Comparison of two Setups for Contactless Power Measurements for Side-Channel Analysis

Arthur Beckers, Benedikt Gierlichs, Josep Balasch, Ingrid Verbauwhede
imec-COSIC, KU Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

***Abstract*—When performing side-channel analysis of (passively powered) contactless devices such as RFID tags the side-channel signal is dominated by the carrier field used to power the device. This carrier field should be removed by the measurement setup in order to expose the power consumption of the target device and enable a side-channel analysis. In this paper we describe and compare two methods for measuring the power consumption of contactless devices. The comparison is done experimentally by running applets on a contactless BasicCard and evaluating the signal to noise ratio of the measurements collected with each setup. Our results show that both setups perform similar, indicating that more research is needed to investigate the differences and strengths.**

I. Introduction

Power analysis attacks [11] are acknowledged as one of the most important security threats against cryptographic implementations. They rely on the fact that the *instantaneous* power consumption of a circuit depends (among others) on the data that is internally processed [14]. This characteristic allows an adversary to infer device-specific secret cryptographic keys used by the implementation, e.g. by performing statistical analyses of the power consumption waveforms using various techniques such as DPA [11], CPA [5] or MIA [7].

The key requirement to mount power analysis attacks is the ability to collect power consumption waveforms during cryptographic executions. In many cases this can be done by monitoring the current drawn by the circuit from its power supply, e.g. by recording with an oscilloscope the voltage drop over a *shunt* resistor placed across the supply or ground lines. This method is, however, not easily applicable to contactless devices such as RFID tags or contactless smart cards. These platforms contain an antenna that harvests energy from the electromagnetic (EM) field generated by a *reader*, and use an on-chip analog front-end to internally convert RF energy to a stable voltage source. Tapping into the supply lines may still be possible for some platforms, but it demands expensive physical manipulations of the target device.

An alternative approach widely used in practice to access the power consumption of contactless devices is to monitor their surrounding EM field. This can be done non-invasively by placing a near-field antenna coil in close proximity to the device under evaluation, and behind it from the reader's point of view. As circuit activity influences the reader's field by drawing more or less power during operation, the power consumption waveform is inherently contained in the collected EM signal. A practical issue with this approach is that the measured signal is strongly dominated by the reader's carrier field, i.e. 13.56 MHz in HF frequency band and 868 MHz in UHF frequency band. The main challenge is thus to devise methods to reduce the influence of the carrier signal, in order to extract the power consumption waveform.

Using a near-field probe to measure EM emanations of a circuit seems related but is conceptually different.

A. Related work

Earlier attempts to obtain power consumption measurements of HF contactless smart cards are due to Carluccio et al. [6]. They propose to reduce the carrier's influence by physical separation of target circuit from both antenna and reader. This demands however an invasive approach to alter the target device, i.e. dissolving the card's plastic enclosure using acids and soldering wire extensions.

An alternative, less invasive approach is to remove the carrier frequency by means of filtering and/or signal cancellation techniques. Hutter et al. [8] propose two measurement setups (based on a spectrum analyzer and a Helmholtz arrangement) to filter data-dependent emissions and show their suitability to attack a custom RFID prototype operating at the HF band. Kasper et al. [9] note that the power consumption of the device modulates the reader's field, making the problem equivalent to an AM-modulation of the carrier frequency. By means of a custom-made reader, they develop an analog setup to subtract the known, constant field of the reader from the signal measured by the EM probe. The resulting signal is then digitally demodulated to obtain the power measurement. In a follow-up work [10] by the same authors, they propose an alternative approach that applies analog demodulation directly to the signal measured by the EM probe. For this purpose, they develop a custom PCB equipped with amplification, rectification and filtering stages. This measurement setup is used by Oswald and Paar [15] to break a commercial MIFARE DESfire smart card. A last measurement approach is described by Korak and Plos [12]. Instead of using analog demodulation, they propose to measure only the peaks of the EM reader signal in order to increase the resolution of the measurement.

B. Our Contributions

The aim of this work is to compare two different setups by evaluating the quality of measurements of a contactless smart

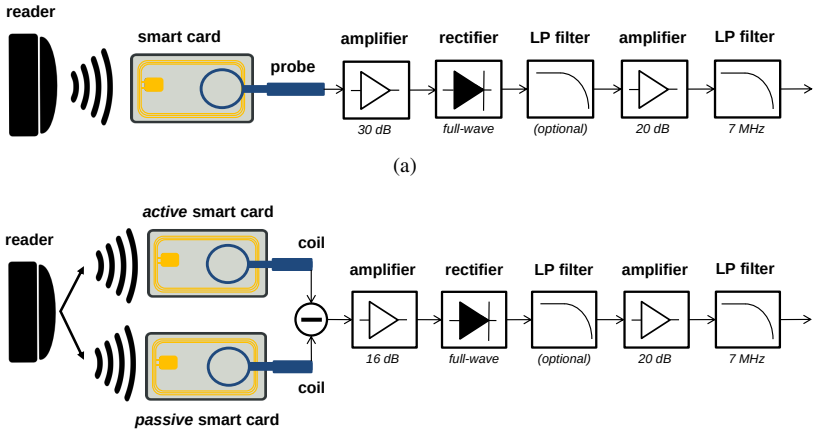

Fig. 1. Diagram of single antenna setup (a) and balanced setup (b)

