# Authenticating resilience of RTL codes against Power Side Channel leakages

Jaganath Prasad Mohanty, Kamalakanta Mahapatra
*Dept. of Electronics and Communication Engineering*
*National Institute of Technology* Rourkela, India
vlsi.nitrkl@gmail.com

***Abstract*—Electronic consumables in the digital era realises smart technology to the very core of innovation and challenges stereotypical livelihood. Within a few years the number of IoT devices will surpass the population of this world. Data shared among them is enormous which needs protection on the network . With such power, the hardware industry, specifically the Electronic Design Automation tool industrial sector plays a significant role, by making available the necessary fabricated chips embedded on the IoT devices. With the emergence of power analysis for side channel attacks, among various ongoing linear and differential cryptanalysis, a RTL code needs to be resilient to all of them prior to fabrication, before it is accepted as a design in the EDA tool process and delivered at the market as a viable chip. This work acts as an aid to the ongoing work on the different testing methods namely Six Sigma, Pearson's chi-squared test and Welch's t-test for tracing leaks in a RTL code with a conceptual method for testing furthermore.**

***Index Terms*—Side Channel Analysis, Information Leakage, Power Attack, RTL, Resilience**

## I. Introduction

An analytical study of the hardware encryption market as per the report [1] shows the trends, drivers and projections of the global market scenario for the secure hardware industry. Smart cards were the initial targets of hackers [3], and for the last few decades FPGAs are also beaming goals in todays cloud computing era, apart from ASICs [7].The Electronic Design Automation (EDA) tool industry plays a vital role in building secure viable chip designs. With numerous acknowledgement of attacks ever increasing daily, white hat hackers use various technology to dodge them ragularly. Many challenges are heralded and adhered to by patches in numerous ways, but the trend of new encounters keep on emerging. A summarized view of the various power side channel attacks [5] is listed in table I with its methodology, which is informed upon shortly. The general tradition is through observations of power traces, analogous to voltage fluctuation measured while the device under test (DUT) is operating certain encryption/decryption functions.

Assuming hackers to be miser in terms of technical knowhow costed huge for the market. And so the advancements in cost effective hardwares with ample resources availabile, the hackers were able to easily tamper with not only hardware configurations but also softcores through firmware. This lead to expansion in research domain to inculcate secure by design metrics from the very initial stages of ideating a chip. Worldwide researchers have acknowledged the significance of this initial loophole and have urged the EDA industry to consider their defacto standard of chip design process [15]. The acceptance will be beneficial to every individual who will be in the design client side as well as consumer user side.

TABLE I: Power Side Channel Analysis methodology

| **Attacks** | ***Tactics*** | ***Group*** |
|---|---|---|
| Simple Power Analysis (SPA) | Visual Inspection of electrical activity | Model Based |
| Differential Power Analysis (DPA) | Power Trace Comparison | Model Based |
| Template Attacks (TA) | Cloned Stencil Comparison | Profiling |
| Correlation Power Analysis (CPA) | Pearson Correlation Coefficient | Model Based |
| Mutual Information Analysis (MIA) | Information Theory | Model Based |
| Machine Learning | Feature Classification | Profiling |

A model based and profiling groups, wherein the device's power consumption and employed secret key were defined to classes based on leakage model is depicted in the table for understanding the background of the presented article. A brief overview can be refered in the statistical analysis and tests including difference of means [10], Pearson correlation coefficient [11], Bayesian classification [12], etc., which were used for determining secret keys.

In 2004, Brier et al. [11] improved the DPA [2] by locating different points of a device model, in the work title Correlation Power Analysis. In the Mutual Information Analysis (MIA), Bet Gierlichs et al. in 2008 [13], compared all dependencies between modelled device leakage and observed leakage. MIA is generic, multivariate by design and uses conditional entropy as a distinguisher, forwarding the two-dimensional search space to a multidimensional space in SCA research.

