Amplifying Side Channel Leakage by Hardware Modification of Xilinx Zynq-7 FPGA Evaluation Boards

Nadir Khan[1], Sven Nitzsche[1], Raffaela Frank[1], Lars Bauer[2], Jörg Henkel[2], Jürgen Becker[1, 3]
[1]FZI Research Center for Information Technology Karlsruhe, Germany
[2]Chair for Embedded Systems, Karlsruhe Institute of Technology, Karlsruhe, Germany
[3]Institute for Information Processing Technologies, Karlsruhe Institute of Technology Karlsruhe, Germany
Email: {khan, nitzsche}@fzi.de, mail@raffaela-frank.de, {lars.bauer, henkel, juergen.becker}@kit.edu

Abstract— **The aim of this work is to enhance the side channel information that is revealed by the power consumption of a Field Programmable Gate Array (FPGA). An initial measurement setup is proposed for measuring the signal quality, and then adjustments and modifications to the hardware are done to enhance this quality. Once an acceptable signal is measurable, data is gathered and useful information in this raw data is determined using a standard leakage assessment methodology. The used methodology generates a quantitative score regarding the presence of useful information in the raw data, and can therefore indicate whether a system is vulnerable to side channel attacks or not. In this work, several modifications are presented along with their effect on the captured signal's quality and the amount of useful information in the collected raw data.**

Keywords- FPGA; Side Channel Attack; Test Vector Leakage Assessment; Advanced Encryption Standard; Power Analysis.

I. Introduction

Even though modern key-based encryption algorithms are in theory considered as mathematically secure, this assumption is not valid for their respective implementations. Sophisticated techniques like Side Channel Attacks (SCAs) can take advantage of certain implementation characteristics to reveal secret information of their inner state [1] - pp.180, which then, in turn, can be used to reconstruct the cryptographic key in use [2]. As the name states, this kind of attack is performed on side channels, information channels, which unintentionally disclose internal information of a device. Common side channels are power consumption, execution time, acoustic and ElectroMagnetic (EM) radiation [1] - pp.181. A power analysis attack for example exploits the data-dependent nature of the switching activity of a cryptographic implementation. Since these attacks can be non-invasive and only use information extracted from physical observation, it is difficult to detect them and consequently one cannot be sure if a secret key is already compromised [2].

The most common side channel analysis is power based, which is also the focus of this work. A measurement setup is presented that gathers side channel information leaked from the power consumption of an FPGA board. The board is modified in multiple stages, while collecting data on every stage and conducting analysis on it to evaluate each modification. The evaluation is performed by collecting side channel information of an Advanced Encryption Standard (AES) implementation running on an FPGA and rating it according to its impact. Contrary to other works in this field [3]-[7], this paper focuses on FPGA evaluation boards that have higher similarity with commercially available products, rather than using boards designed for physical security analysis of cryptographic modules, such as SCA Standard Evaluation Board (SASEBO) and SCA User Reference Architecture (SAKURA) board [7]. One example board designed specifically for security analysis is the SAKURA-X, which is equipped with a Xilinx Kintex-7 FPGA for cryptographic circuits and a Spartan-6 as control unit. Usually, the focus of measurement setups based on these boards is the security evaluation of an algorithm's implementation and corresponding countermeasures. Performing side channel attacks on them is considerably easier, which is also a reason why they are not used in practice [7].

This work aims to depict possible obstacles while preparing off-the-shelf FPGA boards for side channel attacks and show how to overcome them. Rather than performing a successful key extraction itself, it should support other researchers at successfully leveraging all available side channel information. The main contributions of this work are:

- a systematic modification approach for a state of the art FPGA evaluation board to enable power-based side channel attacks,
- an improvement of common measurement setups by FPGA board modifications, e.g., replacing resistors and removing capacitors,
- an improvement of common measurement setups by optimizing soft parameters, such as logic frequency,
- quantifying the quality of a measured signal for specific modifications and
- assessing the amount of useful information within captured raw data, once the signal reaches an acceptable level of quality.

The rest of the paper is organized as follows. Section II presents related work. The measurement setup is explained in Section III, while improvements of the setup are presented in Section IV. Section V presents an evaluation of the measurement data. Finally, Section VI provides a conclusion.

II. Related Work

The first published work on SCA goes back to Kocher in 1996, where it was shown that the variation in execution time of an algorithm can leak information [8]. This leakage information can be used to extract secret keys used in the algorithm. SCAs can be classified in several ways; this work will refer to the classification presented by Zhou and Feng in [9], which is based on the following three criteria.

