The final version of record is available at https://doi.org/10.1109/ISNCC52172.2021.9615696

Generating a PUF Fingerprint from an on-Chip Resistive Ladder DAC and ADC

Christian Zajc[1, 2], Markus Haberler[1, 2], Gerald Holweg[1], and Christian Steger[2]

[1]Infineon Technologies Austria AG, Development Center Graz
Email: {christian.zajc, markus.haberler, gerald.holweg}@infineon.com
[2]Institute for Technical Informatics, Graz University of Technology (TU Graz), Austria
Email: steger@tugraz.at, {christian.zajc, markus.haberler}@student.tugraz.at

***Abstract*—This paper introduces an approach of extracting process variations inside System-on-Chips (SoCs) to derive a Physical Unclonable Function (PUF). The process variations are extracted from the architecture of a Digital-to-Analog Converter (DAC). The DAC consists of two independent resistive ladders to provide one single or two output voltages. The resistive ladder is characterized by the SoC with the on-chip Analog-to-Digital Converter (ADC) module. The developed PUF concept that exploits the process variations of the DAC is described and evaluated in this work. Due to the concept of not accepting an input challenge to the PUF, we designed a so-called weak-PUF. The final generated PUF response or also called fingerprint has a total length of 652 bits when using the maximum number of possible positions. In a typical operation condition, a worst-case intra-Hamming Distance (HD) of approximately 5% is achieved. Over a wide temperature range of -10°C to 70°C the intra-HD is increased to 13% in the worst-case. The inter-HD for all observed operating conditions is approximately 46%.**

***Index Terms*—PUF, Weak-PUF, DAC, $\Delta\Sigma$ ADC, SoC**

I. Introduction

Nowadays, small microcontrollers or specialized System-on-Chips (SoCs) are commonly used in diverse fields of application. Their small size and low cost draw interest to use such devices in Internet-of-Things (IoT) and Point-Of-Care (POC) devices [1]. To additionally enable a high level of security, these applications require to protect data stored on the SoC by cryptographic features. However, at the same time, these applications have a limited budget on available energy and often do not have the possibility to extend the missing functionality by external cryptographic controllers. Therefore, a well-known technology called Physical Unclonable Function (PUF) can be used to generate unique identifications inside the SoCs. These identifications are used for cryptographic methodologies. The basic concept of PUFs is to use process variations of internal components to extract a unique response. This PUF response should be protected from being copied by external attackers. In most cases, the process variations are directly exploited from variations in the manufacturing process, which are supposed to be randomly distributed.

This research is part of a project that has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 761000 (GREENSENSE).

The topology of PUFs is widespread due to the possibility to use different components as sources of randomness. The difference between all available PUF concepts is varying in the way of the extraction of minimal process variations to generate a unique response. PUFs can be available as a weak- or a strong- PUF. A weak PUF accepts no input challenge and produces only one single response, comparable with a fingerprint. A strong PUF has the capability to use an input value to produce different responses. This process is called challenge-response and a strong PUF provides several Challenge-Response Pairs (CRPs). PUFs can be constructed as a stand-alone module or can be processed by the usage of existing modules inside SoCs. A detailed survey of available PUF concepts is presented in the work of McGrath *et al.* [2].

We are focusing on providing existing SoCs the opportunity to extend their level of security by using already integrated modules. The reason for this approach is that already assembled SoCs in diverse IoT applications can be updated via a new software by adding the missing security features. This process is basically adding a Root of Trust (RoT) module to provide a secured environment for storing private information. Therefore, a methodology should be available to introduce this behavior with reasonable effort using existing hardware blocks. For this work was used a test chip which is developed to perform electrochemical measurements for example in POC devices. Therefore, the requirement for security features to protect personal measurement information is an important feature.

II. Related work

Some works already exploited some properties of Digital-to-Analog Converters (DACs) for the generation of PUFs. The work in [3] proposed the usage of calibration data of the trimmed current sources of a feedback DAC of a Sigma-Delta modulator. Another work used a single chip solution to exploit the code deviation in a DAC and Analog-to-Digital Converter (ADC) chain [4]. As the source of randomness was selected the combination of DAC input codes and ADC output codes by continuously increasing the DAC output voltage. The key generation was performed on specially selected points to improve the code generation performance. In this work was not evaluated the stability at diverse environmental temperature ranges. Besides these works, Wang *et al.* in [5] analyzed the

The final version of record is available at https://doi.org/10.1109/ISNCC52172.2021.9615696

possible functionality of an R-2R ladder DAC-based PUF. This work used two R-2R ladders to convert the combined mismatches of resistors and switches to a PUF response. This proposed approach is a self-contained module and the functionality was only verified by simulation results.

