Strengths and Limitations of High-Resolution Electromagnetic Field Measurements for Side-Channel Analysis

Johann Heyszl[1], Dominik Merli[1],
Benedikt Heinz[1], Fabrizio De Santis[2], and Georg Sigl[2]

[1] Fraunhofer Research Institution AISEC, Munich, Germany
{johann.heyszl,dominik.merli,benedikt.heinz}@aisec.fraunhofer.de
[2] Technische Universität München, Munich, Germany
{desantis,sigl}@tum.de

Abstract. The electromagnetic field as a side-channel of cryptographic devices has been linked to several advantages in past contributions. We provide a comprehensive study using high-resolution horizontal and vertical magnetic field probes at close distance to an integrated circuit die. We configured an FPGA device with two uncorrelated digital structures showing similar leakage behavior as symmetric cryptography implementations. We found that measurements from the frontside of the die using a horizontal probe lead to the highest signal-to-noise ratios. Further, high sampling rates are required and no trace compression should be applied. Contrary to previous contributions, we successfully demonstrate that the leakage of design parts is locally restricted and matches their placement. This proves the feasibility of localized side-channel analysis after a profiling phase, however, also means that other locations will lead to inferior results, which is an important limitation. Our analysis confirmed an advantage of measuring localized electromagnetic fields instead of current consumption due to the fact that less parasitic capacitances are involved.

Keywords: EM, high-resolution, side-channel, localization, CPA, SNR

1 Introduction

The past years have seen many publications describing the use of the Electro-Magnetic (EM) side-channel, mostly the magnetic near-field, and cartography thereof [10] to find locations where side-channel analyses lead to the best results [5,12,11]. The magnetic field is vectored and measured using coil sensors. Different coil angles capture different parts of the fields. Agrawal et al. [1] as well as by Standaert and Archambeau [13] provide evidence for this in the context of side-channel analysis. Gandolfi et al. [4] state that inductive probes with high spatial resolutions can be used to locally restrict measurements to specific circuit parts if they are placed close to the surface of an integrated circuit. A variety of magnetic probes have been used in past contributions. Large, hand-crafted ones are used

by Mulder et al. [3] for global measurements of a chip. Peeters et al. [9] use a custom designed probe with a coil diameter of 0.7 mm at a fixed position and close distance to an integrated circuit after partly removal of the package. Sauvage et al. [12] use laboratory equipment with a coil diameter of 0.5 mm outside the chip's package. As a conclusion, they state that observed areas of signal leakage do not coincide with the placement of the leaking design parts on the floorplan of the FPGA. We suggest that the measurement equipment and distance to the die surface have been insufficient leading to mainly observing the magnetic field of bonding wires. Kirschbaum and Schmidt [7] present evidence for successfully localizing EM leakage and performed cartographic measurements. However, they use a hand-crafted coil with 0.5 mm diameter, which has a comparably coarse resolution in our opinion. Heyszl et al. [6] use a high-resolution probe and show that the information leakage significantly depends on the measurement location. They provide first results, however, clear evidence for the feasibility of localizing leakage of circuit parts is lacking.

We fill this gap by performing a comprehensive study of the electromagnetic near-field side-channel using high-resolution measurement equipment at close distance to a decapsulated integrated circuit die. We employ magnetic probes with horizontal, and vertical coils and discuss important parameters of the measurement setup. We analyze a design-under-test configured into an FPGA consisting of a register with a loop feedback through the AES substitution function. Therefore, our results allow conclusions about the side-channel analysis of symmetric cryptography implementations. We conclude, that measurements from the frontside of an integrated circuit using a horizontal probe lead to the highest signal-to-noise ratios. Further we argue, that high sampling rates are required and no trace compression should be applied. Hence, as a main contribution, we clearly demonstrate the feasibility of matching localized electromagnetic fields with placed design parts. This proves the feasibility of restricting side-channel analysis to parts of a design after finding the correct positions through profiling. However, this also demonstrates that incorrect positioning of high-resolution equipment leads to inferior signal-to-noise-ratios. We compared the achieved signal-to-noise ratios against results that we derived from analyzing conventional current consumption measurements. Leakage signals in the EM field are observed within short times after the active clock edge, making local EM measurements favorable for analyzing devices with high clock frequencies since less parasitic capacitances influence the observation.

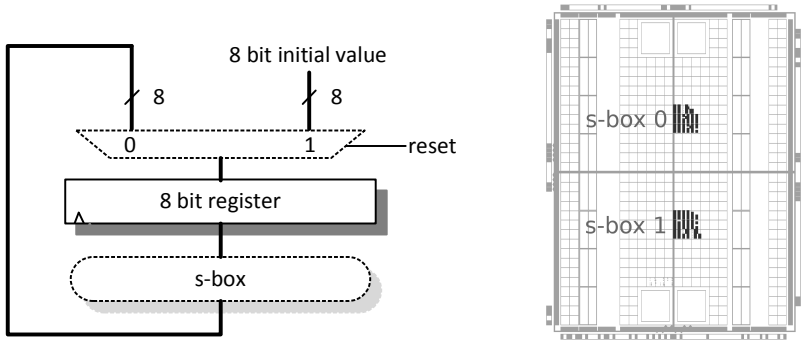
We describe the equipment, design and analysis method in Sect. 2. In Sect. 3, we present and discuss our measurement results and derive conclusions which are summarized in Sect. 4.

