METAPUF A Challenge Response Pair Generator

Abhishek Kumar¹, Suman Lata Tripathi², RaviShankar Mishra³
¹²School of Electronics Engineering, Lovely Professional University
³Symbiosis University of Applied Sciences

ABSTRACT
Physically unclonable function (PUF) is a hardware security module preferred for hardware feature based random number and secret key generation. Security of a cryptographic system relies on the quality of the challenge-response pair, it is necessary that the key generation mechanism must unpredictable and its response should constant under different operating condition. Metastable state in CMOS latch is undesirable since it response becomes unpredictable, this feature used in this work to generate a unique response. A feedback mechanism is developed which forces the latch into the metastable region; after metastable state, latch settle to high or state depends on circuit internal condition and noise which cannot be predicted. Obtained inter hamming variation for 8 PUF is 51.43% and average intra hamming distance is 99.76% with supply voltage variation and 96.22% with temperature variation.

Keyword: Physically unclonable function Metastable CMOS latch Unpredictable Challenge-Response

Corresponding Author:
Abhishek Kumar,
School of Electronics Engineering,
Lovely Professional University
Punjab, India.
Email: abhishek.15393@lpu.co.in

1. Introduction
Security in a cryptographic system represented as how much secured the Response is! Kerckchoff’s principle of cryptographic says “A cryptosystem should be secure even if everything about the system, except the key is public knowledge” [5] it is necessary that key must originate in a secured environment. The response is derived from random number processes by error correcting code to remove biasing error. The randomness of the random number is the strength of the key, classical algorithm based random number was deterministic in nature; it starts with an initial seed and starts repeating after sequence length. It is already proven that based on history upcoming random number can be predicted statically, which ultimately weakens the Response. Another method is physical variable based on a random number generator like thermal noise. In 2007 GE suh and S devadas [1] presented architecture of physically unclonable function (PUF) is an emerging technology for authentication and Response generation. PUF is a computational unit which output (response) is a function of input (challenge) as a well-selected hardware feature. A unique feature of hardware added into the computation [2, 20]. Two silicon ICs cannot have a similar feature; the silicon-based integrated circuit is the preferred choice for implementation of PUF circuit.

PUF circuit is unclonable and its output cannot be predicted. In 2013 NXP semiconductor has quoted that “any physical device characteristic that fluctuates can be turned into PUF”. S.Devdas[1] have introduced delay-based PUF, delay unit implemented with a multiplexer, input signal raced between two parallel paths; at the destination, arbiter decides which decide which path is faster accordingly generate response bit [3]. A ring oscillator PUF introduced in 2009; s election of operating frequency depaend on a large size multiplexer, two
counters operate parallel on selected different ring oscillator. Response bit is high if value of counter1>counter2. [8-11]. In 2015 PUF found application to securing the internet of things (IOT) device. Quality of PUF response is judged by 3 parameters [1, 7, 13, 17, 18].

A) Uniformity- Probability of occurrence of bit ‘1’ and a bit ‘0’ in the key should equal, half of the key length. Ideal value is 50%.
B) Reliability- PUF should same response for a challenge in a different operating condition like variable supply voltage, high temperature, and noisy environment. Ideal value is 100%.
C) Uniqueness- For same challenge different PUF must produce a different response. Ideal value is 50%.

The remaining section of the paper as follows. Section 2 reviews metastability state of CMOS latch. Section 3 describes the schematic details of metastable PUF and their performance and Section 4 concludes with future directions

1.1. Metastable CMOS latch
Metastable in the system is undesirable because system behavior uncontrollable and its response are unpredictable [14] whereas this unpredictable behavior enable to originate randomness of PUF. A cross-coupled CMOS inverter based latch shown in fig 1(a) node Q and QB form bistable remain at high or low state. If we able to apply equal voltage at each node i.e threshold voltage of inverter latch enters onto metastability center of graph shown in fig 1(b), practically not possible to apply equal potential on both node slight variation exist due to circuit non linearity which pull the node settle with high or low state its completely unpredictable. Metastable PUF utilizes this feature to generate a response bit.

