
Device B	Kolmogorov-Smirnov^a			Shapiro-Wilk		
	Statistic	Df	Sig.	Statistic	Df	Sig.
RSS1	0.036	437	0.193	0.036	437	0.532
RSS2	0.054	438	0.004	0.054	438	0.069
RSS3	0.035	437	0.200*	0.035	437	0.598
RSS4	0.025	439	0.200*	0.025	439	0.764
RSS5	0.034	439	0.200*	0.034	439	0.950
RSS6	0.039	438	0.125	0.039	438	0.733
RSS7	0.023	439	0.200*	0.023	439	0.960
RSS8	0.049	439	0.012	0.049	439	0.213
RSS9	0.034	439	0.200*	0.034	439	0.487
RSS10	0.030	440	0.200*	0.030	440	0.232

4.1.2.3 Assumption 3

For third assumption it needed to be proved that variance of the data is homogenous. IBM SPSS is used to perform the Homogeneity of Variances test. The result based on mean shows p-value 0.988 which is higher than α-value 0.05 as shown in Table 4.5 which proves the hypothesis that all variances are homogenous.

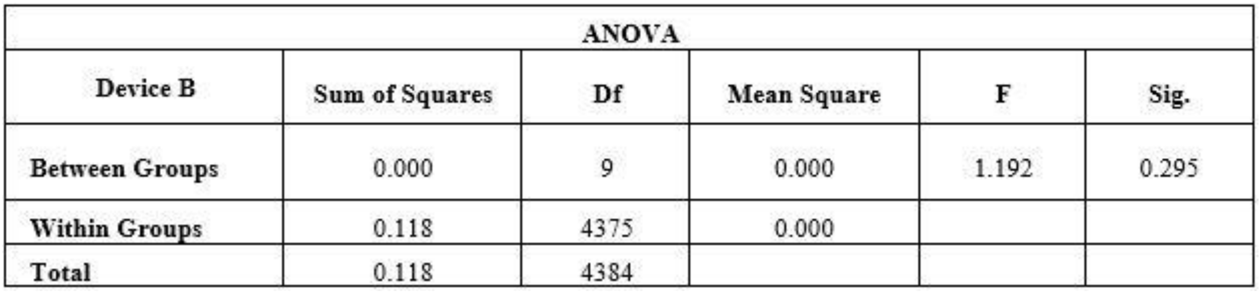
Table 4.5: Results for the Homogeneity Test When Tests are Applied on Device B



Test of Homogeneity of Variances				
Device B	Levene Statistic	df1	df2	Sig.
Based on Mean	0.245	9	4375	0.988
Based on Median	0.263	9	4375	0.984
Based on Median and with adjusted df	0.263	9	4358.095	0.984
Based on trimmed mean	0.250	9	4375	0.987

As all three assumptions are satisfied; now one-way ANOVA can be applied on the samples to compare the means of population. By analyzing the results generated by ANOVA it is clear that the there is significant similarity in the mean, as shown in Table 4.6 (p-value > α-value) $0.295 > 0.05$ null hypothesis is accepted. As mean is similar statically it can also be said that the populations are similar.

Table 4.6: ANOVA for Accelerometer of Device B



ANOVA					
Device B	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	0.000	9	0.000	1.192	0.295
Within Groups	0.118	4375	0.000		
Total	0.118	4384			

4.1.3 Device C

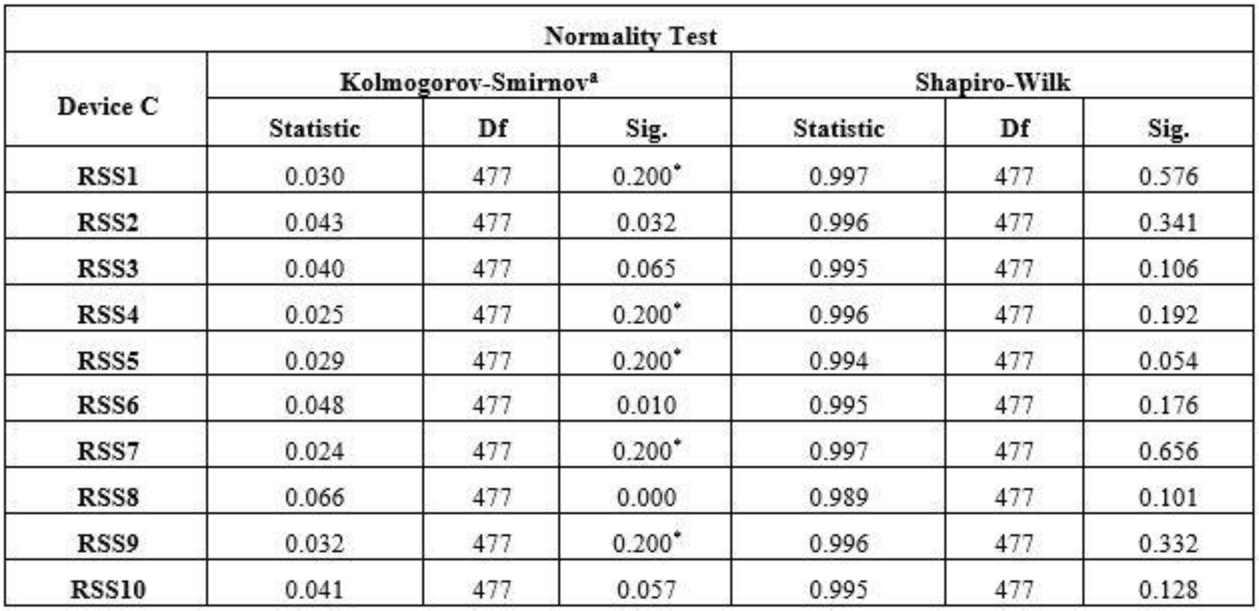
4.1.3.1 Assumption 1

For device C it is also ensured sure that data collected is random and independent of each other in every group.

4.1.3.2 Assumption 2

Shapiro-Wilk and Kolmogorov-Smirnov tests are performed using IBM SPSS tool on the data collected from Device B to prove the normality. Analysis of results generated by SPSS shown in Table 4.7 that data is normalized on both cases in Kolmogorov-Smirnov and Shapiro-Wilk with the exception of run 2, run 6 and run 8 in which (p-value < α-value). It can be seen that p-value in Run 2 is 0.032 which is considerably less than 0.05, while in run 6 and run 8 the p-value is 0.010 and 0.000 respectively which is again less than the target α-value. As there are values in Kolmogorov-Smirnova which prove the null hypothesis so Shapiro-Wilk is considered as all the p-value in Shapiro-Wilk tests are greater than 0.05 [2].

Table 4.7: Results for the Normality Test When Tests are Applied on Device C

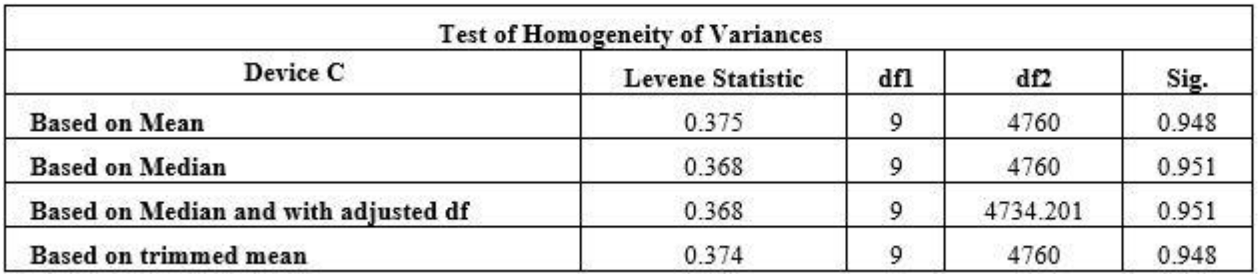


Normality Test						
Device C	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	Df	Sig.	Statistic	Df	Sig.
RSS1	0.030	477	0.200*	0.997	477	0.576
RSS2	0.043	477	0.032	0.996	477	0.341
RSS3	0.040	477	0.065	0.995	477	0.106
RSS4	0.025	477	0.200*	0.996	477	0.192
RSS5	0.029	477	0.200*	0.994	477	0.054
RSS6	0.048	477	0.010	0.995	477	0.176
RSS7	0.024	477	0.200*	0.997	477	0.656
RSS8	0.066	477	0.000	0.989	477	0.101
RSS9	0.032	477	0.200*	0.996	477	0.332
RSS10	0.041	477	0.057	0.995	477	0.128