2 Practical Study

In this section, we present our device-under-test, measurement equipment and analysis methods.

2.1 Device-Under-Test

We use a *Xilinx Spartan 3A XC3S200A* FPGA in a *VQ100* package, as device-under-test. The device is manufactured in a 90 nm technology, uses a 1.2 V supply for the internal logic, and the die measures $4100 \times 4300\,\mu m$. To perform semi-invasive measurements close to the surface of the chip, we decapsulated the FPGA from the front-, and backside using fuming nitric acid, i.e., with a concentration of $> 95\%$.



(a) S-box-structure (b) Placement

Fig. 1. Design-under-test

The FPGA is configured with a hardware design-under-test. We use a specific, simple design to simplify the acquisition of measurements, while being able to draw meaningful conclusions about the side-channel leakage of cryptographic designs. This design is depicted in Fig. 1(a) and contains a feedback loop structure including an 8-bit register and an implementation of the AES substitution function, s-box, as published by Canright [2]. The 8-bit register is loaded with a fixed initial value at synchronous reset and updates the register with the value's s-box-substitution in every cycle. Therefore, every clock cycle contains a value update, i.e. Hamming distance. The design always performs the same operation. Hence, there are no operation-dependencies and the design serves to analyze data-dependent side-channel leakage. This is according to implementations of symmetric cryptographic algorithms which are primarily subject to differential side-channel attacks relying exclusively on data-dependent leakage. According to our opinion, this structure exhibits similar side-channel behavior as implementations of the AES algorithm, because the same non-linear function is used and the amount of combinational logic is representative for such implementations.

To analyze localized aspects of the electromagnetic side-channel leakage, we use two instantiations of this register-s-box structure. We used constraints to place the s-box structures 0 and 1 on the FPGA at a certain distance and to restrict both structures to the same area. The placement on the floorplan of the *Xilinx Spartan 3A* FPGA is depicted in Fig. 1(b). Since both structures are active

at the same time, they consume power at the same time and contribute to the electromagnetic field jointly. To analyze the contributions of the two structures separately, they need to be statistically independent. The two instantiations use different initial values for their feedback loop. If values from a limited space are repeatedly replaced by a substitution function projecting into the same space, the initial values are eventually derived since the number space is limited. The number of substitutions, thus, length of the sequence of values depends on the number space, substitution function and the generating initial value. We achieve an independence, or de-correlation of both structures by using sequences with different initial values and different lengths for both structures. Hence, the offset between the two sequences is different for every repetition of either one. *The s-box structure with index* 0 *has an initial value of* `0x1d`*, resulting in a sequence length of* 87*. The s-box structure with index* 1 *has an initial value of* `0x09`*, resulting in a sequence length of* 81. Obviously, neither of the two sequences contains values from the respective other sequence. The design additionally includes a 16-bit counter to generate an external trigger for the oscilloscope and synchronously reset both structures. Every measurement contains 2^{16} consecutive clock cycles, thus, 753 repetitions of the sequence with length 87 and 809 repetitions of the sequence with length 81.

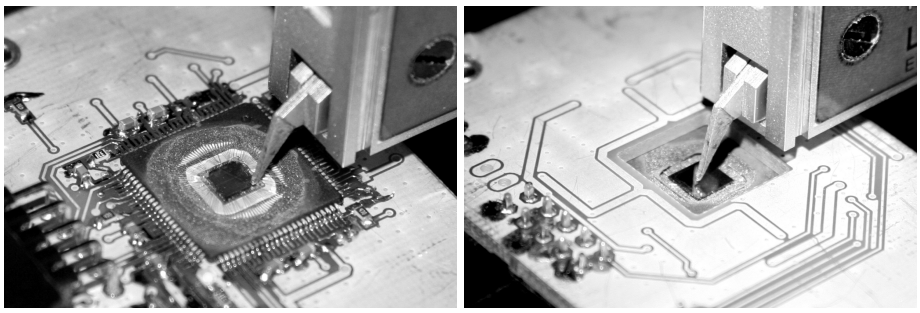
2.2 Measurement Setup

Magnetic fields are vector-fields and magnetic coils only capture components which are orthogonal to the coil. It is not obvious which probe, or which coil direction leads to the best results for side-channel analysis. We used the following magnetic probes to measure the magnetic near-field:

1. Magnetic field probe with 150 µm shielded horizontal coil, 6 windings, 100 µm resolution, and 2.5 MHz – 6 GHz frequency span.
2. Magnetic field probe with 150 µm shielded vertical coil, 6 windings, 80 µm resolution, and 2.5 MHz – 6 GHz frequency span.

The horizontal coil probe will measure the vertical components of the superposed magnetic field generated by the circuit. The vertical probe will record horizontal magnetic field components and provides a choice of direction of the probe. We limited our analysis to x- and y-directions since conductors in integrated circuits are limited in these directions due to manufacturing stability reasons. We also took measurements using a high-resolution electric field probe. *However, the measurements did not reveal any detectable signals, thus, we conclude that this probe is unsuitable for side-channel analysis.* The reason might be that the electric field is shielded by the conductors within the circuit. Ferromagnetic conductors within an integrated circuit also influence magnetic fields, however, our results indicate that the field is still detectable with high SNRs.

