A Pair Selection Algorithm for Robust RO-PUF against Environmental Variations and Aging

Md. Tauhidur Rahman, Domenic Forte, Fahim Rahman, and Mark Tehranipoor
ECE Department, University of Florida, Gainesville, FL
rahman.tauhid@ufl.edu, dforte@ece.ufl.edu, fahim034@ufl.edu, and tehranipoor@ece.ufl.edu

Abstract—**Physically Unclonable Functions (PUFs) have emerged as a promising security primitive for low-cost authentication and cryptographic key generation. However, PUF stability with respect to temporal variations still limits its utility and widespread acceptance. Previous techniques in the literature have focused on improving PUF robustness against voltage and temperature variations, but the issues associated with aging have been largely neglected. In this paper, we propose a reliable pair selection algorithm (RePa) that can generate reliable keys from an RO-PUF under aging, voltage, and temperature variations. The RePa approach selects RO pairs with both initial frequency difference and aging rate/slope in mind. The aging slope is predicted by exploiting correlation that exists between frequency variation with respect to voltage and frequency variation with respect to aging. We evaluate RePa with simulations to show that it achieves significant improvement over the current state of the art in terms of reliability and cost. The proposed approach can achieve $\sim 3.0x$ more robust key with only $\sim 2.3x$ more ROs required than the conventional RO-PUF pair selection for the same key size.**

I. INTRODUCTION

In the effort to design secure systems, Physical Unclonable Functions (PUFs) have emerged as a promising security primitive [1]–[3], [5]. A PUF is an integrated circuit that is capable of generating secret responses and/or cryptographic keys by exploiting inherent physical variations from the manufacturing process. Functionally, a PUF maps a challenge (the PUF input) to a response (the PUF output). Identical PUFs with the same manufacturing process provide a different output because of minute variations that exist between each device. In comparison to conventional approaches based on storing keys in non-volatile memory, a PUF can provide volatile, tamper-resistant key storage.

Various silicon PUFs have been reported in literature using different technologies over the past decade, such as ring oscillator based PUF (RO-PUF), Arbiter-based PUF, SRAM-based PUF, Sense-amplifier based PUF, Butterfly PUF, Optical PUF, Flash PUF, Memristor PUF etc. [1]–[3], [5], [7], [13]. The RO-PUF has been more widely utilized than the other PUF types because it has a simple design and is relatively easy to fabricate [3], [5]. Most silicon PUFs suffer from lower reproducibility because they are impacted by the environment and device aging [3], [5], [11], [13]. This causes different responses for the same applied challenge in a PUF and makes the application of PUF less useful. While some applications can tolerate a certain amount of errors, others such as generation of cryptographic keys cannot. To make the PUF output more stable (i.e., to obtain the same response for the applied challenge to a PUF) post-processing techniques such as error correcting code (ECC) and different enrollment schemes are often used. All these approaches add to the overall footprint required by PUFs which is undesired. Among the enrollment schemes (e.g., [1], [12]), only environmental variations have been targeted, but aging can have significant impact on PUF reliability over time [3], [5].

In this paper, we address the above challenges for RO-PUFs. We explicitly capture the impact of aging on RO frequency degradation rate by exploiting the correlation between V_{dd} variations and aging. Aging degradation rates of ROs are estimated and only require RO measurements at different V_{dd} during enrollment. An RO pair selection algorithm called RePa is proposed that selects RO pairs with both initial frequency difference and the above estimated aging rate/slopes in mind. By choosing ROs with similar slopes and large frequency difference, RO-PUF errors due to aging and environmental variations are completely eliminated. The effectiveness of the proposed RePa is validated using both extensive simulations (based on 90 *nm* technology). Under aging and environmental variations, our proposed approach achieves $\sim 3.0x$ more robust key and improves on existing approaches (1-out-of-k [1] and a longest increasing subsequence-based grouping algorithm (LISA) [12]) by several orders of magnitude.

