PHYSICALLY UNCLONABLE FUNCTION USING SCHMITT TRIGGERS

Ritu Gupta[1]
M.Tech ECE from,
Lovely Professional Univeristy
Phagwara,India
ritz13486@gmail.com

Rishab Goyal[1]
PhD ECE from,
Autonoma University of Barcelona
Barcelona,Spain
goyalris09@gmail.com

Abstract— **Physically unclonable functions or PUFs are innovative physical security primitives which produce unclonable and inherent instance-specific measurements of physical objects; PUFs are in many ways the inanimate equivalent of biometrics for human beings. Since they can securely generate and store secrets, PUFs allow to bootstrap the physical implementation of an information security system. Physically Unclonable Functions (PUF) are security primitives to combat Integrated Circuit (IC) cloning and counterfeiting. The response of the PUF is expected to be stable under environmental fluctuations (e.g., temperature and voltage fluctuation). Our analysis indicates that conventional arbiter PUF experiences significant variations due to environmental fluctuation degrading quality. In this paper we propose a novel Schmitt-Trigger (ST) based PUF that exploits the susceptibility of ST to process variations to realize high-quality robust arbiter type PUF. We have used 5 different types of ST level by level to change overall delay of the circuit. We have used an Inverter-based conventional arbiter PUF structure. The response is determined based on relative delay between paths. The path selection is done by challenges. The overall circuit is 3-bit circuit which includes multiplexers and flip flops as well. To show encryption i.e., to generate a set of keys we have used a 3-bit circuit having eight outputs.**

***Keywords:* - Schmitt Triggers, PUF´s, N-type and P-type Schmitt Triggers, Up and Down Schmitt Triggers**

1. INTRODUCTION

Integrated Circuit (IC) cloning or duplicating includes replicating the plans and manufacturing them with the goal to imitate the bona fide chip, access secure substance as well as release mystery data. Physically Unclonable Function (PUF) is the prime fixing to avoid cloning **[1]**. It replaces the hard coded enter in the IC with particularly composed circuits that work on the rule of test reaction. The reaction to a specific test depends on the physical properties of the chip (e.g., handle). The unclonability of the PUF makes the reaction difficult to anticipate by the foes. A few sorts of PUFs have been proposed however because of its straightforwardness, referee PUF is a generally acknowledged plan. The ordinary judge PUF that produces 1-bit reaction for each arrangement of difficulties **[2,3]**. It contains a mediator and two indistinguishably outlined postpone ways. For confirmation, a flag is dashed in two ways (the correct way is controlled by the test). The reaction is produced by looking at the postponements of the two ways in race.**[4]** The postpone contrast is changed over to 0 or 1 reaction. Mediator PUF depends on the way that the way deferrals will vary because of process varieties. In this manner, the PUF reaction will be arbitrary in nature. **[4,5].** This plan likewise utilizes postpone distinction to limit ecological change (i.e., temperature and voltage variety) incited mistakes.

II. EASE OF USE

A. *Basic Purpose*

The basic purpose of PUFs is to provide ultimate security without getting cloned and hence protecting from all sorts of theft attacks by providing a unique identity which only a particular individual will have and no resemblance with any other user will occur.

B. *Reliability*

When it comes to reliability there is no match to PUFs. They are highly reliable when it comes to performance. And as this PUF uses five different types of Schmitt triggers, it gives a highly reliable output as per requirement.

C. *Cost Effectiveness of PUFs*

As it is possible to authenticate individual ICs using PUF without using costly cryptography primitives it results in reduction of overall cost of the security systems. Physical unclonable functions (PUFs) can be utilized as a financially savvy intends to store cryptographic key material in an unclonable way. A solid PUF will supplant the protected memory and crypto equipment on an inserted gadget and is utilized to safely distinguish the gadget to a server. Since the PUF does not require secure non-volatile memory, hostile to alter hardware, or extra supporting crypto speeding up equipment, a PUF-based arrangement requires less range, power, and cover layers than a conventional way to deal with secure confirmation.