4.1.3.3 Assumption 3

For third assumption it needed to be proved that variance of the data is homogenous. IBM SPSS is used to perform the Homogeneity of Variances test. The result based on mean shows p-value 0.988 which is higher than α-value 0.05 as shown in Table 4.8 which proves the hypothesis that all variances are homogenous

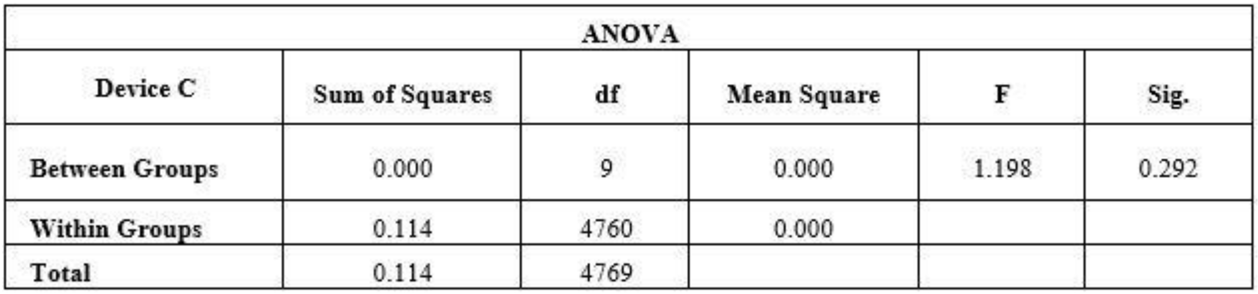
Table 4.8: Results for the Homogeneity Test When Tests are Applied on Device C



Test of Homogeneity of Variances				
Device C	Levene Statistic	df1	df2	Sig.
Based on Mean	0.375	9	4760	0.948
Based on Median	0.368	9	4760	0.951
Based on Median and with adjusted df	0.368	9	4734.201	0.951
Based on trimmed mean	0.374	9	4760	0.948

As all three assumptions are satisfied, now one-way ANOVA can be applied on the samples to compare the means of population By analyzing the results generated by ANOVA it is clear that the there is significant similarity in the mean, as shown in Table 4.9 (p-value > α-value) $0.292 > 0.05$ null hypothesis is accepted. As mean is similar statically it can also be said that the populations are similar.

Table 4.9: ANOVA for Accelerometer of Device C



ANOVA					
Device C	**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	0.000	9	0.000	1.198	0.292
Within Groups	0.114	4760	0.000		
Total	0.114	4769			

4.2 Gyroscope

Two features are being used to generate the fingerprint. The data collected from the accelerometer of MPU-6050 is analyzed in the above section. In this section data gyroscope is analyzed. Data is collected from the 3 different MPU-6050 devices and every device is run for 10 times. Then to perform ANOVA all three assumptions are verified and proved that data collected from one device is significantly similar or mean is same for all the runs.

4.2.1 Device A

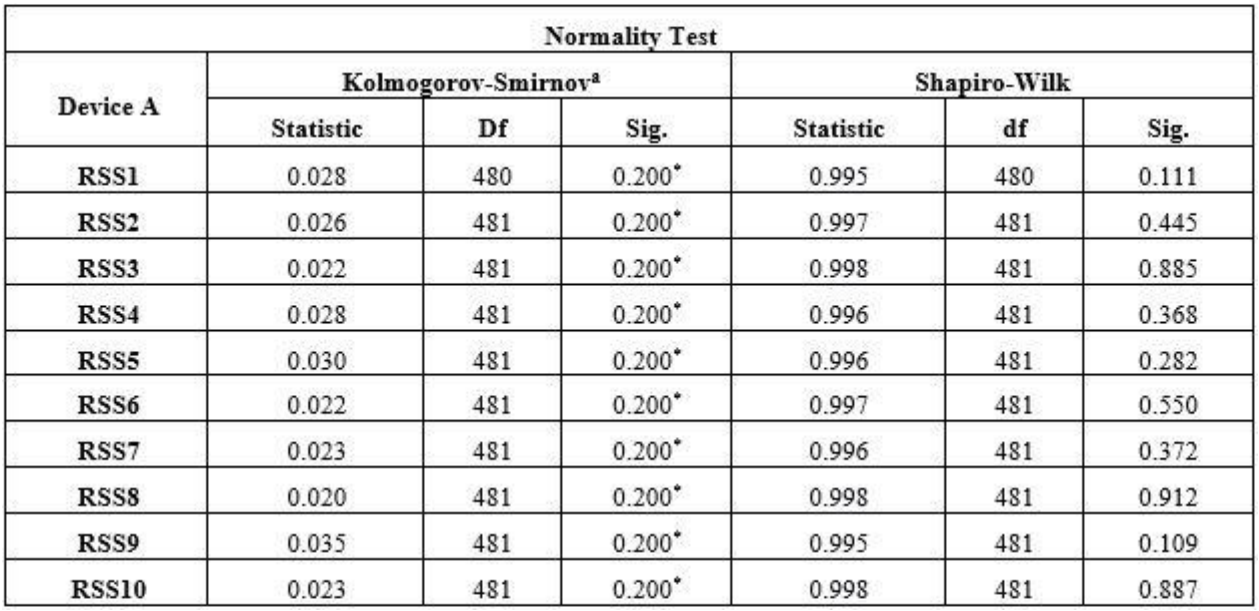
4.2.1.1 Assumption 1

All the offsets values collected for every round are independent of each other and are random.

4.2.1.2 Assumption 2

Data is collected in 10 runs of 10 second each. For each run root sum square is calculated. Normality of the data is checked by running two tests, Shapiro-Wilk and Kolmogorov-Smirnov . These test are performed on root sum square of every run using IBM SPSS tool. As discussed if p-value or sig value is greater than α-value than data is normalized whereas α-value is 0.05. As it can be seen in Table 4.10 every p-value (sig) value is greater than α-value (p-value $>$ α-value) which prove that data is normalized.

Table 4.10: Results for the Normality Test When Tests are Applied on Device A

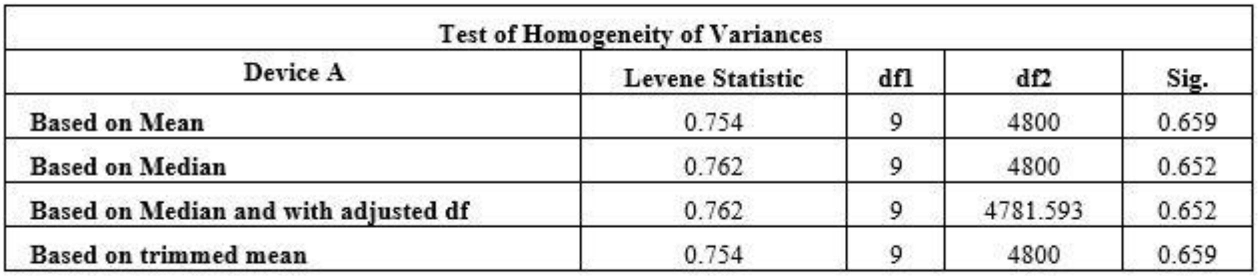


Normality Test						
Device A	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	Df	Sig.	Statistic	df	Sig.
RSS1	0.028	480	0.200*	0.995	480	0.111
RSS2	0.026	481	0.200*	0.997	481	0.445
RSS3	0.022	481	0.200*	0.998	481	0.885
RSS4	0.028	481	0.200*	0.996	481	0.368
RSS5	0.030	481	0.200*	0.996	481	0.282
RSS6	0.022	481	0.200*	0.997	481	0.550
RSS7	0.023	481	0.200*	0.996	481	0.372
RSS8	0.020	481	0.200*	0.998	481	0.912
RSS9	0.035	481	0.200*	0.995	481	0.109
RSS10	0.023	481	0.200*	0.998	481	0.887

4.2.1.3 Assumption 3

To prove the third assumption Leven test is used that shows the homogeneity of variance in the data collected from Device A as shown in Table 4.11 that (p-value $>$ α-value).