We moved the probes over the front- and backside surface of the FPGA die using a stepping table at a resolution of 100 µm and recorded one measurement at every position. The backside measurement is depicted in Fig. 2(b). The probe



(a) Frontside (b) Backside

Fig. 2. Probe positioned and moved over the surface of the FPGA die

touches the surface of the circuit and we recorded 43×41 measurements. The frontside measurement is depicted in Fig. 2(a). To prevent damaging probe and die, the probe to surface distance is $\approx 50\,\mu m$. The bonding wires prevent measurements over the complete surface and we recorded 27×27 measurements in the area enclosed by the bonding wires.

All probes contain a built-in 30 dB amplifier with a noise figure of 4.5 dB. Additionally, we use a 30 dB amplifier with a bandwidth of 3 GHz and noise figure of 4.5 dB. Our *LeCroy WavePro 715Zi* oscilloscope has an analog input bandwidth of 1.5 GHz at $50\,\Omega$ impedance. As an approximate upper boundary for the sampling rate, twice the bandwidth of the equipment, thus, 5 GS/s seems reasonable. We used a zero offset for all measurements and a vertical resolution of 50 mV/DIV and confirmed that all measurements stay within scale. The noise contribution from the measurement setup, i.e., the probes, the two amplifiers, and the oscilloscope was determined by turning of the clock and voltage supply and recording a trace containing noise exclusively. This resulted in noise with a standard deviation of $\approx 22.3\,\mu V$ for the horizontal magnetic probe, and noise with a standard deviation of $\approx 20\,\mu V$ for the vertical one.

We use a 20 MHz clock signal for the design on the FPGA. Through synchronization of the oscilloscope and the function generator, we prevent frequency jitter and drift in the measurements. Every measurement contains 16384000 byte samples for the 2^{16} recorded clock cycles.

We took a current consumption measurement to compare its quality for side-channel analysis to high-resolution EM measurements. We use a *LeCroy* active differential probe with a bandwidth of 500 MHz and a $10\,\Omega$ measurement resistor.

2.3 Analyses

In every measurement, the two different s-box structures contribute a repeating sequence of value updates of different length. To determine these two independent signal components, every measurement trace is split into sub-traces in two ways according to the different sequence lenghts. First it is split into sequences

containing 87 clock cycles each, and second, it is split into sequences containing 81 clock cycles each. Both sets of sequences are averaged separately, thus, the noise is removed from both signals at a statistical sample size of 753, and 809 respectively. The two independent signals remain separately. After subtracting one of those two signals from the trace the noise remains. It includes power supply noise, clock supply noise, measurement noise, quantization error and switching, or algorithmic noise from parts of the circuit which did not contribute to the signal. In our case, the counter as well as the respective other s-box structure, which exhibits an uncorrelated sequence with different length, contribute to this switching noise. By comparing all clock cycles, the noise is observed as a Gaussian mixture with zero mean and standard deviation σ_{noise} at every relative sample index within the clock cycle.

We regard the constant influence of clocking the registers, i.e., the clock tree and common logic parts, in every cycle as an operation-dependent part of the signal. The variance between the clock cycles in the two derived signal sequences is due to the processed data, thus, the data-dependent part of the signal. We estimate the data-dependent signal part by averaging the clock cycles from each signal sequence and subtracting this operation-dependent part from the sequence. The data-dependent signal remains. By comparing all cycles in the sequence, we get a data-dependent Gaussian distribution at every relative sample index within the clock cycle and we describe it using the standard deviation σ_{data}. We compute the Signal-to-Noise Ratio (SNR) over the clock cycle in decibel as the quotient between the signal and noise standard deviations, $\text{SNR} = 20 * \log(\frac{\sigma_{data}}{\sigma_{noise}})$ dB. The SNR is derived for both identical signal sources and it depends on the location, which one results in a higher SNR.

We performed a Correlation Power Analysis (CPA) to evaluate the quality of the measurements for differential power analysis. We use the Hamming distance leakage model between values from consecutive cycles. The sample size n for the correlation equals the number of recorded clock cycles, 2^{16}, and a correlation coefficient of 0 results in values of $\pm 4/\sqrt{n} = \pm 0.015625$ with a confidence level of 99.99% [8]. Therefore, absolute correlation coefficients below this significance level are disregarded.

3 Discussion of Measurement Results

In this section, we discuss measurement results and derive conclusions. Since the measurements from the frontside with the horizontal coil led to the best results, we provide details for this case and use it as a base for comparison.