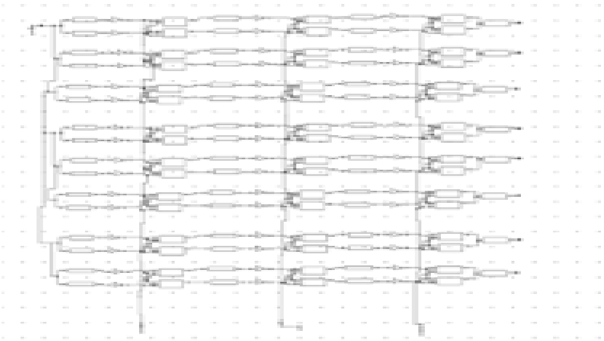

Figure 1. Basic block diagram of 3-Bit PUF using five different types of Schmitt Trigger (ST) circuits.

As the diagram shows that it has ten different delay paths, and each path consists of a single type of or two type of at max Schmitt Triggers connected in series along with 2X1 Multiplexers and S-R Flip-Flop at the output. Each Multiplexer has a different select lines and each pair of delay lines have a single S-R Flip-Flop at the output. The five different types of Schmitt Triggers are as follows:

D. *General Schmitt Trigger*

It's a comparator which switches the yield negative when the info goes upward through a positive reference voltage. It then uses positive criticism of a negative voltage to forestall changing back to the next state until the information goes through a lower limit voltage, therefore balancing out the exchanging against quick activating by clamour as it passes the trigger point. That is, it gives criticism, which is not turned around in stage, but rather for this situation the flag that is being sustained back is a negative flag and keeps the yield driver to the negative supply voltage until the info dips under the lower outline limit. These devices are frequently used in signal conditioning applications to eliminate noise, particularly mechanical contact bounce in switches, from signals utilized in digital circuits. In function generators and switching power supply, relaxation oscillators are implemented using them in closed loop negative feedback setups.

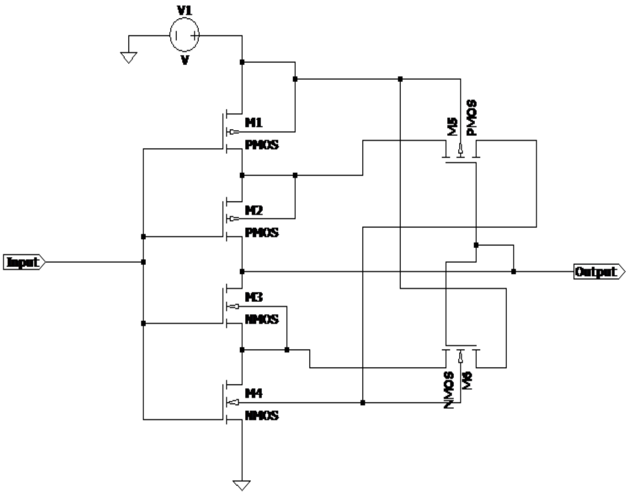

Figure 2. General Schmitt Trigger

III. PRINCIPLE OF OPERATION

A. *N-Type Schmitt Trigger*

As the name indicates N-Type Schmitt Trigger includes NMOS as a dominating component as the functioning of the circuit, as shown in Fig3 mainly depends on the flow of electrons. Its bit faster as compared to the general Schmitt Trigger as the mobility of electron is more. This type of Schmitt trigger basically acts as a low power Schmitt Trigger. This circuit was referred by Swati Kundra and Priyanka Soni.

