

Process Variation Evaluation Using RO PUF for Enhancing SCA-Resistant Dual-Rail Implementation

Wei He¹(✉), Dirmanto Jap², and Alexander Herrmann¹

¹ Physical Analysis and Cryptographic Engineering (PACE),
Nanyang Technological University, SPMS, MAS 05-31,
Singapore 637371, Singapore
{he.wei, aherrmann}@ntu.edu.sg

² School of Physical and Mathematical Sciences (SPMS),
Nanyang Technological University, SPMS, MAS 05-31,
Singapore 637371, Singapore
dirm0002@e.ntu.edu.sg

Abstract. The security of the implemented cryptographic algorithm in hardware has been certified to be vulnerable against physical-level Side-Channel analysis. As a typical countermeasure, dual-rail precharge logic theoretically thwarts Side-Channel analysis because of its compensated data-dependent fluctuations in observable power or EM traces. However the security grade of the dual-rail behavior is significantly impacted by silicon technological bias due to its non identical alterations to each rail's electrical characteristics. In this paper, a technique is proposed to evaluate the in-die process variation, which relies on the Hamming Distance of the PUF responses by intentionally heating up the silicon. Based on the observed PV distribution, a secure dual-rail placement against SCA in FPGA is devised. To validate the security variants, EM based surface scan is performed for investigating the leakage distribution. Correlation and mutual information analyses are used for jointly evaluating the security variants of a lightweight crypto coprocessor in variant placements. Experimental results demonstrated enhanced dual-rail symmetry owing to the reduced process variation in the interleaved placement.

Keywords: Side-Channel Attack (SCA) · Process Variation · Physical Unclonable Function (PUF) · Dual-Rail Precharge Logic (DPL) · CEMA · MIA

1 Introduction

In modern cryptography, data is protected by utilizing strong cryptographic algorithms, which inevitably draws into numerous vulnerabilities within its implementations. Conventional cryptanalysis centers to the exploitations of algorithmic decipherable weaknesses. Impeded by complex cipher systems, pure mathematic cryptanalysis became far to be viable when attacking the mathematically robust

crypto algorithms. In Contrast, Side-Channel attacks specially exploit the unintentionally leaked physical information for retrieving the hidden *things*. Side-Channel Attack in this context was originally sketched in [9] by Paul Kocher, *et al.* for analyzing the implementation basing on the tiny data-dependent fluctuations from the real-time power consumption.

A typical protection approach is to remove the data-dependent variations from the security critical logic elements. In this way, the dual-rail precharge logic (DPL) can be used which bases on a ‘*dual-rail*’ and ‘*dual-phase*’ protocol, where each logic value a is replaced by a pair of complementary values a_t and b_t respectively in two rails (*True* (T) and *False* (F) rails). In the ‘*evaluation*’ phase, all the effective values are propagated through the combinatorial logic chain, and in the ‘*precharge*’ phase, all the non-register values are reset to a fixed state (normally ‘0’). A proper realization of this structure ensures one and only one switch in each clock cycle in view of each compound gate, where in view of the two rails the logic behavior is constant. Hence the data dependencies can be theoretically removed. Since the continuously shrinking size of transistors, *Process Variation* (PV) is posing significant impacts to security assurances that makes some design essentials probabilistic and unpredictable [2, 3, 13]. Numerous researches have certified that silicon process variation affects power consumption within both routings and gates (output capacitive load [17]). This influence become even prominent in term of dual-rail logics, wherein a phenomena arose is that the mismatch between the logic behavior over complementary rails is likely to emit revealable Side-Channel leakage.

In this paper, a novel PV evaluation technique is proposed relying on the thermal influenced Ring-Oscillator Physical Unclonable Function (RO PUF), for bolstering the secure placement scheme of a SCA-hardened dual-rail logic. The remainder of paper is organised as follows: Sect. 2 describes the prior relevant work; The silicon process variation evaluation using RO PUF is detailed in Sect. 3; Sect. 4 demonstrates the dual-rail implementation of a lightweight crypto coprocessor; The selections of analysis models and platform setup are presented in Sect. 5; Sect. 6 gives the security evaluations basing on the EM surface scan, using correlation and mutual information approaches. Section 7 draws the conclusions and perspectives.