- Control over the computation process: According to this classification, an SCA can be an active attack if the attacker influences the behavior of the system and observes the difference in the operation or information leaked. A passive attack, on the other hand, refers to SCAs where the attacker does not interfere with the operation of the target system. Fault Injection (FI) attacks are an example of the former, while power analysis attacks are of the later type.
- Way of accessing the module: This classification divides SCAs into three different types, namely invasive, semi-invasive and non-invasive attacks [10]. These types refer to the degree of tampering done to the system for acquiring information. Non-invasive, being the lowest degree equals no hardware modification. On the other hand, invasive attack means extensive modification that could include depackaging the Integrated Circuit (IC), capacitor removal or changing resistors.
- Methods used in the analysis process: This third classification is based on the process used to analyze the acquired data. The attack could be characterized as Simple SCA (SSCA) if there is a direct relation between the leakage information and the secret. However, if SSCA is not possible due to high noise, statistical methods can be used to extract the secret. Such attacks will be classified as Differential SCA (DSCA) [9].

Zhou and Feng in [9] also discussed known SCAs, which are timing, fault, power analysis, Electro-Magnetic (EM), acoustic, visible light, error message, frequency-based, cache-based and scan-based attacks. The measurement setup and modifications presented in this work are intended for power analysis. They require some modification to the board and use statistical methods for information analysis, but they do not control the algorithm’s execution. Consequently, our setup can be used for passive semi-invasive differential SCA. The term “differential” in this case should not be confused with Differential Power Analysis (DPA) [13]. In power-based SCAs, Simple Power Analysis (SPA) comes under SSCA, while DPA, Correlational Power Analysis (CPA) [11] and Test Vector Leakage Assessment (TVLA) [17][18] come under the category of DSCA.

SPAs interpret the power consumption measurements directly, which means that the attacker tries to extract a key using one or few traces [12]. In practice, these attacks are not considered a major threat because they require detailed knowledge of the implementation of the cryptographic algorithm. In contrast, DPA does not require detailed knowledge of the target setup and can extract a key even if traces contain noise [12]. A trace is a set of measurement points that are measured during execution of the target algorithm, in this case AES. CPA, introduced by Brier et al. [11] and currently the most commonly used SCA, is based on the estimated correlation between the power traces of a hypothetical model and measured power traces.

In this work, evaluation of the leaked information is done using TVLA [18]. TVLA was first introduced in 2011 in Non-Invasive Attack Testing Workshop [17]. This approach requires execution of a cryptographic algorithm with pre-specified input vectors and then performs statistical tests on the measured power consumption. These tests produce scores, which can clearly show whether a cryptographic algorithm is leaking sensitive information or not. The advantage of performing TVLA analysis is that it is faster by multiple orders of magnitude in comparison to key extraction attacks, such as DPA and CPA. In addition, it is also real-time meaning the test can be performed as the measurement data is being collected. Between the two types of TVLA tests, this work utilizes general TVLA, which compares measurements from a device performing AES on fixed inputs and from a device performing AES on random inputs. According to [18], non-specific tests are most successful in leakage assessment.

For executing a successful attack, authors in [14] showed that removing decoupling capacitors and powering the device from accumulators via linear stabilizers make the environment ideal. They were able to extract the key by analyzing just 5,000 traces. The target device used in this attack was a Spartan 3E Starter Board. Moradi et al. in [16] presented a successful SCA on Virtex 4 and Virtex 5 Xilinx devices by targeting the internal bitstream decryption engine. In addition, a comparison of SASEBO and SAKURA boards, discussed earlier, is presented by Nomata et al. in [6], where it is said that one thousand to two thousand waveforms are required for obtaining all bytes of the key with SASEBO-G, SASEBO-GII and SAKURA-G boards. On SAKURA-X, additional amplification of the waveform is required to extract keys. SASEBO-G comes with a Xilinx Virtex-II, SASEBO-GII with a Xilinx Virtex-5, SAKURA-G with a Xilinx Spartan-6 and SAKURA-X with a Kintex-7 [7]. Our work is different from the rest as we are targeting a comparatively newer FPGA placed on a Xilinx Evaluation Board rather than on a FPGA board designed for side channel analysis specifically.

III. Measurement Setup

A. *Target Cryptographic Algorithm*

In the measurement setup, the target algorithm is a hardware implementation of AES [15] with 128-bit key length. Implementation executes within 13 clock cycles, where the round keys are generated in the first two, and then a round of AES is executed during each clock. The 16 S-boxes of the Byte Substitution (BS) Layer are implemented as lookup tables and are executed in parallel in one clock that should make the attack harder in comparison to an implementation that executes one S-box per clock. AES is packaged in the Advanced Extensible Interface (AXI) and communication between AXI-wrapped AES on the FPGA and host computer is realized via a JTAG-to-AXI interface.