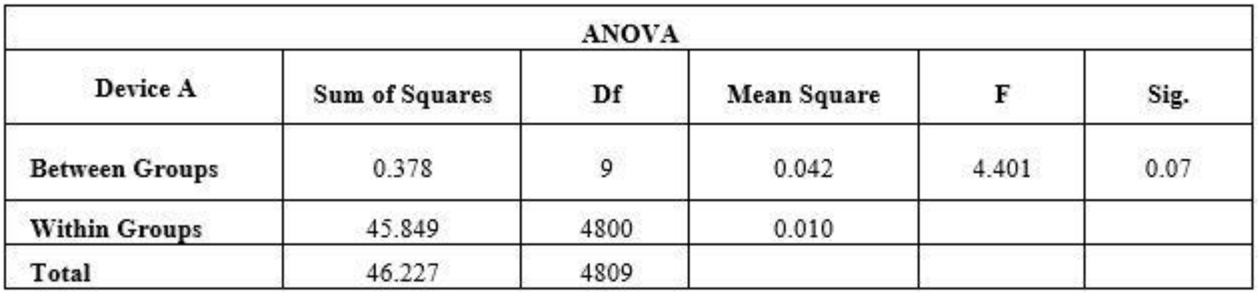
Table 4.11: Results for the Homogeneity Test When Tests are Applied on Device A



Test of Homogeneity of Variances				
Device A	Levene Statistic	df1	df2	Sig.
Based on Mean	0.754	9	4800	0.659
Based on Median	0.762	9	4800	0.652
Based on Median and with adjusted df	0.762	9	4781.593	0.652
Based on trimmed mean	0.754	9	4800	0.659

As all three assumptions are satisfied, now one-way ANOVA can be applied on the samples to compare the means of population. By analyzing the results generated by ANOVA it is clear that the there is significant similarity in the mean, as shown in Table 4.12Table 4.6 (p-value > α-value) $0.07 > 0.05$ null hypothesis is accepted. As mean is similar statically it can also be said that the populations are similar

Table 4.12: ANOVA for Gyroscope of Device A



ANOVA					
Device A	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	0.378	9	0.042	4.401	0.07
Within Groups	45.849	4800	0.010		
Total	46.227	4809			

4.2.2 Device B

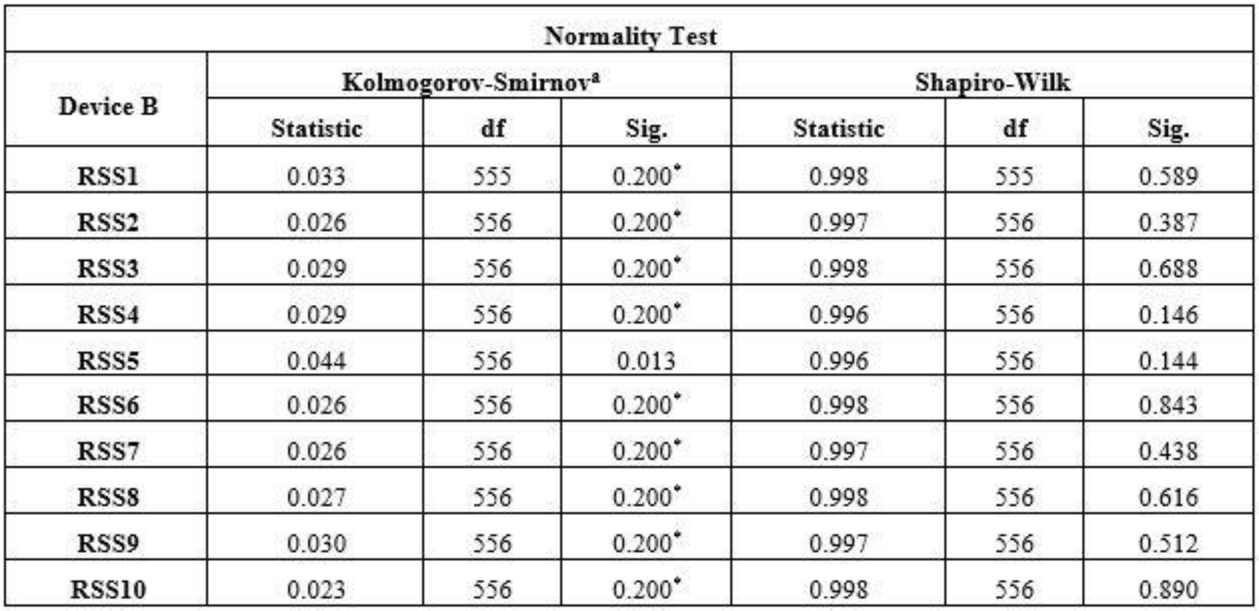
4.2.2.1 Assumption 1

For device B it is also ensured sure that data collected is random and independent of each other in every group.

4.2.2.2 Assumptions 2:

Data is collected in 10 runs of 10 second each. For each run root sum square is calculated. Normality of the data is checked by running two tests, Shapiro-Wilk and Kolmogorov-Smirnov . These test are performed on root sum square of every run using IBM SPSS tool. As discussed if p-value or sig value is greater than α-value than data is normalized whereas α-value is 0.05. As it can be seen in Table 4.13 that every p-value (sig) value is greater than α-value (p-value $>$ α-value) which prove that data is normalized.

Table 4.13: Results for the Normality Test When Tests are Applied on Device B

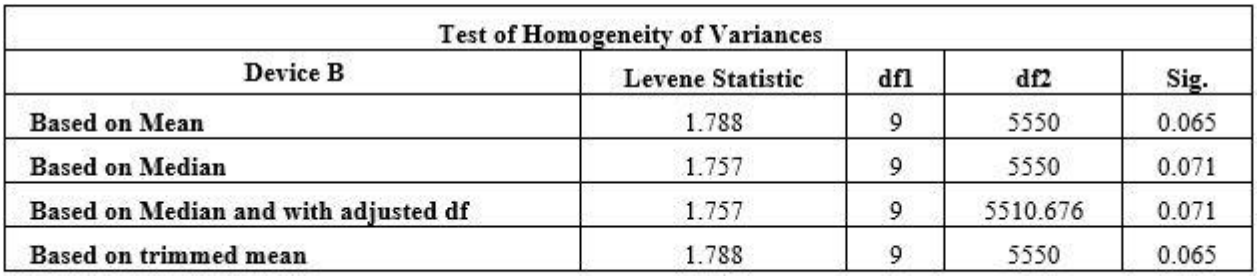


Normality Test						
Device B	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
RSS1	0.033	555	0.200*	0.998	555	0.589
RSS2	0.026	556	0.200*	0.997	556	0.387
RSS3	0.029	556	0.200*	0.998	556	0.688
RSS4	0.029	556	0.200*	0.996	556	0.146
RSS5	0.044	556	0.013	0.996	556	0.144
RSS6	0.026	556	0.200*	0.998	556	0.843
RSS7	0.026	556	0.200*	0.997	556	0.438
RSS8	0.027	556	0.200*	0.998	556	0.616
RSS9	0.030	556	0.200*	0.997	556	0.512
RSS10	0.023	556	0.200*	0.998	556	0.890

4.2.2.3 Assumption 3

To prove the third assumption Leven test is used that shows the homogeneity of variance in the data collected from Device A as shown in Table 4.14 that (p-value $(sig) > \alpha$-value).

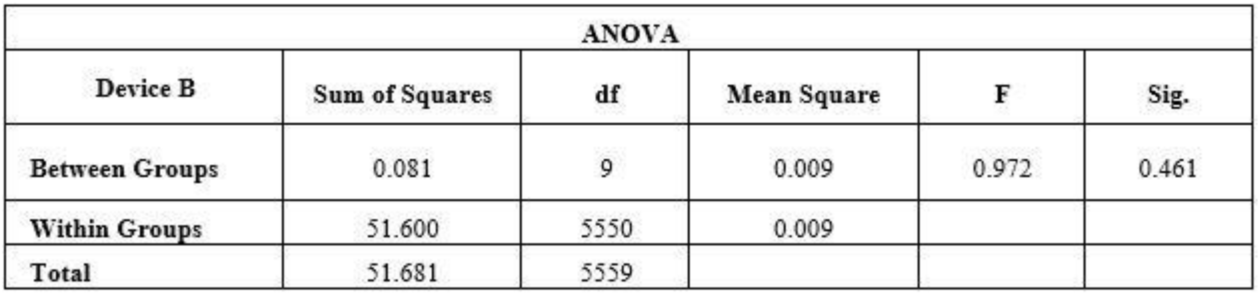
Table 4.14: Results for the Homogeneity Test When Tests are Applied on Device B



Test of Homogeneity of Variances				
Device B	Levene Statistic	df1	df2	Sig.
Based on Mean	1.788	9	5550	0.065
Based on Median	1.757	9	5550	0.071
Based on Median and with adjusted df	1.757	9	5510.676	0.071
Based on trimmed mean	1.788	9	5550	0.065

As all three assumptions are satisfied, now one-way ANOVA can be applied on the samples to compare the means of population. By analyzing the results generated by ANOVA it is clear that the there is significant similarity in the mean, as shown in Table 4.15 Table 4.6 (p-value > α-value) $0.461 > 0.05$ null hypothesis is accepted. As mean is similar statically it can also be said that the populations are similar.

