**CHAPTER 1: INTRODUCTION**

* 1. **What is a PUF ?**

A Physical Unclonable Function or a PUF is a die – specific random function which is unique for every instance of the die. PUF’s derive their randomness from the uncontrolled random variations in the IC manufacturing process to create practically unclonable functions.

PUFs are recently produced by many Multi national Companies and are widely being used for their security applications because of their randomness nature. Some of the security applications are IP Piracy, Device Authentication, injecting a Hardware Trojan (HT) in the IC or an IP or an FPGA such that they can be made to use at evaluation time and then we can disrupt the functionality after the specified time.

PUFs also provide an interesting functionality when compared to other security devices is that we don’t need to store any of the secret bits in a volatile or a non – volatile memory instead we generate the responses for the PUF for evaluation.

* + 1. **Challenge and Response**

An input to a PUF is usually called the challenge and the generated output is typically called as the response for the PUF. An applied challenge and its response are generally knowns as the challenge-response pair (CRP). These terms are from the field of security, where challenge-response pair authentication is used to verify the information.

* 1. **Classification of PUF:**

PUFs are modelled as CRP’s (Challenge Response Pairs), which means that when we give a challenge(c) to the PUF we get a response(r). So, depending on the challenge we can we get different response. The mathematical representation is given as:

r = f(c), where the function represents the unique property of PUF.

Broadly PUFs can be classified into two categories:

**Weak PUF**: Used For key storage. A weak PUF (also called as Physically Obfuscated PUF’s) has a very small range such that we can have collisions with one or other challenges that give the same response. We define the Weak PUF function as r=F(.) where F(.) means it has only very small domain. Even though it can be used as a fingerprint to generate cryptographic functions, the number of responses of the weak PUF is related to the number of components subject to manufacturing variation. A weak PUF can have only some secret keys (i.e the domain range is less).

**Strong PUF**: Commonly used for authentication. Strong PUf’s have a large domain and supports a lot of CRP’s that means it can be used effectively and securely.

**Silicon and Non-Silicon Based PUFs:**

PUFs totally depend on variations in the circuit behavior. They are classified as silicon based PUFs where the PUFs are made up of digital circuits. These PUFs are used commercially which are designed and fabricated like any other Integrated circuit. Recently we use the fabric of the FPGA to make the silicon based PUFs. The other type of PUF is the non- silicon based PUF like the optical PUFs are said in the literature [2]. But due to their limitability in integrating with the circuit design we are not using it commercially.

**Physical Unclonable Functions: Metrics**

Just like other components which are distinguished based on metrics, even the PUF’s have the security metrics like uniqueness, randomness and reliability followed by the conventional VLSI metrics of area, power and performance.

Uniqueness:

Uniqueness (or inter-die randomness) is the measure of how random the response bits are across the dies. We can observe this by generating responses of different regions of the die for the same design files and technology. Since each bit on a die differs from one another because even the die is getting manufactured all the regions are not doped same. We exploit this behaviour for security authentication. Since we get new unique response bits in different regions of the die we can say that the PUF gives a good unique behaviour.

Randomness:

Randomness is a measure of