2 Technical Background

2.1 Silicon Process Variation and Dual-Rail Impacts

Process variation is the innate silicon feature of the randomly dispersed articles and etching deviations introduced from the chip manufacture. These non identical distributions unfavorably cause tiny spatial differences in electrical characteristics. The parasitic capacitances of ideally implemented net pair must consume the same amount of power. In Eq. (1), P_w denotes the power consumption from a routing assuming its parasitic capacitance is C_{pc} , working on the average flip frequency f and voltage swing V .

$$P_w = \frac{1}{2} \cdot C_{pc} \cdot f \cdot V^2 \quad (1)$$

For DPL researches in FPGA, routings in a long-term exist as a concern since the innate C_{pc} for each complementary routing pair should be as identical as possible. As previously stressed, parasitic parameters differ across the entire chip owing to the uncontrollable silicon bias. Hence, the rigorous requirements for a nicely constructed dual-rail circuit mainly reside within how to diminish the PV influence.

2.2 Silicon Process Variation Alleviation

A number of logics have been proposed in literatures, which helps to alleviate the security defects from process variations. In [14], the interconnect pairs are randomly swapped using a bit masking, which makes the routing bias ignorable. But the unbalanced routings still performs as the main leakage sources. A technique described in [10] increases the transistor channel lengths to mitigate the PV influence, using *Spice* simulation. However, a new fabrication technology is required which greatly increases the design cost. A technique proposed in [12] purposely minimizes the skews between T/F routing delays in a swapped dual-rail format. Since the routing pairs are estimated by length, instead of the precise shapes, the T/F routing pairs still leave exploitable leakage due to the unbalanced parasitic capacitances. In order to effectively remove the influence from technological biases, some expensive efforts must be devoted.

2.3 RO PUF Architecture

Inverter Based Ring Oscillator: RO is a low-cost logic that has been widely used in security specific Random Number Generator (RNG). The basic framework of RO is a cascaded delay stages in a closed chain, for yielding regulated and stable frequency oscillation at a fixed temperature. Figure 1(a) illustrates a generic inverter based Ring Oscillator in digital logic.

The flip frequency f of this RO can be computed by:

$$f = \frac{1}{\sum_{i=1}^n (d_{G_i} + d_{L_i})} \quad (2)$$

RO PUF: Because of the variations of physical characteristics in silicon, d_{G_i} and d_{L_i} have slight difference from different chips, locations, and even thermal environments, hence the observed frequencies can also be different. One of the most important RO usages in security domain is the RO based Physical Unclonable Function (PUF) [15], which takes into account of the unclonable and chip unique features. In an ordinary RO based PUF, identically laid-out ROs are implemented together. Due to the manufacturing variations across the chip, each RO delivers different frequencies that cannot be cloned to another chip. By deploying a number of identical ROs and comparing the frequencies obtained from the same sequence of RO pairs, a particular output bit combination can be achieved. Importantly, due to the PV from chip to chip, these bit orders are

not able to be duplicated even if the internal structure and sequence are disclosed. Hence this logic can be safely used as a unique signature for security authentication. Figure 1(b) sketches a type of RO based PUF.