3.1 Signal and Noise

Figure 3 depicts the mean and standard deviation of all clock cycles from one measurement at position $(x, y) = (24, 17)$. This position is approximately above s-box structure 1 and will serve as an interesting example. The figure spans

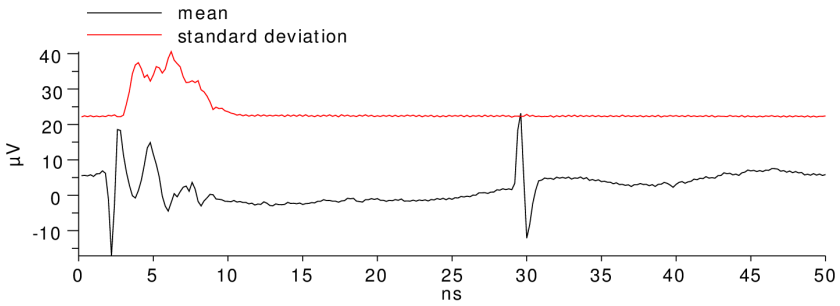


Fig. 3. Mean and standard deviation of all clock cycles at position (24, 17) (frontside, horizontal coil)

the time of one clock cycle, thus, 50 ns. The mean represents the operation-dependent part of the signal which is for instance due to clocking the registers and the active and inactive clock edges can be observed as significant peaks. The standard deviation is constant throughout most of the cycle which can be explained by constant noise factors from the measurement setup and corresponds well to the measured noise floor mentioned in Sect. 2.2. The standard deviation is significantly higher during a time after the active clock edge which is due to data-dependent switching activity in the circuit. At this stage, this switching activity cannot be attributed to specific parts of the design and contains contributions from all circuit parts.

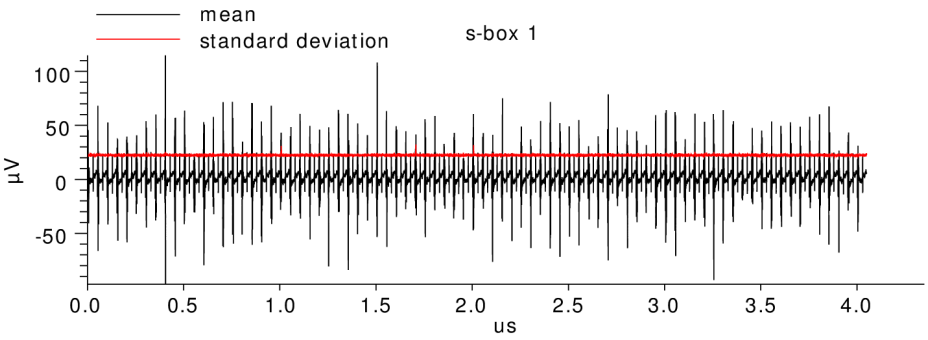


Fig. 4. Mean and standard deviation of repeated s-box 1 sequence at position (24, 17) (frontside, horizontal coil)

We determined the data-dependent signal and noise for both structures in every measurement as described in Sect. 2.3. Figure 4 shows the mean and standard deviation of the repeated sequence of values processed by s-box structure 1 which contains 81 clock cycles. The standard deviation trace is similar to the one depicted in Fig. 3, however, there are no times with significantly high

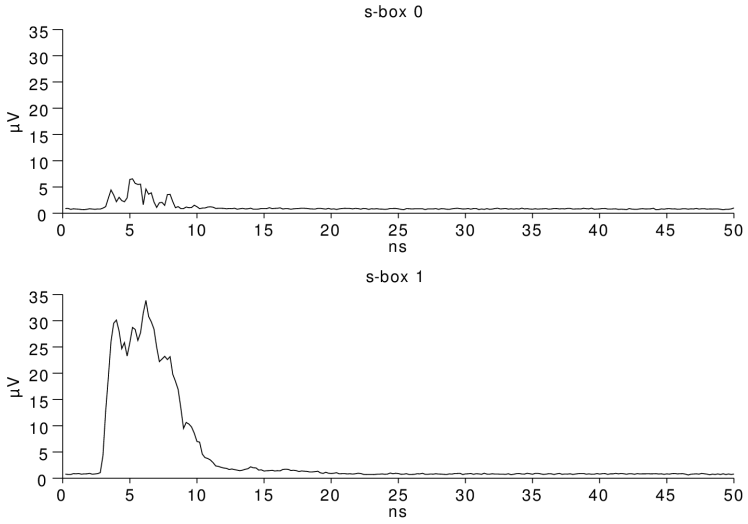


Fig. 5. Data-dependent signal standard deviation σ_{data} over clock cycle for s-box 0 and 1 at position $(24, 17)$ (frontside, horizontal coil)

standard deviations like in the previous figure. This is due to the fact that the data-dependent signal parts are now included in the mean trace. This is clearly visible in Fig. 4, where the mean exhibits significantly different amplitudes. To determine the data-dependent part, we repeatedly subtracted the mean clock cycle (Fig. 3) from the mean depicted in Fig. 4. Figure 5 depicts the result, which is the data-dependent signal within the clock cycle of s-box structure 1 in the bottom diagram. The maximum signal amplitude is clearly significant when compared to the noise level mentioned before. The constant floor of $\approx 1\,\mu V$ seems to be due to statistical artifacts. We performed the same procedure using the same measurement for s-box structure 0 resulting in the upper diagram in Fig. 5. The signal from s-box structure 0 exhibits a significantly low amplitude which is explained by the fact that the measurement position is close to s-box structure 1 and further away from s-box structure 0. *We conclude that the distance to parts of the design in x- and y-directions is important for the detection of leakage signals.*

Significant signal amplitudes are observed within the first 10 ns after the positive, active clock edge. The synthesis tool reported 12.5 ns delay as the longest combinational path of our design. *It is an important observation, that signal leakage is exclusively restricted to a time-span as short as the combinational path after the active clock edge when analyzing local EM measurements close to the source of the leakage.*