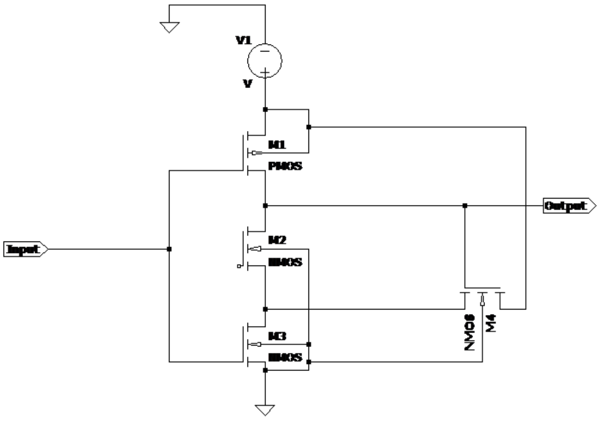

Figure 3. N-Type Schmitt Trigger.

B. *P-Type Schmitt Trigger*

This circuit is proposed by me keeping in mind the concept of N-Type Schmitt Trigger. As the name indicates P-Type Schmitt Trigger includes PMOS as a dominating component as the functioning of the circuit, as shown in Fig4 mainly depends on the flow of holes. Its bit slower as compared to the general Schmitt Trigger as the mobility of holes is less. So, as a result it gives a larger delay comparatively.

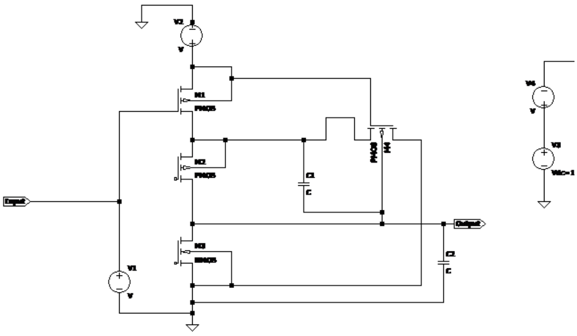

Figure 4. P-Type Schmitt Trigger

C. *UP and Down Schmitt Trigger*

These are basically he normal Schmitt Triggers. the only difference is that both the Schmitt Triggers have different W/L parameters than the general Schmitt Triggers and also from each other. The circuit diagrams are as shown below:

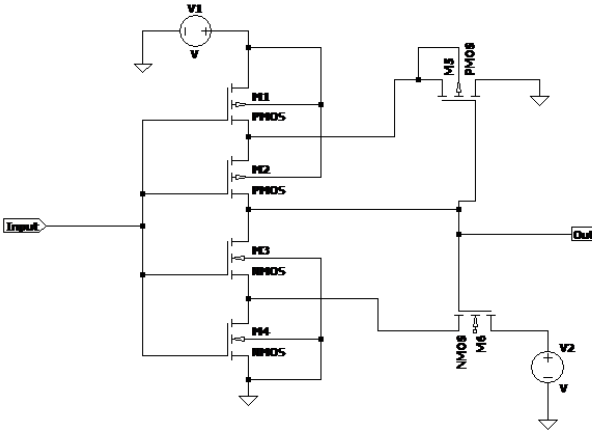

Figure 5(a) UP Schmitt Trigger

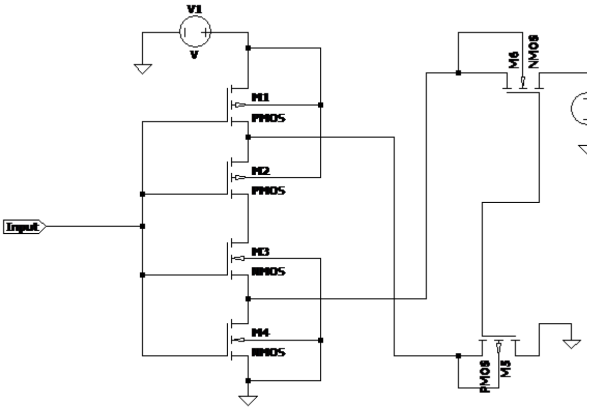

Figure 5(b) Down Schmitt Trigger

As we see that both the diagrams are basically same. There is the difference of width parameters only.

