Static Power Side-Channel Analysis of a Threshold Implementation Prototype Chip

Thorben Moos, Amir Moradi, and Bastian Richter
Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum, Germany
firstname.lastname@rub.de

***Abstract*—The static power consumption of modern CMOS devices has become a substantial concern in the context of the side-channel security of cryptographic hardware. The continuous growth of the leakage power dissipation in nanometer-scaled CMOS technologies is not only inconvenient for effective low power designs, but does also create a new target for power analysis adversaries. In this paper, we present the first experimental results of a static power side-channel analysis targeting an ASIC implementation of a provably first-order secure hardware masking scheme. The investigated 150 nm CMOS prototype chip realizes the PRESENT-80 lightweight block cipher as a threshold implementation and allows us to draw a comparison between the information leakage through its dynamic and static power consumption. By employing a sophisticated measurement setup dedicated to static power analysis, including a very low-noise DC amplifier as well as a climate chamber, we are able to recover the key of our target implementation with significantly less traces compared to the corresponding dynamic power analysis attack. In particular, for a successful third-order attack exploiting the static currents, less than 200 thousand traces are needed. Whereas for the same attack in the dynamic power domain around 5 million measurements are required. Furthermore, we are able to show that only-first-order resistant approaches like the investigated threshold implementation do not significantly increase the complexity of a static power analysis. Therefore, we firmly believe that this side channel can actually become the target of choice for real-world adversaries against masking countermeasures implemented in advanced CMOS technologies.**

I. Introduction

Ever since the introduction of power analysis attacks in 1999 [12] researchers have concentrated almost exclusively on the exploitation of the operation- and data-dependency that can be observed in the dynamic power consumption of cryptographic hardware. However, in the year 2007 the authors of [10] provided the first concrete evidence for the fact that the leakage currents in modern CMOS gates exhibit a strong data-dependency as well. Additionally they pointed out that the static power consumption had already reached a considerable dimension for sub-micron CMOS technologies by then. These discoveries consequently led to the first attempts to exploit the emerging new side channel. In [13] a DPA-based attack on (simulated) static power measurements using a single-bit power model is proposed. The works presented in [6] and [7] verify the soundness of the Hamming weight model in the static power domain and conduct a successful CPA attack. Further investigations revealed extensively that multiple DPA-resistant logic styles are rather ineffective against static power analysis [4], [5], [11], [13]. The results of [8] do even suggest that an unprotected CMOS implementation of the block cipher PRESENT-80 is less vulnerable to such attacks than the same cipher implemented in the DPA-resistant logic style WDDL. Even though all the previously mentioned articles are solely based on simulations, they already point out the significant impact of the temperature on the static power dissipation and conclude that it must be kept constant during measurements. Currently, the only accessible research results in this field that are based on actual static power measurements instead of simulations are presented by [15] and [20]. The former one provides detailed information about the leakage currents of different FPGA elements in various process technologies. Furthermore, the higher-order moments of the static power consumption are utilized to perform a successful key recovery on a masked and shuffled AES-128 implementation. It is clearly demonstrated in [20] that the ability to control the clock enables an adversary to arbitrarily reduce the noise in the measurements. This possibility is expected to pose a serious threat to algorithmic DPA countermeasures that require high noise levels, such as masking.

When taking a look at the amount of publications on this topic, especially the ones that are based on actual measurements, one has to conclude that up to now the static power side channel was not taken as serious threat by the side-channel community. Indeed, none of the aforementioned case studies was able to report a significant reduction of the complexity of an attack in comparison to a corresponding dynamic power analysis yet. But since only a small number of (protected) implementations has been investigated, this fact is hardly informative. It is important to consider that the static power consumption is predetermined to increase with the further down scaling of the CMOS technology, which continuously favors the feasibility of such attacks. Hence, it has become a crucial and urgent task to thoroughly examine the effectiveness of established DPA countermeasures in the static power domain, which also has been the main motivation for this work.