This contribution presents a concept for PUFs to use internal available modules of an existing SoC to provide a unique fingerprint. In detail, manufacturing variations of the construction of a resistive ladder inside a DAC module are exploited by measurements. The characterization of these process variations is performed by differential measurements with an integrated ADC. The specialty in this concept is the possibility to measure every single resistor of the entire ladder for characterization without increasing the construction size of the DAC. All calculations to receive the final PUF response can be done by the SoC.

This work is organized as follows: Section III introduces the used SoC architecture. Section IV discusses the proposed PUF concept. Section V presents the process of converting the measurement results into a unique PUF response. The complete processing chain of the newly developed PUF concept is summarized in Section VI. The proposed concept is evaluated in Section VII and is concluded in Section VIII.

III. SoC Architecture

In this work, a test chip is used which is processed in a 130nm standard CMOS process. This test chip is developed to perform electrochemical measurements with a dedicated sensor interface. Furthermore, this SoC is designed to operate in a resource-limited environment with the opportunity to fully operate out of the harvested energy of a provided Radio Frequency Identification (RFID) field. The fact of limited available energy resources leads to the possibility to have several mechanisms available to reduce the overall power consumption and provides a modular usage of available components inside the SoC.

Fig. 1 illustrates the high-level architecture of the used SoC. This SoC is an ARM Cortex-M0-based microcontroller with several memory spaces. These memory spaces are divided into Read-only Memory (ROM), Random-Access Memory (RAM), and Non-Volatile Memory (NVM). Furthermore, this SoC consists of several analog and digital modules. Among these modules is a sensor interface for electrochemical measurements, which contains a separate ADC and DAC. The ADC is a differential delta-sigma ($\Delta\Sigma$) ADC [6]. This $\Delta\Sigma$ ADC provides several configuration possibilities like input gain setup, continuous or single measurements, and filtering settings. The DAC is constructed as a 16 bit interleaved DAC with two resistive ladder output stages. Each output stage has a resolution of 8 bits. Due to the interleaved construction, the DAC provides several output configurations: one single output with 16 bits or two outputs with a resolution of 8 bits per output. This SoC allows to set up an internal connection between the ADC and DAC without external components or wiring. In addition, this SoC includes more modules like hardware-supported cryptographic methods, in detail an Advanced Encryption Standard (AES) module, a wireless communication unit for RFID enabled devices, and standard peripherals.

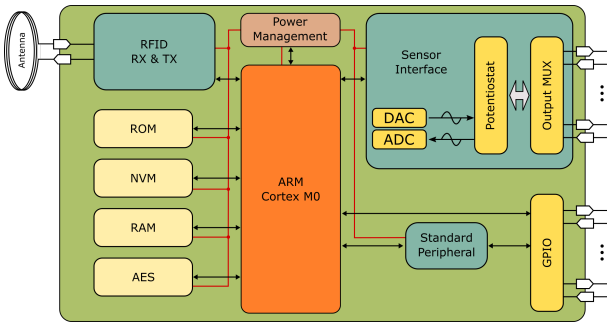

Fig. 1. High-level architecture of used SoC test chip developed for electrochemical measurement platforms in a resource-limited environment.

This SoC contains further modules that enable the device to support several applications. However, a secured environment for storing cryptographic keys is not implemented (as a hardware block) on the SoC. A RoT module would be required for this approach to use unique information to create a trusted and secured platform. Thus, we developed a concept based on PUFs, which only uses available modules on the existing SoC to provide the base for a secured environment.

IV. Novel PUF concept based on DAC with ADC

In this PUF concept, we focused on using only internal available modules of the existing SoC. For PUFs, it is required to use process variations to generate a unique response of the device. Therefore, we analyzed the internal process variations of the chip on the resistors of the resistive ladder of the DAC. The SoC does all measurements and calculations for processing this unique response, even in operation in environments with limited energy. Furthermore, an important goal of this developed process is to provide good stability over temperature changes in the operational environment. The field of application is widespread for this SoC architecture, therefore we cannot rely on a stable operational environment. The overall process can be separated into three sub-processes: A) Physical measurement procedure, B) Data extraction, and C) Data post-processing. In the following paragraphs, these sub-processes will be discussed in more detail.

A. Physical measurement procedure

This part of the work describes the process of extracting physical process variations of the DAC. As previously described, the DAC consists of two independent output stages; Stage0 and Stage1. Each of these two stages is constructed as a resistive ladder with a resolution of 8 bits and two taps. Thus, one stage consists of 256 single resistors connected to one string and each of these resistors typically underlay process variations. With the usage of these process variations, we demonstrate the possibility of extracting unique information from it.