The rest of the paper is organized as follows: In Section II, we discuss the background of conventional RO-PUF, RO-PUF reliability, related work for reliable key generation and limitations of the existing work. In Section III, we discuss the correlation between RO frequency at different V_{dd} and time. We also describe the proposed reliable pair selection algorithm (RePa).The experimental results are presented in Section IV. We conclude the paper in Section V.

II. BACKGROUND AND RELATED WORK

A. Ring Oscillator-based PUF (RO-PUF)

A conventional RO-based PUF generally consists of N identically laid out ROs, two counters, a comparator, and two N-bit multiplexers. Each RO consists of an odd number of inverters and oscillates with a particular frequency. Because of process variation and inherent random noise each RO oscillates with a slightly different frequency than others even though they are designed to be identical. A response bit is generated by comparing the frequency of two identical ROs.

B. RO-PUF Reliability

Both aging and environmental variations (i.e. temperature and V_{dd} variations, measurement noise, intrinsic noise etc.) affect the reproducibility or reliability of a PUF [1]–[3], [5], [9], [12], [13]. Negative bias temperature instability (NBTI) can increase the threshold voltage of a pMOS. On the other hand, hot carrier injection (HCI) results decreased in drain current of nMOS but increases in pMOS [3], [5], [9].The degradation due to HCI depends on switching activity. Both NBTI and HCI shift the device threshold voltage with aging which results in permanent increase in delay.

Like aging, temperature and voltage also directly impact the electrical characteristics of a device. The operating temperature affects the delay of a device by changing its mobility and threshold voltage [3], [5]. As the temperature increases, the threshold voltage of the MOSFET decreases, which leads to an increase in the drain saturation current. At the same time, this decreases the carrier mobility which, in turn, causes a decrease in the drain saturation current. However, mobility degradation dominates, and consequently, the delay in the device increases. Deviation from nominal V_{dd} changes the delay of a circuit and might make the system less robust. However, unlike aging, these effects can be reversed by returning the device to its nominal operating temperature and nominal voltage.

---

*This work was supported in part by AFOSR under award FA9550-14-1-0351.

C. Related Work

RO-PUFs' sensitivity to noise makes it very challenging to provide stable outputs under different operating conditions throughout the chip lifetime. One very common post-processing technique is error correcting code (ECC), which corrects up to a certain number of errors in the PUF output. For example, BCH, [10], is used to obtain reliable key. The syndrome of Index-Based Syndrome (IBS) coding, proposed in [11], does not follow a linear mapping from PUF outputs and parity bits. The concern however is that all these ECC approaches require redundant ROs and ECC decoding unit to support the scheme. Thus, ECC requires large area, power, and timing overheads making it impractical in resource-constrained applications.

Besides ECC, several prior work have attempted to reduce the number of errors in RO-PUF output through intelligent enrollment approaches [1], [5], [12], [14]. 1-out-of-*k* grouping, [1], is used to reduce these errors. However, this grouping mechanism consumes *k* times more area and still does not assure 100% reliable keys. Chain of neighbors pairing for RO-PUF, proposed in [5], for high entropy and reliability. Longest increasing subsequence algorithm (LISA), [12], groups ROs such that PUF output does not change with temperature within the same group. A simplified grouping algorithm with entropy distiller to filter the systematic variation, proposed in [14], is used to increase the robustness. However, none of these work address PUF reliability due to aging. [3] proposed an aging-resistant RO-PUF that shifts the crossover point to the right so that crossover points do not occur during chip lifetime but still requires ECC scheme.

D. Limitations of Existing Work

The limitations of the related prior work can be summarized as follows:

- The prior RO pair selection algorithms are based on initial (at time zero, i.e. enrollment) frequency difference only. This approach does not account for degradation rate/slope due to aging.
- While coding techniques can correct errors in PUF output, they do not directly address reliability issues. In general, they have high area and run-time power overheads.

