**PROJECT REPORT (CS203)**

**SUBMITTED TO:-** Dr. Neeraj Goyal

**SUBMITTED BY:-**

1. G Pradyumn 2018CSB1088

2. Arnav Bansal 2018CSB1075

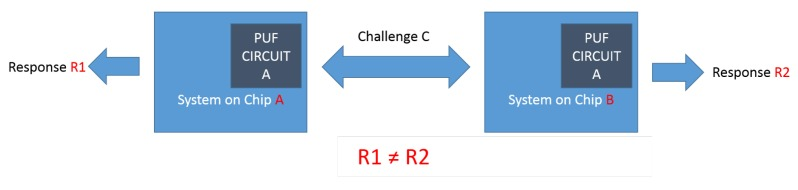
**PROJECT TITLE:-** A XOR Arbiter Physically Unclonable Function (PUF)

**WHAT IS A PUF?**

Physical Unclonable Functions (PUFs) emerged from the effort to bypass the drawbacks of non-volatile memory to store secret keys.

Authentication, authorization, and privacy are three sides of the security triangle in IoT. Authentication is the first barrier in front of cyber-attacks. Physical Unclonable Functions (PUFs) have been proposed as a lightweight, cost-efficient, and ubiquitous solution. Importantly for IoT developers, PUFs promise to achieve perfectly secure authentication without any cryptographic assets on the device, which makes them especially interesting for resource-scarce IoT devices.

Like humans, each chip has its own fingerprint, which is created during manufacturing. This intrinsic characteristic is extractable by adding a specific circuit architecture, a so-called PUF circuit, to the chip . PUF circuits receive a sequence of bits (alleged challenges) as the input and generate a sequence of bits (so-called responses) as the output. No two chips generate identical responses for a particular challenge. The combination of a challenge and its corresponding response is called a Challenge Response Pair (CRP).



Hence, it is pretty clear that the basic principle behind the working of PUF is the natural delay that is a property of every different module. No two modules have same kind of delay and hence the pattern can not be predicted by any hacker.

PUF is a really interesting concept in the world of cryptography; several kinds of PUFs are made.

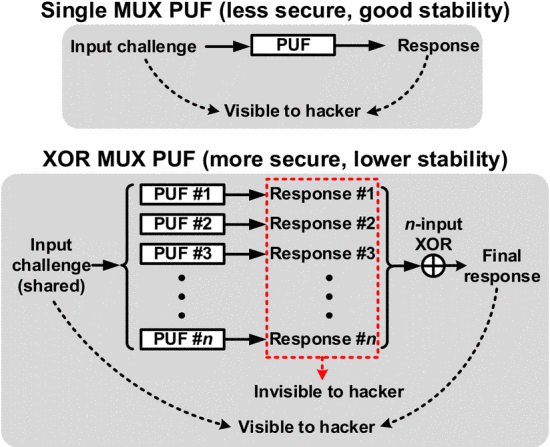
We in our project have worked on XOR Arbiter PUF.

**XOR Arbiter PUF**

Multiplexer (MUX) based arbiter Physical Unclonable Function (PUF) is a promising candidate for hardware authentication applications as the total number of challenge response pairs (CRPs) is an exponential function of the number of delay stages. Security, stability, requirement, test complexity, and authentication time are important considerations when designing MUX arbiter PUFs. In particular, ensuring a stable and consistent response across a wide range of temperature, voltage, and aging conditions is a critical challenge. When the arbiter compares two path delays with a small delay difference, random thermal noise can cause intermittent errors. To overcome this issues, an authentication strategy based on only stable CRPs was recently proposed and verified through silicon data. Here, stable CRPs were selected based on “soft response” measurements, which indicate the degree to which a response is stable. Soft responses were measured using an on-chip counter that repeatedly samples the response for a given challenge to generate the average response value.

**Now, the question is why we are using a XOR gate after using MUX.**

The basic principle is described in where a bank of PUFs presented with a common challenge generates *n* output responses, which are then XOR-ed together to produce the final 1-bit response. The premise for XOR PUFs is that estimating the responses of individual PUFs based on the final XOR output is very difficult and time-consuming. This is why XOR PUFs are believed to be more secure than standard MUX PUFs.

****

*REFERENCES*

1. <https://ieeexplore.ieee.org/document/7302326>
2. <https://ieeexplore.ieee.org/abstract/document/6132673>
3. <https://drive.google.com/open?id=0B_0nrCTw7HFkZElMcmFxcWhsTlB3ZU1qOFBOTDJ3NGxmYk5F>
4. <https://drive.google.com/open?id=0B_0nrCTw7HFkNFBUOWU1WDBpaXRHbkxPdXNnN01iNDQ1TmRB>
5. <https://drive.google.com/open?id=1p-_y1WDQWJVZDLyQrnsg-0K-GUm0eNL0>
6. <https://drive.google.com/open?id=1FM0hjWCeQ9aqmn1cuzrcqrMtQCtePOb1>