Our contribution: In this paper we provide, to the best of our knowledge, the very first experimental results of a static power side-channel analysis targeting a full state-of-the-art block cipher on an ASIC chip. In this regard we confirm the FPGA-based results of [15] for ASIC platforms. Additionally, for the first time, we examine the efficiency of a provably first-order secure implementation technique in presence of static power analysis attacks. Our target is hereby a 150 nm ASIC prototype chip including a PRESENT-80 core that is realized by a 3-share threshold implementation technique. The previously mentioned articles [15] and [20] do both suspect on the basis of their studies that first-order resistant approaches (like our target) will be vulnerable to static power analysis. We

investigate this hypothesis and provide informative numbers for the effectiveness of masking countermeasures in presence of a leaking static power side channel. In contrast to all previous works (and as recommended by [15]) we extensively test and document a dedicated measurement setup for static power analysis, including a super low-noise DC amplifier with a very high gain as well as a climate chamber to neutralize the temperature effects. We evaluate the measurement process and the obtained results and compare them to corresponding dynamic power analysis attacks.

II. Measurement Setup

In order to measure the static power consumption of our target ASIC, we inserted a precision $1\,\Omega$ resistor with low temperature coefficient into the Vdd path. In contrast to dynamic power measurements the amplifier cannot be AC coupled since AC coupling works as a kind of high-pass filter and would eliminate our static target signal (DC offset). Thus, common AC-coupled amplifiers like the `ZFL-1000NL+` from Mini-Circuits cannot be used in this setup. Instead, the voltage drop over the resistor needs to be measured differentially and with a DC-coupled amplifier. There are two main problems when measuring the static leakage. At first, the voltage difference we would like to measure is very small, typically in the range of a few micro volts. To get an accurate measurement, a high DC amplification is needed. The second problem is the susceptibility to temperature variations. The static leakage itself is highly temperature dependent which results in huge shifts of the measured signal e.g., when the measurement room is accessed. Also, many amplifiers and differential probes suffer from a DC shift when they heat up during use. In [15] a LeCroy AP 033 differential probe which features a $\times 10$ amplification was used. While this probe is capable of measuring the signal with its high common DC offset, it only features a low amplification and is susceptible to thermal shifts in the measurements when the probe heats up during the long measurement procedure. To overcome these drawbacks, we developed a sophisticated amplifier to measure the static leakage. The first stage of the amplifier consists of an Analog Devices AD8421 instrumentation amplifier [1]. This stage removes the common voltage between its two inputs which are connected to the two terminals of the shunt resistor and applies an amplification with a gain of 2. Since we only want to measure the data-dependent difference in the current, which is much smaller than the total current to the ASIC, we subtract an adjustable offset from the measured voltage using the offset input of the instrumentation amplifier. This enables us to use a smaller range in the oscilloscope and thus get a higher resolution. A second stage consisting of an Analog Devices AD8676 operational amplifier (op-amp) [2] applies a $\times 500$ amplification to the resulting signal. The same type of op-amp is used to buffer the offset voltage. All components, including the passive ones like resistors to adjust the offset, are selected to offer a very low temperature dependency. The PCB of the amplifier is housed in a custom aluminum case which provides SMA connectors. Due to the high gain, the bandwidth of the amplifier is below $20\,\mathrm{kHz}$ which does not pose a problem since we are working with static signals.[1]

[1]Detail of the developed amplifier (schematic, PCB, components' list) is accessible through the authors' webpage.

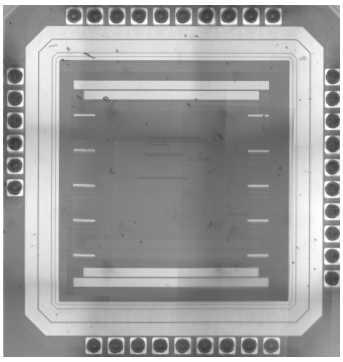


Fig. 1: ASIC prototype with 6 cores in 150 nm CMOS.

The Side-channel Attack Standard Evaluation Board (SASEBO-R) [3] that we used for our experiments was specifically designed to evaluate the security of cryptographic hardware implementations against side-channel attacks. The board provides a socket for an ASIC prototype which is connected to a Xilinx Virtex-II Pro FPGA for control and communication purposes. Since measuring small signals over long wires can induce measurement errors, we kept the distance between the shunt resistor and the amplifier short by designing the housing of our developed amplifier in such a way that it can be plugged directly on top of the SASEBO-R board by the SMA connectors. It is noteworthy that for both static and dynamic power measurements, we used a Teledyne LeCroy HRO 66zi oscilloscope.