Table 4.15: ANOVA for Gyroscope of Device B



ANOVA

Device B	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	0.081	9	0.009	0.972	0.461
Within Groups	51.600	5550	0.009		
Total	51.681	5559			

4.2.3 Device C

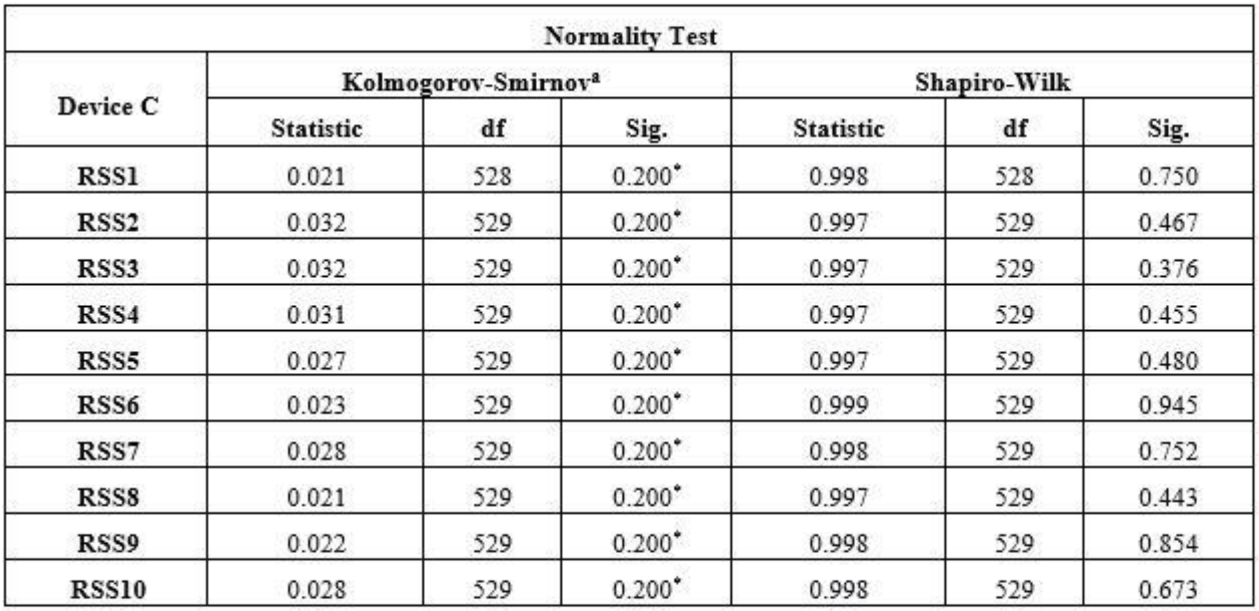
4.2.3.1 Assumption 1

For device C it is also ensured sure that data collected is random and independent of each other in every group.

4.2.3.2 Assumption 2

Data is collected in 10 runs of 10 second each. For each run root sum square is calculated. Normality of the data is checked by running two tests, Shapiro-Wilk and Kolmogorov-Smirnov . These test are performed on root sum square of every run using IBM SPSS tool. As discussed if p-value or sig value is greater than α-value than data is normalized whereas α-value is 0.05. As it can be seen in Table 4.16 every p-value (sig) value is greater than α-value (p-value $>$ α-value) which prove that data is normalized.

Table 4.16: Results for the Normality Test When Tests are Applied on Device C

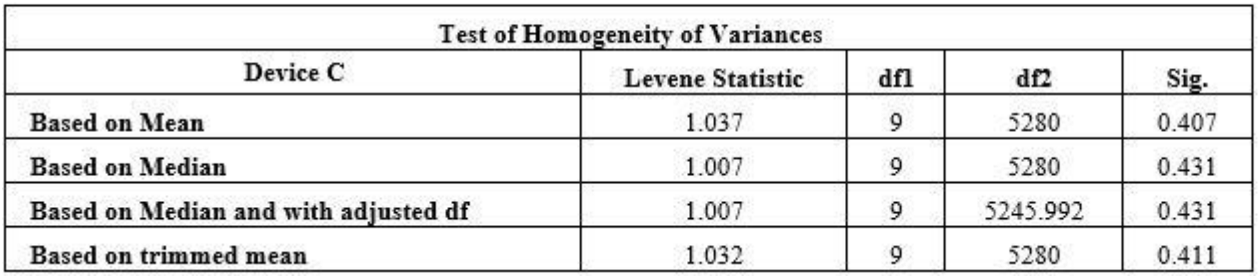


Normality Test						
Device C	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
RSS1	0.021	528	0.200*	0.998	528	0.750
RSS2	0.032	529	0.200*	0.997	529	0.467
RSS3	0.032	529	0.200*	0.997	529	0.376
RSS4	0.031	529	0.200*	0.997	529	0.455
RSS5	0.027	529	0.200*	0.997	529	0.480
RSS6	0.023	529	0.200*	0.999	529	0.945
RSS7	0.028	529	0.200*	0.998	529	0.752
RSS8	0.021	529	0.200*	0.997	529	0.443
RSS9	0.022	529	0.200*	0.998	529	0.854
RSS10	0.028	529	0.200*	0.998	529	0.673

4.2.3.3 Assumption 3

To prove the third assumption Leven test is used that shows the homogeneity of variance in the data collected from Device A as shown in Table 4.17 that (p-value (sig) $>$ α-value).

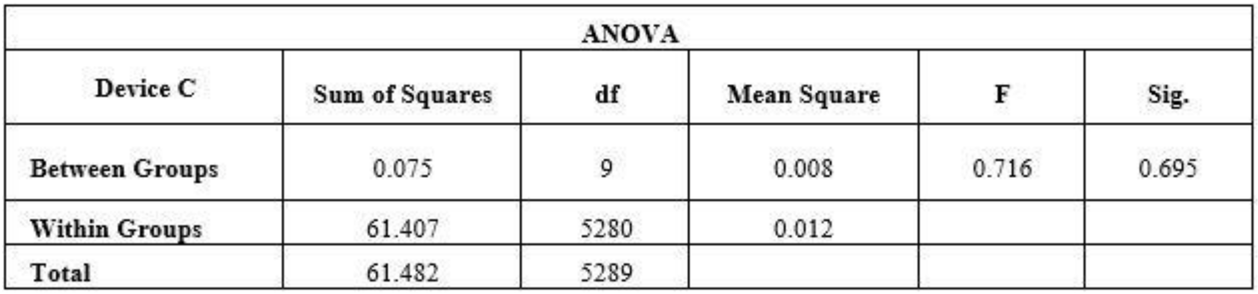
Table 4.17: Results for the Homogeneity Test When Tests are Applied on Device C



Test of Homogeneity of Variances				
Device C	Levene Statistic	df1	df2	Sig.
Based on Mean	1.037	9	5280	0.407
Based on Median	1.007	9	5280	0.431
Based on Median and with adjusted df	1.007	9	5245.992	0.431
Based on trimmed mean	1.032	9	5280	0.411

As all three assumptions are satisfied, now one-way ANOVA can be applied on the samples to compare the means of population. By analyzing the results generated by ANOVA it is clear that the there is significant similarity in the mean, as shown in Table 4.18Table 4.6 (p-value > α-value) $0.695 > 0.05$ null hypothesis is accepted. As mean is similar statically it can also be said that the populations are similar.

Table 4.18: ANOVA for Gyroscope of Device C



ANOVA					
Device C	**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	0.075	9	0.008	0.716	0.695
Within Groups	61.407	5280	0.012		
Total	61.482	5289			

4.3 Summary

Many systems are now provide MEMS sensors capability like gyroscope and accelerometer. It is studied that these sensors possess a biasness in the data collected from these sensors. By performing statistical analysis on the data collected by the sensors, it is clear that values collected from one sensor shows a significant similarity and show these values can be used to create a PUF for this device as in every single run values are generated are similar and there is no significant difference between them.

CHAPTER 5: AUTHENTICATION

Designing a scheme for secure authentication is a difficult task as achieving higher security can reduce system efficiency. With the increase in computation powers it is even harder to achieve the task as the adversary resources cannot be predicted. Therefore it is important to ensure that the scheme and its basis is mathematically sound. This is obvious when considering RSA or schemes based on RSA as both are based on the factorization problem. It is important to make sure of two things, one that scheme follows the cryptographic workflow and the other is the correct functioning of the system. In this chapter an analysis of the PUF scheme is done to show that a PUF_{ID} generated through using PUF technology is not producible by the adversary and PUF_{ID} cannot be extracted from the hash of the PUF_{ID}. Later an authentication scheme is presented which can be used for the device authentication using PUF_{ID}. The notations are used in this chapter are given in Table 5.1.