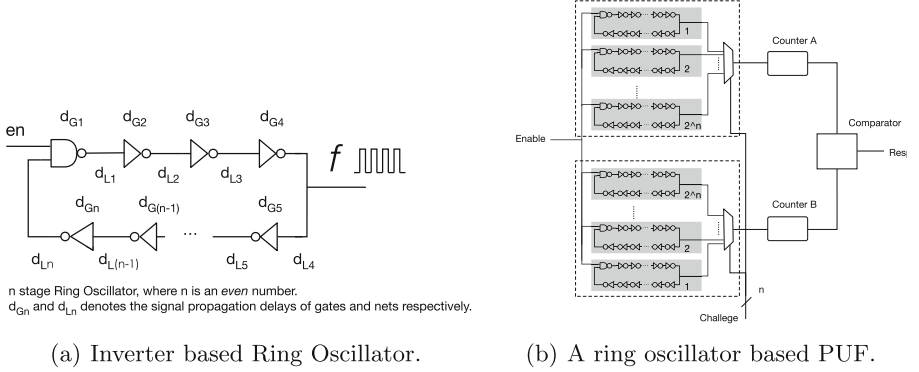


Fig. 1. Ring oscillator based physical unclonable function.

3 Dual-Rail PV Evaluation Using RO PUF

3.1 Thermal Effect to RO Pair

Temperature alters the physical behavior of a silicon circuit by influencing the mobility of the dopant electrons (n-type) and holes (p-type). More concretely, the higher thermal environment, the lower the signal propagation is. Since the frequency of a RO is determined by the summed up signal delays (see Eq. 2), the temperature can hence change the RO frequency in a predictable direction, *i.e.*, increasing the temperature would slow down the frequency as illustrated in Fig. 2(a). Assuming that identical ROs have different base frequencies at temperature T_0 . If the silicon where RO_a and RO_b are placed have smaller process variation than that between RO_a and RO_c, RO_a should have closer base frequency to RO_b, and larger base frequency to RO_c. Furthermore, owing to the similar physical characteristics, the frequency-temperature plots should be more likely to be a pair of parallel lines between RO_a and RO_b. An immediate hypothesis can be deduced that by increasing the temperature, the frequency flip between RO_a and RO_c occurs earlier (at T_1) than that between RO_a and RO_b (at T_2), which has been elaborated in Fig. 2(b).

3.2 FPGA Evaluation

To further certify this phenomenon, we employed two RO PUF in the Virtex-5 FPGA on SASEBO-GII board, where each RO has the same placement and route configuration to guarantee that the response variability is only rooted at the technological bias. For any challenges, frequencies from two unique ROs

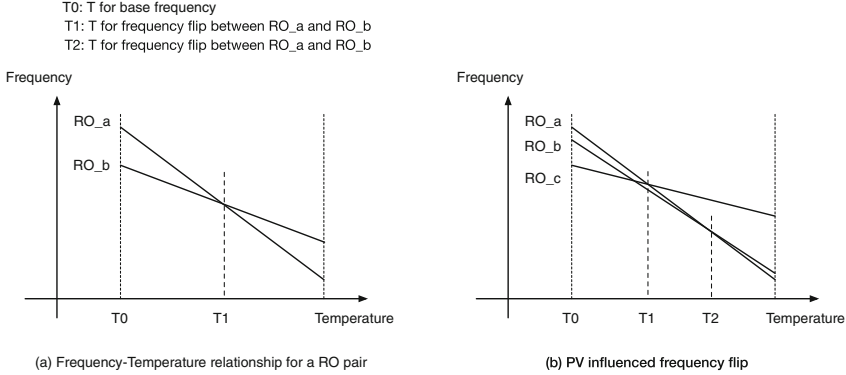


Fig. 2. Process variation influenced frequency flip for RO pair in changing temperature.

are compared, we can hence ensure the weakest dependency among each RO. Our work is based on the comparison of two settings: (i) All the ROs are randomly deployed in the logic array. We set the distance relevant process variation between any pair of ROs as $PV_{(a)}$, as shown in Fig. 3(a). (ii) The two ROs from any of the 64 RO pairs are intentionally deployed in an interleaved fashion, as given in Fig. 3(b), hence the distance relevant process variation is set as $PV_{(b)}$. Since all the RO pairs are interleaved in (b), the distances are all minimized and unified. By scanning the 6-bit challenge vector, we can extract 64 response bits respectively from the two settings. The two implemented RO PUF are shown in Fig. 4. To test the temperature influence to the PUF response, we used the hair dryer to heat up the silicon.

Table 1 shows the flipped response bits at the beginning (lowest temperature T_{low}) till the ending point (highest temperature T_{high}) to the differently placed PUFs in Fig. 4. The number of the flipped bits to the randomly placed

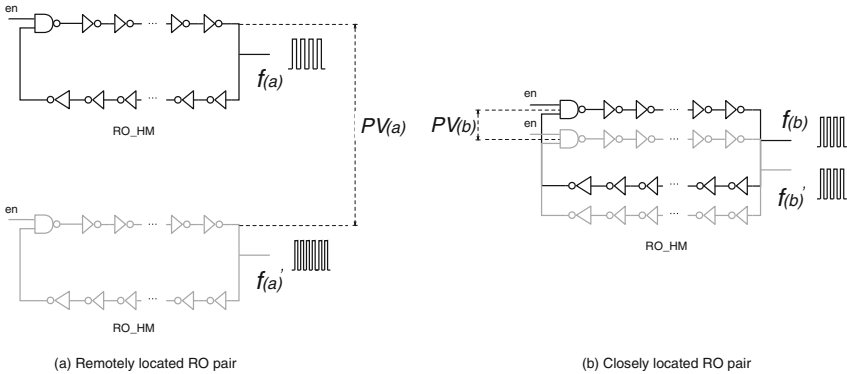


Fig. 3. Distance relevant process variation to Ring-Oscillator pair.

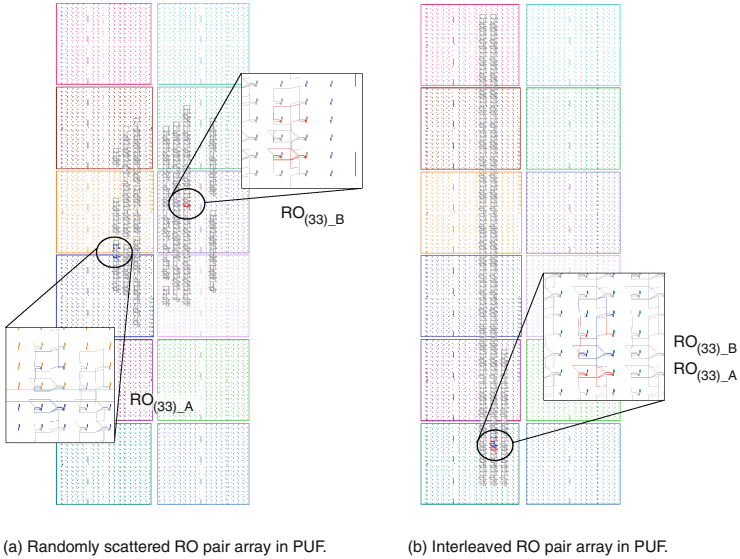


Fig. 4. FPGA editor view of the implemented RO pairs in PUF.

Table 1. Thermal influenced RO PUF responses

PUF_1	T_{low}	0	7	E	0	3	D	5	7	F	6	0	3	9	8	B	7	HD:13
	T_{high}	2	F	2	0	7	D	3	7	F	5	8	3	1	B	9	7	
PUF_2	T_{low}	F	D	C	F	F	4	6	8	6	B	F	4	E	E	C	0	HD:2
	T_{high}	F	D	C	F	F	C	6	8	4	B	F	4	E	E	C	0	

*A smaller HD represents fewer flipped response bits by heating up the silicon, time window for heating is 5 min.

PUF (PUF_1 in Table 1) during the heating process is 13 (*e.g.*, Hamming Distance (HD) of responses from T_{low} to T_{high}). In contrary, the counterpart HD to the interleaved PUF (PUF_2 in Table 1) is only 2. This observation shows that the thermal influence to the interleaved RO pairs are generally more identical, so they are comparatively difficult to be flipped (see RO_a and RO_b in Fig. 2(b)) by altering the temperature, which in turn implies smaller PVs between the corresponding logic and routing segments if the two identical rails can be interleaved.

4 Dual-Rail Implementation

4.1 Dual Core Placement

The viable placements of the paired rails reside on twofold metrics: (a) the resource configuration in FPGA device and (b) the logic structure to be handled. Since the selected DPL is a separate dual-rail format, or more precisely, the two

T/F networks have no swapped signals between each logic intermediates. Three placement styles are schemed which consists of (1) unprotected single-rail circuit, Fig. 5(i); (2) separate dual-rail one, Fig. 5(ii); (3) interleaved dual-rail, Fig. 5(iii).

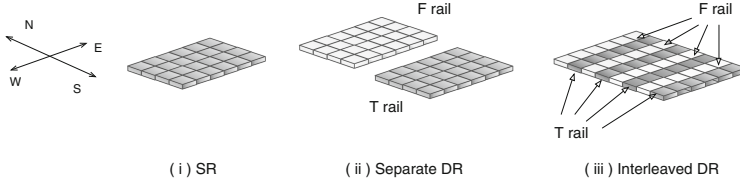


Fig. 5. Schemed dual-rail placements in FPGA resource array.

A lightweight *Present* block cipher [1] is selected in our experiments, which follows the principle of *Substitution-Permutation network* [11], to use either 80 bit or 128 bit key for en-/de-encrypting 64-bit plaintext/ciphertext in 32 computation rounds. Figure 6 briefs the basic parallel architecture of the selected cipher.

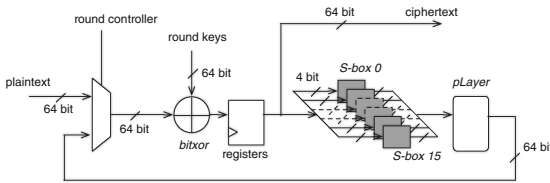


Fig. 6. Structure of *Present* lightweight crypto core.

4.2 Symmetric Dual-Rail Precharge Logic (DPL)

In our work, Precharge Absorbed-DPL (PA-DPL) [6] is selected for its high symmetry in dual-rail routing networks. Figure 7 presents the logic frameworks of the generic WDDL logic [16] and the used PA-DPL. The main difference here is that WDDL requires the swapped T/F routings to realize the *inverse factor* in logic functions, as seen in Fig. 7(a). Hence the routing pairs are impossible to be maintained physically identical in FPGAs. In contrary, the T/F rails in PA-DPL are independent, so a pair of identical T/F routing networks are possibly to be achieved, as shown in Fig. 7(b).

The implementation is approximately similar to the described 2-stage design flow in [12, 18], which consists of: (1) the generic FPGA single-rail implementation stage; (2) the back-end Xilinx Design Language (XDL) dual-rail transformation stage. We used the technique presented in [7] for the entire design flow for the following automatic routing repair process for finding non-identical or conflict routings, and restoring the identical T/F paths.

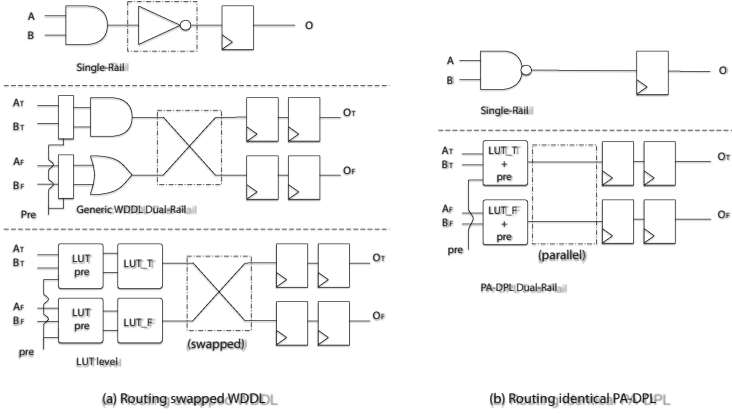


Fig. 7. WDDL and PA-DPL comparison.

5 Experimental Analysis

5.1 Selection of Distinguisher

Correlation EM Analysis (CEMA). The most widely utilized analysis metric is Correlation Power/EM Analysis (CPA/CEMA), which was originally proposed in [4]. Pearson correlation is used as distinguisher to determine the linear relationship between the hypothetical model and the measured leakage, using the following model:

$$r_{x,y} = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 \sum_{i=1}^n (y_i - \bar{y})^2}} \quad (3)$$

For any pair of vectors $\mathbf{x} = \{x_1, \dots, x_n\}$ and $\mathbf{y} = \{y_1, \dots, y_n\}$, \bar{x} and \bar{y} denote the means of x and y respectively. The \mathbf{x} and \mathbf{y} are substituted with the vector of measured traces and the hypothetical value. A higher $|r_{x,y}|$ shows some linear dependencies between x and y . The main restriction using correlation analysis is that it only reveals the linear relationship. Hence, if the constructed analysis model doesn't fit the circuit quite well, or the environmental noise is high, the correlation analysis might not be preferable.

Mutual Information Analysis (MIA). Mutual Information Analysis (MIA) was sketched in [5], which is constructed on the information theory for measuring the dependency between any two random variables. The entropy of random variable X in its space \mathcal{X} (discrete) is defined by:

$$H(X) = - \sum_{x \in \mathcal{X}} Pr[X = x] \cdot \log_2(Pr[X = x]) \quad (4)$$

$Pr[X = x]$ denotes the probability of $X = x$.

The higher the mutual information is, the stronger the relation among X and Y . Mutual information only concerns about general dependencies and thus, it could be generalized to construct both linear and non-linear relations between the logic value and the Side-Channel leakage. Hence in some cases, it outperforms the correlation analysis in condition of higher environmental noise and vague analysis model. Kernel Density Estimation (KDE) is utilized for estimate the probability distribution:

$$Pr[Y = y] = \frac{1}{qh} \sum_{i=1}^q K\left(\frac{y - y_i}{h}\right) \quad (5)$$

5.2 EM Surface Scan Acquisition

The cipher system is implemented in SASEBO-GII board [8], wherein *Present* is deployed into the main Virtex-5 cipher FPGA and the peripheral part is situated into the Spartan-3A controller FPGA. The main Virtex-5 FPGA is mechanically decapsulated (Thermal Interface Material(TIM) layer is EM transparent), hence the micro EM probe can be closely situated to the bottom-layer logic/routing elements. Riscure EM Station is used to perform the EM trace acquisition.

We conducted a preliminary thorough chip scan for positioning the logic region. An EM-proof shield is wrapped to the EM probe to increase the SNR. To collect the EM traces, a more precise EM acquisition is mounted to the pre-positioned clock regions. We set the surface rectangle region roughly over the clock regions where the cipher part resides. More precisely, the scanning matrix is set as 30×30 . In each location, 50,000 EM traces are collected, which exclusively aim at the time window between the last and the second last encryption rounds of *Present* cryptography at a sampling rate of 1GS/s.

6 Security Evaluation

6.1 CPA Analysis

For every 50,000 traces in each of the 900 locations, we performed the correlation coefficient analyses respectively for each of the total 16 4-bit subkey nibbles. The 2D correlation values for the scanned region yielded from the three implementations can be seen in Fig. 8, where the pixels showing the dark red colour refer to the locations where strong EM leakage appear, and vice versa. It is clear that Single Rail (SR) circuit shows the strongest local leakages in the locations where the cipher core is implemented (center in the array). Note that in the left-down corner, the leakage is also strong, which is generally due to the nearby IO pins that emanate strong EM information. Comparatively, the two dual-rail circuits demonstrate much lower leakage and smoother correlation distributions. More precisely, the separate Dual-Rail (DR) circuit still shows distinguishable leakages in the cipher part, while the interleaved DR shows even weaker leakages in the cipher deployed regions.

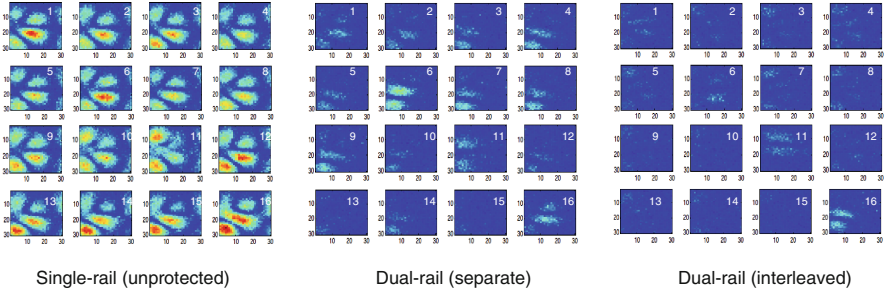


Fig. 8. 2D correlation plots of the EM scanning for different implementations.

6.2 MIA Analysis

MIA analysis is advantageous compared to correlation solution in case the data-leak relevancy is not linear, or the environmental noise is strong. As demonstrated in Fig. 9, the strong leakages widely exist in the unprotected single rail one (left in Fig. 9). The leakage distribution is similar to the CPA result where high leakages appear in crypto parts. For the DR candidates, leakages are significantly reduced because of the rail compensations. The separate DR (middle in Fig. 9) reveals some strong and distinguishable leakage in certain nibbles, and comparatively, the interleaved DR (right in Fig. 9) shows low and unidentifiable leakages in positions of all nibbles.

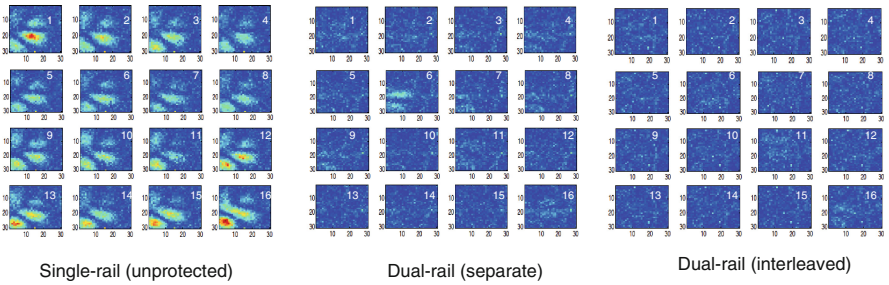


Fig. 9. 2D correlation plots of the EM scanning for different implementations.

6.3 Experimental Summary

According to the observations of the CPA and MIA leakages to the scanned region on chip, CPA shows high and distinct leakage peaks at the expected leak points where the cipher cores are deployed. MIA, in contrary, as well demonstrates the local leakages, while the distributions are not sharp *w.r.t.*, CPA, *i.e.*, the leakage locations are not precisely localized. This is mainly owing to the MIA nature, which is functional for revealing not just linear relevancy, but also non-linear dependency, which inevitably introduces of considerable environmental

noise that partially matches the hypothesized relationship between the EM field and the processed data. However, the leakage maps of the interleaved DR circuit from both correlation and mutual information analyses jointly certify a higher security grade. Since all the experiments are done in the same setups and similar temperature/EM environments, we can safely conclude that the interleaved DR placement outperforms the separate DR placement in term of correlation and mutual information based SCAs.