Due to the significant impact of the temperature on the static power consumption we performed the static leakage measurements inside a CTS climate test chamber of series C-40/100. The chamber can hold the temperature with a variation of $0.3\,^{\circ}\mathrm{C}$ at a maximum thermal load of 1200 W at +20 $^{\circ}\mathrm{C}$. This should highly suffice for our purposes as the target is not expected to radiate a considerable amount of heat (resulting in even smaller temperature variations). We placed the SASEBO-R board together with the mounted ASIC prototype and the DC amplifier inside the chamber, whereas the oscilloscope and the power supply units for the board and amplifier have been placed outside of the chamber. Hence, we put the required cables between the oscilloscope and the setup through a vent in the chamber that was carefully sealed with silicone foam.

III. Target

The target for our experiments is an ASIC prototype chip including a PRESENT-80 core realized as a 3-share threshold implementation. The ASIC is implemented in 150 nm CMOS technology using the LFoundry 150 standard cell library and is operated with a supply voltage of 1.8 V. A photo of the prototyped chip is shown by Fig. 1. Its package was specifically selected to fit into the SASEBO-R socket to ease the evaluations.

PRESENT-80 is an ultra-lightweight block cipher (ISO/IEC 29192-2:2012 standard) that operates on a block size of 64 bit as well as a key length of 80 bit and consists of 31 computation rounds [9]. The term threshold implementation refers to a masking scheme based on Boolean secret sharing and multi party computation that implements non-linear functions of symmetric block ciphers efficiently in such a

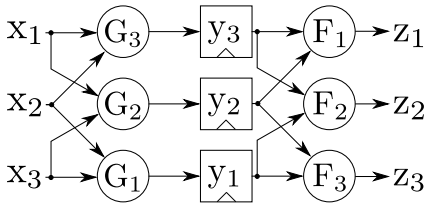


Fig. 2: Threshold implementation of the 4-bit PRESENT S-box with 3 shares. $\mathrm{S}(x_1 \oplus x_2 \oplus x_3) = z_1 \oplus z_2 \oplus z_3$

way that provable security against first-order power analysis attacks can be guaranteed, even in the presence of glitches [18]. The specific application of this scheme to the PRESENT-80 block cipher is introduced in [19]. Our investigated ASIC core implements the profile 2 of [19]. This profile refers to a serial implementation of PRESENT-80 with a shared data path (with 3 shares) but an unshared key schedule.

Fig. 2 illustrates the threshold implementation of the PRESENT S-box with 3 shares. All intermediate values and data buses are 4-bit wide. As the graphics show, the S-box – which has an algebraic degree of 3 – is decomposed into two non-linear quadratic functions F and G. Those 4-bit boxes are then split into 3 shares each. The three G-boxes are processed at the same time in the ASIC and each of them receives 2 inputs out of the 3 data shares x_1, x_2, x_3. The corresponding outputs y_3, y_2, y_1 are stored into registers. Afterwards, the three F-boxes are evaluated in parallel. The 4-bit words of the round state are processed in a pipelined manner by one instance of the shared S-box. Thus, (due to the register between the F and G functions) 17 clock cycles are required to evaluate the complete substitution layer of the cipher for one round. After the last nibble of the shares has been processed, the outputs are routed according to the linear layer of the cipher and saved into a register again. Therefore, each full computation round of the PRESENT-80 cipher takes 18 clock cycles on the investigated ASIC core.

The initial masking of the input as well as the unmasking of the output are performed on the chip itself. Hence the communication with the ASIC is performed in an unshared, conventional manner. Consequently the power consumption that refers to the I/O activity of the chip depends greatly on the unshared values. The two random 64-bit masks that are needed for the initial sharing process are generated and delivered by a PRNG on the control FPGA, which in turn is seeded by the PC via UART.

IV. Evaluation

In order to provide a meaningful comparison between the dynamic and the static power side channel we perform a vulnerability analysis for each of these power consumption sources separately on the same target chip. It is noteworthy that the ASIC is implemented in 150 nm CMOS technology, which implicates that the static power dissipation of the device is still much smaller than its dynamic power consumption. The consequences of this disparity are discussed at the end of this article. We apply both vulnerability analyses to the target implementation with `PRNG OFF` and with `PRNG ON`. The former one refers hereby to the execution of the PRESENT-80 threshold implementation core with all masks set to zero.