Table 5.1: Table of Notations

PUF	Physical unclonable function
PUF_{ID}	Unique Id of the device generated using PUF
PUF'_{ID}	PUF'_{ID} generated by Adversary
$f(x\ )$	PUF generation algorithm that accepts challenge/ input x
y	Output of PUF generation algorithm
I	Set of all feature that can be used to create PUF
i	Set of feature that are used to generate PUF specific to device
i_1	A single feature of the device
$f'(\ )$	PUF generation algorithm used by adversary to create adversarial PUF
$H(\ )$	Hash function
X	Input of hash function
Y	Output of hash function
Y'	Output of hash generated using PUF'_{ID}
$PBKDF$	Password Based Key Derivation Function

ID	ID of the device such as IMEI used to identify device uniquely
$Salt$	Random Number to be used for input of PBKDF and freshness of key

5.1 Security of PUF

Here it is important to prove that in comparison to conventional cryptography, PUFs can provide higher levels of security. The PUF device generates the keys at run time and the PUF_{ID} can only be compromised if the adversary have the PUF_{ID}device thus leaving the security of the whole system compromised. Security of the PUF is compromised if adversary successfully forges all the features that are used to generate the PUF_{ID}.

PUF is generated by using specific device features. These features are a unique property of the device. PUF functions like a black-box and is fundamentally a challenge and response method. PUF receives a challenge x and a response y is generated such that the response cannot be used to reveal the inner functioning of the PUF. It can be simplified as $y = f(x)$ where $f(\,)$ is the PUF generation algorithm. The response generated to the challenge x is unique for the device and can be used as a unique device signature.

5.2 Reroducibility of the PUF

To authenticate itself, an adversary can try to reproduce the PUF_{ID} by guessing the features of the device. The security of the authentication is strong if the adversary cannot reproduce the PUF_{ID} even if to some feature of the device can be accessed by adversary.

Assuming I represents a complete set of features that can be used to generate PUF and i are feature specific to that device. If a feature $i \in I$ is sent to $f(\,)$, a PUF generation algorithm $f(\,)$ will produce a unique PUF_{ID} for the device. If a subset feature i_1 such that $i_1 \in i$ is sent to the adversary as a challenge, the adversary will try to generate a response using the adversarial PUF $f'(\,)$ and use different software and hardware to produce an adversarial response $y_a = f'(\,i_1\,)$. On the basis of knowledge of i_1 adversary later sends the forged response back to challenger in an attempt to falsely authenticate itself.

If response generated by adversary $y_a = f'(\,i_1\,)$ is identical to the legitimate device response $y = f(\,i_1\,)$ then $f'(\,i_1\,) \equiv f(\,i_1\,)$ holds and adversary has successfully generated the legitimate response and can create a PUF_{ID} to authenticate. If $f'(\ i_1\ ) \neq f(\ i_1\ )$ than adversary will not be authenticated.

PUF_{ID} is generated using a collection of device features which makes it difficult for an adversary to forge a PUF_{ID}. A commonly used scheme in cryptography is the one-way hash function. Hashing functions can be defined as “Hash functions are mathematical computations that take in a relatively arbitrary amount of data as input and produce an output of a fixed size. The inputs to a hashing function are typically called messages and the outputs are often referred to as message digests” [50]. Input of hashing function can be many types such text, network packets and binary files. An application of hashing function is that it can be used to check the integrity of data as when given the same input hashing function will always produce the same output. So any unauthorized change in file, text, network traffic or in any arbitrary data can be detected by using the message digest [50].

Being a one-way function means that it is impossible to learn anything about the message if hash of the message is given. Collision resistant property in hashing means that finding another input that produces the same output (called a collision) is non-trivial. It is impossible or near impossible to find an input M' that generates the same hash Y [51]. When PUF_{ID} is used with hash function, it does not violate any of its properties. An attacker may try to find the $PUF_{ID}$from the hash of the PUF_{ID}. Such that $Y = H(X)$ where H is the publically known hash function, X is the input and Y is the hash generated. This action is not possible owing to the one way property of the hash functions.

If a feature $i \in I$ is sent to $f(\ )$, a PUF generation algorithm $f(\ )$should produce a unique PUF_{ID} for the device. The resulting PUF_{ID} is then used to create a hash by providing PUF_{ID} as input to hash function. Hash function can be known to both, adversary and challenger as it could be any publicly available hash function. Challenger creates the PUF_{ID} by using a set of already defined hardware and software features and creates a hash of the PUF_{ID} such that $Y = H(PUF_{ID})$. Challenger then sends that hash Y to authenticate itself.

Adversary creates $PUF_{ID}{}'$ from known set of feature and create hash Y' such that $Y' = H(PUF'_{ID})$ and sends the hash Y' back to the challenger. Challenger receives Y' and computes an outcome. If $Y' = Y$ then adversary has successfully generated a PUF_{ID} from given hash or found a value which can generate the same hash as Y. If $Y' \neq Y$ then adversary is unsuccessful in generating PUF_{ID} from given hash and challenger has won.

5.3 Authentication Protocol

In this section authentication protocol for PUF devices is proposed and discussed. Two schemes are presented that can be used for authentication of PUF device. So no adversary can falsely authenticate itself and only authorize device can authenticate. Some assumptions are also discussed in this section on which the protocol is based. For both authentication schemes the assumptions remains the same. In both schemes PUF device needs to register its PUF_{ID} with the authentication center. The registration protocol for both schemes remains the same.

5.3.1 Assumptions

The protocol is performed on the basis of following set of assumptions:

1. The structure of protocol consists of a PUF device and authentication center to perform the registration and identification processes during the authentication session.
2. The PUF devices can register with the authentication center using secure communication channels during the registration phase.
3. The communication channels between the authentication entities during the authentication phase are susceptible to various attacks.
4. The authentication center can verify the identities of a PUF device by sending a set of the authentication messages.

5.3.2 Design Requirements

To resist against the attacks, both schemes needs to follow these design requirements;

1. Pseudo random numbers produced by authentication center.
2. Hash functions to hide the $PUF_{ID}$of the devices.
3. $PBKDF$ to create sessions keys that are used for authentication process.

5.3.3 Registration Phase

In registration phase, each PUF device must sign itself into the authentication center. The communication channels are secured between the PUF devices and authentication center during the registration phase. For the first time, PUF device needs to register itself with the authentication center. PUF device generates its PUF_{ID} and its hash is sent to authentication center. PUF_{ID} will be stored against a unique ID of the device and authentication center will use this ID to recognize which hash of $PUF_{ID}$to be used in future. In this scenario, authentication center is a trusted party. Authentication center saves the hash of PUF_{ID} denoted by sig $H(PUF_{ID})$ against the PUF devices and later uses it when device need to authenticate themselves over the insecure channel.

5.3.4 Authentication Phase

In this phase, two authentication schemes are discussed in detail. Both schemes follow the same registration phase as discussed before and have similar assumptions.

5.3.4.1 Scheme 1

Initially, the authentication entities have the following data:

1. Each PUF device can generate its PUF_{ID}at run time.
2. Each PUF device have a unique identity such as the IMEI of a device called ID
3. Authentication center contains the Hash $PUF_{ID}$of PUF device.
4. Input parameters of $PBKDF$ $H(PUF_{ID})$ as password, $salt$ as salt, SHA512 as hash function, 64 bytes as key length (512 bit Key) and iteration counts.

Figure 5.1 shows the steps and protocol used for authentication of PUF devices. To start authentication, PUF device sends an authentication request message to authentication center that it needs to authenticate. This message contains the request Req to authenticate with its unique ID. The ID is used by authentication center to recognize which device is trying to authenticate. Once the Req and ID is received by Authentication center, Authentication center send the Authentication challenge back to PUF device on the basis of ID. The authentication challenge message has a random number $salt$. PUF device creates a PUF_{ID} at run time as $PUF_{ID}$is not stored. Then it creates a hash of PUF_{ID} $H(PUF_{ID})$. $PBKDF$ receives following parameters as inputs $H(PUF_{ID})$ as password, $salt$ as salt, SHA512 as hash function, 64 bytes as key length and iteration counts. $PBKDF$ used these input to generates a key. This key is used for encryption in this session only. $H(PUF_{ID})$ is concatenated with $salt$ and encrypted with key such as $key[H(PUF_{ID}) \,||\, salt]$ and is transferred to authentication center.

Authentication center uses the $H(PUF_{ID})$ stored against ID use $salt$ and other parameters similar to the PUF device and sends it to the Password Based Key Derivation Function $PBKDF$.