The final version of record is available at https://doi.org/10.1109/ISNCC52172.2021.9615696

The measurement setup inside of the SoC is illustrated in Fig. 2. The DAC is configured in a dual output mode, which enables to use each stage separately as output. Each resistive ladder stage has two independently configurable taps, hence we have in total four output opportunities with these two stages. This opportunity leads to a complete characterization of every single resistor in the stages. In order to use all these taps of the DAC as input for the ADC with reduced components in the path, only internally available test paths are used for this intention. This means that we are only using the existing hardware which is required for the verification process of the module without increasing overhead. These two stages are supplied by a temperature stable voltage of 1.5V, derived from an on-chip bandgap circuit. A variation in the environmental temperature changes the impedance value of each resistor. Due to the close relation in the area of each resistor, we can assume that each of them is affected by the same temperature. The construction of the DAC with a temperature compensated voltage supply provides equally distributed voltage drops at the resistors. With this construction, only the amount of current through the resistors changes due to temperature variations. In the proposed measurement process, each stage is characterized one after the other.

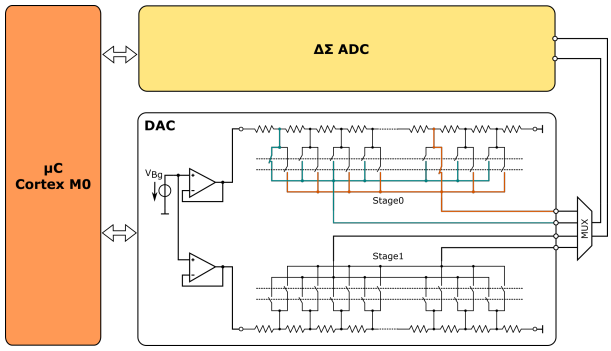

Fig. 2. Simplified schematic of the measurement setup. The microcontroller manages the interactions between the DAC and ADC. The DAC has two output stages and each of them has two taps from the resistive ladder. One possible tap option is visualized with two colors in Stage0.

Due to the opportunity to use the differential input mode of the ADC and the two taps of the DAC, we are enabled to measure the voltage drop of each resistor of the entire ladder by a single measurement. In addition, the differential measurement removes influences of supply noise during the measurement, thereby enhancing the accuracy of the measurement. The voltage of 1.5V on the ladders leads to a voltage drop of approximately 5.9mV for each of the 256 resistors in a ladder. To increase the voltage measurement accuracy, n-resistors of the ladder are combined to increase the voltage drop to be measured by the ADC. The choice to use 20 resistors for one measurement proves to be a good trade-off between optimizing the input signal to the requirements of the ADC and a reasonable reduction of possible codes for PUF generation. This combination of setting the taps over 20 resistors leads to a voltage drop of approximately 117mV.

Fig. 3 illustrates the analog measurement process of the DAC in combination with the ADC. This measurement process has to be performed separately for each stage. In the beginning, the first tap of the DAC stage is configured to the resistor position 70 and the second tap to position 90. The first position starts with 70 of the DAC stage, representing a starting voltage level of approximately 410mV above ground level. This starting voltage level is required due to the input range limitations of the ADC to receive reasonable values. The configured voltage at the DAC module has to be settled on the internal output for 300μs. The ADC has based on the differential input two configurations: Normal- and crossed-input. These two modes enable the ADC to compensate for the offset introduced by the mismatch in the input stage. Thus, we start with the normal mode, direct input configuration, of the ADC and measure the applied voltage. Each position of the DAC output configuration is measured multiple times with an interval of 30μs. The time of 30μs is required to wait on completing the post-processing of the integrated ADC filter. For precise measurement results, the voltage on the ADC input is averaged 32 times. After these measurements, the ADC is configured to measure the applied voltage on the second input configuration with the same averaging process. The second configuration crosses out the differential input lines to the ADC. After these two input configurations, the resistive tapping position is incremented by one position. This procedure is continued until all possible positions are measured from the DAC. If all positions are measured, then the post-processing of the ADC output values can be performed. The first step is to divide the summarized measurement values by the amount of performed repetitions. Secondly, the digital ADC values are converted to analog voltage values, to calculate the absolute mean value of the two different ADC input values. After this step, the entire process has been finally completed for the first stage. This measurement process is now applied to the second stage of the DAC.