The SNR of the signal leakage of an s-box structure is computed as the maximum of the ratio of data-dependent signal amplitude σ_{data} over noise σ_{noise} within the clock cycle. Strong signal components of an s-box structure add to

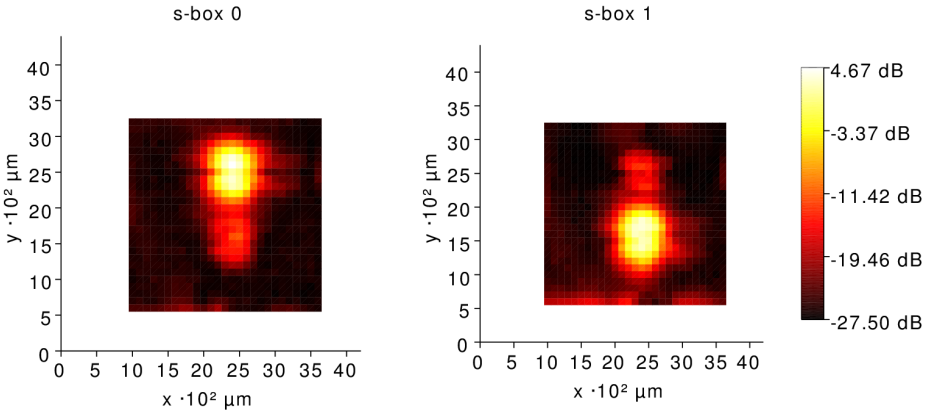


Fig. 6. SNR for both signals (frontside, horizontal coil)

the algorithmic noise for the respective other s-box structure. The measurements from the frontside using the horizontal coil led to the highest SNRs. Figure 6 depicts a map of those SNR values for all positions and both s-box structures. We emphasize that a maximum of $\approx 4.7\,\mathrm{dB}$ represents a significant signal strength. *It is remarkable how the signals from the s-box structures are significant in areas above the placed logic of the structures as depicted in Fig. 1(b). This is an important result of our study.* Surprisingly, the SNRs are also higher close to the respective other structure. We suspect that this is due to modulation effect as described by Agrawal et al. [1]. *As another important conclusion, we realize that it is only possible to achieve high SNRs using a high-resolution probe when it is correctly positioned. This requires that adversary is able to find such positions, e.g., through profiling.*

The two s-box structures only occupy a very small area on the FPGA as depicted in Fig. 1(b). We took a measurement where the same s-box structures were distributed over a broader area, thus, requiring longer routing wires. We observed a significantly higher SNR for this case, thus, we conclude that the SNR highly depends on the design and placement.

3.2 CPA and Localization

We performed CPA as described in Sect. 2.3. Figure 7 depicts the correlation coefficient over the clock cycle for both s-box structures at the position $(24, 17)$. We observe high correlation values, positive as well as negative, for s-box structure 1 and insignificant correlation values for s-box structure 0. Correlation peaks are only 1 to 3 samples wide. Therefore, we estimate a minimal required sampling rate of $\approx 2\,GS$ in this case. *This will vary for other devices, but it can be generally expected, that a high sampling rate is required for localized EM measurement.*

Figure 8 depicts a map of maximum absolute correlation coefficients for every measurement on the map. *We strongly emphasize how perfectly distinct the areas*

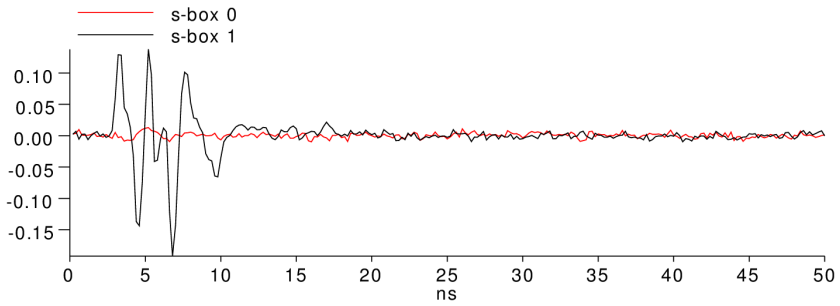


Fig. 7. CPA over cycle at position (24, 17) (frontside, horizontal coil)

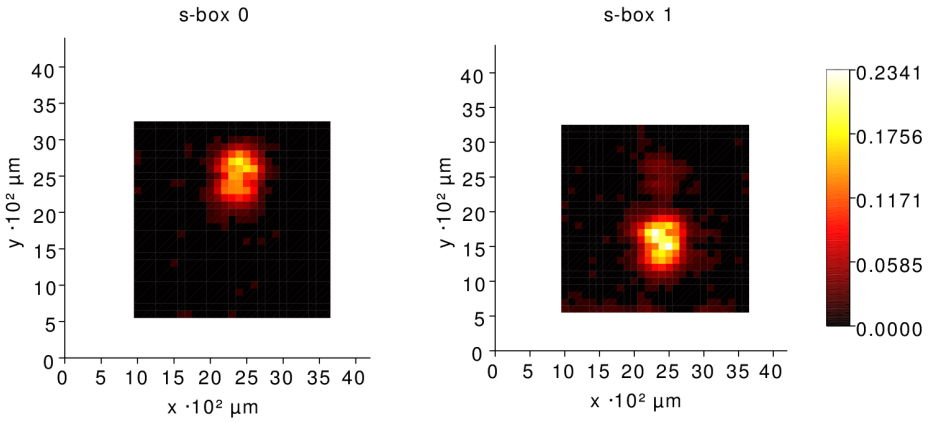


Fig. 8. CPA coefficients (frontside, horizontal coil)

with high correlations of the two s-box structures are. This provides the perfect precondition for localized CPA attacks where only a single s-box structure is targeted. However, it must be noted, that an adversary must be able to find those positions.