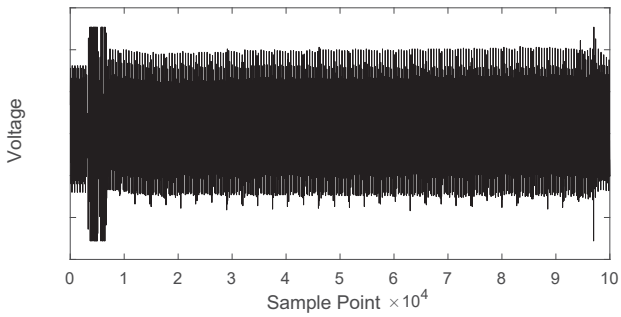


Fig. 3: Sample dynamic power consumption trace over a full PRESENT-80 encryption

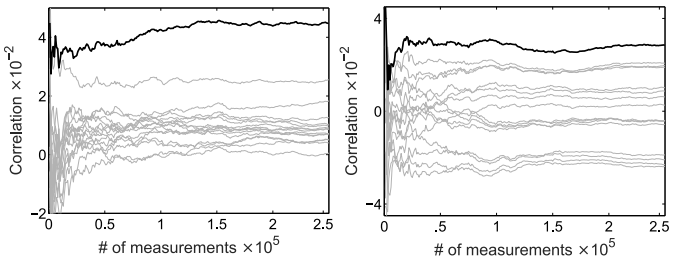
Thus, during the attack we can predict the shared intermediate values that are actually processed by the ASIC and consequently estimate the power consumption precisely. This way, we emulate attacks on an unprotected implementation. `PRNG ON`, on the other hand, means that the threshold implementation is operated as provided for, with randomly generated masks that are unknown to the adversary. Accordingly, in an attack only the unshared intermediate values can be predicted that are not actually processed by the circuit.

A. Dynamic Analysis

The dynamic power measurements were carried out using the sequence mode of the employed oscilloscope to guarantee a maximum time efficiency. Hereby, several consecutive traces are recorded at once between two UART communications of the PC and the control FPGA of the SASEBO-R. The traces have been collected while the target chip was supplied by random plaintexts. Each of those measurements was conducted with a sampling rate of 500 MS/s and 100,000 samples per trace. The ASIC prototype was operated at 3 MHz and the power consumption was measured by means of a 1 Ω resistor in the Vdd path. Further, due to a very low signal amplitude, we employed two $\times 10$ AC amplifiers in series, resulting in a $\times 100$ gain and an almost complete elimination of the DC part of the signal. Fig. 3 depicts a sample trace of the dynamic power consumption which has been recorded over a full execution of the encryption, where 31 rounds can be identified.

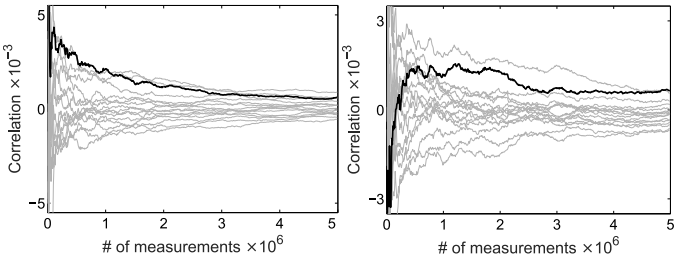
The following analysis targets exclusively the 26th cipher round, because our measurement setup entails the memory effect that is described in [16]. When taking a look at the beginning of the power trace in Fig. 3, it can be observed that the power consumption peaks around the points 3000 to 6000, that refer to the I/O activity of the chip, have a visible impact on the measured power consumption for at least the first three rounds (shifted upwards). This is especially an issue for our target implementation because the I/O communication is performed in an unshared manner and its power consumption depends greatly on the unmasked values. Hence, the 26th cipher round has been chosen arbitrarily as one of the later rounds to make sure that these effects do not influence our measurements. Obviously, the presented analyses are based on evaluation purposes because knowledge of the secret key is required to compute the input of the 26th cipher round.