The Test Vector Leakage Assessment (TVLA) is an approach different than the rest in a way that aids in analyzing a DUT for leakages, rather than developing attacks to recover secret key information. Gilbert et al. [14] in 2011 explained devices running cryptographic algorithms, loaded with countermeasures to known hardware implemented vulnerabilities, demonstrated leakages by examining traces collected with

978-0-7381-4264-7/20/$31.00 ©2020 IEEE
DOI 10.1109/IEEE-iSES50453.2020.00067

fixed vs. varying data. This work follows Welch's t-test for providing confidence level to accept (or reject) a hypothesis of finding vulnerabilities in the algorithm and intermediate influencing side channel in a DUT. Another statistical test for identifying leakages in a device is Pearson's chi-squared test, wherein the hypothesis is done on unpaired observations, unlike Welch's t-test where traces are averaged for comparison on class basis.

## II. Opportune Traction

Electronic Design Automation (EDA) tool industry for ICs have focused primarily on the traditional power, performance and area look out [15]. Nevertheless, secure by design and hardware composition must also be absorbed noticing the rise in threats toward hardware security at all levels of the supply chain management as shown in "Fig. 1". A security-driven design method need to be hypothesized and eventually incorporated into EDA tools, for secure alignment of designs against the attack vectors often imminent foreseeable advances in technology.

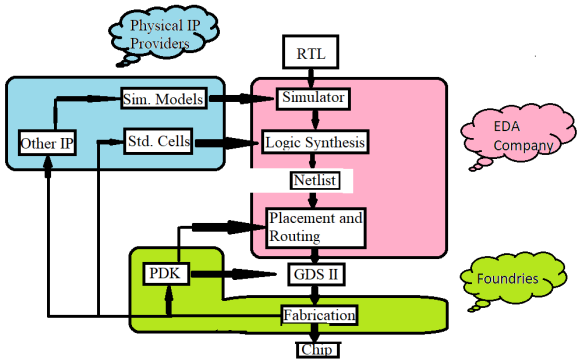



Fig. 1: Level of a Semiconductor (EDA) Supply Chain Management.

Using statistical analysis to check a RTL code designed in a hardware description language is a skill which tests perseverance. A master database, which provides the best case and worst case power estimation of the variety of coding styles, is need of the hour which will be a benchmark for further comparison and testing. A method is conceptualized to investigate an RTL code compared with the available knowledge base of leakages, based on the different data and corresponding power consumption from the master database by means of exhaustive investigation. This data base is used to compare any RTL code of a specific HDL and give an estimate of leaking potential points in the modelling style.

Further, using feature selection and the classification analogy of a DNN based machine learning algorithm [8], the data is collected and trained iteratively until a good enough sorting is lead automatically to identify quality of a particular RTL design modelling style and estimate power leakage defects when synthesized in a compiler to certain accuracy. Deploying the model is yet another facet wherein the Welch's t-test assists to a greater extent. The caveat at this level of testing is to select the arbitrary points using EDA synthesis tool and observing the measurements for all data to keep it intact throughout the iterations. This concept, to the best of our knowledge is not publicly available for academic and/or industrial use till now in literature, and can be marketed in open source for further investigation towards its claims and merit.

## III. Simulated Environment

An abstract method is identified to embrace at the initial stage of the EDA tool process in order to assess the viability of a design as a resilient one against a robust power leakage technique. The proof of work concept is a progressing research which will include all of the existing power SCA attacks and to the best of our knowledge try to imbibe future threats and is robust against it. A benchmark is being created for the power estimation of differing coding style for various HDLs currently available in literature. A model specific test generation will be suitable to accurately analyze the loopholes in a RTL coding style, but this would require a better understanding of the twists and turns of the mixed style of designing architecture. With time this is also predictable in the near future, till then one needs to collect data, share it in the open community, train the particular data set in a model and deploy it, if not taken the aid of Artificial Intelligence.