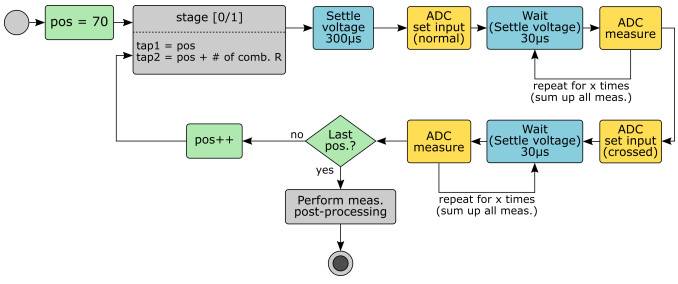

Fig. 3. Illustration of the entire measurement process with a focus on interaction with ADC and DAC. Each step is depicted, which is required to perform the measurements to detect the process variations.

Fig. 4 depicts the measured differential voltage drops over 20 combined resistors of the two independent stages (Stage0 and Stage1) for one SoC. The x-axis describes the first tapping position of the resistive ladder and the y-axis holds the measured voltage drop values. In this graph are added 50 independent measurement repetitions to illustrate the stability

The final version of record is available at https://doi.org/10.1109/ISNCC52172.2021.9615696

over time at a constant ambient temperature. The small outliers in the graph lines are caused by quantization errors of the $\Delta\Sigma$ ADC module.

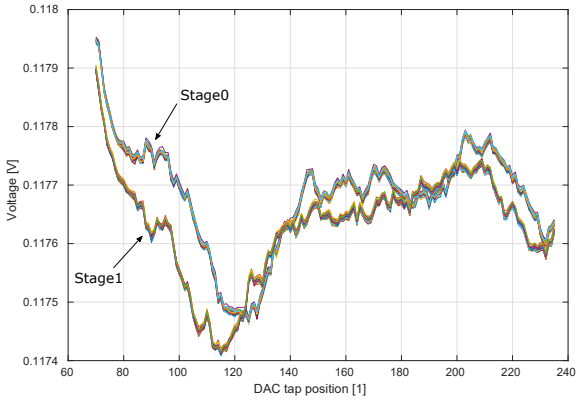

Fig. 4. Differential voltage measurement results of Stage0 and Stage1 over 20 combined tapping positions for one SoC. The first tap is started at position 70. This graph contains 50 independent measurement repetitions of a single SoC, measured at a constant room temperature of 20°C.

B. Data extraction

After completing these measurements, two differential voltage curves over a combination of 20 DAC resistors are received. One curve for Stage0 and one for Stage1. The next step extracts more variations out of the raw measurement data. Therefore, the difference between the measured data set of Stage0 and Stage1 is calculated. This step increased the course of the curves significantly in comparison to the two differential measured voltage curves. The new calculated curve for one device can be seen in Fig. 5. The comparison between the different variations is evaluated in Section VII by calculating the entropy.

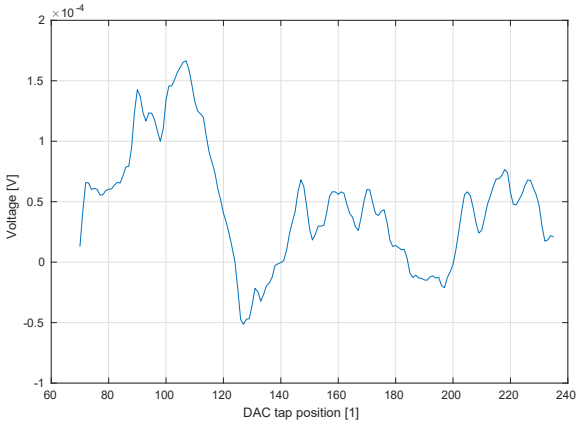

Fig. 5. This graph represents the calculated difference between Stage0 and Stage1 of the differential voltage drop over a combination of 20 resistors. The measurement for this graph is performed at a constant environmental temperature of 20°C.

In addition, this calculation was performed for several environmental temperatures in a range from -10°C to 70°C. The archived results are depicted in Fig. 6. The analysis of these curves showed an offset in the single curves on the y-axis. Each curve in the graph corresponds to a performed environmental temperature. This lead to the consideration to have additional temperature-dependent components in the measurement setup.

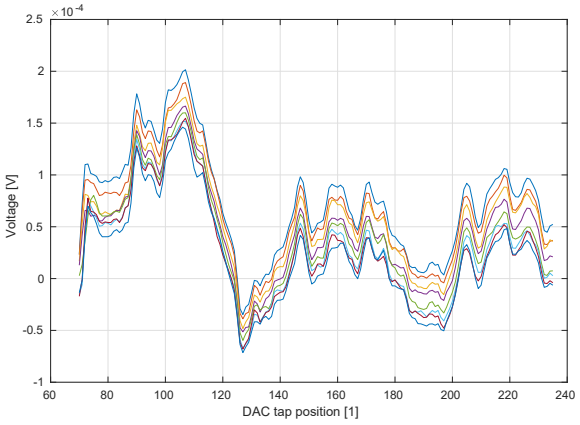

Fig. 6. Representation of the calculated difference between Stage0 and Stage1 at an environmental temperature range from -10°C to 70°C for a single SoC.

C. Data post-processing

After calculating the difference between Stage0 and Stage1 for various SoCs, the resulted data were not mapped to the same range of values due to a mismatch in the bandgap voltage. Additionally, we have seen a variation in the offsets of the output signals over temperature, as mentioned earlier. In the analysis of this phenomenon, we have seen a temperature dependency in the resulting measurements. These deviations over temperature are mainly attributable to the temperature-dependent offsets in the voltage buffers that drive the resistive ladders of the DAC. However, when normalizing the measured results to provide a comparable base, the temperature-dependent part of the measurement data was intensely reduced. Furthermore, to reduce the quantization noise of the ADC and to increase the stability of the result, a weighted averaging of the raw measurement data (y) given by (1) is performed. The resistive ladder position is defined as the variable “n”. This filter helps to smooth the data and to remove spikes in the measurement. The final measurement results with all applied post-processing steps can be seen for five different SoCs in Fig. 7. This graph shows that each curve provides its own course and is suitable for extracting unique information.

$$y_{filt}(n) = \frac{1}{11}[3 \cdot y(n) + 5 \cdot y(n-1) + 3 \cdot y(n-2)] \quad (1)$$

V. Binary Data Extraction of PUF Response

To generate a key out of the PUF response of the SoC, a valuable cryptographic bitstream has to be extracted. The requirements on such cryptographic bitstreams are to be unique from chip to chip and to be stable on the same chip under several operating conditions.

The final version of record is available at https://doi.org/10.1109/ISNCC52172.2021.9615696

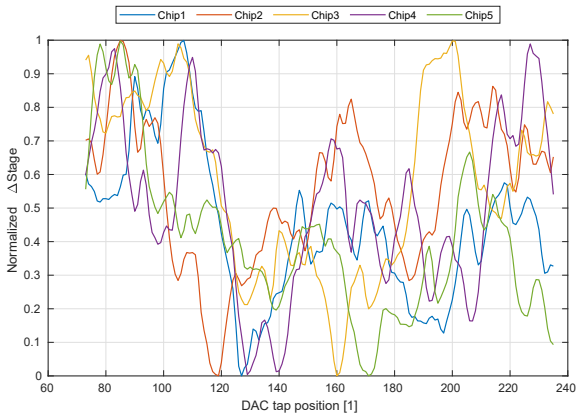

Fig. 7. Final measured and post-processed PUF extracted curves. This graph includes five averaged curves across all measured temperatures of different SoCs. Each SoC provides a unique course in the measured data.

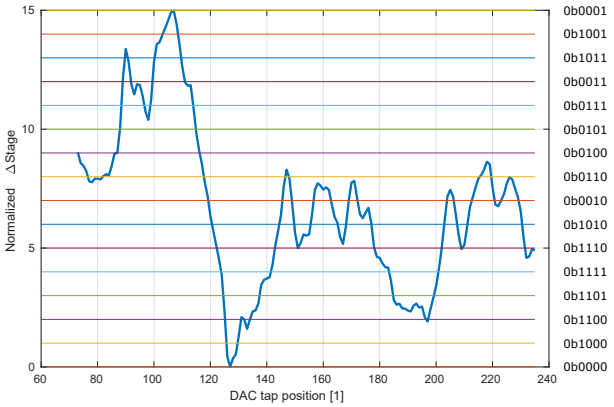

Fig. 8. Stretched normalized data of one SoC with all quantization steps. On the right side are the corresponding binary values of each quantization step.

In the previously described PUF response generation out of the DAC process variations (Section IV) is generated a curve, which has been normalized between the range zero and one. The basic idea for generating a cryptographic bitstream is to select several positions on the x-axis (DAC taps) to convert the values from the y-axis (voltage difference) to binary values. Therefore, the values on the y-axis of the resulted PUF response have to be quantized. For the selection of the number of quantization steps, a trade-off between the number of resulting steps and the stability of repeatability has to be performed. More quantization steps increase the granularity of the possible values, but the stability decreases due to the variation of repeatability of the measurements.