The result of a Correlation Power Analysis (CPA) attack using the Hamming weight (HW) of the output of the three



(a) CPA (b) MCDPA

Fig. 4: Dynamic power, PRNG OFF, first-order attacks, (a) CPA with HW of the output of the 3 F-boxes, (b) MCDPA



(a) second-order (b) third-order

Fig. 5: Dynamic power, PRNG ON, higher-order MCDPA attacks

F-Boxes (12 bits) targeting one key nibble (4 bits) is presented in Fig. 4a, for the PRNG OFF case. For all attack results we present the correlation coefficients for the most leaking sample point over the number of traces, which allows us to apply the Measurements-to-Disclosure (MTD) metric, introduced in [21], to our comparisons. It can be seen that not more than 8,000 measurements are required to identify the correct key candidate. In contrary, with PRNG ON none of our attempts to conduct a higher-order CPA (by HW model on the F-box output) using 5 million measurements led to a successful key recovery. Therefore, we performed a collision-based Moments-Correlating DPA (MCDPA) [17] to relax the necessity for a precise hypothetical power model and a correct choice of the intermediate value to attack. The result of both, second- and third-order attacks (PRNG ON), can be seen in Fig. 5.

Conducting the same MCDPA with PRNG OFF revealed around 9,000 measurements to be sufficient to identify the correct key difference (due to the underlying collision setting). Whereas, almost the entire 5 million measurements are required for a univariate third-order attack with PRNG ON. Hence, *in our case study* the threshold implementation increases the data complexity of an MCDPA attack on the dynamic power traces by a factor of over 500. As shown by graphics, the second-order attack unexpectedly did not succeed with 5 million traces.

B. Static Analysis

In order to measure the static power consumption of our target chip, we used the procedure that was suggested in [15] and confirmed in [20]. At the specific clock cycle, where the targeted intermediate value is processed, the clock signal is stopped and all other input signals of the ASIC are kept

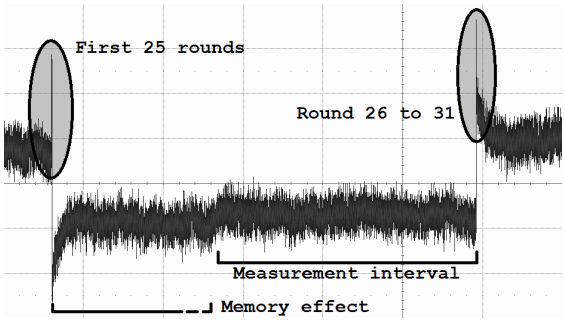
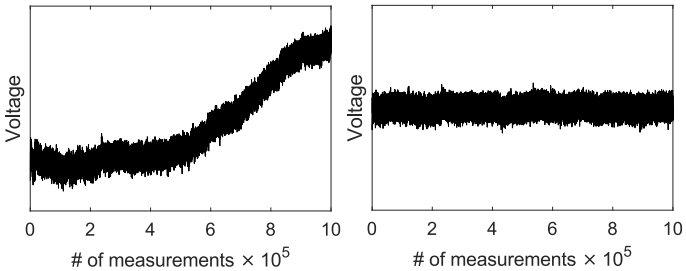


Fig. 6: Static power measurement procedure

constant at a deterministic value. This idle state of the target is held for an arbitrarily long time interval during which the static power consumption of the device can be measured before the clock signal is switched back on. Thus, in our experiments recording the static leakage traces requires a stronger attacker model than that of the dynamic power, as full control over the clock signal is necessary. The power consumption values that are obtained in the mentioned time interval are then averaged to a singular value. Since the leakage currents are not supposed to change during that period, all occurring variations are noise and can be averaged out. This technique is called intra-trace averaging and constitutes one major advantage of static power analysis in comparison to classical attacks when control over the clock signal is obtained (see [20]).

Due to the very high gain of our developed DC amplifier ($\times 1000$) the memory effect that we already observed regarding the dynamic power measurements is even more problematic. The sudden drop of the power consumption when the clock signal is stopped influences the measured static power values for up to the next 20 ms. Hence the first 20 ms of the idle state are disregarded and not included in the measurements. After that period, the actual measurement interval starts. This procedure is illustrated in Fig. 6. Similar to what shown in [20], we observed a clear trade-off between intra-trace averaging and inter-trace averaging. But in contrast to the previous investigations, we actually approached the limits of these noise reduction techniques. When we extended the measurement interval (see Fig. 6) from 10 ms to 500 ms and averaged over 500,000 time samples, the standard deviation of the measured static power values decreased by a factor of over 2.5. This indicates that a significant chunk of noise was still included in the 10 ms traces. We figured out that beyond the 500 ms threshold only minor improvements could be achieved by stretching the time interval even further (2000 ms was the longest interval we investigated). Thus, our 500 ms traces do already contain a very low noise level. Note that we cannot reduce the noise which arises from the leakage currents of other intermediate values by averaging over the time samples (indicated as switching noise in [14]). Hence, the application of inter-trace averaging is still indispensable, regardless of the length of the measurement interval.