In this paper, we investigate ways to overcome these issues for the popular RO-PUF. A naive approach would be to extend LISA [12] to aging. For example, one would perform accelerated aging (burn-in) on the RO-PUF, measure each RO frequency after aging, and choose the most reliable RO pairs. However, aging analysis is an extremely slow and expensive process which would not scale well for high volume products. In this paper, we propose an aging-aware RO pair selection algorithm called Reliable Pair selection algorithm (RePa). Our proposed approach avoids accelerated aging. Instead, the rate of aging is estimated from measurements at different temperatures and/or voltages (which are shown to be correlated with aging rate). RO pairs are then selected with frequency difference and aging rate/slope in mind. We also show that the proposed RePa offers robust RO-PUF output against supply voltage and temperature variations.

III. REPA: RELIABLE PAIR SELECTION ALGORITHM IN RO-PUF

Our algorithm is discussed in this section. At first, we discuss the correlation between degradation due to aging and degradation to due environmental variations. Optimal prediction of aging degradation and its associated error is then discussed. Finally, the complete RePa algorithm is given.

A. Predicting Aging Degradation for Reliable RO-PUF

In an RO pair within an RO-PUF, the RO with the higher frequency might experience larger degradation than the lower frequency and might attain the crossover point due to aging (or due to environmental variations) as shown in Figure 1 (b). By knowing the degradation rate due to aging, one could choose the best pairs. A naive approach for identifying such slopes involves accelerated aging. However, accelerated aging of fabricated PUFs is extremely slow and very expensive, making it impractical to apply to millions of PUFs/chips during enrollment (at t=0). Fortunately, we have found that the degradation of a device due to aging (especially, due to NBTI and HCI) can be correlated. The delay degradation parameters influence the change in RO frequency when voltage and/or temperature is changed (as shown below).

Table I. CORRELATION BETWEEN RATE OF FREQUENCY CHANGE DUE TO AGING AND DUE TO ENVIRONMENTAL CONDITIONS

Year	Avg.Frequency Degradation	Corr. Coeff, ρ		
		NT	HT	LT
2.5	8.62%	0.43	0.27	0.31
5.0	9.41%	0.47	0.34	0.34
7.5	11.52%	0.54	0.39	0.34
10.0	13.63%	0.63	0.41	0.47

Evidence demonstrating the correlation between aging degradation and variation from voltage variation for 1024 ROs is shown in Table I (with the same simulation setup described later in Section IV). The correlation coefficient, ρ, between the rate of changing frequency due to aging and due to environmental variations is reported in Table I. The correlation is performed by changing operating voltage, $V_{dd} = 1.2V$, from $V_{dd} - 0.1 * V_{dd}$ to $V_{dd} + 0.1 * V_{dd}$, at nominal temperature (NT), high temperature (HT), and low temperature (LT) while $t = 0$. The results show that the degradation experienced at these corners is positively correlated with aging degradation, meaning that they statistically increase together. The highest correlation is attained by changing V_{dd} at room temperature, which implies that V_{dd} variation alone can predict the aging. The simulation results also show that the correlation becomes stronger with aging.

B. RePa Algorithm

Inspired from the above observation, we propose an algorithm to select ROs in a pair in order to get the most reliable key. At first, we perform additional mathematical analysis of the RO-PUF reliability. The acceptable frequency degradation of an RO in a pair depends on both the initial frequency gap at the nominal operating condition and the frequency degradation of each RO in that pair. Let us consider RO_x and RO_y form a pair in the PUF to generate one bit of the key (as shown in Figure 1 (c)). Let f_{x0} and f_{y0} denote the initial frequencies of the ROs respectively and $f_{x0} > f_{y0}$. After any time t^*, the frequency of RO_x and RO_y are f_{xt^*} and f_{yt^*}, respectively. To obtain a reliable bit, regardless of the aging, the pair must satisfy $f_{xt^*} > f_{yt^*}$ for all $t <= t^*$.