D. *Multiplexer*

We are using here a 2:1 one multiplexer which has two inputs and is taking its inputs from the two different delay path and generating output which is fed to the next stage. We have used transmission gates for designing mux to reduce the number of transistors. Instead of having a device for each input signal, a multiplexer enables several input signals to share a single device or resource, such as an analog-to-digital converter or a communications transmission medium. Boolean functions with numerous variables can also be implemented using multiplexers. Computer systems include multiplexers to choose data from a particular source, such as a memory chip or a hardware device. The data and address buses of a computer are controlled by multiplexers, allowing the processor to choose data from several data sources. By coupling the single output of the multiplexer to the single input of the demultiplexer (Time-Division Multiplexing), multiplexers in digital communications enable multiple connections over a single channel.

A complementing demultiplexer is typically needed at the data link's receiving end to separate the single data stream back into the individual streams. In some situations, the far end system may be more advanced than a straightforward demultiplexer, and although though demultiplexing technically continues to take place, it may never be implemented discretely. This might occur, for example, when a multiplexer serves several IP network users before feeding directly into a router, which immediately reads the content of the entire link into its routing processor before performing the demultiplexing in memory before being converted immediately into IP sections.

Frequently, a multiplexer and a demultiplexer are merged into one piece of technology and referred to as a single multiplexer. Since most communications systems broadcast in both directions, both circuit elements are required at both ends of a transmission link.

A multiplexer is a unique kind of analog switch used in analog circuit design that connects a signal chosen from several inputs to a single output. The circuit Diagram is shown below:

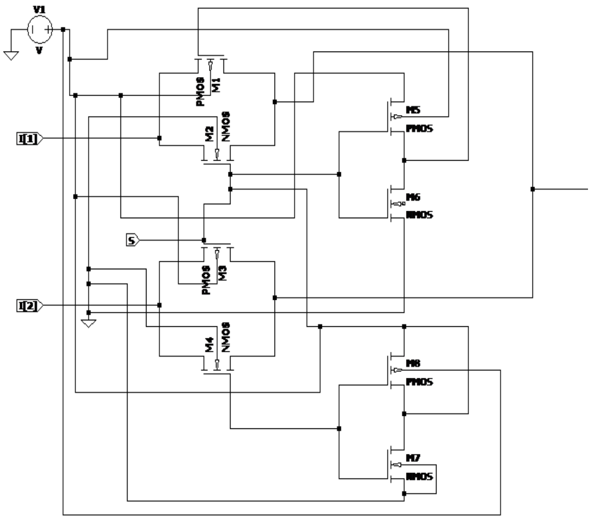

Figure 6. 2:1 Multiplexer using transmission gates.

E. *S-R Latch*

The prefix bi in the name of a bistable multivibrator indicates that it has two stable states. The terms "set" and "reset" are commonly used to describe the two states. Set-reset, or S-R, latches are consequently the most basic type of bistable device. We can connect two NOR gates so that the output of one feed back into the input of the other and vice versa to make an S-R latch as follows:

The not-Q output is designed to be in the opposite state from the Q output. Because both Q and not-Q are 0 when the S and R inputs are set to 1, I say "supposed to" rather than "actually." For the S-R multivibrator, having both S and R equal to 1 is referred to as an invalid or illegal state.