Thanks to the fact that we performed the measurements in a climate chamber, (in contrast to [15] and [20]) we did not have to force our device into a deterministic RESET state before each measurement. This already improved the procedure of [15] by a factor of 2 with respect to the required



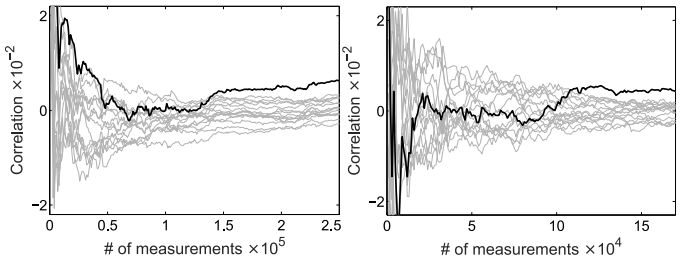
(a) w/o climate chamber (b) w/ climate chamber

Fig. 7: One million static power measurements recorded (a) with an ordinary setup and (b) in a climate chamber.
(a) $\Delta(\text{min, max}) = 35.47$ mV (b) $\Delta(\text{min, max}) = 8.36$ mV

time per measurement. Additionally, it allows us to set the oscilloscope to a much more precise range. These positive impacts of the use of a climate chamber are shown in Fig. 7. One million static leakage values have been acquired using our developed low-noise DC amplifier over a measurement interval of 10 ms. At first, with an ordinary setup in the measurement laboratory that was exposed to temperature variations, and secondly inside a controlled climate chamber. The trace in Fig. 7a shows that the temperature has a huge impact on the static power consumption. For the experiments that led to the trace in Fig. 7b we kept a constant temperature of +21 °C inside the climate chamber to ensure the least amount of interaction from the temperature regulation units. Note that previous research results based on simulated measurements (e.g., in [8]) referred to a temperature of +100 °C to amplify the data dependency of static leakages. We did not evaluate whether higher temperatures improve the static power measurements, for example by increasing the signal-to-noise ratio, but leave this investigation to future works.

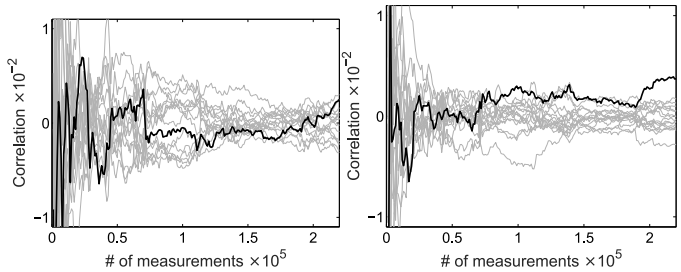
In the following we show that the previously mentioned noise level also has a major impact on the success of attacks. In accordance to the dynamic power analysis we targeted the 26th cipher round and the same key nibbles as before. At first, with `PRNG OFF` we performed a CPA attack using the Hamming weight of the output of the 3 F-boxes. With a measurement interval of 10 ms, the correct key candidate can be revealed after roughly 2 million measurements. By increasing the measurement interval to 500 ms, the same attack requires only 138,000 measurements. This result is depicted in Fig. 8a. However, since the acquisition of the 2 million measurements with the 10 ms interval took around 25 hours, whereas the 138,000 measurements with the 500 ms delay required roughly 39 hours, this does not improve the attack in terms of the required time. In this case, the intra-trace averaging in each single trace is not able to keep up with the inter-trace averaging between the different traces. For the sake of completeness, we have to state here that we used the sequence mode of the underlying oscilloscope for the static power measurements as well, to guarantee a maximum time efficiency and a fair comparison between the two side channels.