B. *Basics of Power Analysis*

The power consumption of FPGAs, as with all integrated circuits, is divided into dynamic and static power. Dynamic Power Consumption (DPC) is caused by changes of signal values, while static power is always present even when no signal transitions occurs [24]. DPC can be correlated with specific bits [1] - pp. 300. At a fixed point in time, an output signal of a Complementary Metal-Oxide-Semiconductor (CMOS) cell can perform one of four transitions [12] - pp. 29. The transitions 0→0 (P_{00}) and 1→1 (P_{11}) cause only static power consumption, while 0→1 (P_{01}) and 1→0 (P_{10}) consume both static and dynamic power. The exact values of P_{00}, P_{01}, P_{10} and P_{11} depend on the cell type and process technology, but generally $P_{00} \approx P_{11} << P_{01}, P_{10}$. In addition, they depend on the data being processed [12] – pp. 29.

Since registers in digital circuits are typically synchronized by a clock signal, a current flow is caused by the simultaneous switching of the logic cells at each rising edge of the clock. This current flow or the respective voltage drop can be measured using a digital oscilloscope and thus electrical signals can be recorded over a certain period. To measure characteristics such as power or current with an oscilloscope, it is necessary to generate a voltage signal that is proportional to these characteristics. In a measurement setup for power analysis attacks, there are two common ways for SCAs to generate a voltage signal that is proportional to the power consumption of the cryptographic device. It can either be generated by placing a small measurement resistor between negative (V_{SS}) or positive supply voltage (V_{DD}) of the device and the source or ground. The current flowing through this resistor causes a voltage that can then be measured.

The structure of all hardware components for doing so and their communication is shown in Figure 1. An AES implementation on the FPGA is triggered to encrypt multiple plaintexts while the attached oscilloscope measures the consumed power and transfers all captured data to a host machine.

The target device is a Xilinx Zynq-7000 All Programmable SoC ZC702 Evaluation Kit v1. This board contains a Zynq-7000 XC7Z020-1CLG484C with 85,000 logic cells.

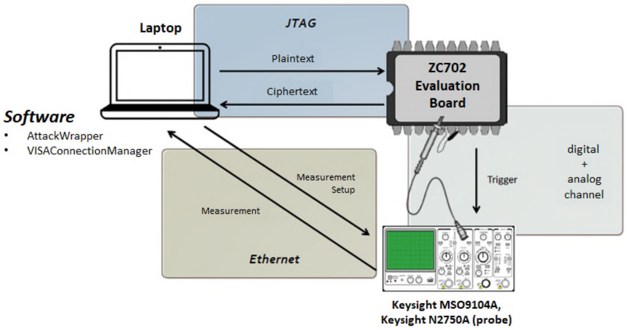

Figure 1. Measurement Setup

The Zynq-7000 series integrates an ARM Cortex-A9 based processor and a 28nm programming logic (PL). The evaluation board includes Low Pin Count - FPGA Mezzanine Card (FMC) connections to attach an FMC debug board. This is used to connect the digital channels of the oscilloscope.

Additionally, the board has three power controllers, each managing several switching regulators. The power controllers are PMBus-compliant system controllers from Texas Instruments. This allows the voltage and current levels to be set [25]. Every controller monitors different voltages. One is responsible for the core voltages, one for the auxiliary voltages and the third for the 3.3 V and 2.5 V supply voltages. The core voltage includes V_{CCINT} and V_{CCPINT} among others. V_{CCINT} is the 1V internal supply voltage for the PL [26] and therefore the target voltage for power analysis attacks on the PL. The evaluation board by default contains a $5m\Omega$ measurement resistor connected to a voltage amplifier that can be used for this purpose.

A Keysight MSO9104A oscilloscope with a resolution of 8 bits, a bandwidth of 1GHz and up to 20 GS/s sampling rate is used to perform the actual measurement. The settings of this oscilloscope are adjusted to match the target AES algorithm. The horizontal resolution is set to equal the period of one full AES round. For vertical resolution, the entire vertical range of the oscilloscope is used. The signal is sampled with a Keysight N2750A active differential probe with 1.5 GHz bandwidth. The tip of the probe is soldered to the corresponding measuring point on the board.

Test data in form of plaintexts is generated according to the TVLA specifications and sent to an AES core implementation on the programmable logic, utilizing a 128-bit symmetric key. A measurement is started at the beginning of every first AES round and all results are transferred back as raw data using Ethernet. Each measurement consists of an averaging of the same plaintext, which is performed directly on the oscilloscope. Figure 2 shows the resulting measurement plot.