In the absence of this, setting S=1 and R=0 "sets" the multivibrator such that Q=1 and not-Q=0. Making R=1 and S=0, on the other hand, "resets" the multivibrator in the opposite state. The outputs of the multivibrator "latch" in their previous states when S and R are both equal to 0. The circuit diagram is shown below:

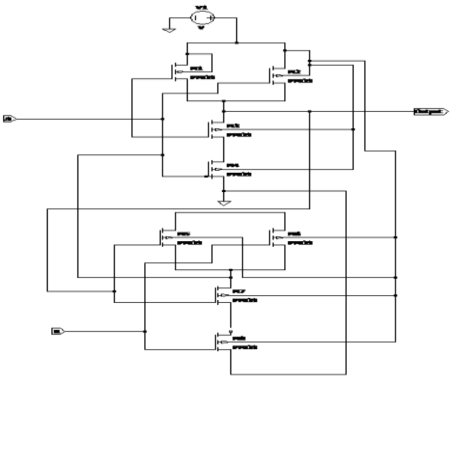

Figure 7. S-R Latch

A condition of Q=1 and not-Q=0 is set. Resetting a Q=0 and not-Q=1 condition. Any multivibrator circuit's output states can be described using these terms. The keen observer will see that both gates (coils) start in the de-energized mode upon initial power-up of either the gate or ladder variety of S-R latch.

As a result, it is reasonable to assume that the circuit will begin operation with both the Q and not-Q outputs in the same state. This is the case! The circuit will rapidly stabilize in either the set or reset condition since one gate (or relay) is bound to react a little bit faster than the other, making the invalid condition unstable with both the S and R inputs inactive.

On power-up, both gates (or coils), if identical, would swing between high and low like an astable multivibrator and never reach a stable state! Thankfully, such a close fit between the components is an uncommon option for situations like these.

It should be emphasized that although while an astable (constantly oscillating) condition would be exceedingly unlikely, the circuit will most likely oscillate for one or two cycles before reaching its ultimate state (set or reset) after powering up.

The two relays, CR1 and CR2, are in a competition, which is the cause of the issue.

1V. SIMULATION RESULT

A. *Result and Discussion*

We can use **Monte Carlo** method to check that whether the output can be converted to required set of keys or not. So, here we are considering a 3-bit circuit which can generate eight outputs and is using Monte Carlo method to check as a reference that the main circuit will also be capable to generate required set of keys.

Little irregular varieties happen amid the assembling of circuit gadgets, bringing about behavioural contrasts between indistinguishably outlined gadgets. These varieties, or gadget confounds, are frequently rejected as an immaterial or troublesome part of simple circuit plan. This is not astonishing because it is hard to logically anticipate the conduct of any non-unimportant circuit because of the aggregation of the confuse mistakes from individual gadgets. Monte Carlo recreation can be utilized to examine how the individual gadget befuddles of a circuit may aggregate and influence the circuit all in all. This is accomplished by investigating a substantial arrangement of circuit instantiations, whose circuit gadgets have each been independently randomized in understanding to the jumble model of the specific gadget sort. As circuit architects have trouble appropriately surveying the impacts of gadget confound, the primary objective of this paper is to show an adaptable instrument that can re-enact and break down information, as well as enable others to further research into gadget jumble. Monte-Carlo simulation is used to analyse how the proper selection of arbiter element and gate sizing can affect the delay. The Monte Carlo strategy utilizes rehashed arbitrary testing to produce mimicked information to use with a numerical model. This model frequently originates from a factual investigation, for example, an outlined examination or a relapse investigation.

B. *How Can Monte Carlo Simulation Help You?*

- Monte Carlo analysis can be used to:
- Simulate item comes about while representing the fluctuation in the data sources.
- Optimize handle settings.
- Identify basic to-quality elements.
- Find an answer for decrease surrenders.

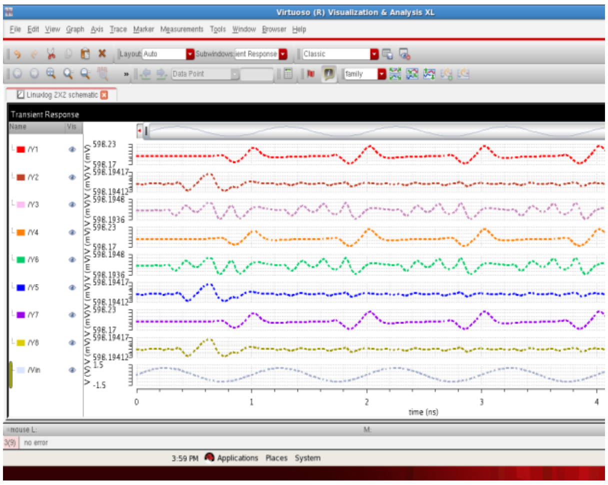

Figure.8 Output waveform for 3-bit circuit.