Unfortunately, there is no available information about the physical size of the FPGA cells. During the scanning of the surface, we used a step size of 100 µm. In Fig. 8 and Fig. 6 we observe distinct leakage regions corresponding to the two s-box structures. We assume that the distance between the centers of the leakage regions equals the distance of the structure centers in the placement. From this, we derive an assumed distance of the s-box structure centers of $\approx$ 900 µm and an assumed logic area of the two structures of $\approx 250 \times 250$ µm. In Fig. 8, we observe that the regions with significant correlation coefficients do not overlap. *We assume from the presented evidence that there are non-overlapping regions of significant correlation coefficients even when the two s-box structures are adjacent to each other, thus, when the centers are only* $\approx$ 250 µm *apart.* This is strongly dependent on the logic structure of the device, hence, we do not

suggest generalization. *An interleaved placement of s-box structures will render this significantly more difficult, if not impossible, because of entirely overlapping regions of correlation coefficients. However, measurement equipment with higher resolution may still support localization.*

3.3 Backside versus Frontside Measurement

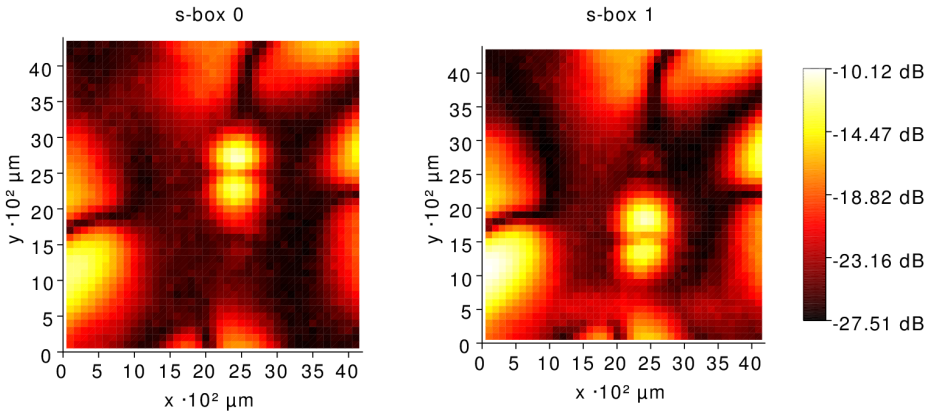


Fig. 9. SNR is ≈ 15 dB lower on backside (horizontal coil)

Decapsulating a chip from the backside can be achieved with less effort than from the frontside. Hence, it is an important question which preparation leads to better results. Figure 9 depicts the SNR map from using the horizontal coil from the backside. In the middle of the device, the localized signal leakage of both structures is clearly visible in distinct, confined regions. Additionally, regions with high SNRs are observed on the edges of the die. Those regions have not been covered by the frontside measurements and exhibit signals from *both* s-box structures. However, since those regions contain contributions from both structures, they are useless from a localized perspective. We assume that the magnetic field in those regions is caused by bonding wires or parts of the chip supply. The maximum SNR is ≈ 15 dB lower than in case of frontside measurement. This might be due to the silicone substrate and the fact that the conductors within the integrated circuit, which carry the exploitable signals, are on upper metal layers and therefore, further away when measuring from the backside. *We conclude that backside measurements lead to significantly lower SNRs.*

3.4 Probe-to-Chip Distance

An important question is whether high-resolution EM measurements require semi-invasive decapsulation to achieve minimal probe-to-die distances. We re-

peated the measurement from the frontside using the horizontal coil and increased the distance of the probe to the surface of the chip by 300 µm which roughly equals the package thickness above the die. The measurements lead to a significantly lower maximum SNR of −16.5 dB. This is ≈ 21 dB lower than the maximum SNR observed in the original measurement depicted in Fig. 6. *We conclude that the semi-invasive decapsulation is important to achieve high SNRs.*

3.5 Vertical Coil

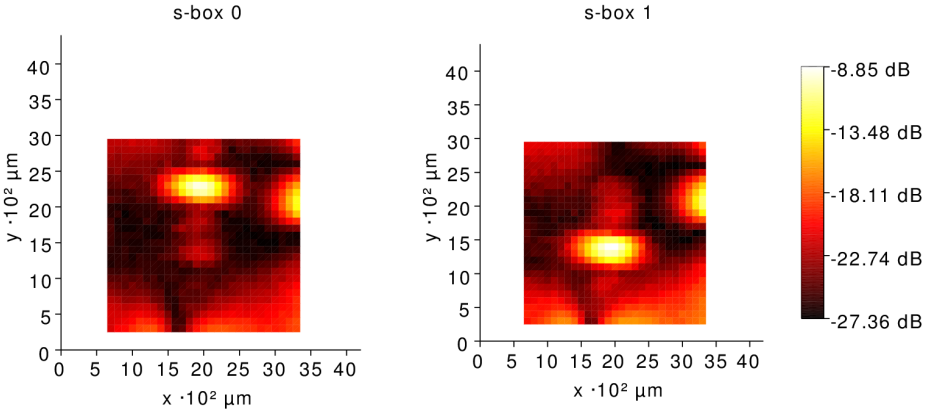


Fig. 10. SNR using vertical coil in the x-direction (frontside)