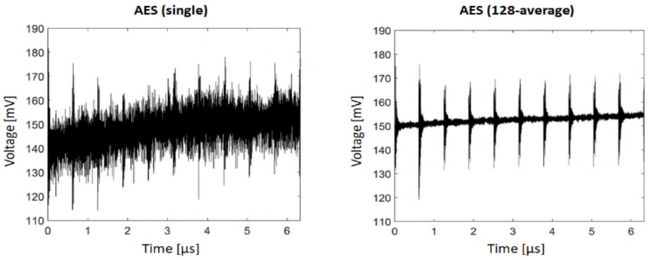

Figure 2. Measured voltage signal using the original setup for a single AES run (left) and an average of 128 AES runs (right) respectively.

IV. Improving the Measurement Setup

In order to perform a power analysis attack, the captured data needs to meet certain quality standards. Data quality can be compared using peak-to-peak voltage (V_{P2P}) during execution of AES encryption, which should be at least 3mV according to related measurements on a SAKURA-X board [6] in order to allow successful power analysis attacks. The initial measurement, shown in Figure 2, shows ten peaks corresponding to the ten AES rounds performed. The signal quality is not sufficient to isolate intermediate computations like S-Box calculation, which are typically needed for differential power analysis, therefore no V_{P2P} can be calculated.

In order to improve data quality, multiple changes are possible. First, the internal measuring resistor can be replaced to generate a higher voltage drop and therefore a stronger signal. Secondly, the supply voltage V_{CCINT} can be stabilized by using an external power source to eliminate unrelated fluctuations [21]. Finally, fluctuations related to the actual AES execution can be amplified by removing capacitors from the board. The descriptions and results of the individual steps are discussed in the following sections.

A. Replacement of the Internal Measuring Resistor

As explained before, a measuring resistor is needed to generate an observable signal, where the exact resistance has to be chosen in a prudent manner. A higher value means higher voltage fluctuation, which is easier to measure [21]. However, the voltage drop across the resistor reduces the voltage that arrives at the cryptographic circuit. This in turn results in a lower power consumption of the cryptographic device, making it harder to measure. Therefore, a suitable trade-off has to be found for the resistance. Due to the very low resistance of the internal resistor, the resulting voltage drop is comparably low; consequently, it should be replaced. Based on experiments with other boards [19] [20], a 0.1Ω and a 1Ω resistor respectively is evaluated for best results. The plotted data is shown in Figure 3 and Figure 4. Even though the single AES rounds are still not visible using higher resistance, the V_{P2P} amplitude increased to roughly 1mV (0.1 Ω) or 1.5mV (1 Ω). Since the 1 Ω resistor yields better results it will be used in all subsequent experiments.

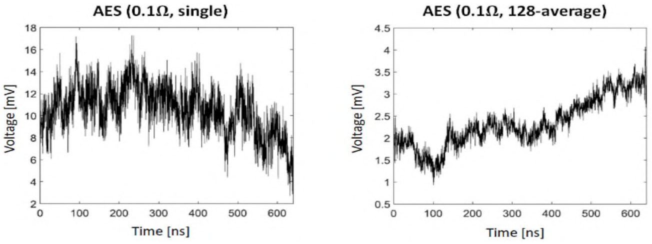

Figure 3. Measured voltage signal using a 0.1 Ω for a single AES run (left) and an average of 128 AES runs (right) respectively.

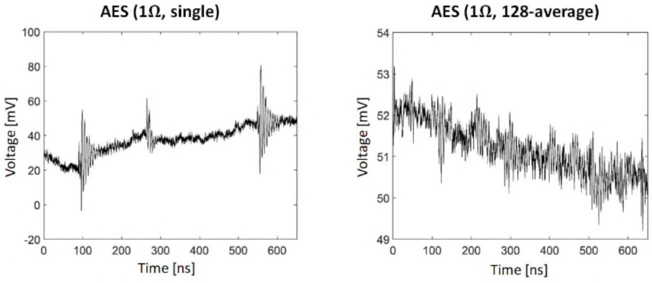

Figure 4. Measured voltage signal using a 1 Ω for a single AES run (left) and an average of 128 AES runs (right) respectively.

B. External Power Supply

Using an external power supply can further improve measurement quality by reducing noise on the voltage line, i.e., V_{CCINT} and V_{CCPINT} [22] – pp. 6. Therefore, an Agilent 66319D Power Supply Unit (PSU) is used to power the programmable logic instead of the internal power supply. This, however, interrupts the FPGA's power-on sequence; hence, it must be taken care of manually. For the programming logic, the required power-on sequence is $V_{CCINT} \rightarrow V_{CCBRAM} \rightarrow V_{CCAUX} \rightarrow V_{CCO}$, meaning the PSU has to be switched on before the FPGA board. The switch-off sequence consequently is in reverse order [26]. This change results in a voltage amplitude of up to 2.3mV, as can be seen in Figure 5 (right). Moreover, this time the single S-Box calculations are visible in the signal.

