Introduction to VLSI (CSE 593)

Project Report

SECURE AND ENERGY EFFICIENT ARBITER BASED 32 BIT PUF

TEAM – I

Name: Anish Madurai Narayanamurthy
UB Person #: 50249279

Name: Avishek Deb
UB Person #: 50246426

Date: 12-08-2017

ABSTRACT

A PUF or Physically Unclonable Function is a “digital fingerprint” that serves as a unique identity for a semiconductor device. The PUF was conceptualised as a response to the basic problem of storing digital information in a device that is resistant to physical attacks and yet is inexpensive at the same time. It can be defined as a function in which for a given input the system produces a random or an unpredictable output which is unique to the system. This is the result of inherent process variations in the CMOS chip manufacturing process. This makes it impossible to fabricate two ICs with the exact same physical properties. Hence, there is a difference in delay and power characteristics of the ICs. Experiments[1] have been conducted in which identical circuits with identical layouts were placed on different FPGAs and it has been observed that the path delays vary enough across ICs to use them for identification purposes. This variation is leveraged for the unique identification of each IC.

PUFs implement the ***challenge-response authentication mechanism*** to evaluate a semiconductor device. When an input signal is applied, the circuit reacts in an unpredictable (but repeatable) way due to the complex interaction of the stimulus with the physical microstructure of the device. The exact microstructure depends on the physical factors introduced during manufacture which are unpredictable. The applied signal is called the challenge and the reaction of the PUF is called the response. A specific challenge and its corresponding response together form a challenge-response pair (CRP). As the physical structure of the device is not directly revealed by the challenge response mechanism, such a device is resistant to spoofing attacks. The term ‘unclonable’ in PUF means that each PUF device has a unique and unpredictable way of mapping challenges to responses even if it was manufactured with the same process as a similar device.

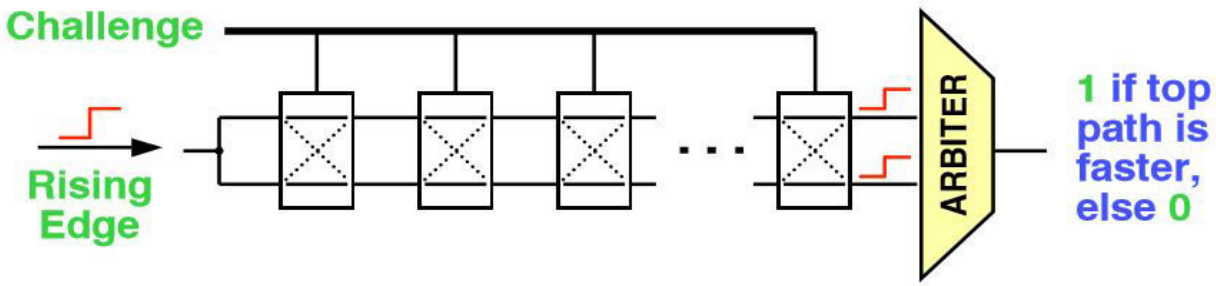


Figure 1: Operation of a PUF

Using a key extractor, PUFs can also be used to extract a unique strong cryptographic key from the physical microstructure. The same unique key is reconstructed every time the PUF is evaluated. The

challenge response mechanism is then implemented using cryptography.

Types of PUF

Usually PUFs are classified as Strong PUFs and Weak PUFs. Strong PUFs support a large number of inputs typically called as challenge response pairs (CRPs) and complete measurement of all CRPs within a feasible time frame is impossible. Hence, it is extremely difficult to break into a strong PUF even with the knowledge of a few CRPs. This makes it ideal for IC identification and secret key generation. For example, arbiter PUF, feed forward PUF, XOR arbiter PUF, light weight secure PUF. Weak PUF supports only a limited number of CRPs. Hence it is easier to break into a weak PUF. Examples include SRAM PUF, butterfly PUF, Physically Obfuscated Key (POK).

Quality of a PUF

The quality of a PUF is determined by three important metrices – *uniqueness, reliability* and *security*. Uniqueness is the most important property of a PUF and refers to the ability to distinguish between different ICs. It is measured in hamming distance between responses obtained from different PUF instances. Hamming distance is a parameter to measure the number of different elements of two strings of the same length. An ideal PUF has a relative hamming distance of 0.5.

Reliability refers to the fact that a PUF circuit must be capable of reproducing CRPs in the presence of noise and varying environmental conditions. Most PUF circuits use relative comparison to generate CRPs achieving a high degree of reliability.

Security indicates the susceptibility of a PUF circuit to different types of modeling attacks.

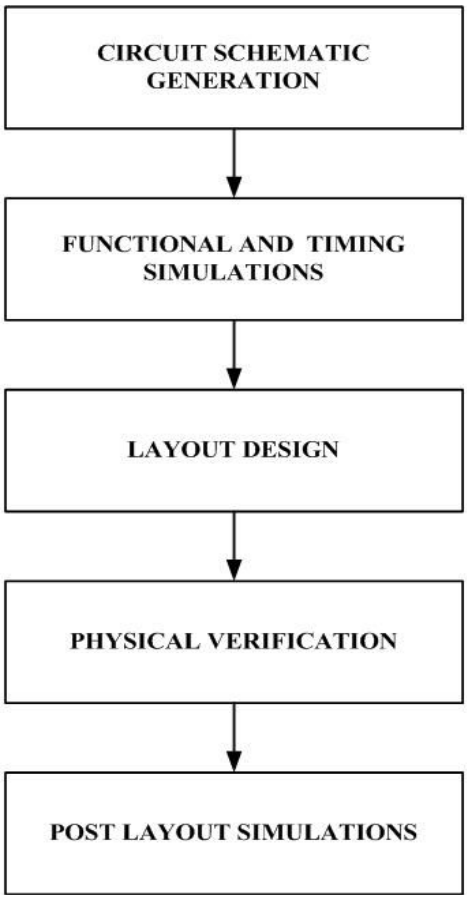
DESCRIPTION OF THE PROJECT

This project is about an Arbiter based 32 bit PUF which offers a strong PUF construction achieving high degree of uniqueness and reliability. The arbiter based PUF circuit is a representative of delay based PUFs such as feed-forward arbiter based PUFs and XOR arbiter PUFs.

The arbiter based PUF is constructed using 32 delay stages and an SR Latch as an arbiter. Each delay stage comprises of two multiplexers to which the inputs are connected. SR Latch serves as a better arbiter as compared to an edge triggered D Flip Flop due to a smaller bias. The challenge bits generated by the LFSR (Linear Feedback Shift Register) selects the path through which the top and bottom signals are passed and the response bit is decided by the arbiter based on the delay difference between the top and bottom signal arrival times at the final stage. The response bit is set

to a 1 if the top signal arrives early and vice versa. The delay difference at the final stage is a function of the path chosen through the 32 delay stages determined by the challenge bits. A 32-bit Arbiter PUF offers 2^{32} challenge response pairs making it a very robust PUF circuit capable of preventing replay attacks that can occur due to limited number of Challenge Response Pairs (CRP's). The CRPs are generated by a 32-bit Pseudo Random Number Generator (PRNG). The 32-bit PRNG has been implemented using a 32-bit Linear Feedback Shift Register.

DESIGN METHODOLOGY



CIRCUIT ELEMENTS

1 Clock, 1 Input, 32 delay stages, 32-bit LFSR, 2 XOR'S, SR latch Arbiter, 1 Output

SCHEMATIC OF THE CIRCUIT BLOCKS

The approach we took is to generate an 8-bit Arbiter PUF first and then cascade it to obtain a 32-bit Arbiter PUF.