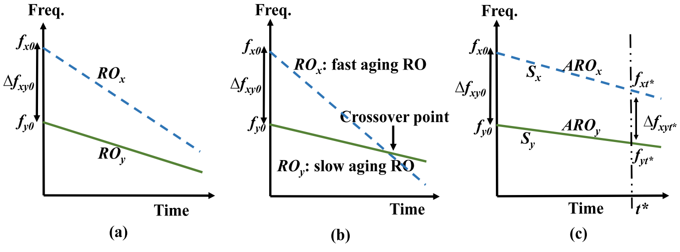

Figure 1. Reliability issue of RO-PUF. (a) stable pair does not experience any crossover-point (b) unstable pair: ROs cross each other and flips the output bit, and (c) ROs to be considered to form a reliable bit.

Because of variations, each RO has a different degradation rate (a different slope) in their frequencies. In the worst-case scenario, RO_x experiences the maximum degradation rate and RO_y experiences the minimum degradation rate so that they cross each other, resulting in a flipped bit. Let S_x and S_y represent the degradation rates (slopes) of RO$_x$ and RO$_y$. Let t^* denote the time over which we want the RO PUF to operate without errors (i.e., bit flips due to aging). In this case, the frequency of the ring oscillators would follow the equations below:

$$\begin{aligned} f_x(t^*) &= f_{x0} - S_x.t^* \\ f_y(t^*) &= f_{y0} - S_y.t^* \end{aligned} \tag{1}$$

where f_{x0} and f_{y0} denote the frequencies of RO$_x$ and RO$_y$ at time zero. Let $\Delta f_{xy0} = f_{x0} - f_{y0}$ denote the initial difference in frequency. Now, the frequency differences at time t^* can be given by:

$$\Delta f_{xyt^*} = \Delta f_{xy0} - (S_x - S_y).t^* = \Delta f_{xy0} - \Delta S_{xy}.t^* \tag{2}$$

To get a stable bit from this pair, the frequency differences at time t^* for ROs, i.e. Δf_{xyt^*}, have to be greater than or equal to zero so that there is no crossover point. This implies

$$\Delta f_{xyt^*} \geq (S_x - S_y).t^* = \Delta S_{xy}.t^* \tag{3}$$

From Equation (3), it is apparent that the reliable bit output can be only obtained, with arbitrary aging degradation, by forming the RO-pair in such a way that it maximizes the initial frequency difference (Δf_{xyi}) and/or minimizes the difference in frequency degradation slope between the ROs (ΔS_{xy}), so that the inequality holds true and the degraded frequencies of the paired ROs do not cross each other.

Algorithm 1: Reliable Pair Selection Algorithm (RePa)

```
Input: Lists of RO physical location $P = p_1, p_2, ..., p_k$,
and corresponding nominal frequency $F = f_1, f_2, ..., f_k$,
predicted rate of frequency change (slope)
$\hat{S} = \hat{s_1}, \hat{s_2}, ..., \hat{s_k}$,
frequency threshold $\Delta f_{th} \geq \Delta f_{th_{min}}$.
begin
1   Create virtual clusters $C = C_1, C_2, ..., C_k$ using X-mean clustering from $\hat{S}$.
2   Resort all ROs within each cluster wrt nominal frequency ($F$) in ascending order into each cluster.
3   For $\forall C_i \in C$ ; $i \in \{1, 2, ..., k\}$
      While (threshold is met)
        Do intra-cluster pair forming
            $\{Pair_{intra} \Rightarrow (f_j, f_{(j+m/2+1)})$ ; $j \in [1, m/2]$;
            $f_{(j+m/2+1)} - f_j \geq \Delta f_{th}; m = clustersize\}$
      ElseDo inter-cluster pair forming
            $\{Pair_{inter} \Rightarrow (f_j, f_r); f_j \in C_i, F_r \in C_l, l > i$;
            $f_j - f_r \geq \Delta f_{th}\}$
      EndWhileLoop
    EndForLoop
4   Deliver list of physical location of formed reliable pairs.
Output: Reliable RO pair list with respective physical locations.
```

