Enhanced Arbiter PUFs using custom sized structures for reduced noise sensitivity

Andreas Herkle, Markus Schuster, Joachim Becker and Maurits Ortmanns

University of Ulm

Institute of Microelectronics,

Albert-Einstein-Allee 45, Ulm, Germany

Email: andreas.herkle@uni-ulm.de

Abstract—This paper presents a simple yet effective way of improving delay based Physical Unclonable Functions by changing transistor gate sizes only. All utilized components of an Arbiter PUF were simulated in a 90 nm CMOS process with sweeps applied to each gate dimension. By evaluating an Arbiter PUF consisting of the proposed enhanced components, we show that the intra Hamming distance can be decreased by over 60 % and the inter Hamming distance can be fixed at 50 %.

I. INTRODUCTION

Physical Unclonable Functions (PUFs) are an efficient way of generating random bits from custom designed submicron circuits. By utilizing the uncontrollable mismatch of integrated circuits resulting from fabrication, each instance of a PUF provides a unique behavior, enabling identification and authentication without the need for secure storage. Although the majority of publications in this emerging field of research were published within the last six years, the most common delay based PUFs, namely the Arbiter PUF and the Ring Oscillator PUF, have already been published in 2004 [1] and in 2007 [2] respectively. Since then, much effort has been spent on improving their statistical metrics, mainly by increasing the circuits overall delay and variance. Most prior work used additional circuitry [3], modified circuit components [4] or manipulation of the production process [5], [6]. To our best knowledge, no investigation on improving Arbiter PUFs by modifying the existing structures' sizes was done yet. In this work, we will present enhanced components for an Arbiter PUF which were analyzed by extensive Monte Carlo simulations in Cadence Virtuoso with models of a 90 nm CMOS process and applied transient noise with a maximum frequency of 100 GHz. All components' transistor gate size parameters were investigated by sweeping and statistical analysis.

The paper is organized as follows. Section II presents the Arbiter PUF and the methodologies of our approach. Section III presents our proposed enhancements of the individual components. Section IV evaluates the results of an enhanced Arbiter PUF. Section V concludes our work.

II. ARBITER PUF METHODOLOGY

A. Working principle of Arbiter PUFs

Fig. 1 illustrates an Arbiter PUF which instantiates multiple rows of delay-line-arbiter circuitry. A single row consists of a

Fig. 1. Illustration of an Arbiter PUF consisting of switches (green), delay elements (red) and RS-Latches as Arbiters (blue)

signal source triggering a rising edge on two delay lines racing against each other. Based on the configuration set by challenge bits $c_{1...8}$, the signal paths are either swapped by switching elements or stay unaltered. Additional buffers between the switches increase the overall delay. The decision element at the end of the delay lines produces an output bit of either '1' or '0' depending on whether the upper or lower input arrives first. The output bits of all rows together form the response of the Arbiter PUF, which can vary significantly depending on the challenge. The union of a challenge and its respective response is called a Challenge-Response-Pair (CRP), which enable the use of authentication schemes. Since collecting a large amount of CRPs is necessary to model the PUFs behavior, the Arbiter PUF is classified as a "Strong PUF" in opposite to "Weak PUFs", which have no CRP functionality and rather serve identification or key generation purposes.

B. Method

In order to get a good overview of the influence of all transistor parameters regarding the gate sizes, we performed Monte Carlo simulations on them for every building block of an Arbiter PUF [7], utilizing the same blocks as in [1] to achieve a good comparison. We define characterizing measures for each block and mainly focus on evaluating two standard deviations on them: due to mismatch (σ_{mc}) and transient noise (σ_N). These are the most influencing factors which define the quality of the PUF's metrics at stable environmental conditions, which are the intra Hamming Distance (HD) as the average number of flipping output bits from repetitive readout of a single PUF as well as the inter-HD as the average number of output bits which are different on two individual

Fig. 2. Decision accuracy $\Delta t_{20\%}$ of a standard sized latch over arrival time difference of two mismatched delay lines

PUFs. For the Arbiter PUF's delay elements, the mean delay μ does not contribute to the quality measures, as every row is designed symmetrically. But increasing the mismatch related variation of the delay elements σ_{mc} enables better distinctness as individual instances of the circuit in average differ more from each other. Reducing the influence of circuits noise σ_N relatively enables more stable readouts which benefit the quality of the PUF greatly.