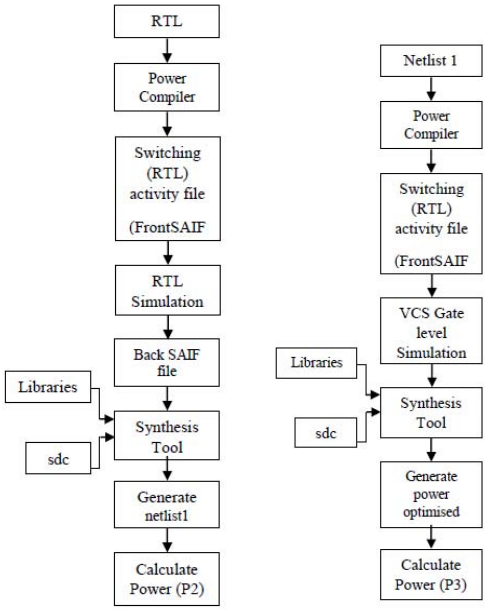
The resources used in this method of testing a RTL code for power leakage can be standardized by the EDA synthesis and compiler tool. The initial investment will be on making the master database for various coding style of different Hardware Description and/or Verification Languages making an estimation for the versatile power scenario, which as mentioned earlier will be a benchmark, outsource or inbuilt from the EDA based company. In this work we are not considering the outsourced IP piracy through third party intermediaries, or any such adversarial inclusivity while designing the code, though this concept should be valid for checking the IP trafficking to a certain extent as well. The technical, business and ethical diligence of the value of such a methodology is needed to be further analyzed, since it is created in an academic environment, and the future economic value is not taken into consideration.

Power analysis is the task of evaluating the power consumption of an existing design at any level. The system-level power analysis with its common principles at any level is introduced. Switching activity based power analysis method is a widely accepted process. Simulation based methodology or estimation based methodology falls under this switching activity. It can be modelled in different levels of detail based on the analysis flow.

Power analysis is done in three stages: RTL level, gate level and post layout level. P1 is the RTL power estimator that calculates power in the initial stage. In this case Switching Activity Interchange Format (SAIF) file is generated using power compiler, which is an open ASCII format. It captures the switching statistics for each node in the design in terms of static and dynamic attributes that should be state and

path dependent. State dependent static attributes are useful for computing state dependant leakage power and computing dynamic power.

Power analysis based on RTL simulation is displayed in “Fig. 2. RTL simulation captures the switching activity at the synthesis invariant points in the design, which includes the hierarchy boundaries and sequential elements. Capacitance and power models for wires and gates are taken from the library. Along with all the constraints, RTL design is synthesized to gate level. Front SAIF file generated by the Power Compiler is used in RTL simulation to generate back annotated SAIF file from simulator. The back annotated SAIF is fed into synthesis tool (Design Compiler) and synthesizing the design, after which power P2 can be calculated, as is shown in “Fig. 2’(a).




(a) RTL Power (b) Netlist based Power

Fig. 2: Simulation based power analysis flow.

The gate-level simulation based power analysis flow is similar, except that no internal activity propagation is required because activity is captured at the input pins of all the cells in the gate-level netlist via gate-level simulation. Because this activity is captured in full detail, it is possible to use the state and path dependent information in the library models and in SAIF to perform a more accurate power analysis (P3). The detailed flow is similar to RTL simulation flow as shown in “Fig. 2’(b). The complete time-based power profile view of the chip is calculated using the value change dump (VCD) or VCD formats, which are generated based on gate-level based switching activity. Post placement and routing netlist, the wire capacitances and other parasitics are back annotated from layout. Primepower provides a detailed analysis of the power dissipation in a design (P4) and relies on the complete VCD switching activity format and back annotated parasitic file. It works on a gate-level netlist with gate-level simulation data and is targeted to full-chip capacity. Along with the average power numbers, it also gives the time-based waveforms of power consumption in different ports of design and allows designers to locate hot spots in design. The detailed flow is shown in “Fig. 3’.

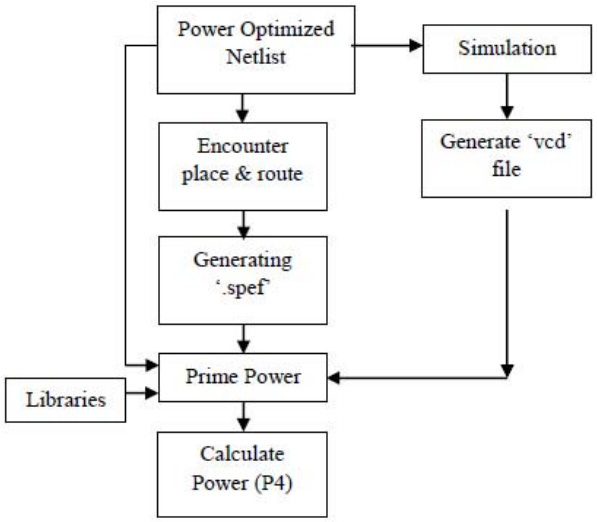



Fig. 3: Post Layout Power.

The above details shows an approximately accurate power estimations which can be further used in the process of evaluating power metrics and creating a database to refer. A proposed concept is ideated as shown in “Fig. 4’ detailed in the next section to thwart the side channel leakage metrics analogous to the work described in experimentation through [16], [17] and [18]. This work in progress discuss the merit of such proposal, which are explored within the EDA industry and researchers are requesting the authorities to consider these steps for future designs.

## IV. Conceptual Framework

Side Channel Attacks are one of the vital threats to electronics hardware and design engineers have to come up with solutions as to thwart these attacks in the current Digital world. A single event cannot be attributed to a single cause. Intuitively a small change on the means can have a significant effect on extreme. Stages in Business as usual runs amuck– 1) No commitment to take actions, 2) Intermediate scenario has to be considered. 3) Aggressive scenario – mitigation strategy should start immediately to reduce effects, but not yet started

But fundamental change in infrastructure will take several decades. Assessment report suggests, that as shown in figure 4, using intermittent available resources, RTL resiliency can be checked

A design engineer needs to check for Vulnerability points comparing the RTL code with the standard database, as portrayed by the economical viable consumer electronics industry. If adaptation measure is available – consider as secondary

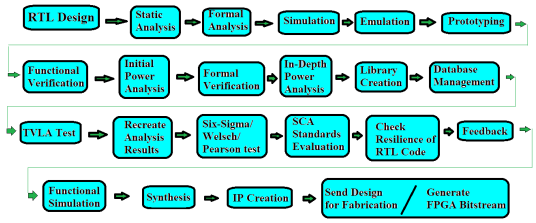



Fig. 4: Proposed framework for SCA resilient RTL design.

prevention. If absolutely necessary to take steps and adapt, consider limits and tolerance level Mitigating measure are primary prevention consideration. Immediate benefits of taking up measures can be endured citing the economy for industry. Design engineer also needs to study Fracking energy impacts benefits - Mitigation focuses on interventions to reduce attacks or enhance comparative security, whereas adaptation focuses on interventions to reduce vulnerability to and to increase resilience against adverse effects of attack strengths and change in attacker attributes

## V. Conclusion

Side channel analysis and attacks have reached certain maturity level which the EDA tool will accept as a necessity to be resilient to in future electronic systems. Ensuring uniformity with the testing and verification development phase of the industry, the leakage models needs to be robust against any future threats as well, which needs expertise. Point is whether the EDA tool and manufacturing industry will accept this secure composition as a key enabler for complex ICs is yet to be seen. In this work, a brief review of the state-of-the-art analysis technique against side channel leakage and assessment has been discussed and a proof of concept has been presented for checking vulnerabilities in a designed RTL code. And the EDA tool process is entreated to identify concepts likewise for secure composition of countermeasures and for security metrics.

## Acknowledgment

The authors would like to thank SMDP-C2SD project sponsored by MEITY, Government of India. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Indian Government.

## References

[1] Ashraf, N., Masood, A., Abbas, H. et al. , “Analytical study of hardware-rooted security standards and their implementation techniques in mobile. Telecommun Syst 74, 379–403 (2020). https://doi.org/10.1007/s11235-020-00656-y

[2] P. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis,” Advances in Cryptology - Crypto 99 Proceedings, Lecture Notes In Computer Science Vol. 1666, M. Wiener, ed., Springer-Verlag, 1999

[3] Mangard, S., Oswald, E., Popp., T.“Power Analysis Attacks – Revealing the secrets of smart cards,” Springer, 2007, ISBN 0-387-30857-1

[4] S. Moein, T. A. Gulliver, F. Gebali and A. Alkandari, “HARDWARE ATTACK MITIGATION TECHNIQUE ANALYSIS,” International Journal on Cryptography and Information Security (IJCIS), pp. Vol. 7, No. 1, pg 9 - 28, March 2017

[5] Mark Randolph and William Diehl, “Power Side-Channel Attack Analysis: A Review of 20Years of Study for the Layman,” Cryptography 2020, 4, 15; doi:10.3390/cryptography4020015.

[6] H. E. Project, “Enhancing Critical Infrastructure Protection with Innovative SECurity Framework (CIPSEC),” [Online]. [Accessed 22 May 2019].

[7] M. Tehranipoor, S. Brown and S. Aftabjahani, “The Vulnerability Database,” 2018. [Online] Available: http://www.trust-hub.org/vulnerability-db/physical-vulnerabilities.

[8] S. G. X., Adrien Facon, “Hardware-enabled AI for Embedded Security A new Paradigm,” in 3rd International conference on Recent Advances in Signal Processing, Telecommunications and Computing (SigTelCom), 2019

[9] W. He, J. Breier, S. Bhasin, N. Miura and M. Nagata, ”An FPGA-compatible PLL-based sensor against fault injection attack,” 2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC), Chiba, 2017, pp. 39-40, doi: 10.1109/ASPDAC.2017.7858291.

[10] Cohen, A.E.; Parhi, K.K, “Side channel resistance quantification and verification. In Proceedings of the 2007 IEEE International Conference on Electro/Information Technology (EIT 2007), Chicago, IL, USA, 17–20 May 2007; pp. 130–134.

[11] Brier, E.; Clavier, C.; Olivier, F.“Correlation power analysis with a leakage model. In Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), Cambridge, MA, USA, 11–13 August 2004; pp. 16–29

[12] Chari, S.; Rao, J.R.; Rohatgi, P. “Template attacks,” In Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), Redwood Shores, CA, USA, 13–15 August2002; pp. 13–28.

[13] L Bet Gierlichs, B Batina, L.; Tuyls, P.; Preneel, B. “Mutual information analysis: A generic side-channel distinguisher,” In Cryptographic Hardware and Embedded Systems—CHES 2008, Proceedings of the 10th International Workshop, 10–13 August 2008; Springer: Berlin, Germany, 2008; pp. 426–442.

[14] Goodwill Goodwill, G.; Jun, B.; Jaffe, J.; Rohatgi, P. “A testing methodology for side-channel resistance validation,” In Nist Non-Invasive Attack Testing Workshop; NIST: Gaithersburg, MA, USA, 2011.

[15] Johann Knechtel, Elif Bilge Kavun, Francesco Regazzoni, Annelie Heuser, Anupam Chattopadhyay, Debdeep Mukhopadhyay, Soumyajit Dey, Yunsi Fei, Yaacov Belenky, Itamar Levi, Tim G"uneysu, Patrick Schaumont, and Ilia Polian, “Towards Secure Composition of Integrated Circuits and Electronic Systems: On the Role of EDA,” arXiv:2001.09672v1 [cs.CR] 27 Jan 2020.

[16] Y. Nasser, J. Lorandel, J. Prévotet and M. Hélard, “RTL to Transistor Level Power Modelling and Estimation Techniques for FPGA and ASIC: A Survey,” in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, doi: 10.1109/TCAD.2020.3003276.

[17] V Ganesan, R Bodduna, C Rebeiro,“ PARAM: A Microprocessor Hardened for Power Side-Channel Attack Resistance,”- arXiv preprint arXiv:1911.08813, 2019.

[18] Madura A Shelton, Niels Samwel, Lejla Batina, Francesco Regazzoni, Markus Wagner, Yuval Yarom, “Rosita: Towards Automatic Elimination of Power-Analysis Leakage in Ciphers,” 2020, arXiv:1912.05183 [cs.CR].