We took measurements using the vertical coil in x-, and y-direction. Figure 10 depicts the SNR maps for the x-direction. A maximum SNR of ≈ −8.9 dB is achieved which is significantly lower than in case of using the horizontal coil. However, the coil seems to capture the magnetic field more selectively than the horizontal coil. We observe, that the regions with high SNR corresponding to the s-box structures have a different, more compact shape than in case of using the horizontal coil which is depicted in Fig. 6. This corresponds to the expectation that different coil orientations 'select' different parts of the field. The results from the y-direction resulted in even lower SNRs and the two regions with high SNRs are dispersed over a wider area, thus, making localization more difficult. *Given those observations, we conclude that the probe with the vertical coil leads to lower SNRs compared to horizontal coils. However, a better selectivity can be achieved for better localization if the coil direction supporting this is known.*

3.6 Frequency Domain

Frequency filtering of EM signals is generally promising for selecting data-dependent signals. We used the Fast Fourier Transform (FFT) to calculate frequency spectra at several positions on the die using the measurements from the backside

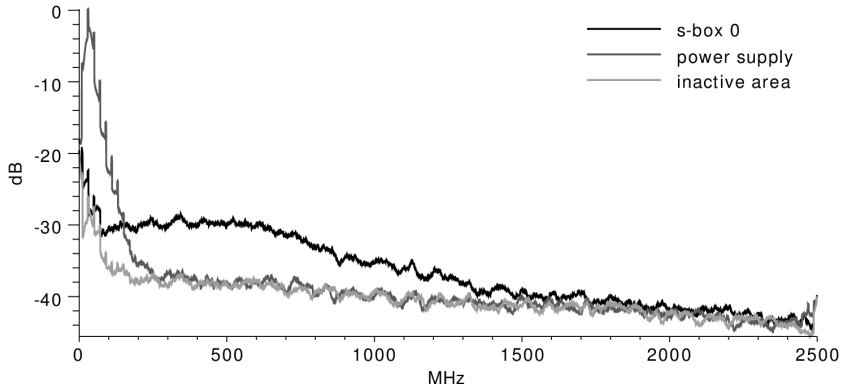


Fig. 11. Frequency spectra at different positions (backside, horizontal coil)

using the horizontal coil. We cut the measurement into 753 parts corresponding to the repeated s-box 0 value sequence. Then, we performed FFT transformations and decreased phase and amplitude noise by averaging the frequency spectra. Figure 11 shows the resulting power spectral density at three different positions on the die. Our results show frequency components up to 2.5 GHz because of the sampling rate of 5 GS/s. The first position is close to the s-box structure 0. The second one is close to an area where we assume a big influence of the power supply, and the third is at a position which exhibited a low SNR in Fig. 9. A comparison of the position close to s-box 0 to the position with minimum SNR leads to the observation, that the information leakage is contained in a frequency span between 100 MHz and 1.5 GHz. The upper frequency limit might be determined by the bandwidth of our measurement equipment. The position close to the power supply exhibits higher amplitudes, thus, information leakage, in a frequency span lower than 200 MHz. We argue that this is due the low-pass characteristic of the series of on-chip capacitances between the leaking s-box structure and the power supply. Therefore, a high-pass filter with a cut-off frequency of 200 MHz could be applied to focus on localized signals and this fact could be used as a heuristic to find exploitable positions on the circuit.

3.7 Trace Compression

Trace compression is popular to reduce data and computational complexity during side-channel analysis. We evaluated four methods which reduce 250 samples per clock cycle to a single value and repeated the CPA from Sect. 3.2 to benchmark the outcome. During *maximum extraction*, one sample index is selected which exhibits the maximum mean value over all cycles. This resulted in a maximum correlation of 0.086. *Peak-to-peak extraction* derives the distance between the two values with highest and lowest mean over all cycles. This resulted in a maximum correlation of 0.030. *Sum-of-absolutes* integrates absolute values over whole clock cycles. This resulted in a maximum correlation of 0.063. *Sum-of-*

squares integrates squared values over whole clock cycles and resulted in a maximum correlation of 0.086. The original traces lead to a maximum correlation coefficient of 0.234 in Sect. 3.2, Fig. 8.

Hence, all compression methods resulted in significantly lower correlation coefficients and we conclude that trace compression is generally inadvisable when analyzing high-resolution EM measurements. However, a compression method, which simply removes unimportant parts in each clock cycle, e.g., samples between 75 ns and 250 ns in Fig. 5, will not influence the outcome. This becomes obvious from Fig. 7, where the correlation is detectable in the first part of the cycle only.