III. ARBITER PUF COMPONENT IMPROVEMENT

A. Decision element design improvement

The most commonly used decision element in an Arbiter PUF is a simple latch. Most simply, it consists of two cross-coupled NAND gates forming a Set-Reset-Latch (SR-Latch). When both inputs S and R of the latch are low, the output Q is undefined and can only be settled by the first rising edge on the faster delay line. Mismatch induced bias and transient noise influence the decision, especially when the rising edges at both inputs arrive within a short time frame which is the case if the delay lines show little mismatch. A standard sized latch from the used 90 nm CMOS process was simulated and its decision accuracy determined using transient noise simulations. Thereby, we defined the accuracy measure $\Delta t_{20\%}$ as the threshold for which 20 % of the decisions for the output Q are set correctly to a binary '1' for a positive input time mismatch as illustrated in Fig. 2. With this threshold being zero this resembles an ideal decision element providing a sign decision function. After sweeping all the latch's gate sizes, the best improvement was found as an increase of W_n , the gate width of the NAND's nMOS transistors, while all other parameters are left at minimum size. Fig. 3 (a) illustrates the effect, showing that the arbiter's sensitivity to noise reflected as $\Delta t_{20\%}$ is reduced by 76 % from 0.17 ps at $W_n = 120$ nm to 0.04 ps at $W_n = 1 \mu\text{m}$. This improvement can be explained by reducing the input referred noise by increasing the input transistors' transconductance gm , while the gain of the latch drops only slightly.

We also analyzed the latch decision accuracy for the input signals at S and R, differing from each other in a delay Δt in the arrival time. The analysis was done for rising edges with a slow slew rate ($t_{rise} = 1$ ns) and a fast slew rate ($t_{rise} = 10$ ps) with transient noise influence. The probabilities for incorrect decisions are plotted in Fig. 4 (a) for the difference in time

Fig. 3. Influence of latch's nMOS width on noise sensitivity and bias.

Fig. 4. Influence of the signal rise time on the latch's decision accuracy

Δt and (b) for the difference in voltage ΔV . For the fast rising edge, the decision accuracy becomes much higher if Δt as the difference in the arrival time is large enough. The fast rising edge offers a greater potential to reduce erroneous decisions, when Δt becomes larger then 0.5 ps. For an arbiter PUF, edges on both delay paths have the same rise time due to the symmetric design of the circuit. Thus, ΔV depends on Δt , which itself depends on the delay statistics of the signal paths and can not be influenced directly by the arbiter. Therefore, to improve the arbiters' decision ability even further, it is important that at least the last stage driving the latch's inputs produces a fast rising edge.

The decision element should ideally be mismatch free, which would yield a bias-free arbiter decision. The result of unavoidable mismatch in the latch is shown in Fig. 5 (a), where the switching point of a standard sized latch is illustrated over a few Monte Carlo runs without noise. Ideally, the switching point should be at $\Delta t = 0$ ps, deciding any negative Δt to a binary '1' and vice versa; but for mismatch in the latch, a bias in the switching point with a standard deviation of 1.45 ps impacts the decision on the delay lines. Simulations have shown that the most efficient reduction comes with the same changes applied before to reduce the latch noise sensitivity, namely an increased size of W_n . The effect is illustrated in Fig. 3 (b) as a drop by 62.4 % from 1 ps at $W_n = 120$ nm to 0.38 ps at $W_n = 1 \mu\text{m}$. Concludingly, as known from analog circuit design, the decision elements input referred noise can be reduced by increasing its input transistor transconductance by increasing its width W_n , while with this also its own mismatch and a resulting decision bias is reduced significantly.