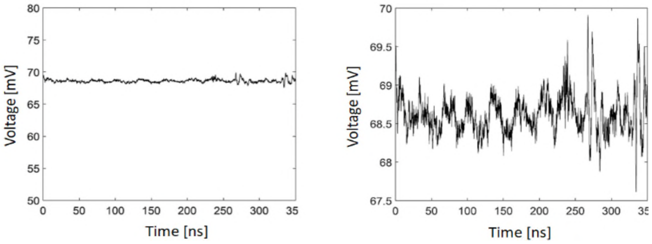

Figure 5. Average measured voltage signal using an external power supply for 128 AES runs (left) and detailed zoom of the signal (right).

C. Removing Capacitors

As can be seen in Figure 5 (left), the voltage signal is almost constant on a larger scale. This is due to multiple capacitors between V_{CCINT} and GND, which effectively prevent the power consumption from fluctuating – they smooth the signal. This causes a masking of the required power information and thus prevents power analysis attacks [23][28]. TABLE 1 provides an overview of all relevant capacitors named according to device schematic.

TABLE 1. CAPACITORS BETWEEN V_{CCINT} AND FPGA

Label	Capacity	Removed	Label	Capacity	Removed
C306	330μF		C237	4.7μF	✓
C167	100μF		C356	0.47μF	✓
C168	100μF		C357	0.47μF	✓
C169	100μF	✓	C358	0.47μF	✓
C139	47μF	✓	C359	0.47μF	✓
C233	4.7μF	✓	C360	0.47μF	✓
C234	4.7μF	✓	C361	0.47μF	✓
C235	4.7μF	✓	C362	0.47μF	✓
C236	4.7μF	✓			

To overcome this limitation, capacitors are removed if possible. Some are necessary to ensure correct operation of the FPGA. Again, the voltage is measured and plotted in Figure 6. Compared to Figure 5 the individual AES rounds are visible now. The V_{P2P} signal amplitude increases to 3mV.

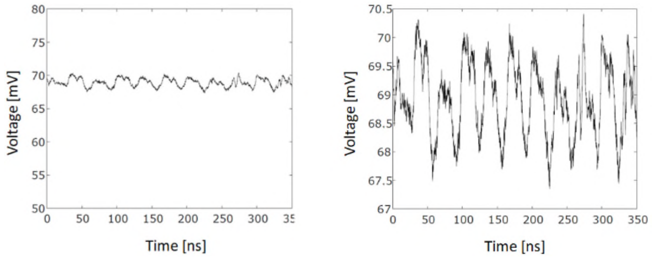

Figure 6. Average measured voltage signal using an external power supply for 128 AES runs (left) and detailed zoom of the signal (right).

D. *Reducing AES Clock Frequency*

High clock frequencies can cause the power consumption signals to overlap in successive clock cycles, resulting in noise in the measured data [12] - pp. 58. Quality of the measured traces can therefore be further improved by lowering the clock frequency of the cryptographic algorithm. Consequently, the clock frequency is reduced from 30MHz to 3.125MHz. In order to keep the scenario as realistic as possible [6][12] - pp. 58 and [1] - pp.296, the frequency is not lowered further. Average results for 128 measurement are shown in Figure 7 next to the result for a frequency of 30MHz as comparison. The signal amplitude is clearly increased, now ranging up to 4.3mV.

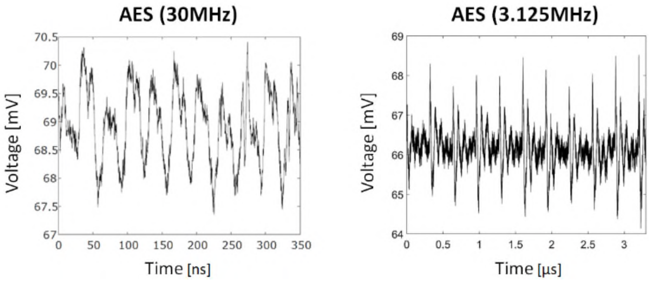

Figure 7. Average measured voltage using a frequency of 3.125 MHz for a 128AES runs (right). Results with f=30MHz for comparison (left).

This section concludes here with TABLE 2, showing results after each modification. The final value of 3.16mV shows that the quality of the captured signal is high and is comparable to the P2P value of 3mV reported in [6] using SAKURA-X Board.