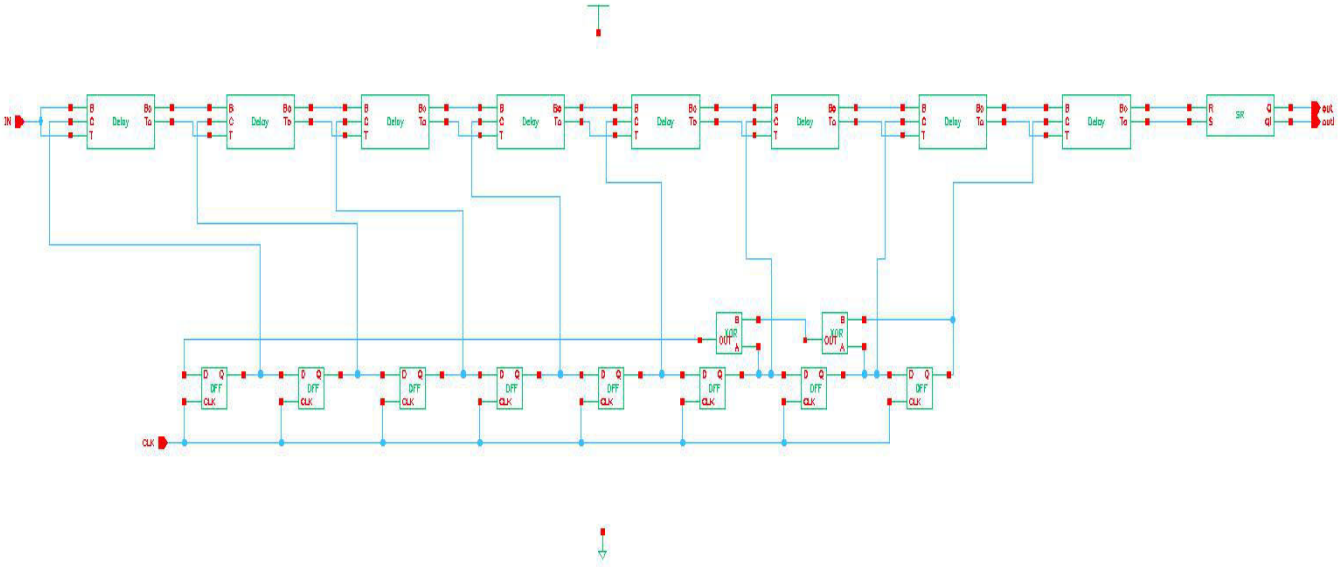


Figure 2: 8 bit Physically Unclonable Function schematic

Given above is the schematic of the 8-bit PUF. On top are the 8 delay stages (consisting of two multiplexers each) and the SR latch which acts as the arbiter. At the bottom is the Linear Feedback Shift Register (LFSR) which has been designed to generate an 8-bit challenge. It is a pseudo-random sequence of bits. The eight output nodes of the LFSR are connected to the eight delay stages respectively and select the path through which the top and bottom signals are passed. As can be observed there are only two input pins: the CLK and the IN.

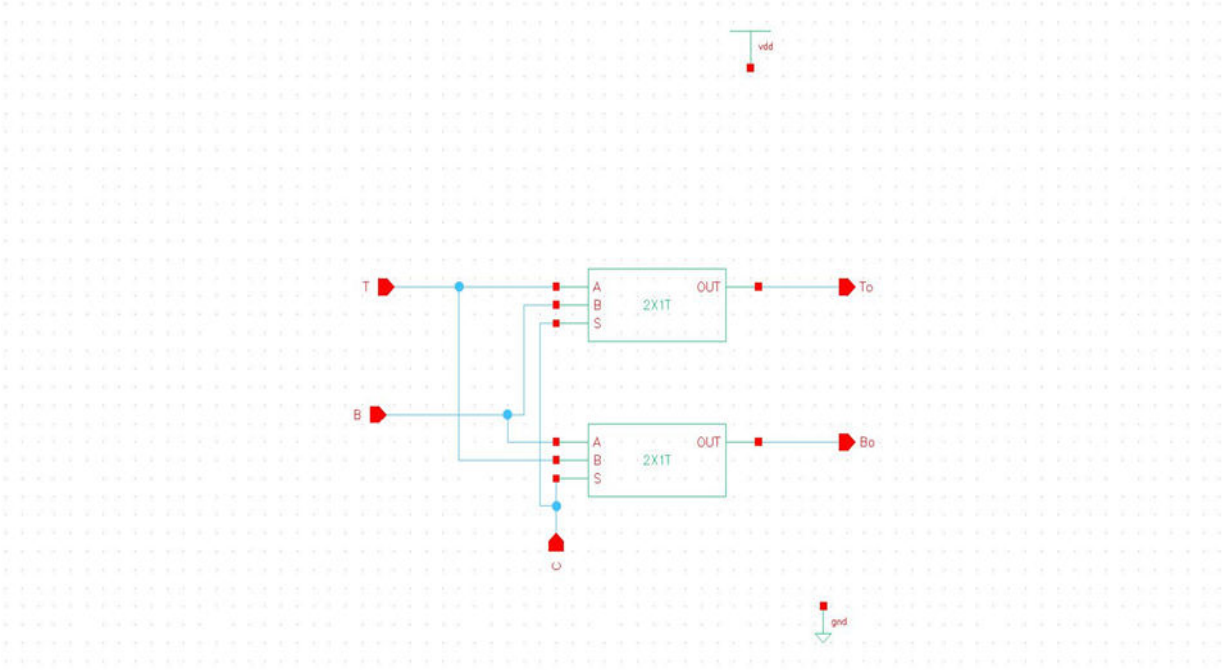


Figure 3: Schematic for the delay stage

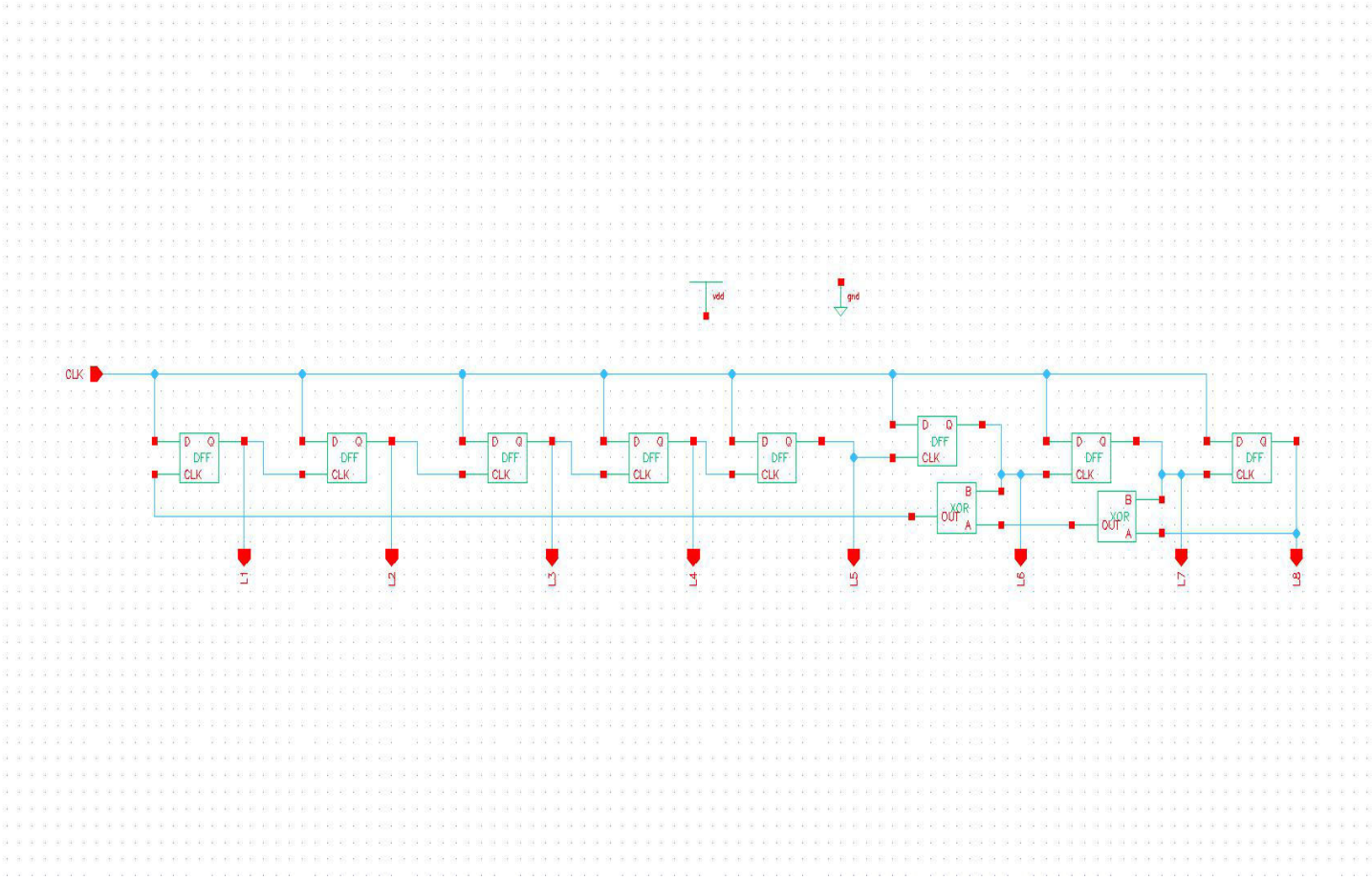


Figure 4: Linear Feedback Shift Register (LFSR)

Each delay stage consists of two 2:1 multiplexers with the output of the LFSR acting as the select input. Either T or B is passed on to the output port depending on the value of the select input.

The LFSR has been constructed using D flip flops with the output of each acting as the input of the next one. The outputs of the last two D flip flops are fed to a XOR gate. The output of the first XOR is fed to the next XOR gate along with the output of the 6th D flip flop. The output of the second XOR gate then acts as the input to the first D flip flop. The outputs of each D flip flop act as select inputs to the delay stages respectively.

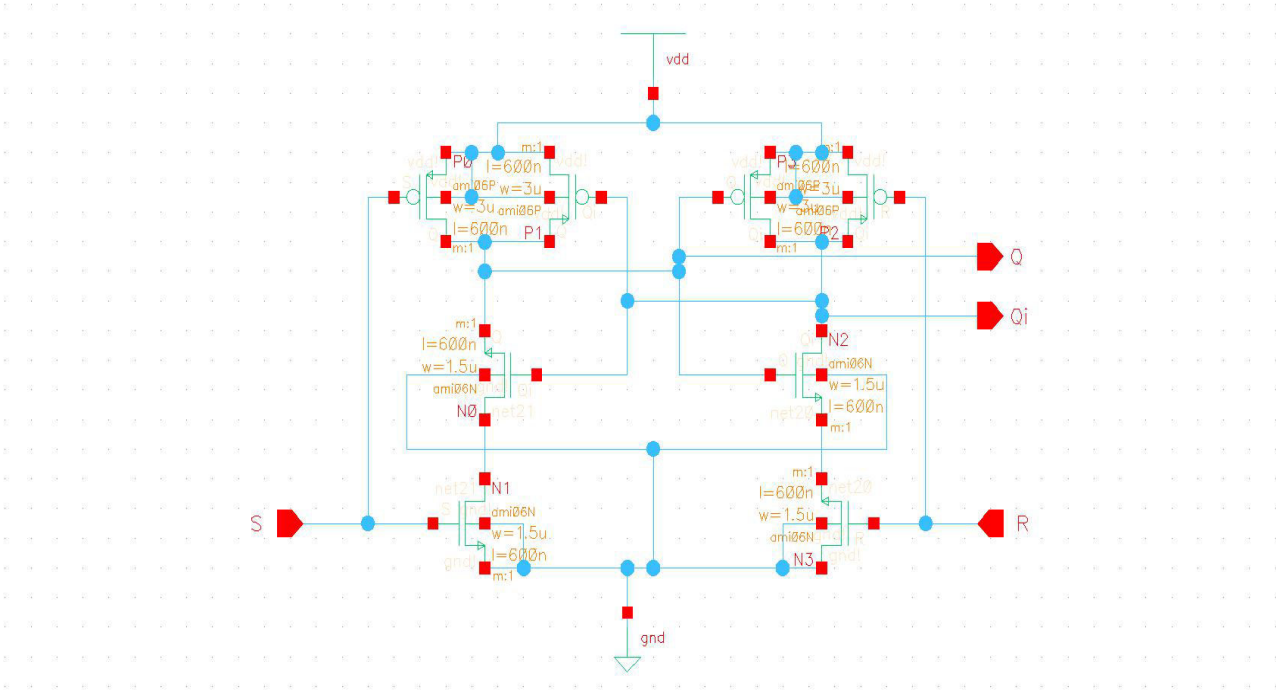
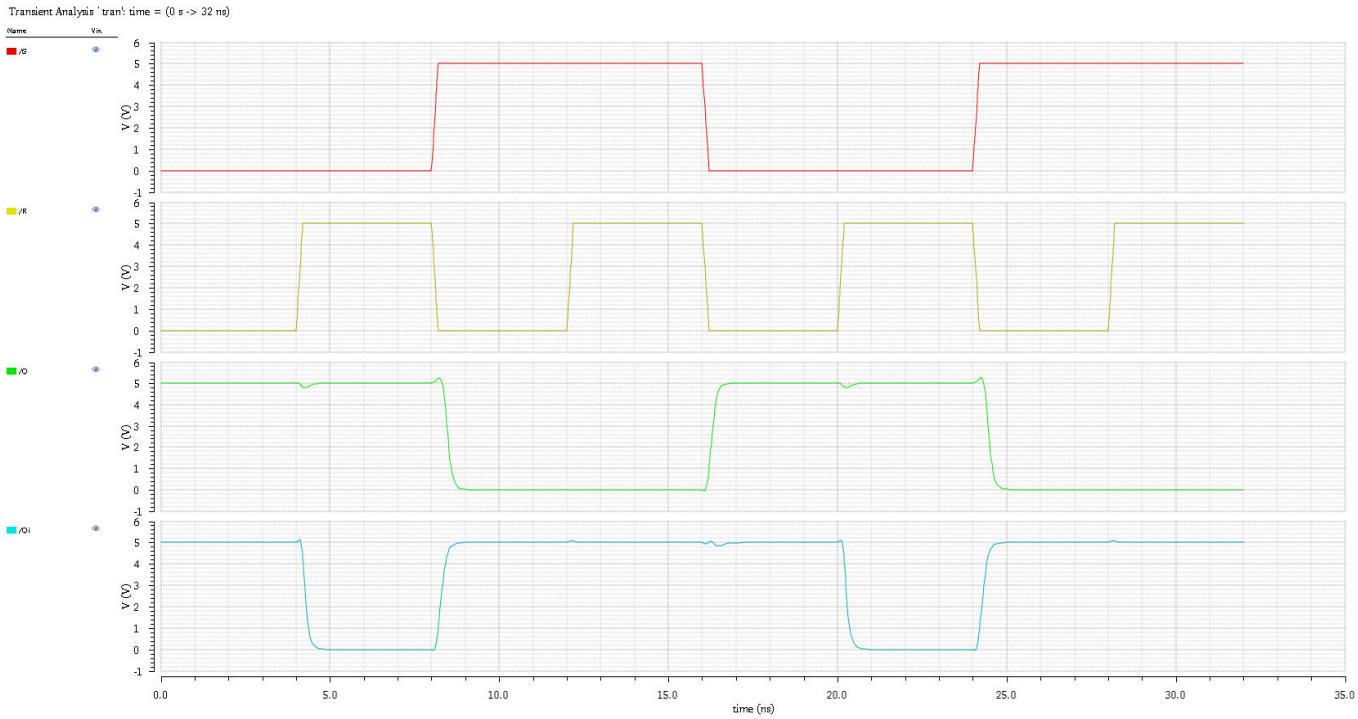


Figure 5: SR latch schematic

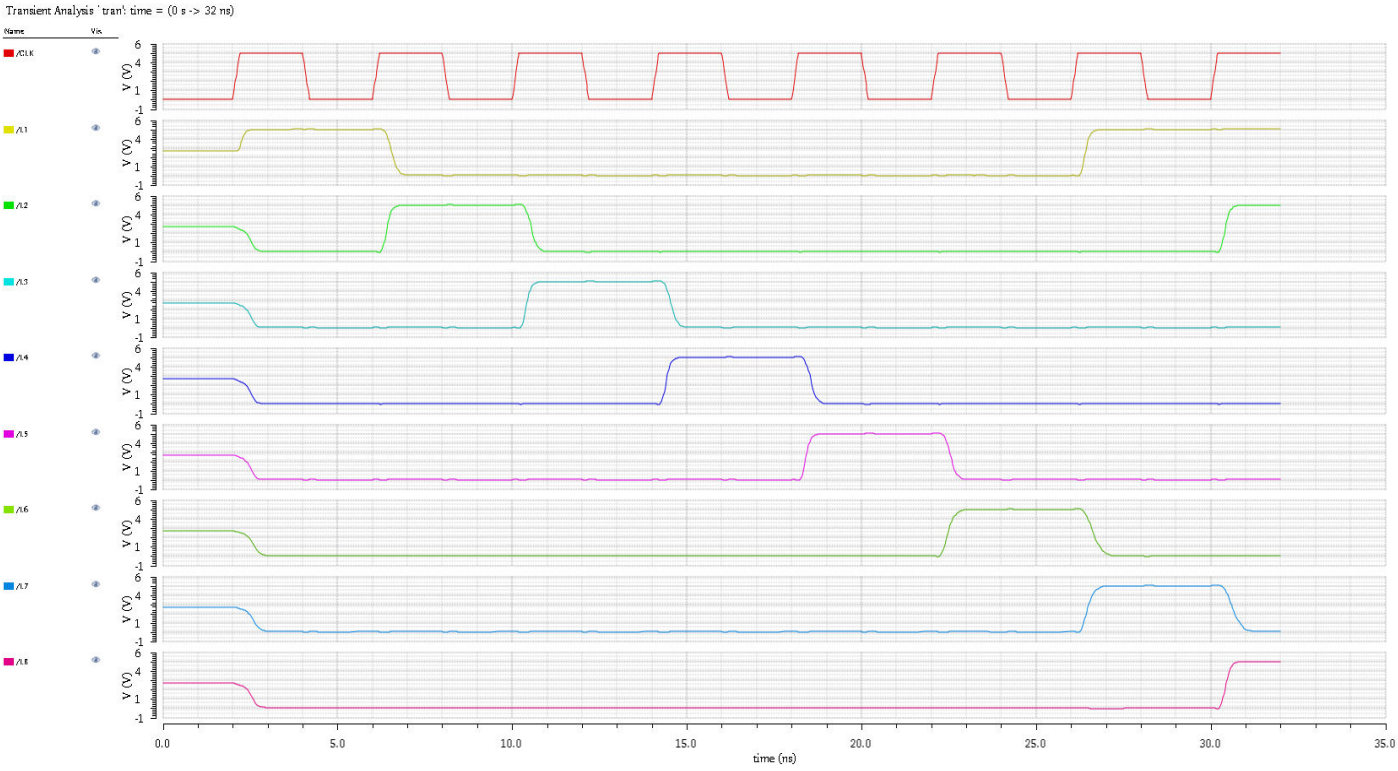
All the above schematics and their respective layouts were generated first. After that LVS netlist matches were obtained for each of them and they were simulated to check whether they are functioning as desired. The output waveforms obtained on simulation has been provided in the next section.