Algorithm 1 shows the proposed RePa algorithm. The algorithm takes the physical location(P), nominal frequency (f), and frequency degradation rate/slope estimates ($\hat{S}$) of all ROs as input. In step 1, all the N-ROs are virtually sorted with respect to frequency degradation rate ($\hat{S}$) using $K-mean$ clustering algorithm (more below). A number of W virtual clusters are generated taking ROs that have close/similar slopes. The number and the size of these clusters are optimized using X-means algorithm, [15], which depends on total number of ROs and slope variation. It is preferable that the slope variation of ROs within a cluster show minimum difference (and thus have small cluster resolution) to enhance the reliability of the output. In step 2, all the ROs within each cluster are sorted again with respect to initial frequencies, in ascending order. In step 3, a combination of ROs is checked and RO pairs are formed within each cluster (intra-cluster pairing). However, RePa algorithm searches for other clusters and forms RO pairs within different clusters (inter- cluster pairing) to get target key with least number of ROs. In this step, cluster with lower slope must be paired with another cluster with higher slope in such a way that lower slope cluster's RO must have higher frequency than higher slope cluster's RO so that lower frequency RO experiences higher degradation than higher frequency RO in order to obtain a reliable bit. In RePA, only the physical locations of the pairs are known which does not reveal any information to the attackers.

IV. RESULTS AND DISCUSSION

We validated RePa through HSPICE simulations in 90nm technology node. 20 RO-PUFs were implemented in HSPICE [17] with the Monte Carlo simulations in 90nm technology node. The process variations for 20 different chips were generated with 10% inter-die, 5% intra-die, and 3 sigma variations for L (channel length of transistor), W (channel width of the transistor), V_{th}, and T_{ox} (gate oxide thickness). A total of 1024 ROs were used to implement each RO-PUF, and each RO had 41 inverting stages. A 64-bit response was generated from each PUF. The robustness against environmental variations was also validated by taking measurements at high temperature (HT), low temperature (LT), high voltage (HV), high voltage high temperature (HVHT), and high voltage low temperature (HVLT), where HV= 12% of nominal $V_{dd} = 1.34V$, HT=80^oC, and LT=0^oC. Also, the reported error is the average from 10 measurements.

Table II. AGING BEHAVIOR AND PREDICTION ACCURACY OF ROS IN RO-PUF

Year	ρ	
	Avg.	Worst
2.5	0.54	0.40
5.0	0.57	0.44
7.5	0.61	0.45
10.0	0.67	0.49

Correlation : Average and the worst case (lowest correlation coefficients for prediction) are reported in Table II for 20 PUFs (41-stage 1024 ROs in each) using both HSPICE [17] simulations. The results show that with time the prediction of frequency degradation due to aging gets better over time (i.e. provides better prediction, with higher ρ). The results also indicate that the proposed prediction method can help tolerating more noise, voltage variations or temperature variation.

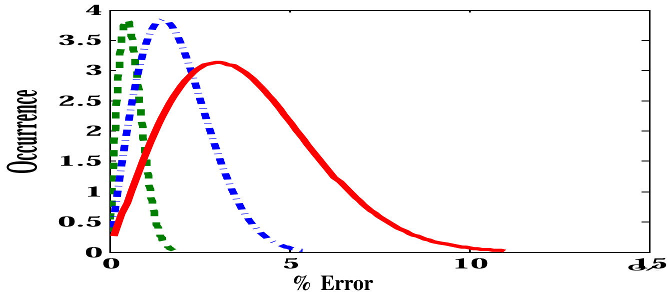

Figure 2. Proposed pair selection algorithm (RePa with $\Delta f_{th} = 2MHz$) improves the reliability of a PUF significantly.

Reliability wrt aging : Figure 2 shows the effectiveness of our proposed algorithm RePa. In RePa, only those two-ROs, that possess almost equal frequency variation rate from the applied V_{dd} variation, are chosen to form a pair. The result shows that the proposed RePa reduces the error by $\sim 2.2x$ compared to that from random selection algorithm without any frequency threshold margin (i.e. the threshold $\Delta f_{th} = 0\ MHz$). However, a threshold of $\Delta f_{th} = 2\ MHz$ improves the result even more by reducing the error by $\sim 11.0x$ than that from the random selection algorithm. A threshold of $\Delta f_{th} = 0\ MHz$ refers that there is no extra RO required but once we increase the threshold, Δf_{th} we need more ROs than random selection. For instance, RePa with $\Delta f_{th} = 2\ MHz$ requires $\sim 1.5x$ ROs than that required by random selection algorithm for $K_{target} = 64$.