TABLE 2. P2P VOLTAGE SUMMARY OF ALL MODIFICATION

Steps	P2P Voltage (mV)	P2P Moving Average[1] (mV)
R = 5mΩ, f = 30MHz	N/A	N/A
R = 100mΩ, f = 30MHz	1.01	0.66
R = 1Ω, f = 30MHz	1.57	0.95
R = 1Ω, f = 30MHz, External power supply	2.32	0.74
R = 1Ω, f = 30MHz, External power supply, Capacitors removed	3.14	1.90
R = 1Ω, f = 3.125MHz, External power supply, Capacitors removed	4.37	3.16

[1] n = 50.

V. Evaluation of side channel information

Until now, the paper presented several modifications and their effect on the quality of a captured signal. In this section, we will evaluate how much information is leaked by the cryptographic module after each modification.

For this, a general TVLA test is performed, which is conducted on two different sets of plaintext, i.e., random and fixed [17]. Encryption is performed on the random as well as on the fixed plaintext with the same key, and the measurement data is randomized for eliminating time dependent distortions. According to [17], if the test score is higher than 4.5 or lower than -4.5, the test is failed meaning the device is leaking enough information for a successful attack.

A. *External Power Supply and 1Ω Measuring Resistor*

Measurement data from the setup with 1Ω measuring resistor and external power supply is used to conduct a first general TVLA test. For fixed and for random input, n traces are collected. Two independent t-tests are performed; one by comparing the first half of traces from both data sets and another using the second half.

As shown in Figure 8, the maximum values of the first t-test after about 20,000 traces are briefly above the threshold of 4.5. However, because the values of the second t-test are below the limit, the test is passed. General TVLA is then applied to all measurements that is 60,000 random and 60,000 fixed inputs, which results in maximum t-value of 6.49.

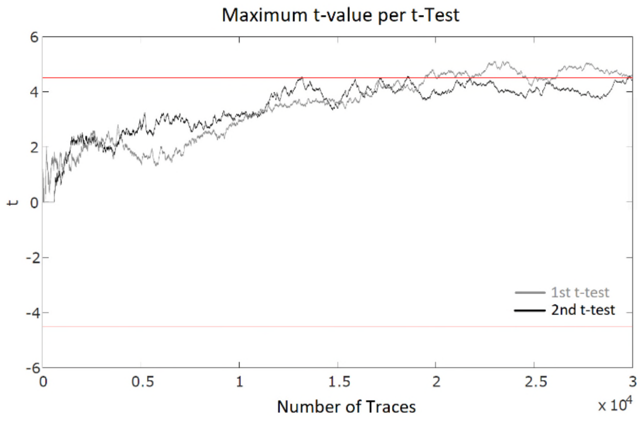

Figure 8. General TVLA test with external power supply

B. *Removing Capacitors*

Measurement data from the setup with external power supply, replaced internal resistor and removed capacitors is analyzed with TVLA as well. The test score crossed the value of 4.5 after 2,373 TVLA traces and stayed above that threshold afterwards, as can be seen in Figure 9. This corresponds to the calculation of t-tests for 9,492 measured traces (one TVLA trace is composed of four measured traces). When the test is applied to all 120,000 traces, a maximum test score of 28.45 results.

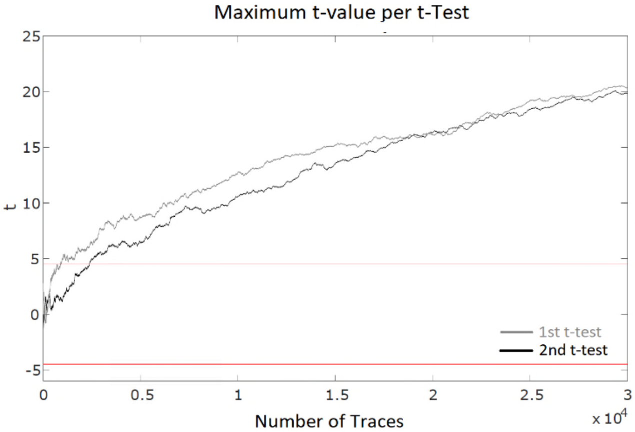

Figure 9. General TVLA test after removing the capacitors.

C. Reduced Clock Frequency and Vertical Resolution

Two more parameters, namely AES clock frequency and vertical resolution, are adjusted in order to get a better TVLA score. TVLA is applied on the measurement data while reducing clock frequency to 3.125MHz and setting the vertical limit to 5.9mV/div including all the previous modifications. This results in a maximum t-value of 14.23, which is lower than the 28.45 with a clock frequency of 30MHz and 5.9mV/div vertical resolution. However, when the vertical resolution is adjusted to 2.3mV/div using Zone Trigger [29][30], a maximum t-value of 60.58 is achieved which can be seen in Figure 10. This is the highest t-value reached by any modification presented in this paper.