SIMULATION RESULTS

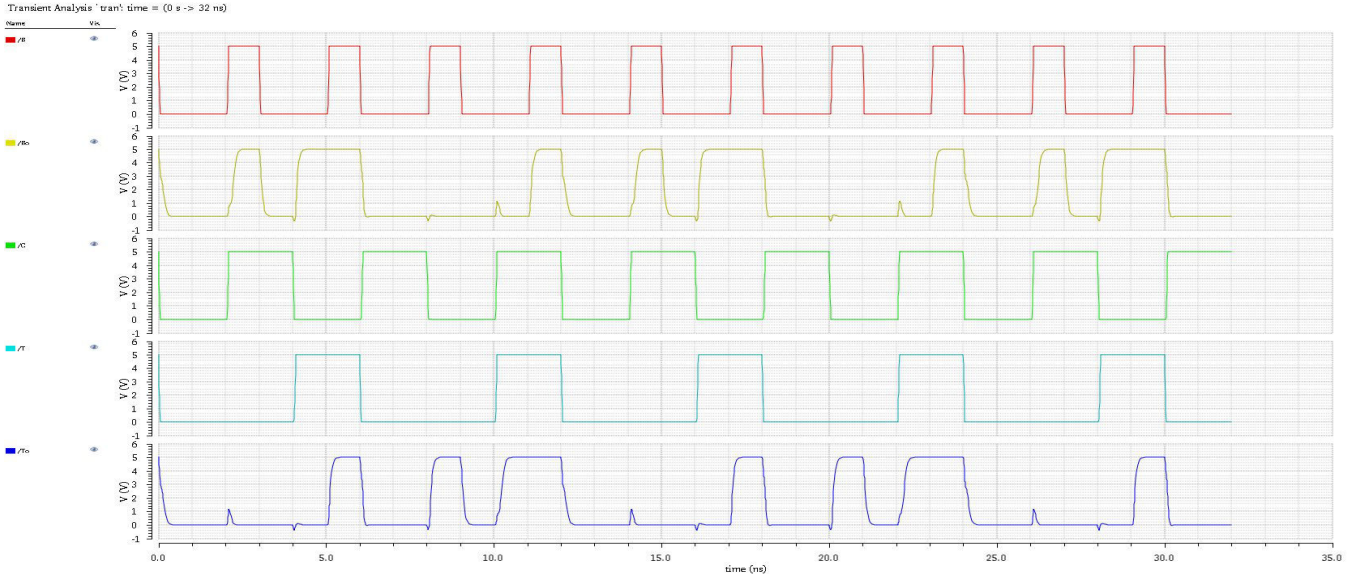
SR LATCH



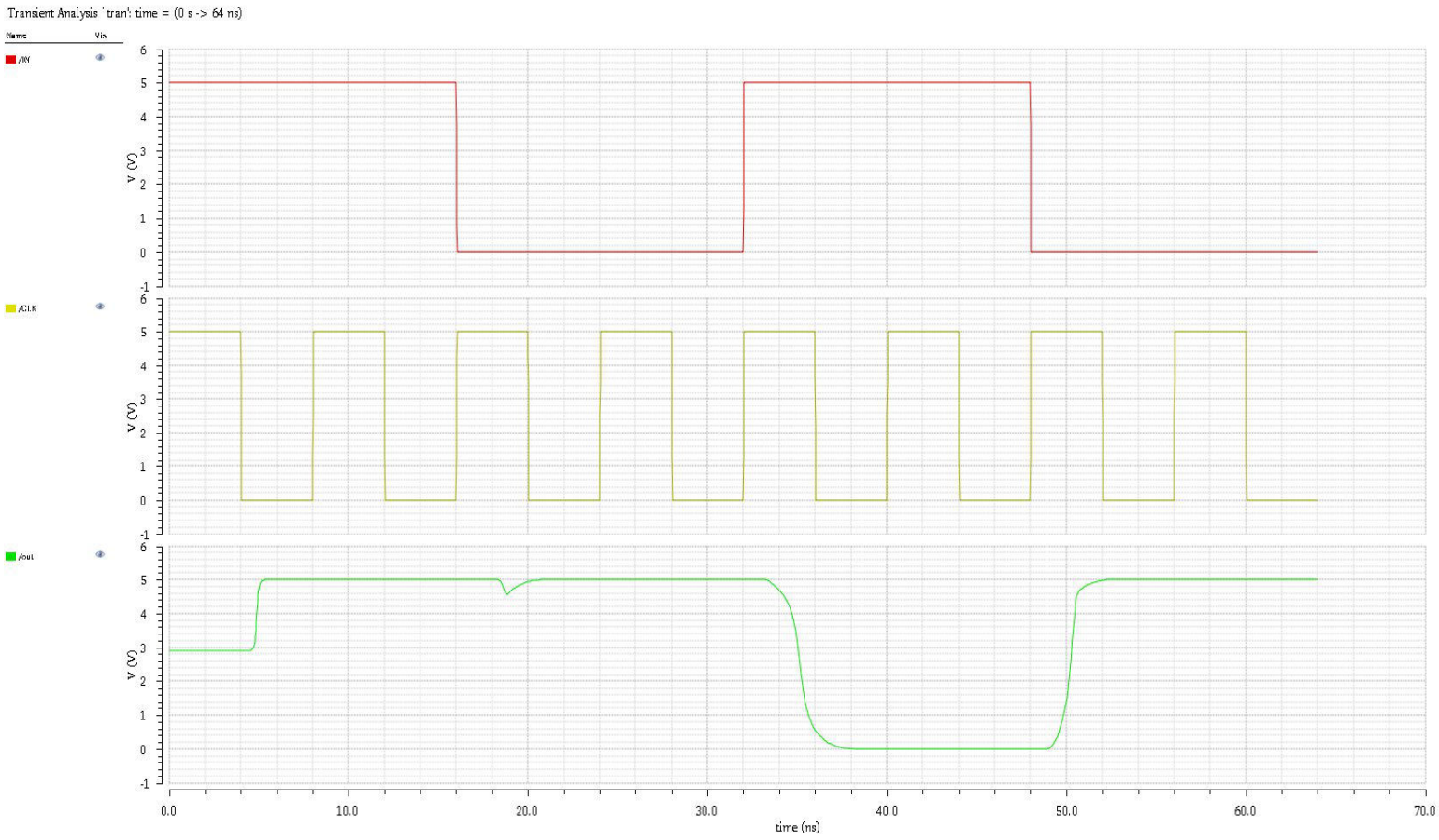
8-BIT LFSR



DELAY STAGE

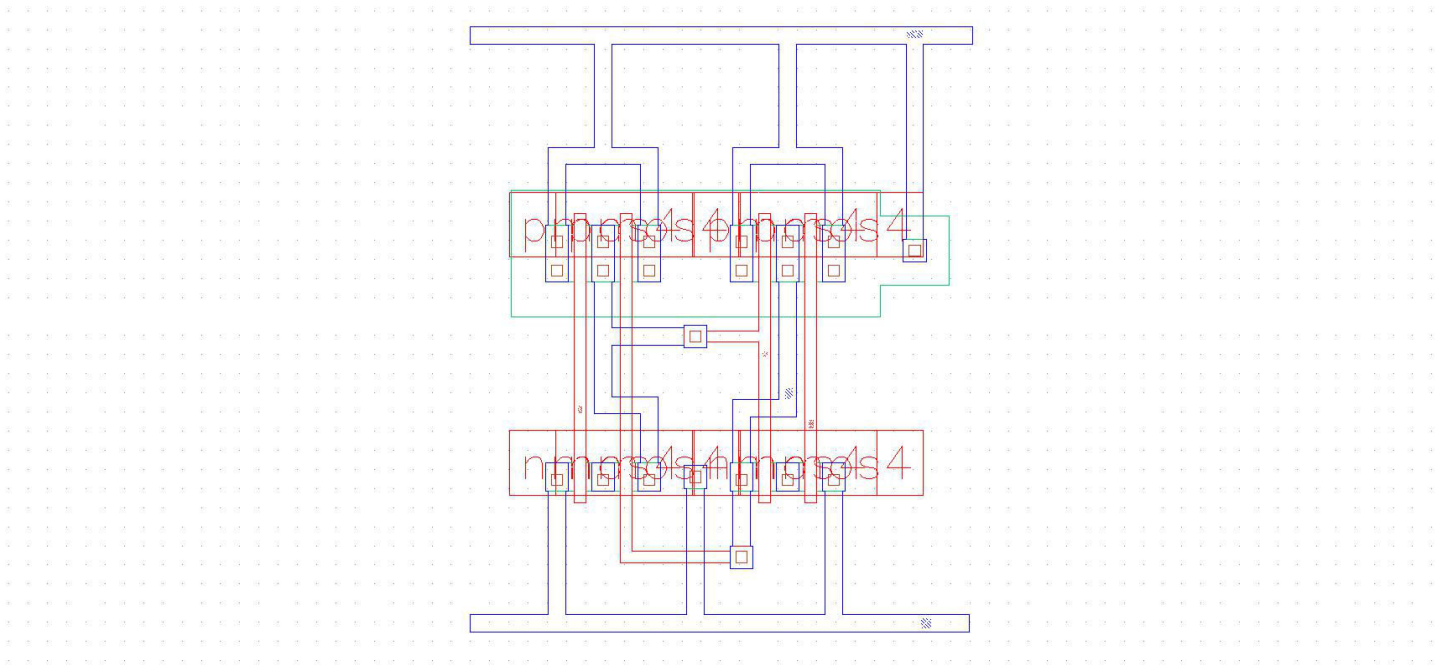


PUF

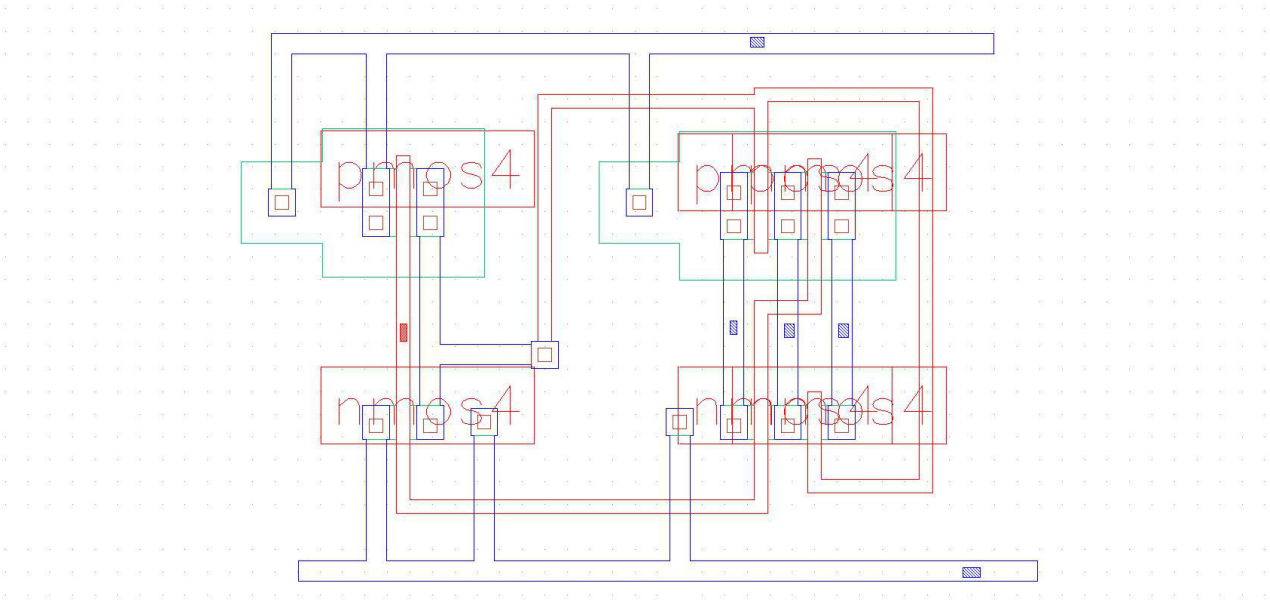


EXTRACTED VIEW OF EACH BLOCK

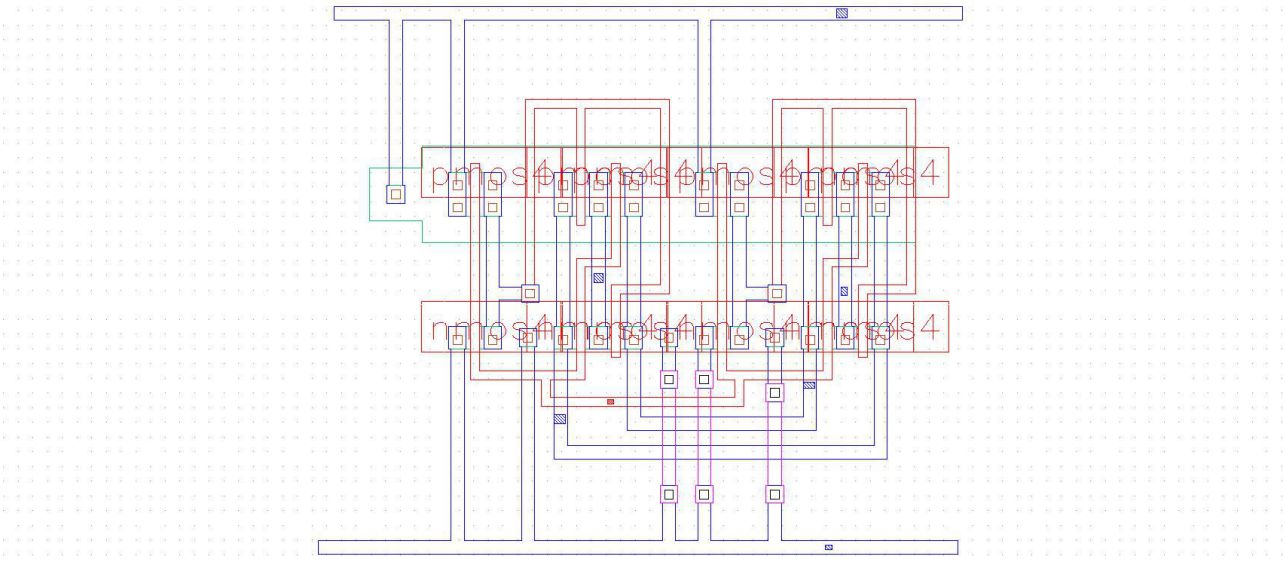
SR LATCH



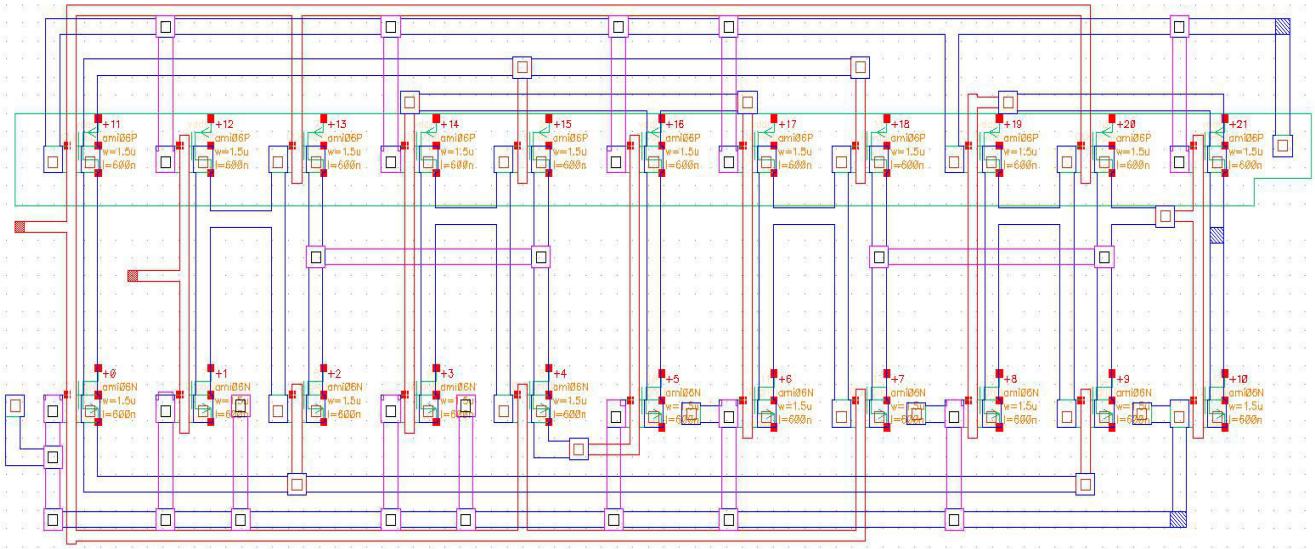
2X1 MUX



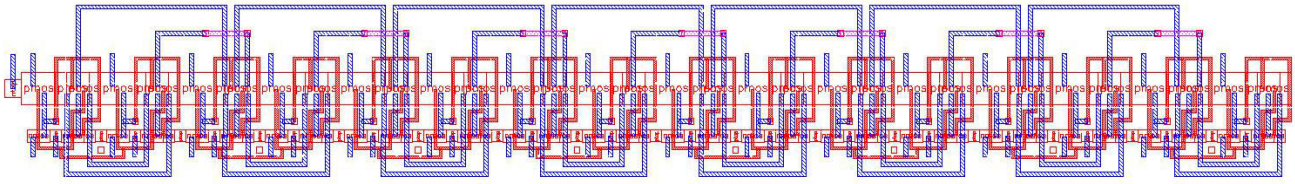
DELAY STAGE



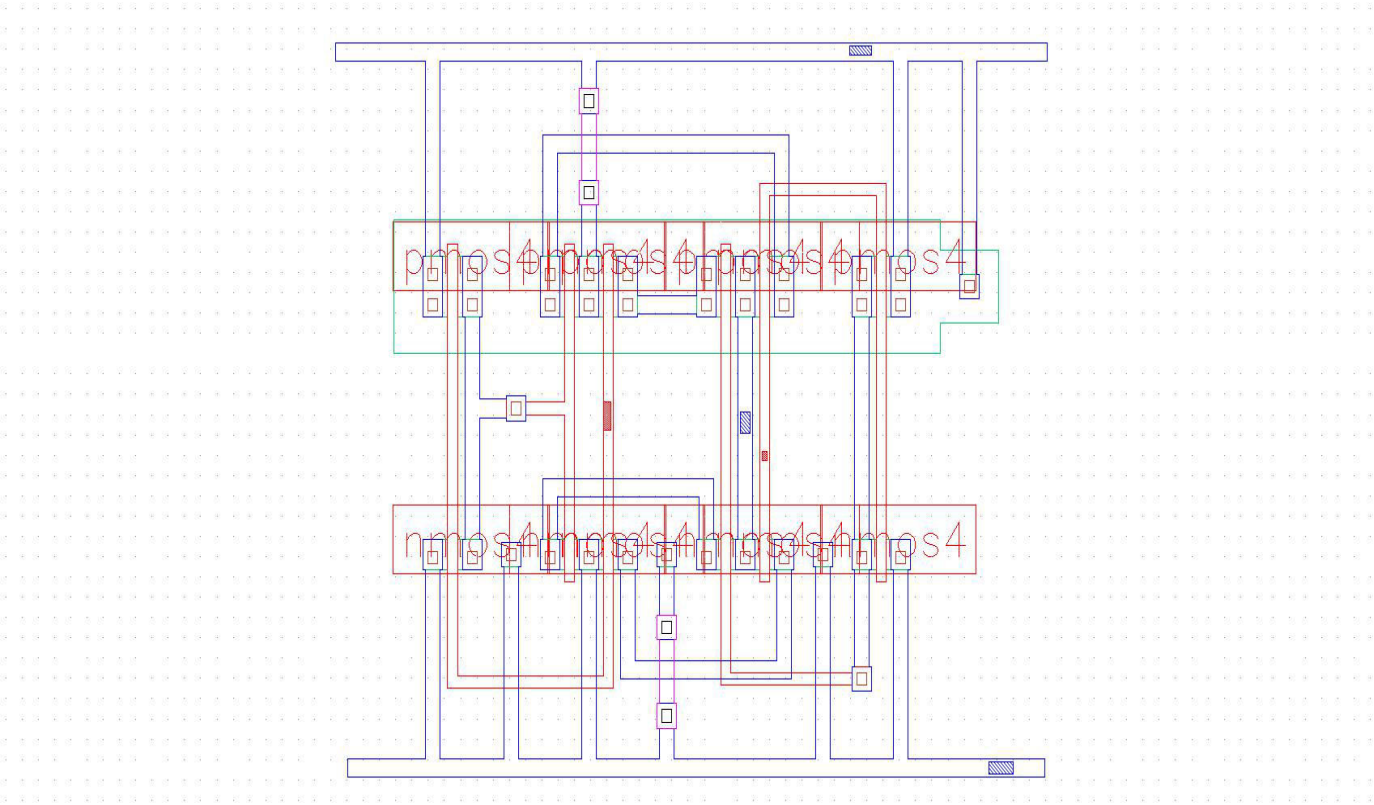
D FLIP-FLOP



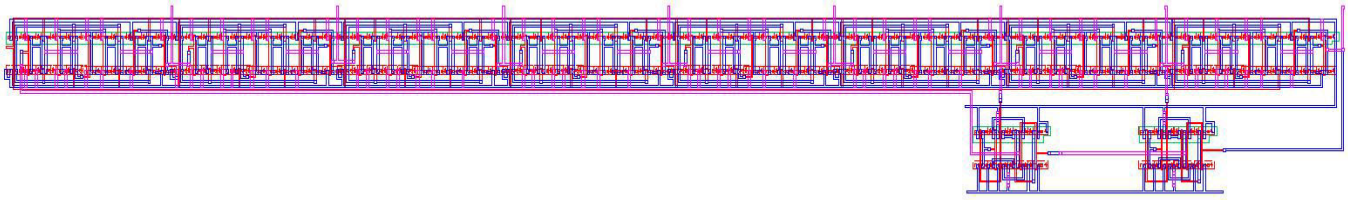
8X1 DELAY STAGES



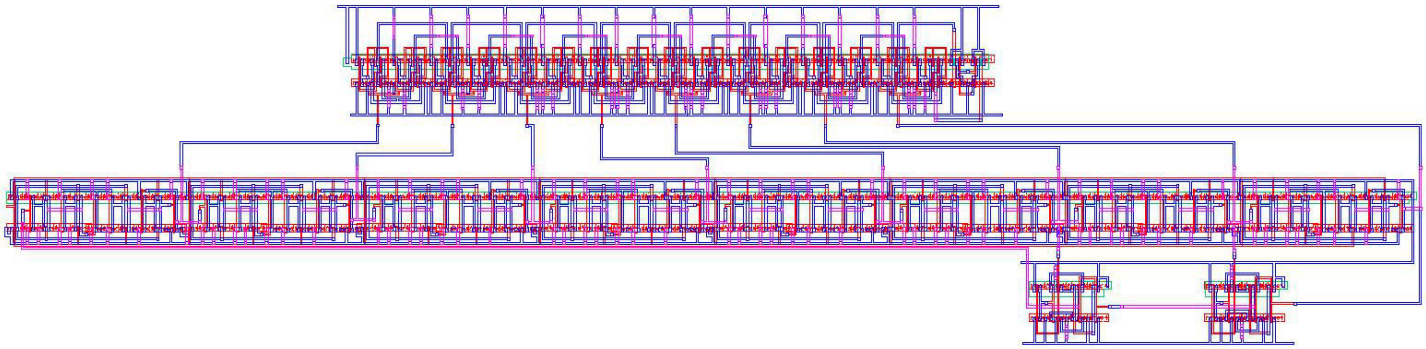
XOR



8X1 LFSR



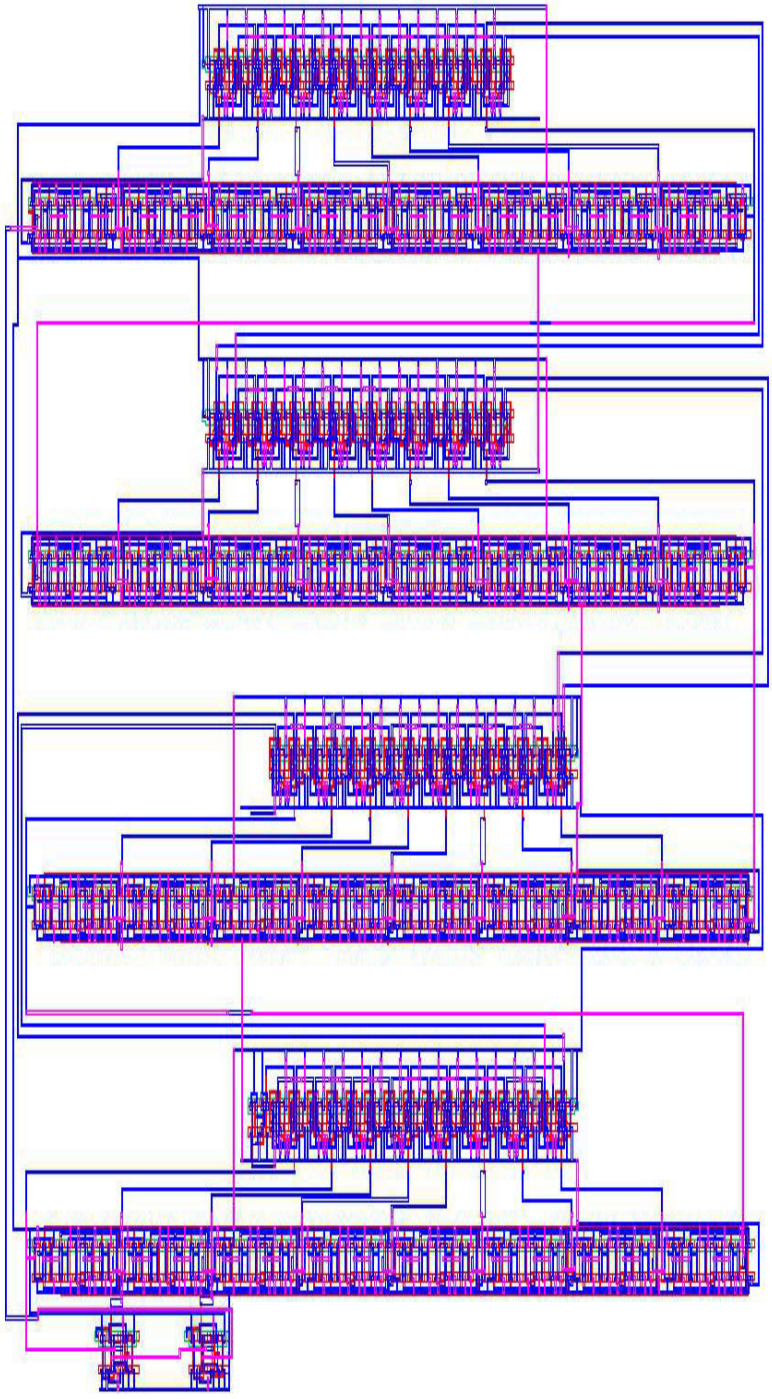
8-BIT PUF



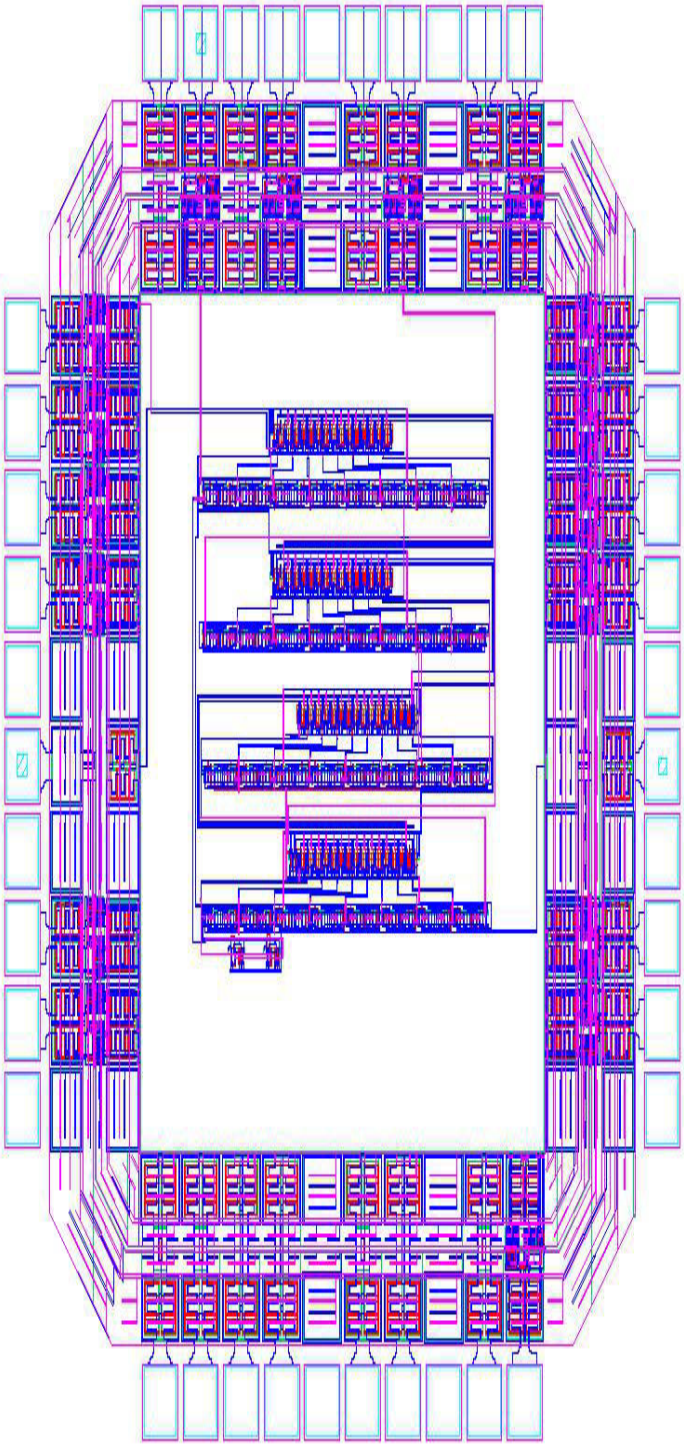
Throughout the process of designing the circuit the primary focus was on making the layout as compact as possible so that area required on the chip for it can be minimized to the largest possible extent.