2. METASTABLE PUF
Physically unclonable function (PUF) is hardware-based security module uses inherited properties of the integrated circuit to generate an unpredictable response. In the proposed MetaPuf a CMOS based latch circuit is the basic element of PUF, which frequently enters into metastability region by maintaining equal potential at Q and QB node, depending upon circuit internal noise latch will come out from metastable state and settle to logic ‘1’ or logic ‘0’ which is completely unpredictable. MetaPuf uses metastability associated with CMOS latch to generate 1-bit response shown in fig2. Q and QB node of the latch is controlled by 2:1 multiplexer applies the same potential on each node and forces the latch to enter in a metastable state. A high EQ and high SEL input enable transmission gate (TG) to apply charge pump output on each node of the latch. Latch enters in metastable state there is a race to Q and QB terminal, minute potential difference on nodes senses by the sense amplifier and produces response bit. When EQ=0 and SEL=0 transmission gate disables it cut off the latch from the charge pump and creates a loop.
The proposed circuit is verified for 8 different PUF fig. Each latch unit is operated by the charge pump. Challenge input is applied to decoder input; the output of decoder increase or decrease the charge pump output for logic ‘1’ and ‘0’ respectively. A high input applies increasing potential and low input applies to decrease potential to latch node. Charge pump potential assures that latch operates near metastable region. During metastable state potential difference between Q and QB cannot be guessed, they form a race and try to reverse. Sense amplifier generates high response bit if the potential at Q > QB else low. Response bit can store in parallel in parallel out shift register. To have more response number of PUF units are parallelized and require the large size of the decoder.

3. RESULTS AND DISCUSSION

Performance of METAPUF is determined by 3 quality measure [4, 6, 12, 15, 16, 19]

3.1 Uniformity: - Uniformity determines by the presence of binary ‘1’ and ‘0’ in the response, it must have equal value and half of the response. Obtain result shows that PUF2 and PUF7 the probability of occurrence of binary ‘1’ and ‘0’ slightly lower than ideal value while 6 PUF achieved an ideal value of uniformity as
shown in fig4. Achieved uniformity value is 50% in 6 PUF while for 2 cases its value falls to 49.6% and 49.2%.

![Fig4 Uniformity of PUF](image)

3.2 Reliability: - Response must unaffected by the different operating condition. Reliability measures how much error generated in Response due to temperature variation and supply voltage variation. Reliability is calculated by intra hamming distance of PUF response at different temperature and different supply voltage. Fig 5 shows the error introduced due to supply variation form 0 to 1v, the reliability value of supply variation for the MetaPuf is 99.76%.

![Fig5 Reliability vs Supply Voltage](image)

Fig6 presents the effect of temperature variation over PUF responses. Intra hamming variation of PUF response is simulated in temperature range 0°C to 120°C, high temperature from 60°C PUF start increasing error and reliability falls, the reliability value with temperature variation for the MetaPuf is 96.22%.

![Fig6 Reliability vs temperature (°C)](image)

3.3 Uniqueness: - It measures how much different PUF generate a different response to the same challenge. Uniqueness is measured by inter hamming distance between the response of different PUF. Ideally, its value should be 50 % of response length. Table1 represents the comparative study of METAPUF with existing ROPUF and MUXPUF with 3 quality metrics. Fig7 presents the inter hamming distance when 16-bit of
response produced from PUF, x-axis presents the average number of bit changes for same challenge applied to 32 different PUF i.e. uniqueness and y-axis presents probability of occurrence. Normal distribution function [21,22] with mean 8.23 and standard deviation 0.884; the average inter hamming distance between PUF is 51.43%.

Fig 7 Inter hamming distance

Table 1 Comparison Table of PUF Parameter

<table>
<thead>
<tr>
<th>Ref</th>
<th>[1]</th>
<th>[12]</th>
<th>[15]</th>
<th>[16]</th>
<th>[17]</th>
<th>[18]</th>
<th>Proposed MetaPuf</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uniqueness</td>
<td>46.14</td>
<td>45.24</td>
<td>50.42</td>
<td>40</td>
<td>95</td>
<td>79.8</td>
<td>51.43</td>
</tr>
<tr>
<td>Reliability</td>
<td>99.52</td>
<td>91.14</td>
<td>97.22</td>
<td>95.2</td>
<td>98.7</td>
<td>88.7</td>
<td>99.76</td>
</tr>
<tr>
<td>Uniformity</td>
<td>41.15</td>
<td>43</td>
<td>49.85</td>
<td></td>
<td></td>
<td>43</td>
<td>49.85</td>
</tr>
</tbody>
</table>

* Variation in supply (Average value)
# Variation with Temperature (Average Value)

4. Conclusion
In this paper, a unique property of CMOS latch i.e. metastability is selected to generate response bit which qualifies for acts as response bit. MetaPuf contains two parallel feedback path contains up-down charge pump control movement of Q and QB terminal towards metastable point afterward latch settle to unpredictable high or low state. Inter and intra hamming distance measure that response value is comparable with existing PUF and ideal value. It is open research question to identify new CMOS properties to have the new architecture of PUF.

5. References