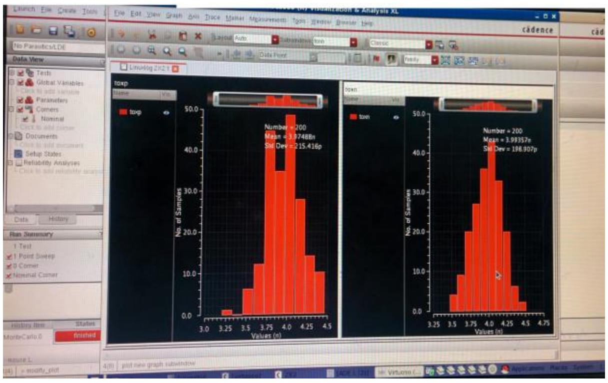

Figure.9.1 Monte Carlo output for 3-bit circuit

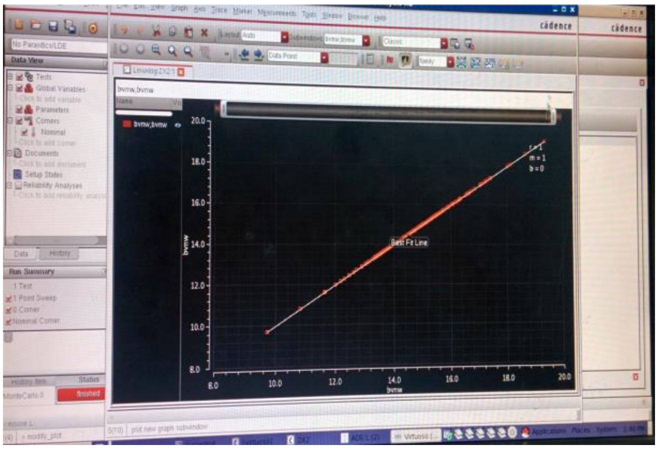

Figure 9.2 Monte Carlo line output for 3-bit circuit

Hence, we can see that encryption of the delay output of a circuit using Schmitt Trigger is possible.

Acknowledgement

This work was supported in part by the VIGILANT Project (PID2019-103869RB-C32 / AEI / 10.13039/501100011033). EU ASCENT project is acknowledged for sample provision.

References

[1] Sakshi Singh;Santosh Kumar Gupta “Design of Low Power and High Noise Immunity Schmitt Triggers, 2023 5th International Conference on Power, Control & Embedded Systems (ICPCES)

[2] Rajendar Sandiri; Yashwanth Chimata; Yashwanth Nalamasa;Pavan Area “Design of Noise Immune Sub-threshold circuits using Dynamic Threshold Schmitt Trigger Logic” 2022 IEEE Region 10 Symposium (TENSYMP)

[3] Zizhen Huang;Jianlin Zhong;Chunwei Xie;Ruoyang Wu;Xiaojin Zhao “A Highly Reliable and Energy-Efficient Schmitt Trigger PUF Featuring Ultra-Wide Supply Voltage Range” 2022 IEEE Transactions on Circuits and Systems II: Express Briefs

[4] Akshay Gireesh;Ramesh Bhakthavatchalu;K N Devika “ Performance Analysis of Different Types of Delay based PUF´s 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)

[5] Khaoula Mbarek;Sami Ghedira;Faten Ouaja Rziga;Kamel Besbes “Design and Analysis of Nonvolatile Memristor-based S-R Latch”2020 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS)