Spatial Correlations in Physical Unclonable Functions

Florian Wilde*, Berndt Gammel†, and Michael Pehl*
*Technische Universität München, Munich, Germany
{florian.wilde | m.pehl}@tum.de
†Infineon Technologies AG, Munich, Germany
berndt.gammel@infineon.com

***Abstract*—Physical Unclonable Functions (PUFs) are circuits which extract a device dependent secret from inherently available manufacturing variations. This work focuses on evaluating the quality of such circuits regarding intra-die correlations, because canonical quality metrics for PUFs do not sufficiently cover them. Correlations reduce the effort for an attacker to guess the secret with the same severity as biases, yet canonical tests focus only on the latter. Three tests which are used to consider topological properties along with the secret are introduced and adapted to quality evaluation of PUFs. To show the efficiency and effectiveness but also the limitations of the tests, we apply them to three real-world measurement datasets from ring-oscillator PUFs on FPGAs, standard SRAM and Two-Stage PUFs on ASICs. The results show that the presented statistical tests are ideal candidates to complement state-of-the-art metrics for PUF quality.**

I. Extended Abstract

Silicon-based Physical Unclonable Functions (PUFs) are security primitives which are used to extract a secret from intrinsic manufacturing variations of an electronic device. A bit is extracted in a PUF cell by measuring and quantizing analog properties of common digital circuits. The goal in designing a PUF is to make the bits hard to predict for an attacker, but reliable over the lifetime of the device. The former can be achieved if random *local* manufacturing variations dominate the behavior of the PUF, such that the response of individual PUF cells is statistically independent. If *global* variations – e.g. a speed gradient over the die – dominate, this allows for the prediction of the behaviour of other PUF cells on the die and thus impairs security [1].

Current quality measures for PUFs mainly focus on measuring biases [2]. Correlations are only considered via Joint Entropy [3] and rarely via Pearson's correlation coefficient. But Joint Entropy can only be bounded, e.g. by compression algorithms, and Pearson's correlation coefficient is limited to analyzing pairs of locations on the die separately. Neither of them is suited to find spatial correlations, especially in datasets with few devices.

This work advances the state of the art in the field of evaluation of PUF quality by adapting and analyzing methods to find spatial correlations. Moran's I [4], Geary's c [5], and Join Count Statistic [6] are introduced as tests to find weaknesses which can hardly or not at all be found with state-of-the-art tests for PUFs. These statistical tests are well known in other scientific fields, e.g., in geographical analysis, and have shown their efficiency there. This work adapts them for PUF analysis.

Modern textbooks on statistics provide generalized versions of Moran's I, Geary's c, and Joint Count Statistic. These can be applied to evaluate dependencies of data points within neighbourhoods instead of only the dependencies of direct neighbours like in the original methods. For this purpose, the generalized methods introduce a two-dimensional weighting matrix, which reflects how close the data points are in some chosen distance metric. The size of the considered neighbourhood can be used to trade insight vs. computational effort and is carefully selected in this work.

Even though an elaborate investigation of the proposed methods will be presented in future work, their application on the following three datasets – all measured on real-world devices – already gives a good overview of their capabilities:

1) Response bits of an array of 4096 Two-Stage ID PUFs [7] on 243 ASICs in a 90nm technology.
2) Frequencies of an array of 512 ring-oscillators (ROs) implemented on 193 Xilinx Spartan 3 FPGAs, measured at uncontrolled room temperature [2]. This data is well explored and can be seen as a reference to show that important design flaws can be identified.
3) Start-up values of 160 KiB of SRAM cells on 144 Infineon XMC4500 microcontrollers, sampled at uncontrolled room temperature.

Figures 1 to 4 exemplify the results for the different tests using Moran's I. For the visualization and hypothesis testing, the Moran's I values are transformed into z-scores, which can be compared to the overlayed standard normal distribution. If the null hypothesis of no spatial correlations within the data cannot be declined with a certain probability $1 - \alpha$, the PUF-structure is considered as sufficiently uncorrelated. The corresponding acceptance intervals for $\alpha = 5\%$ are given in the figures by vertical dashed lines. For an ideal PUF without spatial correlations, the z-scores in the experiment are expected to be standard normal distributed. The outcome for the experiments are given by the histograms; the corresponding kernel density estimate is given as dashed curve in each case.

The results for the first experiment (Two-Stage ID PUF) are given in Figure 1. The figure shows that the kernel density estimate resembles the standard normal distribution (continuous) closely, i.e. no spatial correlations have been found in this data set. Since previous laborious analysis also came to the result that the PUF structure does not contain any spatial correlations, the result shows the behavior of the tests for uncorrelated binary PUF responses.

This work was partly funded by the German Federal Ministry of Education and Research (BMBF) in the project SIBASE through grant number 01IS13020

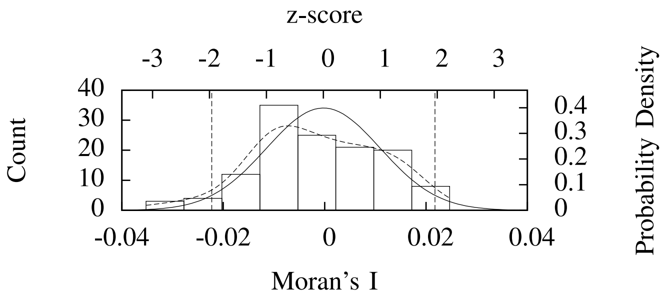

Figure 1. Histogram of Moran's I for Infineon dataset. The second axes are scaled equiareal and shifted so the plotted values match z-scores, which can be compared to the overlayed standard normal distribution. The vertical bars separate the acceptance interval for $\alpha = 5\%$, which contains 121 devices.

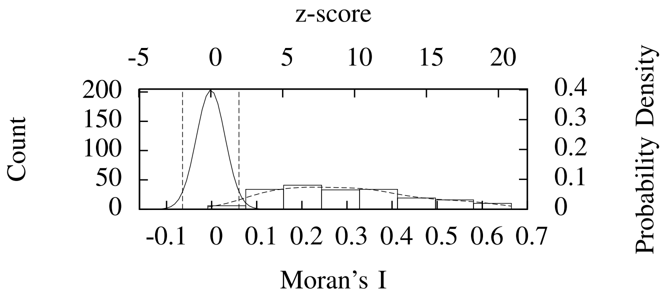

Figure 2. Histogram of Moran's I for Maiti et al. dataset after the mean along samples and devices is subtracted. The second axes are scaled equiareal and shifted so the plotted values match z-scores, which can be compared to the overlayed standard normal distribution. The vertical bars separate the acceptance interval for $\alpha = 5\%$, which contains three devices.

In contrast, Figure 2 exemplifies the results of Moran's I for the second data set (RO PUF) with known design flaws. One of these flaws is a speed gradient over the die [1], which means that slow and fast ROs tend to be on opposite edges or corners of the considered die. This is reflected in Figure 2, since all z-scores lay on the right of the acceptance interval; z-scores on the left side would indicate that fast and slow ROs alternate. The slope of the speed gradient in the data set, however, varies from die to die. This is also covered in Figure 2 by the scores spreading accordingly close or far from the acceptance interval.

Figure 3 and Figure 4 show results from the third data set, arranged as 32 bit and, respectively, as 64 bit rows. Comparing the figures, the result for 32 bit rows (Figure 3) shows that, although the z-scores do not follow the distribution expected for ideal PUFs, the severity of the flaw is strongly underestimated. However, if the data are rearranged to 64 bit rows, all z-scores are positive and far outside the acceptance interval. The reason for this is that positive spatial autocorrelation within a row cancels with negative within a column in the 32 bit-per-row case. In the 64 bit-per-row arrangement, the negative spatial autocorrelation is removed by concatenating every second row to its predecessor, which reveals the actual severity of the contained positive spatial autocorrelation. This example shows that it is important to have good knowledge of the position of the PUF-cells within a die and to carefully preprocess data. Also, it shows that there is room to improve the tests. Therefore, it is important to know the limitations of the tests, as there are cases where other state-of-the-art tests are more fitting.