The use of 16 quantization steps has proven to be a good choice for the particular application. For easier operations with the Cortex-M0, the normalized data curve is stretched to the maximum value of the quantization steps. The maximum value is consequently 15 and the values are in the range between 0 and 15. This stretching from 1 to 15 enables to access the quantization values via an array construction. Each quantization step represents a 4-bit binary value. To increase the stability of the bitstream generation, a balanced gray code encoding is used for the binary values. The use of this encoding increases the stability of the bitstream generation since only one bit is flipped between two contiguous binary values. These performed steps are visualized in Fig. 8.

For the next step to generate a bitstream with a defined length, several positions on the x-axis have to be selected to combine the y-axis values to one binary value. Each position contains a 4-bit value, which is appended to the previous part to generate one long value. In the current analysis, the maximum possible length of the bitstream generation is used, namely all positions on the x-axis. Due to the use of the averaging filter in the post-processing, the bitstream generation has to be started three positions later, namely from position 73 of the normalized data because of the settling of the filter. This leads to a final PUF response value of 652 bits. If shorter bit values are required, the possibility of reducing the number of used positions on the x-axis can generate a new response with fewer bits. This method can be used to generate diverse responses of the same PUF and can further be extended to provide a simple challenge-response architecture. Therefore, it is possible to offer different cryptographic bitstreams depending on the defined challenge with this opportunity. Nevertheless, for showing the maximum limits and ranges of this PUF architecture all possible positions are used for the evaluation.

VI. Complete Processing Chain of Designed PUF

This Section summarizes the entire processing chain of this designed PUF concept to provide a complete overview of performed steps. Fig. 9 depicts all performed intermediate steps from the beginning to the end. All these steps were previously described in more detail in Section IV and V. The process starts with measuring the internal process variations of the used SoC by using the internal DAC and ADC. This measurement provides the raw voltage drops over several resistors of the resistive ladder for each DAC stage (Stage0 and Stage1). In the evaluation process, we have seen that post-processing is required to increase stability and maximize uniqueness. The first step is to filter the measured raw voltage drops with the described filter settings. Another step to increase the stability is to average also the entire measurement of the voltage drops for x times. For this averaging process was selected a value of 64 repetitions for one measurement, which has proven to be a good value. Then the two filtered stage data are combined into one single data set, namely, the difference is calculated between Stage0 and Stage1. This calculated difference has to be normalized to bring the data on one hand to the same range of values and on the other hand to remove uncontrollable temperature influences. The last step is now to quantize the data for the upcoming bitstream response generation.

VII. Evaluation

For the evaluation of the quality of the generated PUF, the intra-Hamming Distance (HD) and the inter-HD are determined [7].

The value of the intra-HD (2) represents the stability or reliability of generated responses of a PUF. An ideal PUF

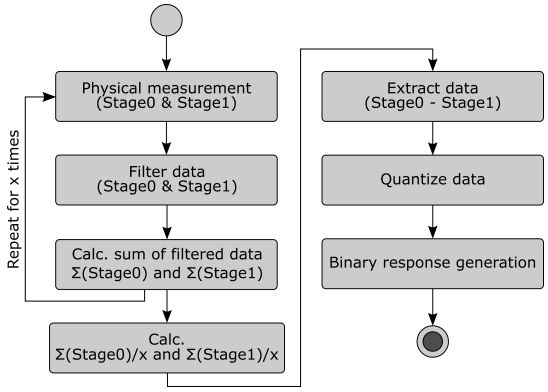

Fig. 9. Complete processing chain of designed PUF concept for an existing SoC with a DAC and an ADC.

has an intra-HD value of 0%. This means that the PUF will always generate the identical response for the same input challenge after several repetitions. The HD represents the distance between two codes. R_i describes the first response of one input challenge with a length of n bits of the PUF. The same challenge is provided several times to the same PUF implementation and is labeled with $R_{i,j}$. The amount of repetitions is defined in the variable j. The calculated HD between two responses is divided by the length of the response n.

$$HD_{intra} = \frac{HD(R_i, R_{i,j})}{n} \cdot 100\% \quad (1 \leq \text{j} \leq \text{\#of repetitions}) \tag{2}$$

The inter-HD (3) represents the uniqueness of the response of a PUF with the same input challenge applied on various devices. This value should be about 50% for an ideal PUF implementation. The inter-HD calculates the HDs for all combinations of observed PUF devices provided with the same input challenge. The responses of the PUFs (R_u and R_v) have a length of n bits. The HD is calculated between all available responses of R_u and R_v. The variable m defines the number of observed devices.

$$HD_{inter} = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \cdot 100\% \tag{3}$$