Similar to the dynamic power analysis, we performed an MCDPA attack on the static leakages for both cases, `PRNG OFF` and `PRNG ON`. When using the 10 ms traces, slightly more than 2 million measurements were required with `PRNG OFF`. In this settings, i.e., 10 ms interval, the third-order MCDPA attack on the implementation with `PRNG ON` did not succeed with 5 million measurements. When using the noise reduced traces (500 ms interval) we obtained the results that are depicted in Fig. 8b and Fig. 9. For this configuration, the first-order MCDPA attack with `PRNG OFF` required roughly 108,000 measurements, whereas for the third-order zero-offset attack with `PRNG ON` around 193,000 measurements were needed. Based on this observation, we can conclude that *in our case study* the application of the threshold implementation scheme increased the data complexity of the static power analysis only to a small extent, namely by a factor of 1.8.



(a) CPA (b) MCDPA

Fig. 8: Static power, `PRNG OFF`, first-order attacks, (a) CPA with HW of the output of the 3 F-boxes, (b) MCDPA



(a) second-order (b) third-order

Fig. 9: Static power, `PRNG ON`, higher-order MCDPA attacks

Finally we compare all successful attacks on both power consumption side channels by their required amount of traces and the respective acquisition time in Table I. It becomes obvious that for all attacks on the unprotected implementation the static power analysis is not even close to being comparable to a classical vulnerability analysis (best case: 0.02 hours vs. 25.1 hours). In contrary, on the protected implementation the best attack required 4.9 million *dynamic* power traces taken in 11.5 hours, but only 193 thousand *static* power traces collected in 54.7 hours. Hence, we can state that the static power analysis on the one hand is able to reduce the data complexity of higher-order attacks significantly and on the other hand is much less affected by the presence of the underlying algorithmic-level masking. But also that it is still not favorable in terms of time efficiency *in our setup*. It is noteworthy, that (like we expected) none of our attempts – including CPA, DPA, and MCDPA – could exploit first-order leakages either in dynamic or static power measurements with `PRNG ON`.

TABLE I: Comparison between the successful attacks

Channel	Attack	Order	PRNG	Interval	MTD	MTTD*
Dynamic	CPA	1st	OFF	–	8000	0.02 h
Dynamic	MCDPA	1st	OFF	–	9000	0.02 h
Dynamic	MCDPA	3rd	ON	–	4900000	11.5 h
Static	CPA	1st	OFF	10 ms	2000000	25.1 h
Static	MCDPA	1st	OFF	10 ms	2060000	25.8 h
Static	CPA	1st	OFF	500 ms	138000	39.1 h
Static	MCDPA	1st	OFF	500 ms	108000	30.6 h
Static	MCDPA	3rd	ON	500 ms	193000	54.7 h

* Measurement Time to Disclosure

V. Conclusions

In this paper we presented a – hopefully – meaningful comparison between dynamic power and static power side-channel analyses on an ASIC prototype chip. We used a low-noise DC amplifier as well as a powerful climate chamber to adjust our measurement setup specifically to the characteristics of the static power side channel. Throughout our investigations we came to the conclusion that the Measurements-to-Disclosure metric is only a rather relative factor in the static power domain as one can always trade a longer measurement interval, i.e. lower electronic noise, for less traces and the other way around (when control over the clock is obtained). Hence, the time that is consumed by the acquisition of the traces seems to yield a far better metric for comparisons, even though it depends strongly on the measurement setup and the parameters. Generally speaking, the data complexity of the static power analysis is significantly lower than that of corresponding dynamic power analysis attacks, but its time complexity is still higher in our setup. Finally, and very importantly, we have been able to show that noise reduction techniques (i.e., longer measurement interval in static leakage measurements) make masking schemes essentially ineffective against static power analysis.

Our target ASIC is built in 150 nm CMOS, which implicates that the combined leakage currents are still several times smaller than the dynamic power dissipation. For targets that are implemented in CMOS technologies beyond 65 nm, where the static leakage is in the same magnitude as the dynamic power consumption or even dominating, we expect such attacks to bring an actual advantage for attackers (even considering the time complexity and maybe even without clock control). Furthermore, masking schemes are often combined with algorithmic noise addition techniques like shuffling, that highly affect the efficiency of higher-order dynamic power analysis attacks. Based on our investigations and analyses, however, such a combination is expected to not significantly increase the complexity of static power analysis attacks. Thus, for future works implementations equipped with masking countermeasures as well as noise addition techniques in advanced CMOS technology (< 65 nm) should be targeted.