The $PBKDF$ receives $H(PUF_{ID})$ as password, $salt$ as salt, SHA512 as hash function, 64 bytes as key length and iteration counts as input and creates key as output. Authentication center uses this key to decrypt message sent by PUF device. Authentication center verifies if the $H(PUF_{ID})$ is equal to the one stored in database. If it gets verified then the device is recognized as the only device that can generate a $H(PUF_{ID})$. $Salt$ is also verified to check if it is the same $salt$ sent as Authentication challenge to PUF device. This step also verifies the freshness of the key.

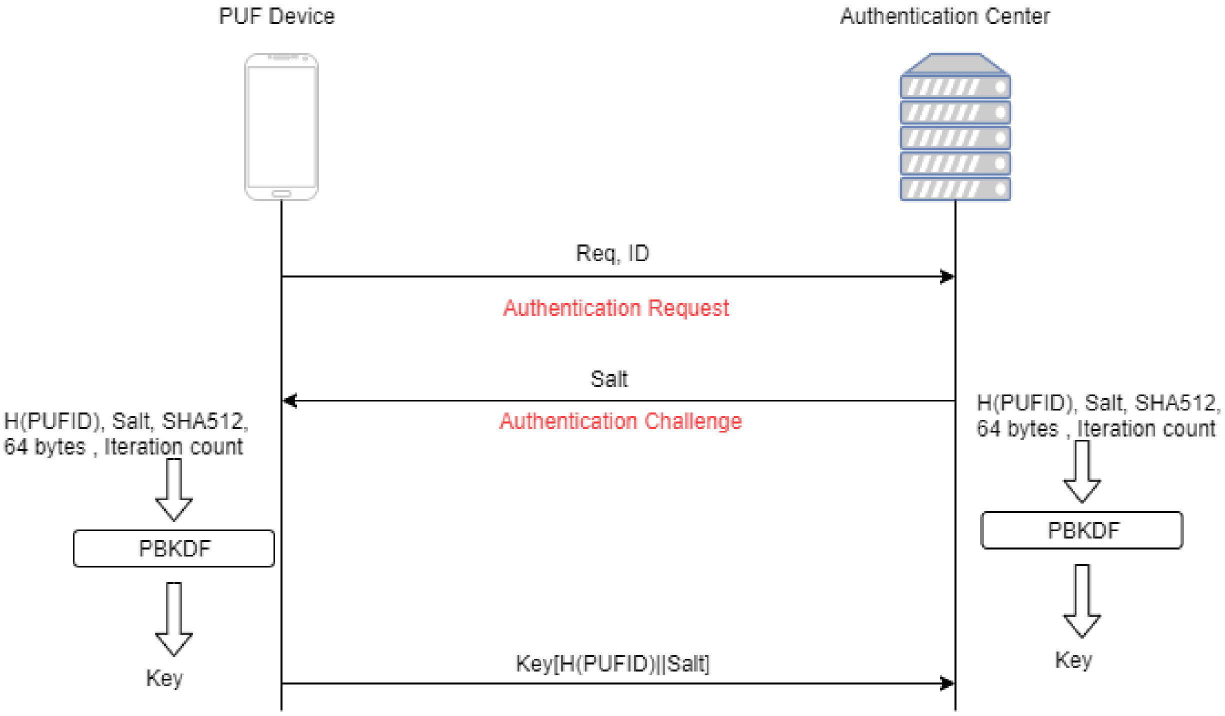


Figure 5.1: Authentication Scheme 1

5.3.4.2 Scheme 2

Initially, the authentication entities have the following data:

(1) Each PUF device can generate its PUF_{ID}at run time.

(2) Each PUF device can create a unique identity such as the IMEI of a device called ID.

(3) Authentication center contains the Hash $PUF_{ID}$of PUF Device.

(4) Input parameters of $PBKDF$ $H(PUF_{ID})$ as password, $salt$ as salt, SHA512 as hash function, 64 bytes as key length (512 bit Key) and iteration counts

Figure 5.2 shows the steps and protocol used for authentication of PUF devices. To start the authentication, the PUF device sends authentication center an authentication request message that it need to authenticate. This message contains the request Req to authenticate with its unique ID. ID is used by Authentication center to recognize which device is trying to authenticate. Once the Req and ID is received by Authentication center, Authentication center uses the $H(PUF_{ID})$ stored against ID and a randomly generated $salt$ and send it to $PBKDF$. $PBKDF$ receives $H(PUF_{ID}), salt$, SHA512, 64 bytes and iteration count as input and creates key as output. Authentication center creates hash of $salt$ and uses key to encrypt $H(salt)$. Authentication center concatenates $salt$ with encrypted hash of salt and sends this as Authentication challenge to PUF device. Authentication challenge is $key[H\ (salt)]\ ||\ salt]$

PUF device receives the Authentication challenge and uses the $salt$ that was received via Authentication message concatenated with encrypted $H(salt)$. PUF device creates a PUF_{ID} at run time and create its hash $H(PUF_{ID})$. PUF device sends $H(PUF_{ID}), salt$, SHA512, 64 bytes and iteration count to $PBKDF$ as input and $PBKDF$ creates a key as output.

PUF device uses this to decrypt $H(salt)$ in Authentication message and verifies this $H(salt)$ with $salt$. If the hash of $salt$ is similar to $H(salt)$ then it is verified that this message is sent by Authentication center as key is generated by using $H(PUF_{ID})$ and $salt$, and $H(PUF_{ID})$ can only be used by Authentication center as it is stored in the database and no other party can create $H(PUF_{ID})$. Once verified, PUF device concatenates $salt$ with $H(PUF_{ID})$ and encrypts it with key generated for this session $key\,[H(PUF_{ID})\ ||\ salt]$ and sends it to Authentication center.

Authentication center uses the key generated above to decrypt the message sent by PUF device. Authentication center verifies if the $H(PUF_{ID})$ is equal to the one stored in the database, if yes then the device is verified as is PUF device because it is the only device that can generate a $H(PUF_{ID})$. $Salt$ is also verified if it is the same $salt$ sent within Authentication challenge to PUF device. This will also verify the freshness of the key.

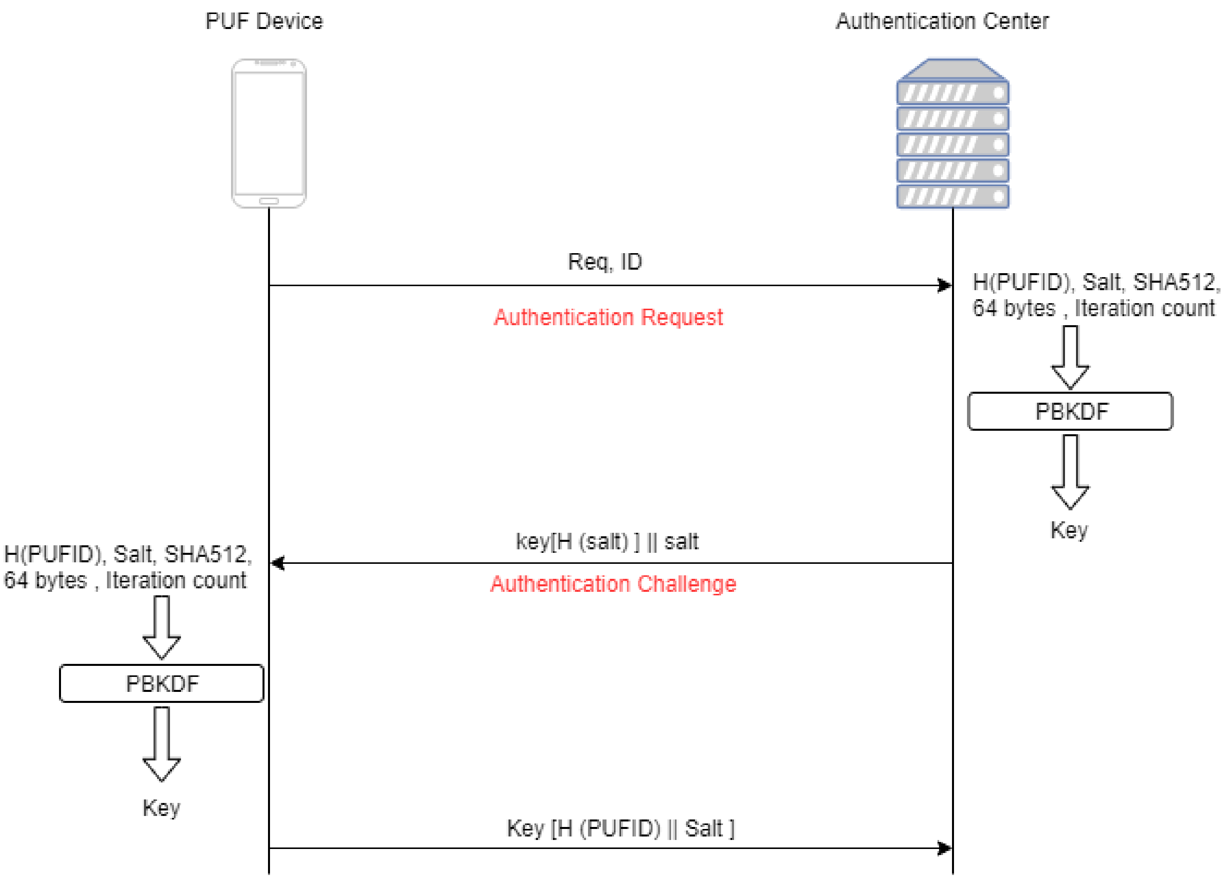


Figure 5.2: Authentication Scheme 2

5.3.5 Security Analysis

Security analysis of schemes discussed above is demonstrated in this section. PUF based device authentication protocol can provide both secure and multifaceted security features.