Table III. EFFECTIVENESS OF REPA ON RO-PUF AGAINST AGING

	Required ROs		Bits Error	
Δf_{th}	Avg.	Worst	Avg.	Worst
$0MHz$	1x	1x	1.25%	3.75%
2 MHz	1.46x	1.56x	1.56%	4.56%
4 MHz	1.64x	1.74x	0.31%	1.56%
5 MHz	2.00x	2.18x	0%	0%

The result shows that the average and worst percentage of error after 5 years of aging for random pair selection are 5.0% and 9.37%. Figure 2 shows that the initial frequency gap between the two ROs in a pair is important besides the slope of frequency from V_{dd} variations. Table III shows the choice of Δf_{th} in order to get more reliable key. Only average and maximum error are reported in Table III. The second column of Table III shows that the reliability goes up with the Δf_{th} but that requires more ROs than that required by conventional RO-pair selection. Table III shows the reliability and required RO results only for 5 years period for HSPICE simulation data due to limited space. However a detail analysis of HSPICE simulation data shows that the proposed RePa algorithm, with $2.24X$ more ROs than that required by the conventional pair selection, results into 100% reliable key for 5 years for HSPICE simulation data. The table is reported for the worst correlation coefficient, ρ (see Table I).

Table IV. EFFECTIVENESS OF REPA ON RO-PUF AGAINST ENVIRONMENTAL VARIATIONS

Env. Condition	Random	Repa with(Δf_{th})	
		0MHz	5 MHz
High Temp. (HT)	2.11%	0.66%	0.00%
High Voltage (HV)	3.13	0.78%	0.00%
Low Temp (LT)	2.89%	0.93%	0.00%
HVHT	3.13%	1.02%	0.00%
HVLT	3.23%	0.93%	0.00%

Reliability wrt voltage and temperature : Table IV shows the response and effectiveness of the proposed RePa against environmental variations. The effectiveness of RePa was validated at different operating conditions. The result shows that pairing based on rate of changing frequency by applying voltage alone , i.e. Δf_{th}, is well effective and reduces the percentage of error significantly without requiring additional ROs. But to make the PUF 100% robust we need to increase the threshold between two ROs in a pair, in cost of some additional ROs.

Uniqueness : The results show that the uniqueness of the proposed RO-PUF is 0.46 (close to ideal value 0.5) which indicates that the proposed RePa algorithm can be identified uniquely with a given challenge. Besides, the RePa is secure because it stores only the physical location of a pair which does not reveal any information.

Randomness : NIST test suite [19], [20] is used to evaluate the randomness of bit streams generated by both RO-PUF with RePa and RO-PUF without applying RePa for 20000 bit-sequence. The RO-PUF also passes NIST random test without RePa ($> 96.7\%$) and with RePa ($> 95.3\%$).

Table V. AREA OVERHEAD COMPARISON FOR 64-BIT KEY WITH BCH SCHEME [10] (FPGA IMPLEMENTATION)

% Error	RO-PUF with RePa	RO-PUF with ECC	1-out-of-*k* [1]	LISA [12]
3.0%	532 LUTs	1889 LUTs	1556 LUTs	1245 LUTs
4.0%	544 LUTs	2078 LUTs	1802 LUTs	1782 LUTs
10.0%	762 LUTs	5013 LUTs	2110 LUTs	2043 LUTs

Area Overhead : Table V shows the area overhead comparison for worst ρ, between RO-PUF without and with the proposed RePa algorithm for a 64-bit key generation (without considering required memory for storing the information of pairs) with BCH scheme [10]. A system with the RO-PUF without any ECC scheme requires a considerably smaller PUF footprint. We compare the reliability, area, etc. for RO PUFs without RePa (random RO pairs used), with RePA, and with existing techniques (1-out-of-k [1] and LISA [12]) for approximated $\Delta f_{th} = 4.67MHz$ in average from 100 ROs of each PUF for K_{target}=64.

