Characterization of the Bistable Ring PUF

Qingqing Chen[*‡]
[*]Institute for Electronic Design Automation
Technische Universität München
Munich, Germany
qingqing.chen@tum.de

György Csaba[†‡]
[†]Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN, United States
gcsaba@nd.edu

Paolo Lugli
[‡]Institute for Nanoelectronics
Technische Universität München
Munich, Germany
lugli@tum.de

Ulf Schlichtmann
Institute for Electronic Design Automation
Technische Universität München
Munich, Germany
ulf.schlichtmann@tum.de

Ulrich Rührmair
Institute for Security in Information Technology
Technische Universität München
Munich, Germany
ruehrmai@in.tum.de

***Abstract*—The bistable ring physical(ly) unclonable function (BR-PUF) is a novel electrical intrinsic PUF design for physical cryptography. FPGA prototyping has provided a proof-of-concept, showing that the BR-PUF could be a promising candidate for strong PUFs. However, due to the limitations (device resources, placement and routing) of FPGA prototyping, the effectiveness of a practical ASIC implementation of the BR-PUF could not be validated. This paper characterizes the BR-PUF further through transistor-level simulations. Based on process variation, mismatch, and noise models provided or suggested by industry, these simulations are able to provide predictions on the figures-of-merit of ASIC implementations of the BR-PUF. This paper also suggests a more secure way of using the BR-PUF based on its supply voltage sensitivity.**

Keywords—physical cryptography; bistable ring PUF; BR-PUF; physical unclonable function; identification; authentication.

I. INTRODUCTION

Since the introduction and the formalization of its concept [1, 2], *physical(ly) unclonable function* (PUF) has become a hot topic in the field of physical cryptography. This new concept for physical cryptography makes use of disordered structural information, e.g., uncontrollable manufacturing variations, to generate and store secrets. Based on the specially and intentionally designed process-variation-sensitive behavior of PUFs, such embedded secrets can be dynamically extracted to serve in various security protocols [3, 4]. The embedded secrets of PUFs are usually represented as *challenge-response pairs* (CRPs). According to the number of CRPs that a PUF can produce, PUFs can be classified into *weak PUFs* (e.g., the SRAM PUF [4]), whose CRPs could be completely read out in a relatively short time period (e.g., seconds to weeks), and *strong PUFs* (e.g., the Arbiter PUF [5]), for which the measurement/characterization of all or a significant part of their CRPs within a reasonable timeframe is infeasible [6, 7]. Due to that difference, weak PUFs and strong PUFs are suitable for different application scenarios: strong PUFs are able to serve in challenge-response authentications, while weak PUFs are usually only used as *physically obfuscated keys* [7]. However, circuit-based realization of PUFs has never been an easy task, especially for strong PUFs, since they require a practically infinite number of CRPs on a size-limited PUF instance. Arbiter PUFs and their variants [5] are one candidate and have been for many years the only one. However, due to their linear nature, Arbiter PUFs as well as some of its variants, e.g., those with feed-forward stages, are vulnerable to modeling and machine learning attacks, with which the CRPs of a PUF can be effectively predicted, given a relatively small proportion of its CRPs that can be collected in a short time period [5, 6].

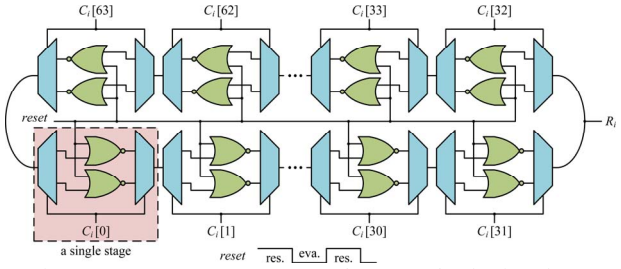

Figure 1. A 64-stage BR-PUF (res./eva.: reset/evaluation phase)

Recently, another strong PUF candidate called the *Bistable Ring PUF* (BR-PUF) was proposed [8]. The basic idea of the BR-PUF is based on the fact that an inverter ring consisting of an even number of inverters, which is called a *bistable ring*, has two possible stable states [8]. Theoretically, the circuit would converge equally possibly in either stable state, when it is released from a "fair" unstable state, e.g., when all the nodes between the inverters are in the 0-Volt state. Due to the nonlinear nature of this converging process, a simple modeling technique of such kind of circuit, which is usually the basis of machine learning attacks, has never been found. According to [8], a BR-PUF (Fig. 1) can be built using NOR-gates (so that the rings can be reset to the 0-Volt state prior to every evaluation phase) and multiplexers (so that an exponential number of bistable rings can be created by applying different C_i challenges). The response R_i could take the voltage of a node between any two neighboring stages. FPGA prototyping has presented a proof-of-concept of the BR-PUF, showing that the new architecture could be a promising strong PUF candidate

978-3-9810801-8-6/DATE12/©2012 EDAA

[8]. However, the results obtained from the FPGA prototype are still some distance away from those of an ASIC implementation, which would be commercially the most realistic application scenario for PUFs. Besides, since the on-chip supply voltage of the prototype in [8] was fixed, the new PUFs' reliability against supply voltage variations has not yet been examined. This paper presents transistor-level SPICE simulations of an ASIC design of the BR-PUF. Compared to FPGA prototyping, SPICE simulations are much slower, but they can provide the possibility to study the BR-PUF in detail and are not limited to predefined FPGA resources.

Based on realistic device models, process variation and mismatch models, as well as noise models provided or suggested by industry, this paper provides a closer look at the figures-of-merit of BR-PUFs with regard to their settling times, uniqueness and the reliability against noises, temperature variations and supply voltage variations, separately. This would be hard to achieve using FPGAs since the impact of environmental variations and circuit noises can hardly be isolated or separated. The rest of the paper is organized as follows: Sec. II presents the circuit design of the BR-PUF and the experimental setup. Sec. III presents the simulation results, i.e., the figures-of-merit of the ASIC BR-PUFs. Sec. IV summarizes the results, and suggests a more secure way of using the BR-PUF based on the results presented in Sec. III.

II. Circuit Design and Experimental Setup

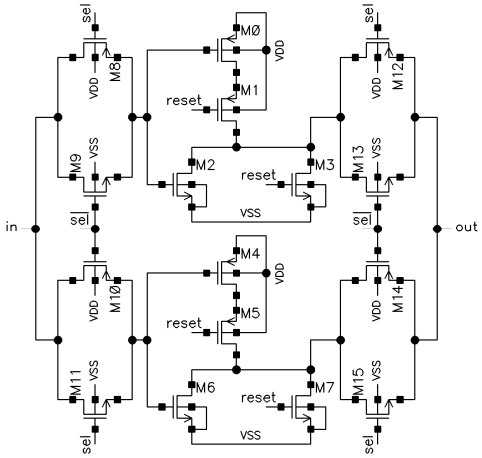

Figure 2. Schematic of a basic stage design for BR-PUFs

In our circuit, which is based on a commercially available technology, a basic stage design shown in Fig. 2 is duplicated multiple times to create the BR-PUF. In Fig. 2, transistors M0, M1, M2 and M3 implement one NOR-gate; M4, M5, M6 and M7 make up the other; M8, M9, M10 and M11 implement the multiplexer at the input; and M12, M13, M14 and M15 constitute the demultiplexer at the output. An even number of such stages are then chained in a ring through their *in* and *out* ports to form the whole BR-PUF. Based on the "nominal" design, randomly generated process variations and mismatch data were applied to the design according to statistical models from industry. With these data, we were able to mimic the fabrication process and create PUFs embedding the secrets that originate from fabrication imperfection. To study the impact of noise, temperature and supply voltage variations on the PUF reliability, noise models suggested by industry were applied, and temperature as well as supply voltage parameters were swept through several discrete values for simulations.

In practice, due to the relatively large number of transistors, and due to the fact that the BR-PUF is basically a loop structure causing many more computational iterations in simulations, the slowness of SPICE simulations has been the main drawback restricting the effectiveness of this work. To combat that, the computational workload was dynamically distributed onto different computational servers using central monitoring and control scripts. Since our simulation tool does not directly support such special requirements, namely, Monte Carlo (process variation and mismatch) simulation, noise simulation, and parameter sweep, all combined at the same time, extra programs were developed to automate our simulations. Process variation and mismatch data were generated and merged into device model cards by MATLAB scripts, and simulation parameters, e.g., transient noise parameters, were added to circuit netlists by scripts. Transistor-level simulations were finally carried out by Cadence Virtuoso Spectre, and noise simulations were achieved through activating the transient noise option of Spectre. Simulation results were collected and post-processed by Perl and MATLAB scripts. As generating CRPs from a BR-PUF with more than about 50 stages could take a huge amount of time, e.g., a single transient simulation for 1000 CRPs of a 64-stage BR-PUF, with each CRP having an evaluation cycle of two microseconds (transient time), could take longer than one month, we decided to use 32-stage BR-PUFs for our simulations. Although a 32-stage BR-PUF is not necessarily secure according to [8], statistical analyses on their CRPs should provide valuable estimations for BR-PUFs with tens of to hundreds of stages. Based on the simulations of 15 instances of a 32-stage design, operating at different temperatures, under different supply voltages, or exposed to random noises, we obtained the results presented in Sec. III.

III. Results and Discussion

A. Settling Time

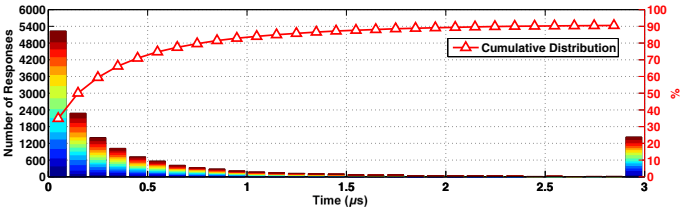

Figure 3. Distribution of the settling times of 15 BR-PUFs

The characterization of response settling times of BR-PUFs can help to determine the transient simulation time for further experiments as well as the evaluation time required before measuring PUF responses. Fig. 3 shows the distribution of the settling times of responses measured from 15 PUF instances, with each instance generating 1000 challenges (in this paper, unless specified otherwise, the default temperature for simulations is 25˚C and the default supply voltage is 2.5 V). In Fig. 3, each color in the stacked bars denotes a different PUF instance, representing the number of responses with settling times in the corresponding range. The rightmost bar denotes all the responses that are still unstabilized in 2.896 μs. The figure

shows that the settling time distribution of the simulated PUF instances generally matches that of the FPGA prototype in [8]. The cumulative distribution shows that 90% of the responses stabilize in 2.315 μs. Besides, it can be seen from Fig. 3 that the distribution does not vary much among different instances. Therefore, the time period of transient simulations and that of evaluation phases determined from a small group of PUF instances should also apply to every additional instance. For the rest of the simulations, we used a transient simulation time of 1 μs for each clock cycle of the *reset* signal (see Fig. 1). In each cycle, the reset phase covers 4 ns and the evaluation takes 996 ns, the last 96 ns of which were used as a confirmation time to determine whether the response has stabilized or not. Therefore, for the rest of our results, the longest possible settling time of stabilized responses would be 0.9 μs. During this period, about 82% of the responses get stabilized.

B. *Uniqueness and Reliability against Noises*

Conventionally, the two most important figures-of-merit, uniqueness and reliability, of PUFs are represented by the (normalized) inter-die and intra-die Hamming distances (HDs) of their responses, respectively [8].

1) *Conventional inter-/intra-die Hamming distances*

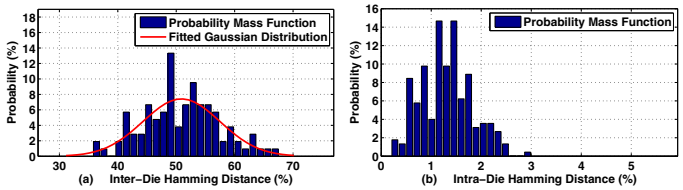

Figure 4. Probability distribution of inter-/intra-die HDs of BR-PUFs

For the calculation of conventional inter-/intra-die HDs, we simply use the readout response values at the end of evaluation phases, regardless of whether the responses have stabilized or not. Based on the CRPs collected from 15 PUF instances, with each providing 1000 CRPs, we obtained the distribution of inter-die HDs shown in Fig. 4(a). The average inter-die HD of all instance pairs is 50.9%, and all the pairwise HDs lie between 35.7% and 67.6%. The distribution generally follows Gaussian distribution. A fitted Gaussian distribution has the following parameters: μ = 50.9, σ = 6.6. Intra-die HDs were calculated from CRPs generated by PUF instances simulated with, for each instance, ten different sets of random transient noises (Spectre transient noise settings: *fmax* = 10 GHz, *fmin* = 1 kHz, *scale* = 1). The probability distribution of intra-die HDs is shown in Fig. 4(b). The intra-die HDs range from 0.2% to 3.0%, with the average value of 1.3%. Therefore, both figures-of-merit of uniqueness and reliability against noises are close to their ideal values, i.e., 50% (highest identifiability) and 0% (ideal reproducibility), respectively, and the highest intra-die HD is still far below the lowest inter-die HD, indicating a much better implementation in the corresponding respects compared to its FPGA-based counterpart presented in [8].

2) *Interval inter-/intra-die Hamming distances*

Due to the specialness of BR-PUFs in the sense that their responses may have a broad range of settling times, [8] suggested a method to make use of this specialness and improve their performance (increase the difference between inter- and intra-die HDs) by selectively[1] using CRPs with the settling time in a proper range. We call such an inter-/intra-die HD calculated from PUF responses that stabilize during a specific time interval an *interval inter-/intra-die HD*. It was found in [8] that the CRPs with longer settling times have larger inter-die HDs that approach 50%, while the intra-die HDs increase relatively slowly as the settling times get longer, making the difference between inter- and intra-die HDs larger and larger until some point where the difference reaches its optimum. Therefore, using the method that enrolls only CRPs which stabilize in a proper interval (e.g., a short interval before the optimum point, where the interval inter-die HD is close to 50% and the interval intra-die HD is still relatively low) in a PUF-based protocol would effectively improve the combined performance of uniqueness and reliability. However, Fig. 5 shows that, for the symmetrical PUF instances in this work, interval inter- and intra-die HDs do not vary much in different settling time ranges up to 0.9 μs. Even CRPs which stabilize very quickly have the same high quality (inter-die HD close to 50% and intra-die HD close to 0%). Therefore, the method proposed in [8] does not make sense for its ASIC-based counterpart in our work, since the performance is already almost optimum in all time intervals.

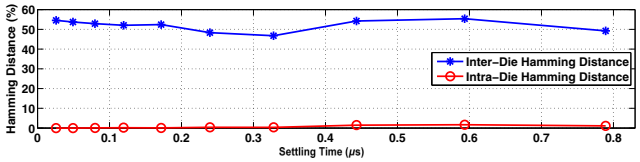

Figure 5. Interval HDs of BR-PUFs (the position of each node in the settling-time-axis is the middle point of its corresponding settling time range)

C. *Reliability against Temperature Variation*

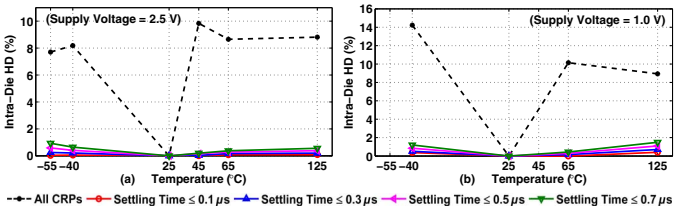

Figure 6. Reliability of BR-PUFs against temperature variations

To analyze the temperature sensitivity of BR-PUFs, we simulated the 15 PUF instances at several different temperatures from -55˚C to 125˚C and under two different supply voltages, 2.5 V and 1.0 V. Taking the CRPs measured at 25˚C as the reference, we calculated the average HDs of all the instances at different temperatures. Fig. 6 shows that when taking all the CRPs, including unstabilized ones, into calculation, the temperature sensitivity is relatively high, which confirms the magnitude of temperature sensitivity observed in [8]. In our work, the average HDs between simulations at different temperatures under the supply voltage of 2.5 V lie between 7.7% and 9.9%. Although these values are already far below the average inter-die HD between PUF instances, the extended authentication protocol for environmental-condition-sensitive PUFs proposed in [8] could be used to further

[1] "Selectively" here refers to the selection of CRPs to be stored in the PUF enrollment phase in, e.g., a PUF-based authentication protocol [3].

diminish the temperature impact. Nevertheless, this paper proposes another simple method to mitigate the impact.

From our simulations, it was found that, by selectively[1] using the CRPs with a proper upper limited settling time, the temperature sensitivity could be practically suppressed. The smaller the upper limit of settling time is chosen, the more the temperature sensitivity is suppressed. This effect could be seen from Fig. 6, in which the curves with different settling time upper limits show the clear trend. Compared to the curve obtained from all the CRPs, the intra-die HDs under the supply voltage of 2.5 V are strongly suppressed to lower than 1.3% by setting a settling time limit of up to 0.7 μs, even measured at extreme temperatures of -55˚C or 125˚C. Similar conclusions can be drawn from Fig. 6(b) for the supply voltage of 1.0 V.

D. *Reliability against Supply Voltage Variation*

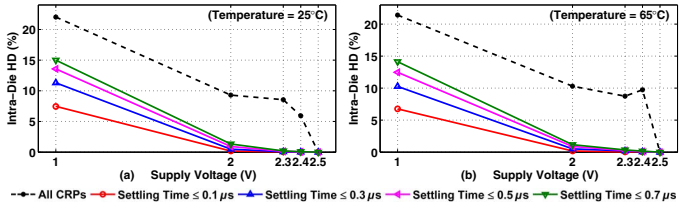

Figure 7. Reliability of BR-PUFs against supply voltage variations

To examine the reliability of BR-PUFs against supply voltage variations, the 15 PUF instances were simulated under several different supply voltages from 1.0 V to 2.5 V and at two different temperatures, 25˚C and 65˚C. Taking the CRPs under the supply voltage of 2.5 V as the reference, intra-die HDs calculated from all the CRPs including unstabilized ones shown in Fig. 7 demonstrate relatively high sensitivity to supply voltage changes in both small (from 2.5 V to 2.4 V) and large (from 2.5 V to 1.0 V) ranges. For example, the intra-die HD shown in Fig. 7(a) could rise up to 22.0% as the supply voltage drops to 1.0 V. Even if the supply voltage changes for only 0.1 V, the intra-die HD brought about is already greater than 5.9%. However, if we take the same method proposed above for combating the unreliability caused by temperature variations, that is to selectively enroll CRPs with an upper settling time limit in PUF-based protocols, we obtain much better reliability against supply voltage drops down to 2.0 V. Fig. 7 shows that at both 25˚C and 65˚C, the intra-die HD can be well controlled within 1.3%. Although the HDs up to 15.0% at 1.0 V are still relatively high, 1.0 V is not in the range of normal supply voltage variations. Instead, this phenomenon can even be taken advantage of. As the reliability under normal supply voltage variations (up to 20% of voltage drop) can already be guaranteed, a voltage control signal can also be included in the challenge signal to switch the supply voltage between, e.g., 2.5 V and 1.0 V, so that another group of responses would be generated when the supply voltage is switched. Even further, we may apply a separate voltage control to each stage, which would further increase the complexity of model building and machine learning attacks.