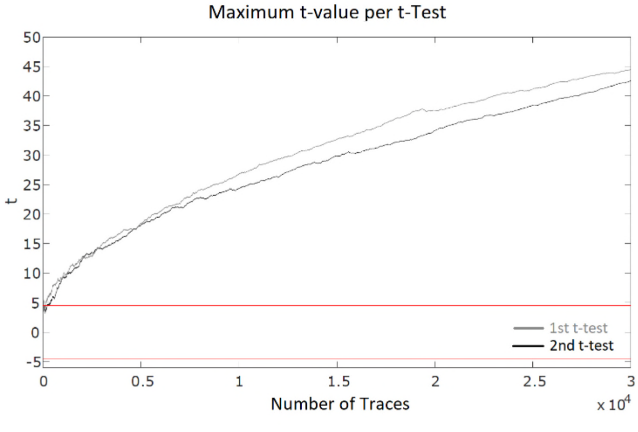

Figure 10. General TVLA test with external power supply, removed capacitors, 3.125MHz frequency.

The maximum t-values for all the modifications are summarized in TABLE 3. The t-value achieved with the final measurement setup is 60.58, which is comparably lower than 190 achieved on a SAKURA-G Board. However, the higher value could be attributed to the 65nm technology node of the Xilinx Virtex-5 used on the SASEBO-GII board [7][17].

TABLE 3. MAXIMUM T-VALUE SUMMARY FOR ALL MODIFICATIONS

Modification	**Resistor** (Ω)	**Frequency (MHz)**	**Vertical Resolution** (mV/div)	**Max. T-Value**
Ext. Power Supply	1	30	5.9	6.49
Ext. Power Supply and Cap. Removed	1	30	5.9	28.45
	1	3.125	5.9	14.23
Ext. Power Supply, Cap. Removed and Zone Trigger [29] for Vertical Resolution adjustment	1	3.125	2.3	60.58

VI. CONCLUSION

This work presents steps to implement a measurement setup that can capture leakage information. The target hardware, a commercial off-the-shelf board, is modified iteratively and the parameters of the setup are adjusted to acquire a higher quality signal for post processing. To compare the quality of the signal, the peak-to-peak amplitude is used. The resulting peak-to-peak voltage is 3.16mV, which is comparable to SAKURA-X Board's P2P value that is approx. 3mV. Once an acceptable quality of signal is achieved, measurement data is gathered, which is then put through a methodology to check whether the data contains useful information or not. For this purpose, Test Vector Leakage Assessment is used. The result of each modification and adjustment is shown for both cases, i.e., signal quality and leakage information. However, results of the general TVLA test show a relatively low t-value (60.58) in comparison to a SASEBO-GII board, which could be attributed to the smaller 28nm node of the device under target. The setup could be further tweaked to increase the t-value if necessary, though the current t-value already suggests that the platform is vulnerable to power analysis attacks.

ACKNOWLEDGEMENT

This work was supported by the German Federal Ministry of Education and Research (BMBF) with funding number 16KIS0610.

REFERENCES

[1] D. Mukhopadhyay and R. Subhra Chakraborty, “Hardware security: Design, threats, and safeguards,” 1^{st} edition, CRC Press Taylor & Francis Group, 2015.

[2] S. A. Huss and O. Stein, “A Novel Design Flow for a Security-Driven Synthesis of Side-Channel Hardened Cryptographic Modules,” Journal of Low Power Electronics and Applications, vol. 7, issue 1, pp. 1-3, 2017.

[3] P. Sasdrich and T. Güneysu, "A grain in the silicon: SCA-protected AES in less than 30 slices," Application-specific Systems Architectures and Processors (ASAP) 2016 IEEE 27th International Conference on, pp. 25-32, 2016.

[4] M. Matsubayashi and A. Satoh, "Side-channel Attack user reference architecture board SAKURA-W for security evaluation of IC card," Consumer Electronics (GCCE) 2015 IEEE 4th Global Conference on, pp. 565-569, 2015.

[5] P. Sasdrich, A Moradi, O. Mischke, and T. Güneysu, "Achieving side-channel protection with dynamic logic reconfiguration on modern FPGAs," Hardware Oriented Security and Trust (HOST) 2015 IEEE International Symposium on, pp. 130-136, 2015.

[6] Y. Nomata, M. Matsubayashi, K. Sawada and A. Satoh, "Comparison of side-channel attack on cryptographic ciruicts between old and new technology FPGAs," 2016 IEEE 5th Global Conference on Consumer Electronics, Kyoto, pp. 1-4, 2016.