In addition to extend the evaluation, we calculated the Shannon-entropy which is used as an indicator to detect possible correlations or weaknesses [8]. An entropy result of 100% means a perfect randomly generated response. For this PUF concept can be evaluated the Shannon-entropy in two different ways. The first way is to calculate the entropy per-device (H_D), which should be ideally close to 100%. The second way is to calculate the entropy per-bit (H_B) over all devices. This value should also be ideally close to 100%. In the entropy per-device H_D (4) is used the probability (p_i) of the appearance of zeros and ones. The variable d describes the used device number and N the bit-length of available PUF responses $R(n)$.

$$H_D(d) = -\sum_{i=0,1} p_i \cdot log_2(p_i) \text{ ,with } p_i = \frac{1}{N} \sum_{n=0}^{N} \begin{cases} 0, R(n) = i \\ 1, R(n) \neq i \end{cases} \tag{4}$$

The entropy per-bit H_B (5) for binary data uses the probability of a fixed bit position n in the PUF response $R_x(n)$ across all observed devices D.

$$H_B(n) = -\sum_{i=0,1} p_i \cdot log_2(p_i) \text{ ,with } p_i = \frac{1}{D} \sum_{x=0}^{D} \begin{cases} 0, R_x(n) = i \\ 1, R_x(n) \neq i \end{cases} \tag{5}$$

The first evaluation of the PUF is done at a constant environmental temperature, room temperature (20°C), to show the quality of the binary response generation. For this process, the maximum response bitstream with a length of 652 bits is generated. This means that each position on the PUF response is only used once. In detail, the DAC taps are beginning at the resistive ladder position 73 and ended up at the maximum position of 235. The entire process of generating the PUF response is repeated 50 times on each device with the same environmental conditions. The results of this evaluation over a set of five chip samples can be found in Table I. The achieved mean intra-HD from a sample set of five different chips is 3.08%. The entropy per-bit H_D shows a minimum entropy of zero percent, which means that all bits at one bit position over the devices have the same bit value. This is a fact of the evaluation of a sample set of five devices. This case occurred 73 times over the entire bit response length of 652 bits. The average entropy per-bit is around 77.94%, which is a good value, but this has to be investigated in more detail with a larger sample set.

TABLE I
PUF METRICS FOR A CONSTANT ENVIRONMENTAL TEMPERATURE (20°C).

	Chip ID	Min [%]	Mean [%]	Max [%]
HD_{intra}	#1	1.28	3.33	4.30
	#2	0.62	4.08	5.45
	#3	1.19	2.47	3.53
	#4	1.24	3.18	4.91
	#5	0.90	2.35	4.29
HD_{intra}	#1 - #5	0.62	3.08	5.45
HD_{inter}	#1 - #5	41.23	46.53	50.93
H_D	#1 - #5	96.65	99.04	99.04
H_B	#1 - #5	0.00	77.94	97.10

The next evaluation focuses on analyzing the PUF concept in terms of stability over the change of environmental temperature. For this reason, we performed measurements in an environment within a controlled ambient by using a temperature chamber. In our evaluation, we started the measurements at -10°C and increased the temperature to 70°C in steps of 10°C. The entire response generation of the constructed PUF is repeated 50 times for each temperature step. The SoC performed all measurements for the PUF response generation. The post evaluations of PUF metrics were performed in Matlab. These

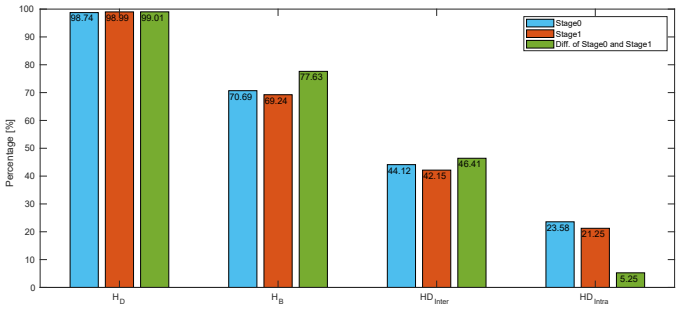

Fig. 10. Comparison of different data extraction options (Stage0, Stage1, and difference between Stage0 and Stage1) by calculating the entropy and HD.

performed measurement results are listed in Table II. The PUF metrics show that the stability for this evaluated temperature range is decreased by approximately 8% in the worst-case for the above-mentioned temperature range. This decrease result in a worst-case intra-HD of 13.62%. The slight increase of the average intra-HD of approximately 2% shows that the concept is performing well. This evaluation result indicates that there is still a temperature-dependent part in the overall PUF concept, visible in the increased maximum intra-HD, which has to be identified and compensated in future work. The inter-HD was not influenced by varying the environmental temperature, achieving a value close to the desired 50% over the considered temperature conditions. Also, the entropy was not affected by the variation of the environmental temperature.