In these schemes, only a legitimate authentication center has the $H(PUF_{ID})$ that can be used for authentication. When transmitted via insecure channel, PUF_{ID} is hashed and even $H(PUF_{ID})$ is encrypted with session keys which can only be generated by authorized entities. Therefore only verified entities can encrypt and decrypt the messages.

Assuming that authentication messages are intercepted by adversary as result of eavesdropping. Also, that the adversary can use these authentication messages to impersonate as authentication entity, these protocols remains secure as messages are either hashed or encrypted. If a message is sent in plaintext later it can be verified that messages have not been tampered with because adversary cannot create session's key as it cannot create $H(PUF_{ID})$. If authentication is not successful, the protocol will be terminated and the whole process will be reinitiated.

It is suspected that in the process of authentication, all channels that are used to communicate between PUF device and authentication center are susceptible to attacks. Therefore hash values and random numbers are used for mutual authentication. In scheme 2, authentication center sends hash of $salt$ encrypted with key. The key can only be generated by the party who is in possession of $H(PUF_{ID})$. When PUF device successfully decrypts $H(salt)$ and verifies that it is the $salt$ sent by authentication center, then authentication is successful and authentication center receives the encrypted data. Authentication center then successfully decrypts and verifies that mutual authentication has been achieved. In this protocol, if adversary tries to modify the $salt$ then $H(salt)$ will not be verified once decrypted and the authentication will be terminated.

5.4 Summary

In this chapter, schemes have been presented that uses the generated $PUF_{ID}$of a device to in cryptographic algorithms. Many cryptographic elements such as hashing, $PBKDF$ and salts are used together with PUF to create keys. As with PUF technology, it is impossible to steal PUF_{ID} because this depends on the inherent sensor features. The PUF_{ID} can be used for authentication. By incorporating $salt$ with PUF_{ID} and $PBKDF$, it will be difficult for an attacker to perform a brute force attack. $PBKDF$ is a function that takes a random salt, a secret entry or password and length of the key as input and generate the key. The length of the generated key is equal to length given as input and it can be increased and decreased according to the requirement.

CHAPTER 6: CONCLUSION AND FUTURE WORK

6.1 Conclusion

Most cryptographic schemes today rely on keys that are meant to be kept secret while the algorithm itself can be made public. Thus in most modern cryptographic schemes whether based on symmetric or asymmetric keys the success of the system lies in keeping the keys secret. This is in accordance with the Kerckhoff's principle which states that “only the secrecy of the key ensures security". Hence the theft of cryptographic keys can make the system vulnerable and this needs to be catered for in any system designed for security.

A cryptographic key is a block of hexadecimal data, where the size of the block ranges 80 to over 256 bits. Cryptographic keys cannot be remembered by human due to their data type and extensive size. To recall the keys when needed, keys are stored in the device [52]. The problem with storing keys on the device is that they can be attacked/stolen by the adversary using a variety of methods. Brute force attacks can be reduced by increasing the size of the keys [53], but has absolutely no impact on the prevention of key theft. This becomes even more critical on devices systems that are resource constrained or poorly implemented thereby presenting no hurdle to the adversary who is in search of a cryptographic key. To create more efficient cryptographic systems that are resilient to key theft, cryptographers now consider other sources of trust, such as Physically Unclonable Functions (PUF).

This thesis has studied the use of MEMS sensors as a suitable PUF. In chapter two a discussion on the deterrent qualities of PUF technology and key theft prevention has been presented. PUF technology allows a device to create an identity using inherent device characteristics. Device identity created using PUF, is used for key generation and authentication. As the keys generated using only when needed PUF technology can be used to deter key thefts as keys can be discarded with any associated data after its used. This makes it impossible for the adversary to find the key as the security keys are not stored anywhere in the system. Since the concept of PUF is based in the physical world therefore if an adversary wishes to attack the keying mechanism then physical access to the device will be needed along with specialized probes/ hardware to facilitate the extraction. Even in the presence of such resources the adversary would most probably fail as the PUF identity is not based on a single device feature.

In Chapter 3, MEMS sensors are used to test characteristics related to PUF generation. Therefore, the first noteworthy contribution of this work is to thoroughly examine the properties of the devices that can be used to generate the PUF. This chapter studies the MEMS accelerometer and gyroscope embedded on a device. The PUF identity is based on the operational bias found in the operations of the above mentioned inertial sensors. A sensor testbed has been established that is composed of identical sensors and a statistical analysis of data from sensors shows that the sensors have a uniqueness that can be used to generate PUF. Here the qualities required for the establishment of a PUF identity are uniqueness, stability, adversarial unpredictability and ease of reproducibility.

Chapter 4 analyzes the data collected from MEMS sensors and performs statistical analysis on it. The generated values are unique to each sensor and can be used to create PUF identifiers that can be used for cryptographic purposes.

Chapter 5 shows an authentication scheme that shows how to authenticate a device using PUF. It generates a key at runtime and sends authentication credentials over the internet in a secure manner thereby demonstrating the practicality of PUF in cryptographic schemes.

In complete, the thesis has demonstrated through research that PUF presents a novel root of trust that is entirely based on the device physical characteristics. Furthermore, the study has shown that a PUF identity can be created using MEMS sensors. Thus these inertial sensors have sufficient individuality which can then form the basis of any cryptographic scheme/ service.

6.2 Future Work

The thesis has demonstrated the use of various device features to create PUF of the device. The features considered in this thesis are in no way an exhaustive list. Therefore, the research should aim to find other features that can improve the strength of the device PUF.

Integrating web browser, operating system and network with PUF technology can be a new way to detect external and internal intrusions. The work can be extended in many interesting ways which should provide a heightened level of security.

As discussed in Chapter 3, MEMS sensors often behave differently due to aging, environmental factors, stress and fatigue [54]. The effect caused by these factors should be analyzed so impact on the PUF production process can be reduce to minimum. By incorporating a correction code in the PUF of the production process, the influence of external factors on the MEMS sensor can be significantly reduced.

Cryptographic and electronic payment systems are rapidly gaining popularity. PUF has not been tested in block chain and bitcoin. When integrated with Bitcoin, PUF technology ensures anonymity and facilitates trading secrets. This could be a very feasible venue of research.

This thesis shows that the integration of PUF technology in portable devices will enhance the confidentiality and security of the device and its users[55]. Research has been shown that it is feasible for a user to be identified through gait. An interesting study would be to combine biometric technology and PUF technology thereby creating a system that is secure and aids both the user and device.

Automated and intelligent vehicles get uses communication systems and on-board computers. One of the major barrier in introducing smart vehicles is the safety of these vehicles. To monitor the behavior of smart vehicles, the vehicles are made up of thousands of sensors these sensors can be used by the PUF for security services. PUF fusion technology and smart vehicles provide unprecedented security that traditional encryption systems cannot promise.

References

[1] R. Rajkumar and I. Lee, “NSF workshop on cyber-physical system,” 2006. [Online]. Available: http://varma.ece.cmu.edu./cps/presentations/workshop-intro.

[2] H. Gill, “NSF perscpective and status on cyber physical system.” [Online]. Available: http://varma.ece.cmu.edu/presentations/gill.pdf.

[3] L. Parolini, N. Tolia, B. Sinopoli, and B. H. Krogh, “A cyber-physical systems approach to energy management in data centers,” in *Proceedings of the 1st acm/ieee international conference on cyber-physical systems*, 2010, pp. 168–177.

[4] F. Zhang and Z. Shi, “Optimal and adaptive battery discharge strategies for cyber-physical systems,” in *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*, 2009, pp. 6232–6237.