The 8-bit PUF layout obtained was cascaded and required changes done in the layout to realize a 32-bit PUF. Given below is the extracted view of the 32-bit PUF.

32-bit PUF



PUF PAD FRAME(32-bit)



OBSERVATIONS AND RESULTS

ROLE OF THE LFSR

It consists of 32 D-flip flops and two XOR gates cascaded to each other. As the name suggests, the linear feedback shift register shifts its output by one time period at each stage. The same can be verified from the output waveform obtained for the 8-bit LFSR layout. As a result, 32-bit challenges are produced by the 32-bit LFSR which act as the 'select' signals for the respective 32 delay stages. Each delay stage selects an input signal depending on the ‘select’ signal that is being generated by the LFSR which acts as the Pseudo Random Number Generator (PRNG).

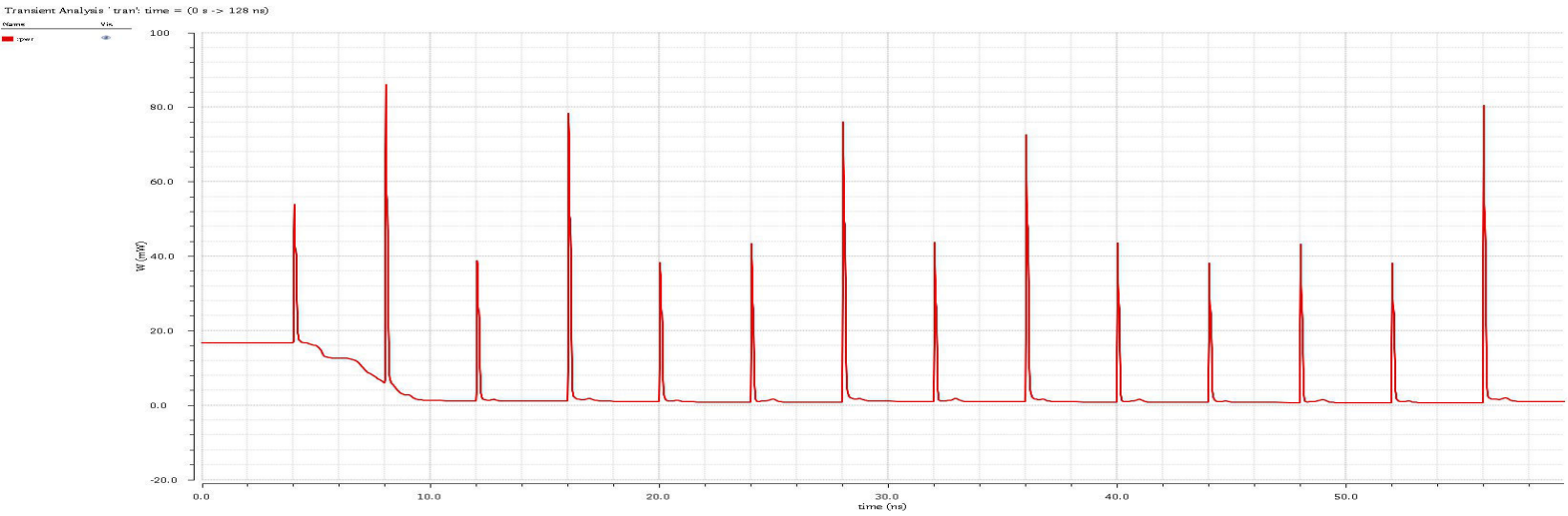
ROLE OF THE DELAY STAGES