TABLE II
PUF METRICS OVER A TEMPERATURE RANGE FROM -10°C TO 70°C.

	Chip ID	Min [%]	Mean [%]	Max [%]
HD_{intra}	#1	1.53	5.91	12.42
	#2	0.61	5.95	13.96
	#3	1.38	4.47	8.59
	#4	1.23	5.82	8.90
	#5	0.92	4.07	8.90
HD_{intra}	#1 - #5	0.61	5.25	13.96
HD_{inter}	#1 - #5	41.53	46.41	50.58
H_D	#1 - #5	99.15	99.01	100.00
H_B	#1 - #5	0.00	77.63	97.10

In the next evaluation were calculated all the above-mentioned parameters for the PUF responses processed out of different data extraction options: measurement results of Stage0, measurement results of Stage1, and the difference between Stage0 and Stage1. For this evaluation was used the entire data set with a wide environmental temperature range. These three options were selected to find the best option to get the maximum of variations out of the PUF response. This evaluation extends the previously described process in the PUF architecture in Section IV-B. Figure 10 shows the comparison of the average values of the calculated HD and entropy of the three different variants. The results show, that with the usage of the difference of both stages, the H_B could be increased and the H_D constantly stayed at the ideal value compared to the separate Stage0 and Stage1. Another advantage of the combined option is the significant reduction of HD_{intra}, representing the stability of the PUF response. This leads us to use the calculated difference between Stage0 and Stage1 for the PUF architecture.

VIII. Conclusion

This work presents a PUF concept for a SoC with an integrated resistive ladder DAC and $\Delta\Sigma$ ADC. As a randomness providing source for the PUF concept, the integrated DAC module of an existing SoC was used. The resistive ladder of the DAC architecture provides enough process variations in order to extract a unique response. Two on-chip resistive ladders are characterized by measurements of the resulting voltage drops over the corresponding resistors. In order to maximize the resulting PUF response, the difference between both stages is determined used for further processing. In the post-processing step, the PUF response is converted into a binary bitstream. The analysis of the PUF showed that the intra-HD is always in the range of 46%. The stability analysis of the PUF for constant environmental temperature provided an intra-HD of 5.45% in the worst-case. Over a temperature range from -10°C to 70°C the maximum intra-HD increased to 13.96%. This instability, which mainly results from the on-chip analog blocks, has to be improved in the future by reducing the influences of the temperature-dependent parts by more post-processing. Furthermore, the stability can be improved by excluding unstable positions inside the generated PUF response for the final bitstream generation. The current process of our PUF concept uses all positions to provide a transparent evaluation of performance. The instability in the generated PUF response requires the use of error-correction codes for the final cryptographic key generation. With this work, we demonstrated the possibility to provide a base for a PUF environment with the availability of a resistive ladder DAC and an ADC inside a SoC.

References

[1] M. Zarei, "Portable biosensing devices for point-of-care diagnostics: Recent developments and applications," *TrAC Trends in Analytical Chemistry*, vol. 91, pp. 26–41, 2017.

[2] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Applied Physics Reviews*, vol. 6, no. 1, p. 011 303, 2019.

[3] A. Herkle, J. Becker, and M. Ortmanns, "Exploiting Weak PUFs From Data Converter Nonlinearity—E.g., A Multibit CT Delta Sigma Modulator," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 7, pp. 994–1004, 2016.

[4] A. Duncan, L. Jiang, and M. Swany, "Repurposing SoC analog circuitry for additional COTS hardware security," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2018, pp. 201–204.

[5] P. Wang, X. Zhang, Y. Zhang, and J. Li, "Design of a reliable PUF circuit based on R–2R ladder digital-to-analog convertor," *Journal of Semiconductors*, vol. 36, no. 7, p. 075 005, 2015.

[6] M. Haberler, C. Steffan, I. Siegl, N. Sailer, and M. Auer, "A 92-dB-DR 126-µV Sensitivity Potentiometric Sensor Interface With High Interference Robustness," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2021.

[7] G. Kömürcü and G. Dündar, "Determining the quality metrics for PUFs and performance evaluation of Two RO-PUFs," in *10th IEEE International NEWCAS Conference*, 2012, pp. 73–76.

[8] M. Pehl, A. R. Punnakkal, M. Hiller, and H. Graeb, "Advanced performance metrics for Physical Unclonable Functions," in *2014 International Symposium on Integrated Circuits (ISIC)*, 2014, pp. 136–139.