V. CONCLUSION

In this work, we have proposed the RO pair selection algorithm, RePa, for robust RO-PUF against aging and environmental variations. We also have proposed a method to predict aging degradation from applied voltage variation. The simulation results show that the proposed RePa reduces the area overhead significantly and provides a more robust key. In future work, we will determine minimum gap between two ROs in a pair, Δf_{th}, for the proposed RePa.

REFERENCES

[1] G. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in Design Automation Conference, pp. 9–14, 2007.

[2] C. Herder et.al., “Physical Unclonable Functions and Applications: A Tutorial,” Proceedings of the IEEE, vol.102, no.8, pp. 1126-1141, 2014.

[3] M. Rahman et.al., “Aro-puf: An aging-resistant ring oscillator puf design,” in Design, Automation and Test in Europe Conference and Exhibition (DATE), pp. 1–6, 2014.

[4] Md. Tauhidur Rahman et.al., “An Aging-Resistant RO-PUF for Reliable Key Generation,”in IEEE Transactions on Emerging Topics in Computing, vol. 3, 2015.

[5] A. Maiti and P. Schaumont, “The Impact of Aging on a Physical Unclonable Function,” Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 22, pp. 1854-1864, 2014.

[6] M. Bhargava and K. Mai, “An efficient reliable PUF-based cryptographic key generator in 65nm CMOS,” in Proceedings of the conference on Design, Automation and Test in Europe, pp. 70, 2014.

[7] A. Mazady et al., “Memristor PUFA Security Primitive: Theory and Experiment,” Emerging and Selected Topics in Circuits and Systems, IEEE Journal on , vol.5, no.2, pp.222,229, June 2015.

[8] Y. Lu et. al., “Statistical reliability analysis under process variations and aging effects,” in Proceedings of the 46th Annual Design Automation Conference, pp. 514-519, 2009.

[9] A. Hosey et al., “Advanced Analysis of Cell Stability for Reliable SRAM PUFs,” Test Symposium (ATS), 2014 IEEE 23rd Asian, pp.348-353, 2014.

[10] J.H. van Lint, “Introduction to Coding Theory,” Springer Verlag, 1992.

[11] M. Yu, and S. Devadas, “Secure and Robust Error Correction for Physical Unclonable Functions,” Design & Test of Computers, IEEE, vol.27, no.1, pp. 48-65, 2010.

[12] C. Yin and G. Qu, “LISA: Maximizing RO PUF’s secret extraction,” in Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on, pp. 100-105, 2010.

[13] K. Xiao et al., “Bit selection algorithm suitable for high-volume production of SRAM-PUF,” Hardware-Oriented Security and Trust (HOST), IEEE International Symposium on, pp. 101-106, 2014.

[14] C. Yin, G. Qu and Q. Zhou, “Design and implementation of a group-based RO PUF,” in Proceedings of the Conference on Design, Automation and Test in Europe, pp. 416-421, 2013.

[15] D. Pelleg et al., “X-means: Extending K-means with Efficient Estimation of the Number of Clusters,” in ICML, pp. 727-734, 2000.

[16] X. Guo et al., “Modeling and Experimental Demonstration of Accelerated Self-Healing Techniques,” in Proceedings of Design Automation Conference on Design Automation Conference, pp. 1-6, 2014.

[17] http://www.synopsys.com/

[18] W. Wang et al., “Statistical prediction of circuit aging under process variations,” IEEE Custom Integrated Circuits Conf., pp. 13-16, 2008.

[19] A. Rukhin et al., “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” NIST Special Publication 800-22 Rev1a, 2010.

[20] M. T. Rahman et al., “TI-TRNG: Technology independent true random number generator,” Design Automation Conference (DAC), 2014 51st ACM/EDAC/IEEE, pp.1-6, 2014.

[21] S.M. Kay, “Fundamentals of statistical signal processing, Volume III: practical algorithm development,” Pearson Education, 2013.