Fig. 5. Mismatch influence on the latch, (a) shifts in the switching point, (b) distribution of the switching point

B. Delay element design improvement

The simple CMOS inverter is the most basic logic element used in delay based PUFs, not only in Arbiter PUFs but also in Ring-Oscillators based PUFs. When used in digital circuits, the width of the pMOS is usually set to approximately the double of the nMOS width due to its lower charge carrier mobility, approximating a switching point at $V_{DD}/2$. In contrast to this paradigm, the most desirable characteristic of the inverter for delay based PUFs is its delay, specifically with a high standard deviation. As already mentioned, both statistics in PUF circuits at nominal conditions mainly vary from their nominal values due to mismatch and transient noise. While mismatch is desired for PUFs, transient noise introduces an unwanted randomness into the inverters delay and therefore contributes to a non-zero intra-HD between multiple measurements. Therefore a small width and a large length of the transistor gates is widely accepted to be the most efficient way to increase both the delay and its standard deviation [4]. Our simulation results confirmed this claim but we found that this is not the only way to improve an inverters delay characteristics for PUFs.

The analyzed delay element is a simple buffer built up by two inverters of equal size in series. When sweeping both W_n and W_p , simulations showed the expected behavior that small gate widths increases the delay's standard deviation of mismatch (which is good for the inter-HD) and noise (which is bad for the intra-HD). However for larger gate widths, the deviation caused by mismatch drops to 48 %, but the deviation caused by noise drops even more to 33 %, indicating that an exploitable trade-off between randomness and stability might exist, which was found for when only the gate width W_n of the nMOS is changed.

Fig. 6 plots the buffers mean delay μ and its standard deviation due to mismatch σ_{mc} , displayed separately for the rising and the falling edge. While the falling edge is almost not affected by changes in W_n , the rising edge contributes to a great increase of both statistics at larger gate widths. Fig. 7 plots the effect of an increase of W_n on the buffers' delay characteristics for a rising edge. The increase of the average delay μ by 140% is outnumbered by the even larger increase of the variation of σ_{mc} by 228%, while the noise standard deviations σ_N increases by only 70 %. This effect is explained by the unaltered mismatch of the pMOS with constant size,

Fig. 6. Influence of the inverter's nMOS width on mean delay (a) and mismatch induced standard deviation (b) for rising (dashed) and falling (dotted) edges

Fig. 7. Delay statistics of the inverter for different widths of the nMOS, (a) mean delay, (b) standard deviation due to mismatch (red) and noise (blue)

while the mismatch of the nMOS becomes smaller with larger W_n , but also its parasitic load capacitor from the next inverter stage becomes similarly larger. Thus, the rising edge delay is increased by the increased load capacitance, while its delay variation is mostly defined by the unaltered pMOS.

C. Switch element design improvement

In [2], switches are used to implement a challenge-response behavior in order to enable applicability in authentication schemes. The utilized switching element was a simple transmission gate. In order to get comparative results we also implemented transmission gates as path switches with additional inverters as driving input buffers and loading output buffers. The signals connected to the inputs of the switch are propagated in either a straight or a crossed way, depending on the respective challenge bit, opening or closing the respective transmission gates.

When analyzing the transmission gate dimensions, a difference has to be expected regarding if either a rising or a falling edge has to be propagated. Therefore the sweeping simulations were adjusted to also propagate a falling edge (t_{fall}) in addition to a rising edge (t_{rise}). An increase of unwanted noise variance σ_N directly proportional to the increase of σ_{mc} was found for both the nMOS and the pMOS transistor of the transmission gate and both types of edges, which is consequently not beneficial for the PUF metrics.

Thus the transmission gates are left at minimum size and the delay variance of the switches is mostly defined by its driving buffers. Obviously, a very similar result is expected as

Fig. 8. Standard deviation of the switch's delay for different nMOS gates widths of the driving buffers, due to mismatch for different edges (a) and for a rising edge (b) due to mismatch (red) and noise (blue)

for the main delay element, where W_n was the most promising gate dimension to be tuned. The mismatch induced standard deviation σ_{mc} for both edges is plotted in Fig. 8 (a), showing that for propagating a rising edge, the increase of W_n causes a beneficial and larger increase than for the falling edge. Fig. 8 (b) shows σ_N in comparison to σ_{mc} for the rising edge. While σ_{mc} increases significantly for larger W_n , σ_N changes only slightly. The behaviour matches that for the inverters in Fig. 7, with the same implications that a larger W_n is beneficial in terms of increasing the delay variance while the noise variance increases less significantly.