7 Conclusions

In this paper, we have reported a technique for evaluating the dual-rail influence from in-die silicon process variations. This approach depends on the thermal influence to the RO PUF in different placements, for validating that the paired ROs in the interleaved PUF have less influence from heating. This result in turn certifies smaller process variations between each interleaved RO pairs. A lightweight block cipher - *Present* is implemented in a symmetric dual-rail logic (PA-DPL). Based on the achieved outcomes, a complete security evaluation has been performed, where an EM surface scan is mounted to collect the local emanations. By drawing the leakage map using both CPA and MIA analyses to each measured logic location in the scan array, the leakage distributions can be plotted. The experimental results certified significantly decreased information leakage by employing DR protections. More concretely, the interleaved DR placement provides an even higher security grade due to the reduced process variations between any paired T/F logic rails.

In the subsequent work, we plan to find more proper distinguisher to evaluate the leakage distribution of a wide variety of DPL styles.

References

1. Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y., Vikkelsoe, C.: PRESENT: An ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
2. Boning, D., Chung, J.: Statistical metrology: Understanding spatial variation in semiconductor manufacturing. In: Microelectronic Manufacturing Yield, Reliability, and Failure Analysis II: SPIE 1996 Symp. On Microelectronic Manufacturing (1996)
3. Bowman, K.A., Duvall, S.G., Meindl, J.D.: Impact of die-to-die and within-die parameter fluctuations on the maximum clock frequency distribution for gigascale integration. *IEEE J. Solid-State Circuits* **37**(2), 183–190 (2002)
4. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004)
5. Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual information analysis. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 426–442. Springer, Heidelberg (2008)

6. He, W., de la Torre, E., Riesgo, T.: A precharge-absorbed DPL logic for reducing early propagation effects on FPGA implementations. In: International Conference on Reconfigurable Computing and FPGAs (ReConFig), pp. 217–222. IEEE (2011)
7. He, W., Otero, A., de la Torre, E., Riesgo, T.: Customized and automated routing repair toolset towards side-channel analysis resistant dual rail logic. Elsevier J. Microprocess. Microsyst. **38**(8), 899–910 (2014)
8. Katashita, T., Satoh, A., Kikuchi, K., Nakagawa, H., Aoyagi, M.: Evaluation of DPA characteristics of SASEBO for board level simulations. In: International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE), vol. 36, p. 39 (2010)
9. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
10. Lin, L., Burleson, W.: Analysis and mitigation of process variation impacts on power-attack tolerance. In: 46th ACM/IEEE Design Automation Conference, DAC 2009, pp. 238–243. IEEE (2009)
11. Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (2010)
12. Moradi, A., Immler, V.: Early propagation and imbalanced routing, how to diminish in FPGAs. In: Batina, L., Robshaw, M. (eds.) CHES 2014. LNCS, vol. 8731, pp. 598–615. Springer, Heidelberg (2014)
13. Nassif, S.R.: Modeling and forecasting of manufacturing variations. In: Proceedings of the ASP-DAC 2001 Design Automation Conference, pp. 145–149 (2001)
14. Popp, T., Mangard, S.: Masked dual-rail pre-charge logic: DPA-resistance without routing constraints. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 172–186. Springer, Heidelberg (2005)
15. Suh, G.E., Devadas, S.: Physical unclonable functions for device authentication and secret key generation. In: Proceedings of the 44th Annual Design Automation Conference, pp. 9–14. ACM (2007)
16. Tiri, K., Verbauwhede, I.: A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In: Proceedings of the Conference on Design, Automation and Test in Europe, vol. 1, p. 10246. IEEE Computer Society (2004)
17. Tiri, K., Verbauwhede, I.: Place and route for secure standard cell design. In: Quisquater, J.-J., Paradin, P., Deswarte, Y., El Kalam, A.A. (eds.) Smart Card Research and Advanced Applications VI. IFIP, vol. 153, pp. 143–158. Springer, Heidelberg (2004)
18. Yu, P., Schaumont, P.: Secure FPGA circuits using controlled placement and routing. In: 2007 5th IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS), pp. 45–50. IEEE (2007)