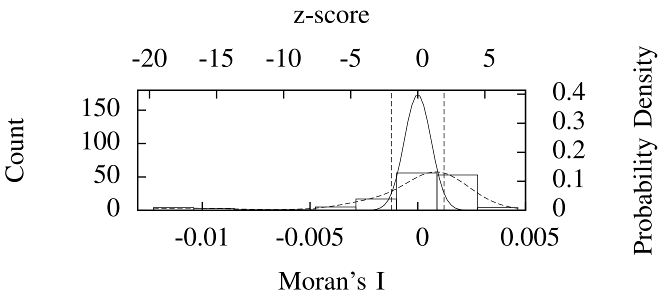

Figure 3. Histogram of Moran's I for XMC dataset considered SRAM is arranged in 32 bit rows. The second axes are scaled equiareal and shifted so the plotted values match z-scores, which can be compared to the overlayed standard normal distribution. The vertical bars separate the acceptance interval for $\alpha = 5\%$, which contains 73 devices.

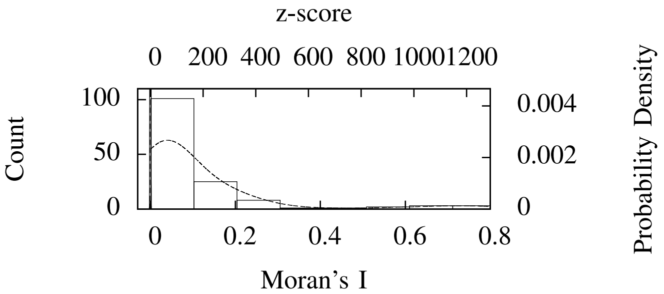

Figure 4. Histogram of Moran's I for XMC dataset considered SRAM is arranged in 64 bit rows. The second axes are scaled equiareal and shifted so the plotted values match z-scores. The overlayed standard normal distribution is unrecognizable due to the large extent of the z-scores. The vertical bars separate the acceptance interval for $\alpha = 5\%$, which contains one device.

The analyses of the discussed PUFs show that the new methods can be used to identify spatial correlations in typical PUF scenarios efficiently, even if only a few PUF devices can be measured. This is the main advantage of the proposed tests. All presented tests are based on the knowledge of the exact asymptotic distribution, such that a sound statistical test for the rejection of the null hypothesis of spatial independence can be set up. These tests can be seen as a complement to existing methods for PUF evaluation.

References

[1] F. Wilde, M. Hiller, and M. Pehl, "Statistic-based security analysis of ring oscillator pufs," in *Integrated Circuits (ISIC), 2014 14th International Symposium on*. IEEE, 2014, pp. 148–151.

[2] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of ro-puf," in *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*. IEEE, 2010, pp. 94–99.

[3] T. Ignatenko, G.-J. Schrijen, B. Skoric, P. Tuyls, and F. Willems, "Estimating the secrecy-rate of physical unclonable functions with the context-tree weighting method," in *2006 IEEE International Symposium on Information Theory*. IEEE, 2006, pp. 499–503.

[4] P. A. P. Moran, "Notes on Continuous Stochastic Phenomena," *Biometrika*, vol. 37, no. 1/2, pp. 17–23, 1950.

[5] R. C. Geary, "The Contiguity Ratio and Statistical Mapping," *The Incorporated Statistician*, vol. 5, no. 3, pp. 115–127+129–145, 1954.

[6] P. A. P. Moran, "The Interpretation of Statistical Maps," *Journal Royal Statistical Society, Series B*, vol. 10, pp. 243–251, 1948.

[7] M. Bucci and R. Luzzi, "Identification circuit and method for generating an identification bit using physical unclonable functions," Nov. 12 2013, US Patent 8,583,710.