Acknowledgment

The authors would like to acknowledge Axel Poschmann for the hardware designs and Stefan Heyse for his help on taping out the prototype chip. This work is partly supported by the German Research Foundation (DFG) through the project "NaSCA: Nano-Scale Side-Channel Analysis".

References

[1] Analog Devices AD8421 Data Sheet Rev. 0. http://www.analog.com/media/en/technical-documentation/data-sheets/AD8421.pdf.

[2] Analog Devices AD8676 Data Sheet Rev. C. http://www.analog.com/media/en/technical-documentation/data-sheets/AD8676.pdf.

[3] Side-channel Attack Standard Evaluation Board SASEBO-R Specification – Version 1.0. http://www.risec.aist.go.jp/project/sasebo/download/SASEBO-R_Spec_Ver1.0_English.pdf. Research Center for Information Security, National Institute of Advanced Industrial Science and Technology, Japan.

[4] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Trifiletti. Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations. In *Transactions on Circuits and Systems*, volume 61, pages 429–442. IEEE, February 2014.

[5] M. Alioto, S. Bongiovanni, G. Scotti, and A. Trifiletti. Leakage Power Analysis Attacks Against a Bit Slice Implementation of the Serpent Block Cipher. In *MIXDES 2014*, pages 241–246. IEEE, June 2014.

[6] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti. Leakage Power Analysis Attacks: Well-Defined Procedure and First Experimental Results. In *ICM 2009*. IEEE, December 2009.

[7] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti. Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits. In *Transactions on Circuits and Systems*, volume 57, pages 355–367. IEEE, February 2010.

[8] D. Bellizia, G. Scotti, and A. Trifiletti. Implementation of the PRESENT-80 Block Cipher and Analysis of its Vulnerability to Side Channel Attacks Exploiting Static Power. In *MIXDES 2016*, pages 211–216. IEEE, June 2016.

[9] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In *CHES 2007*, volume 4727, pages 450–466. Springer, September 2007.

[10] J. Giorgetti, G. Scotti, A. Simonetti, and A. Trifiletti. Analysis of Data Dependence of Leakage Current in CMOS Cryptographic Hardware. In *GLSVLSI 2007*, pages 78–83. ACM, March 2007.

[11] S. S. Immaculate and K. Manoharan. Analysis of Leakage Power Attacks on DPA Resistant Logic Styles: A Survey. *International Journal of Computer Science Trends and Technology*, pages 136–141, September 2014.

[12] P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *CRYPTO 1999*, LNCS, pages 388–397. Springer, December 1999.

[13] L. Lin and W. Burleson. Leakage-Based Differential Power Analysis (LDPA) on Sub-90nm CMOS Cryptosystems. In *ISCAS 2008*, pages 252–255. IEEE, May 2008.

[14] S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, 2007.

[15] A. Moradi. Side-Channel Leakage through Static Power - Should We Care about in Practice? In *CHES 2014*, volume 8731, pages 562–579. Springer, September 2014.

[16] A. Moradi and O. Mischke. On the Simplicity of Converting Leakages from Multivariate to Univariate – Case Study of a Glitch-Resistant Masking Scheme. In *CHES 2013*, volume 8086, pages 1–20. Springer, August 2013.

[17] A. Moradi and F.-X. Standaert. Moments-Correlating DPA. Cryptology ePrint Archive, Report 2014/409, 2014. http://eprint.iacr.org/.

[18] S. Nikova, V. Rijmen, and M. Schläffer. Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. *Journal of Cryptology*, 24:292–321, April 2011.

[19] A. Poschmann, A. Moradi, K. Khoo, C.-W. Lim, H. Wang, and S. Ling. Side-Channel Resistant Crypto for less than 2300 GE. *Journal of Cryptology*, 24:322–345, April 2011.

[20] S. M. D. Pozo, F.-X. Standaert, D. Kamel, and A. Moradi. Side-Channel Attacks from Static Power: When Should we Care? In *DATE 2015*, pages 145–150. IEEE Computer Society, March 2015.

[21] K. Tiri, D. Hwang, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede. Prototype IC with WDDL and Differential Routing – DPA Resistance Assessment. In *CHES 2005*, volume 3659, pages 354–365. Springer, August 2005.