[5] C. J. Xue, G. Xing, Z. Yuan, Z. Shao, and E. Sha, “Joint sleep scheduling and mode assignment in wireless cyber-physical systems,” in *Distributed Computing Systems Workshops, 2009. ICDCS Workshops’ 09. 29th IEEE International Conference on*, 2009, pp. 1–6.

[6] W. Jiang, G. Xiong, and X. Ding, “Energy-saving service scheduling for low-end cyber-physical systems,” in *The 9th International Conference for Young Computer Scientists*, 2008, pp. 1064–1069.

[7] J. Cao and H. Li, “Energy-efficient structuralized clustering for sensor-based cyber physical systems,” in *Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC’09. Symposia and Workshops on*, 2009, pp. 234–239.

[8] K.-D. Kang and S. H. Son, “Real-time data services for cyber physical systems,” in *Distributed Computing Systems Workshops, 2008. ICDCS’08. 28th International*

Conference on, 2008, pp. 483–488.

[9] L. Kong, D. Jiang, and M.-Y. Wu, “Optimizing the spatio-temporal distribution of cyber-physical systems for environment abstraction,” in *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on*, 2010, pp. 179–188.

[10] H. Ahmadi, T. F. Abdelzaher, and I. Gupta, “Congestion control for spatio-temporal data in cyber-physical systems,” in *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems*, 2010, pp. 89–98.

[11] V. Liberatore, “Bandwidth allocation in sense-and-respond systems,” *Report, Available at: http://home. case. edu/~ vxl11/NetBots*, 2015.

[12] M. Lindberg and K.-E. Arzen, “Feedback control of cyber-physical systems with multi resource dependencies and model uncertainties,” in *2010 31st IEEE Real-Time Systems Symposium*, 2010, pp. 85–94.

[13] Z. Xu, X. Liu, G. Zhang, W. He, G. Dai, and W. Shu, “A certificateless signature scheme for mobile wireless cyber-physical systems,” in *Distributed Computing Systems Workshops, 2008. ICDCS’08. 28th International Conference on*, 2008, pp. 489–494.

[14] W. Jiang, W. Guo, and N. Sang, “Periodic real-time message scheduling for confidentiality-aware Cyber-Physical System in wireless networks,” in *Frontier of Computer Science and Technology (FCST), 2010 Fifth International Conference on*, 2010, pp. 355–360.

[15] B. H. Krogh, “Cyber Physical Systems: the need for new models and design paradigms,” *Present. Rep.*, 2008.

[16] J. Shi, J. Wan, H. Yan, and H. Suo, “A survey of Cyber-Physical Systems,” in *2011 International Conference on Wireless Communications and Signal Processing, WCSP 2011*, 2011.

[17] B. Herzberg, D. Bekerman, and I. Zeifman, “Breaking down mirai: An IoT DDoS botnet analysis,” *Incapsula Blog, Bots DDoS, Secur.*, 2016.

[18] D. Genkin, L. Pachmanov, I. Pipman, A. Shamir, and E. Tromer, “Physical key extraction

attacks on PCs," *Commun. ACM,* vol. 59, no. 6, pp. 70–79, 2016.

[19] A. Rae and L. Wildman, "A taxonomy of attacks on secure devices," in *Proceedings of the Australia Information Warfare and Security Conference 2003,* 2003, pp. 251–264.

[20] A. Arnbak and N. A. N. M. van Eijk, "Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain," *Ssrn,* pp. 1–31, 2012.

[21] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," *Proc. 9th ACM Conf. Comput. Commun. Secur. - CCS '02,* p. 148, 2002.

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

[23] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentications and Secret Key Generation," *Proc. 44th Annu. Conf. Des. Autom. - DAC '07,* pp. 9–14, 2007.

[24] R. Maes, *Towards Hardware-Intrinsic Security,* no. October 2010. 2010.

[25] P. Tuyls, G.-J. Schrijen, B. Škorić, J. van Geloven, N. Verhaegh, and R. Wolters, "Read-Proof Hardware from Protective Coatings," in *Cryptographic Hardware and Embedded Systems - CHES 2006,* 2006, pp. 369–383.

[26] J. W. Lee, Daihyun Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," *2004 Symp. VLSI Circuits. Dig. Tech. Pap. (IEEE Cat. No.04CH37525),* pp. 176–179, 2004.

[27] D. LIM, "Extracting Secret keys from Integrated Circuits," 2004.

[28] B. L. P. Gassend, "Physical Random Functions," 2003.

[29] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," in *Cryptographic Hardware and Embedded Systems - CHES 2007,* 2007, pp. 63–80.

[30] D. E Holcomb, W. Burleson, and K. Fu, "Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags," 2007.

[31] S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, and P. Tuyls, "The Butterfly PUF protecting IP on every FPGA," *2008 IEEE Int. Work. Hardware-Oriented Secur. Trust. HOST*, no. 71369, pp. 67–70, 2008.

[32] J. D. R. Buchanan *et al.*, "'Fingerprinting' documents and packaging," *Nature*, vol. 436, p. 475, Jul. 2005.

[33] P. Bulens, F.-. Standaert, and J.-. Quisquater, "How to strongly link data and its medium: the paper case," *IET Inf. Secur.*, vol. 4, no. 3, pp. 125–136, Sep. 2010.

[34] O. Willers, C. Huth, J. Guajardo, and H. Seidel, "MEMS-based Gyroscopes as Physical Unclonable Functions," *Cryptol. ePrint Arch.*, no. 261, pp. 591–602, 2016.

[35] C. M.-E. C. of the EASST and undefined 2009, "Security and privacy challenges in the internet of things," *journal.ub.tu-berlin.de*.

[36] B. Stark, "MEMS reliability assurance guidelines for space applications," 1999.

[37] M. Sheehy, J. Punch, S. Goyal, M. Reid, M. Lishchynska, and G. Kelly, "The Failure Mechanisms of Micro-Scale Cantilevers Under Shock and Vibration Stimuli," *Strain*, vol. 45, no. 3, pp. 283–294, 2009.

[38] D. S. Eddy and D. R. Sparks, "Application of MEMS technology in automotive sensors and actuators," *Proc. IEEE*, vol. 86, no. 8, pp. 1747–1755, 1998.

[39] D. Fonseca, M. S.-I. J. of Quality, and undefined 2011, "On MEMS reliability and failure mechanisms," *downloads.hindawi.com*.

[40] S. Dey, N. Roy, W. Xu, R. Choudhury, S. N.- NDSS, and undefined 2014, "AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable.," *pdfs.semanticscholar.org*.

[41] G. Baldini, G. Steri, F. Dimc, R. Giuliani, R. K.- Sensors, and undefined 2016, "Experimental identification of smartphones using fingerprints of built-in micro-electro mechanical systems (mems)," *mdpi.com*.

[42] K. Rosenfeld, E. Gavas, … R. K.-I. I. S., and undefined 2010, "Sensor physical unclonable functions," *ieeexplore.ieee.org*.

[43] I. Statistics-Vocabulary, “symbols-Part 2: Applied statistics,” 2006.

[44] P. Cappelletti and A. Modelli, “Flash Memory Reliability,” in *Flash Memories*, Boston, MA: Springer US, 1999, pp. 399–441.

[45] K. Unger and J. Novak, *Game development essentials: Mobile game development*. 2011.

[46] D. LeBlanc, *Statistics: concepts and applications for science*. 2004.

[47] “the Data Samples To Variation.”

[48] “Analysis Of Variance (ANOVA) - Statistics Solutions.” [Online]. Available: https://www.statisticssolutions.com/anova-analysis-of-variance/. [Accessed: 19-Nov-2018].

[49] H. C. Thode, *Testing for normality*, vol. 164. CRC press, 2002.

[50] J. Silva, “SANS Institute Information Security Reading Room An Overview of Cryptographic Hash Functions and Their Uses,” 2019.

[51] T. St. Denis and S. Johnson, *Cryptography for developers*. Syngress Pub, 2007.

[52] I. Kizhvatov, “Physical Security of Cryptographic Algorithm Implementations.” University of Luxembourg, Luxembourg, Luxembourg, 2011.

[53] Y. Xiao and Y. Pan, *Security in distributed and networking systems*, vol. 1. World Scientific, 2007.

[54] D. M. Tanner *et al.*, “MEMS reliability in shock environments,” in *2000 IEEE International Reliability Physics Symposium Proceedings. 38th Annual (Cat. No. 00CH37059)*, 2000, pp. 129–138.

[55] R. Tahir, H. Tahir, A. Sajjad, and K. McDonald-Maier, “A secure cloud framework for ICMetric based IoT health devices,” in *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*, 2017, p. 171.