3.8 Current Consumption versus Electromagnetic Field

In our current consumption measurement, the signals from consecutive clock cycles interfere which decreases the SNR due to additional data-dependent switching noise from other cycles. This is caused be the low bandwidth in the supply network containing on- and off-chip capacitances and inductances [8]. We excluded the lower bandwidth of the differential probe as a cause by analyzing the field of bonding wires of the supply exhibiting the same interference. As expected we found that the signal leakage is detectable over the whole clock cycle almost constantly instead of just during a short time after the active edge. This makes current consumption measurements more robust against misalignment in differential attack settings. We detected a maximum SNR of 0.9 dB and a maximum correlation coefficient of 0.094. This is significantly lower than the maximum observed SNR of 4.7 dB and maximum correlation coefficient of 0.234 in the case of high-resolution EM measurement. We assume that this is due to the overlap and additional switching noise from other circuit parts. *We conclude, that localized EM measurements prevent interference of signals across multiple cycles at high clock frequencies of the design under test and provides significantly higher SNRs.* However, this requires to be able to position the probe correctly.

4 Conclusion

We suggest that some of our conclusions about high-resolution EM measurements can be generalized to other integrated circuits such as FPGAs or ASICs. Localized measurements are only superior, if correct positions for measurement are known. Then, the signal of circuit parts can be recorded selectively and with higher SNRs without interference due to low-pass behavior of the supply network. Measurements from the die frontside lead to better results, and we generally recommend semi-invasive decapsulation to achieve minimal probe-to-die distances. The horizontal probe provided higher SNRs while the vertical coil could be used to increase selectivity. High sampling rates, e.g., at least $> 1\,\mathrm{GS/s}$ will be required in most cases and compression of traces is generally not recommended.

References

1. Agrawal, D., Archambeault, B., Rao, J., Rohatgi, P.: The EM side—channel(s). In: Kaliski, B., Koç, C., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2002. Lecture Notes in Computer Science, vol. 2523, pp. 29–45. Springer Berlin / Heidelberg (2003)
2. Canright, D.: A very compact s-box for aes. In: Rao, J., Sunar, B. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2005, Lecture Notes in Computer Science, vol. 3659, pp. 441–455. Springer Berlin / Heidelberg (2005)
3. De Mulder, E., Buysschaert, P., Ors, S., Delmotte, P., Preneel, B., Vandenbosch, G., Verbauwhede, I.: Electromagnetic analysis attack on an fpga implementation of an elliptic curve cryptosystem. In: Computer as a Tool, 2005. EUROCON 2005.The International Conference on. vol. 2, pp. 1879 –1882 (nov 2005)
4. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic analysis: Concrete results. In: Koç, C., Naccache, D., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems — CHES 2001. Lecture Notes in Computer Science, vol. 2162, pp. 251–261. Springer Berlin / Heidelberg (2001)
5. He, W., de la Torre, E., Riesgo, T.: An interleaved epe-immune pa-dpl structure for resisting concentrated em side channel attacks on fpga implementation. In: Schindler, W., Huss, S. (eds.) Constructive Side-Channel Analysis and Secure Design. Lecture Notes in Computer Science, vol. 7275, pp. 39–53. Springer Berlin / Heidelberg (2012)
6. Heyszl, J., Mangard, S., Heinz, B., Stumpf, F., Sigl, G.: Localized electromagnetic analysis of cryptographic implementations. In: Dunkelman, O. (ed.) Topics in Cryptology – CT-RSA 2012. Lecture Notes in Computer Science, vol. 7178, pp. 231–244. Springer Berlin / Heidelberg (2012)
7. Kirschbaum, M., Schmidt, J.M.: Learning from electromagnetic emanations - a case study for iMDPL. In: Workshop Proceedings COSADE 2011. pp. 50 – 55 (2011)
8. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security). Springer-Verlag New York, Inc., Secaucus, NJ, USA (2007)
9. Peeters, E., Standaert, F.X., Quisquater, J.J.: Power and electromagnetic analysis: improved model, consequences and comparisons. Integr. VLSI J. 40(1), 52–60 (Jan 2007)
10. Quisquater, J.J., Samyde, D.: Electromagnetic analysis (EMA): Measures and counter-measures for smart cards. In: Attali, I., Jensen, T. (eds.) Smart Card Programming and Security. Lecture Notes in Computer Science, vol. 2140, pp. 200–210. Springer Berlin / Heidelberg (2001)
11. Real, D., Valette, F., Drissi, M.: Enhancing correlation electromagnetic attack using planar near-field cartography. In: Design, Automation Test in Europe Conference Exhibition, 2009. DATE '09. pp. 628 –633 (Apr 2009)
12. Sauvage, L., Guilley, S., Mathieu, Y.: Electromagnetic radiations of fpgas: High spatial resolution cartography and attack on a cryptographic module. ACM Trans. Reconfigurable Technol. Syst. 2, 4:1–4:24 (Mar 2009)
13. Standaert, F.X., Archambeau, C.: Using subspace-based template attacks to compare and combine power and electromagnetic information leakages. In: Oswald, E., Rohatgi, P. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2008. Lecture Notes in Computer Science, vol. 5154, pp. 411–425. Springer Berlin / Heidelberg (2008)