The output of each stage of the LFSR acts as the 'select' signal to each delay stage which consists of two multiplexers cascaded to each other. Depending on the 'select' signal the multiplexer decides which input to pass on to the output port. This increases the randomness and uniqueness of the circuit. The circuit is designed in such a way that all the wires in the delay stage are of the same length exactly so as that the delay is entirely caused by the inherent properties of the path through which the signal is traveling. Therefore, this demands symmetry while implementing the circuit.

ROLE OF THE ARBITER (SR LATCH)

The role of the Arbiter is to give an output depending on the input which reaches it first. It basically senses the input which arrives first from the delay stages and produces an output accordingly.

POWER CONSUMPTION ANALYSIS OF THE 32-BIT PUF



Upon analysing and evaluating the power consumption of the circuit for V_{dd} = 3V:

Total Power consumption = 294µW

CONCLUSION

A robust 32-bit PUF circuit was built using Cadence. It was fitted on a given pad-frame and simulated. The energy consumption of the entire circuit was also measured and reported.

Throughout the design process, care was taken to ensure that the area on chip required for the layout is minimized. The circuit has been tested and is performing as per requirement.

PUFs find a wide variety of applications for security and cryptographic purposes. A very important application in cryptography is as a “key” generator. It can be used for anti-counterfeit applications, software licensing, anonymous computation, etc.

REFERENCES

- Secure and Energy Efficient Physical Unclonable Functions - Mr. Sudheendra Srivathsa (February 2012) University of Massachusetts, Amherst.
- Digital Integrated Circuits (2nd edition) – Jan M Rabaey, Anantha Chandrakasan, Borivoje Nikolic
- Roel Maes auth. Physically Unclonable Functions Constructions, Properties and Applications
- Physical Unclonable Functions by Srini Devadas