IV. CONCLUSION

Sec. III has shown that BR-PUFs can provide satisfying identifiability, immunity to noises, and temperature/supply-voltage sensitivity. By restricting the CRPs that are enrolled in applications with a settling time upper limit, their reliability against temperature and supply voltage variations can be further improved. BR-PUFs show significant sensitivity to intentional supply voltage changes at a large scale. This could possibly be taken advantage of to further increase the hardness of modeling and machine learning attacks.

To achieve this, we suggest a design and way of usage for BR-PUFs in ASIC-based applications with the following setup: Take, for example, a chip containing a BR-PUF that is used for challenge-response authentication. Besides a basic 64-stage BR-PUF according to Sec. II, a voltage switch with two possible output voltages (e.g., 2.5 V and 1.0 V) is built (it should be noted that the voltage switch may require much extra design effort) to switch the PUF supply voltage. The select signals (all together 64 + 1 bits) of the PUF and the voltage switch are output of an on-chip hash function which hashes the real challenge signals. The chip has two different operating modes, the enrollment mode and the authentication mode. In the enrollment mode, a monitoring module will check whether the response can stabilize within a predefined time limit (e.g., 0.5 μs). If it stabilizes, the response is output and enrolled; otherwise, that module indicates through its output that the challenge should be abandoned and another one should be sent. In the authentication mode, responses are simply bypassed by the settling-time monitoring module, regardless of whether a response has stabilized or not. The design rests on the uniqueness and the reliability of PUF responses with a proper settling time upper limit. The responses' sensitivity to supply voltage changes at a large scale has been made use of to increase the complexity of the PUF. Be aware that although the extra hash module may further increase the hardness of the design as long as it is carefully protected and dealt with, the ultimate security and usability should still come from the PUF with its uniqueness, reliability, and its sensitivity to large scale supply voltage changes.

Our ongoing work includes the generation of much more CRPs for further investigations of the hardness of the BR-PUF.

REFERENCES

[1] R. S. Pappu, *Physical One-Way Functions*, Ph.D. Thesis, MIT, 2001.

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," *Proc. ACM Conf. on Computer and Communications Security*, ACM Press, Washington, DC, USA, Nov. 2002, pp. 148–160.

[3] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secure key generation," *Proc. ACM/IEEE Design Automation Conf.*, San Diego, CA, USA, Jun. 2007, pp. 9–14.

[4] J. Guajardo, S. S. Kumar, G. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," *Proc. Intl. Workshop on Cryptographic Hardware and Embedded Systems* (CHES 2007), Springer-Verlag, Vienna, Austria, Sept. 2007, pp. 63–80.

[5] D. Lim, *Extracting Secret Keys from Integrated Circuits*, MIT, 2004.

[6] U. Rührmair, J. Sölter, and F. Sehnke, "On the foundations of physical unclonable functions," Cryptology ePrint Archive, Jun. 2009.

[7] U. Rührmair, H. Busch, and S. Katzenbeisser, "Strong PUFs: models, constructions, and security proofs," in *Towards Hardware-Intrinsic Security*, Springer-Verlag, ISBN 978-3-642-14451-6, 2010, pp. 79–96.

[8] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rührmair, "The bistable ring PUF: a new architecture for strong physical unclonable functions," *Proc. IEEE Intl. Symposium on Hardware-Oriented Security and Trust* (HOST 2011), San Diego, CA, USA, Jun. 2011, pp. 134–141.