IV. ENHANCED ARBITER PUF EVALUATION

Based on the previous findings we present an enhanced Arbiter PUF in comparison to an implementation utilizing minimum sized transistors as a reference. For the enhanced components, it was found that asymmetrically increasing the gate width of all inverter nMOS transistors improves the delay standard deviation and the arbiters decision accuracy, while the delay elements noise is minorly affected. The proposed enhanced Arbiter PUF therefore utilizes transistors of minimum sizes except for the nMOS gate widths: $L_{n,p} = 100$ nm, $W_p = 120$ nm, $W_n = 1 \mu\text{m}$. This affects every inverter, both as delay element and as buffer for the transmission gates, and the latch as the arbiter element.

For evaluation purposes, the test Arbiter PUF is build up by 8 rows of delay lines with 8 switches and an arbiter in order to create an 8 bit output per 8 bit challenge. Following each switch, two inverters act as additional delay elements. The final results are illustrated in Fig. 9. The inter-HD stays almost constant, changing from 50.3 % to 50.0 %, but this had to be expected as no process-variation was taken into account. But regarding the intra-HD as the measure of stability, the results show a large improvement, reducing the intra-HD by more than a factor of 2 from 6.57 % to 2.59 %. This means, that at the reasonable expense of an increased circuit area, an improved stability of repeated readouts can be achieved due to the highly reduced noise sensitivity of the several components.

Fig. 9. Histograms illustrating (a) intra-HD (reproducibility) and (b) inter-HD (uniqueness) of the proposed enhanced Arbiter PUF

V. CONCLUSION

In this paper, we presented a study on an enhanced Arbiter PUF. The enhancements were limited to changes in the transistors gate dimensions to highlight the possibilities of custom designed components for PUFs. We have found that two major improvements can be easily achieved by increasing the gate width of all nMOS transistors. First, the decision capability of the RS-latch acting as an arbiter for signals rising edges with short time difference is enhanced. This enhancement becomes even better when the propagated edges have short rise times which translates either to a minimum L in all devices, or in an additional driver buffer in front of the latch. Secondly, the influence of noise can be decreased for both the decision element and the delay elements by increasing W_n . It was shown that the standard deviation due to noise increases with a significantly smaller magnitude than the standard deviation due to mismatch. The evaluation of a simulated Arbiter PUF composed of these enhanced components with adjusted transistor dimensions showed a highly improved intra-HD, reducing it by a factor of more than 2.

REFERENCES

- [1] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on*, June 2004, pp. 176–179.
- [2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02. New York, NY, USA: ACM, 2002, pp. 148–160. [Online]. Available: <http://doi.acm.org/10.1145/586110.586132>
- [3] R. Kumar, V. C. Patil, and S. Kundu, "Design of unique and reliable physically unclonable functions based on current starved inverter chain," in *2011 IEEE Computer Society Annual Symposium on VLSI*, July 2011, pp. 224–229.
- [4] M. Cortes, G. Araujo, and J. Capovilla, "Improving the statistical variability of delay-based physical unclonable functions," in *2015 28th Symposium on Integrated Circuits and Systems Design (SBCCI)*, Aug 2015, pp. 1–7.
- [5] R. Kumar, S. N. Dhanuskodi, and S. Kundu, "On manufacturing aware physical design to improve the uniqueness of silicon-based physically unclonable functions," in *2014 27th International Conference on VLSI Design and 2014 13th International Conference on Embedded Systems*, Jan 2014, pp. 381–386.
- [6] D. Forte and A. Srivastava, "Manipulating manufacturing variations for better silicon-based physically unclonable functions," in *2012 IEEE Computer Society Annual Symposium on VLSI*, Aug 2012, pp. 171–176.
- [7] M. Schuster, "Enhanced physical unclonable function structures in mixed-signal mos technology," Masters's Thesis, University of Ulm, Germany, 2013. [Online]. Available: <http://dx.doi.org/10.18725/OPARU-2525>