[7] SAKURA Hardware Security Project. [Online]. Available: http://satoh.cs.uec.ac.jp/SAKURA/hardware.html [Accessed: 09, 2019].

[8] P. Kocher, "Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems," CRYPTO 1996, LNCS 1109, pp.104-113, 1996.

[9] Y. Zhou and D. Feng, "Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing," IACR Cryptology ePrint Archivet, 2005.

[10] R. Anderson, M. Bond, J. Clulow, and S. Skorobogatov, "Cryptographic Processors-A Survey," in Proceedings of the IEEE, vol. 94, no. 2, pp. 357-369, Feb. 2006.

[11] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," Proc. of CHES'04, pp. 16-29, 2004.

[12] S. Mangard, E. Oswald, and T. Popp, "Power analysis attacks: Revealing the secrets of smart cards," Springer Science & Business Media, pp 29, 45, 56-58, 2007.

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proc. of CRYPTO'99, pp. 388-397, 1999.

[14] L. Mazur and M. Novotný, "Differential power analysis on FPGA board: Boundaries of success," 2017 6th Mediterranean Conference on Embedded Computing (MECO), Bar, pp.1-4, 2017.

[15] J. Daemen and V. Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard," Springer Science & Business Media, 2002.

[16] A. Moradi, M. Kasper, and C Paar, "On the Portability of Side-Channel Attacks – An Analysis of the Xilinx Virtex 4, Virtex 5, and Spartan 6 Bitstream Encryption Mechanism," 2011.

[17] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi, "A testing methodology for side-channel resistance," Non-Invasive Attack Testing Workshop (NIAT) 2011. [Online]. Available: https://csrc.nist.gov/CSRC/media/Events/Non-Invasive-Attack-Testing-Workshop/documents/08_Goodwill.pdf [Accessed: 09, 2019].

[18] G. Becker et al., "Test vector leakage assessment (TVLA) methodology in practice," International Cryptographic Module Conference, 2013. [Online]. Available: https://pdfs.semanticscholar.org/97b6/be2eaeebe1e13696e928e94f66b4c93719b8.pdf?_ga=2.4850867.1045323827.1568296811-418108430.1560420660 [Accessed: 09, 2019].

[19] A. Moradi, "Advances in side-channel security," Ruhr-Universität Bochum, Habilitation, 2014.

[20] N. E. Mrabet, G. Di Natale, and M. L. Flottes, "A practical Differential Power Analysis attack against the Miller algorithm," 2009 Ph.D. Research in Microelectronics and Electronics, Cork, pp. 308-311, 2009.

[21] R. Velegalati and P. Yalla, "Differential power analysis attack on FPGA implementation of AES," ECE 746 Statistical Signal Processing (2008).

[22] M. Aigner and E. Oswald, "Power analysis tutorial," 2000. [online]. Available: https://pdfs.semanticscholar.org/5ad9/fe2c8936052e9ac2a71833caa96a119218d1.pdf?_ga=2.7543858.1045323827.1568296811-418108430.1560420660 [Accessed: 09, 2019].

[23] A. Moradi, M. Kasper, and C. Paar, "Black-box side channel attacks highlight the importance of countermeasures," Topics in Cryptology CT-RSA 2012, pp. 7, 2012.

[24] I. Kuon, R. Tessier, and J. Rose, "FPGA architecture: Survey and challenges," Foundations and Trends in Electronic Design Automation, vol. 2, issue. 2, pp 162, 2008.

[25] Xilinx: ZC702 Evaluation Board for the Zynq-7000 XC7Z020 All Programmable SoC - User Guide - UG850 (v1.5). pp 58, 2015.

[26] Xilinx: Zynq-7000 All Programmable SoC (Z-7007S, Z-7012S, Z-7014S, Z-7010, Z-7015, and Z-7020): DC and AC Switching Characteristics. In: Xilinx, DS187 (v1.20), pp 2-8, 2017.

[27] M. Masoomi, M. Masoumi, and M. Ahmadian, "A practical differential power analysis attack against an FPGA implementation of AES cryptosystem," 2010 International Conference on Information Society, London, pp. 308-312, 2010.

[28] Song Sun, Zijun Yan and J. Zambreno, "Experiments in attacking FPGA-based embedded systems using differential power analysis," 2008 IEEE International Conference on Electro/Information Technology, Ames, IA, pp. 7-12, 2008.

[29] Keysight Oscilloscope Triggering. [Online]. https://www.rs-online.com/designspark/triggering [Accessed: 09, 2019]

[30] 5 Questions about Oscilloscope Zone Triggering. [Online]. https://www.electronicdesign.com/test-measurement/5-questions-about-oscilloscope-zone-triggering [Accessed: 09, 2019]

ISBN: 978-1-61208-746-7