card operating in the HF band. Both setups use an analog demodulation stage based on the design in [15] containing full wave rectification, low pass filtering and amplification stages. The main difference in the setups lies in the way the *raw signal* (i.e. input to the analog demodulation stage) is obtained. In the first setup, the signal is obtained by positioning the target device between the reader and a *single antenna* coil. In the second setup, the signal is obtained by subtracting the EM fields of two identical target devices (one operating normally, the other being idle) driven by identical carrier fields. We denote this as *balanced* approach. In this work, we provide a description of these setups and a first evaluation using software applets running on a contactless BasicCard smart card. Understanding the strengths and weaknesses of different measurement methods is key to obtaining high quality measurements and therefore eventually vital to security testing laboratories.

II. Experimental Setups

The two setups under comparison have different approaches to obtain the raw signal. The rest of the measurement setup is kept the same for both approaches in order to solely compare the influence of the used measurement method. Figure 1 gives a general overview of the two measurement setups.

The contactless smart cards whose power consumption is measured in order to compare the measurement setups are driven by a smart card reader. Their power consumption is probed by a single antenna or by the balanced setup. The raw signal produced by the probe is then put through an analog post-processing stage and finally sampled by an oscilloscope. In the remainder of the section we describe the individual components of the measurement setup in more detail.

A. Single antenna setup

In the single antenna setup we measure a single smartcard with a wideband EM probe (Langer LF-R 400). The EM probe simply measures the EM field emitted by the reader on the backside of the card and is followed by a sequence of analog post-processing stages.

The probe is placed at a small distance from the smart card in order to prevent clipping of the first amplification stage.

B. Balanced setup

The balanced setup was designed and developed by Brightsight [1], a leading security evaluation laboratory. With the balanced setup we place two identical smart cards in two identical carrier fields. One of the cards runs the targeted application while the other is idle. The carrier field is provided by the Microprocess smart card reader, see below. The reader antennas in this setup consist of two round ferrite cores, one for each card, which have a thin cutout to hold the card. The field is delivered through the antenna coils wound around the ferrite core.

Two sense coils that are also wound around the ferrite cores measure the carrier field. The fields in both cores have the same common mode signal since both house an identical smart card. The only difference in field should be the result of the power consumption of the target card. The common mode signal from both coils is subtracted and the remaining differential signal is put through further analog post-processing. In order to have a good cancellation of the carrier field the cards need to carefully positioned inside the ferrite cores.

The carrier field of the reader is distorted when a smart card is placed in the field. If we provide the same field to two identical smart cards the distortion of the field due to the cards will be equal. Therefore the subtraction of the common mode signal measured by the sense coils will result in a good cancellation of the carrier signal. If we would simply subtract the carrier signal from the measured carrier signal [9] the cancellation will not be as effective. This is due to the mismatch between the sinusoidal signal generated by the reader and the distortion of the carrier field by the smart card.

C. Analog post-processing

We keep the same analog post-processing steps for all experimental setups in order to have a difference in measure-

ment quality that solely depends on the measurement method. Although we keep the analog post-processing consistent there might still be a bias on the results since one set of filter values might favour one or the other measurement method.

The raw signal gets amplified using a 30 dB pre-amplifier (Langer PA 303) in the single antenna setup. The balanced setup has a build in 16 dB amplifier. The signal is then rectified using a full-wave rectifier (ADL5511 development board [3]).

The ADL5511 development board allows to add low pass filtering by soldering on some analog components. Two versions of this board were used, the plain version without additional low pass filtering and an adapted version which has a low pass filter with a 2 MHz cutoff frequency. Without the 2 MHz, a portion of the carrier is still present in the sampled signal. After the rectification the signal is amplified again using a 20 dB pre-amplifier (Langer PA 203). Subsequently the signal is put through a final filtering stage using a 7 MHz second order low pass filter. The resulting analog signal is sampled at 200 MS/s by a Tektronix DPO 7254C oscilloscope. The analog post-processing setup remains unchanged for the different target implementations.

D. Microprocess

We use a Microprocess MP300 TCL1 to interface with the BasicCards. The Microprocess is a smart card tester that allows us to communicate with the cards and to tune the carrier field. The Microprocess provides a clean 13.56 MHz sine wave as a carrier signal. Besides communication with the BasicCard, the Microprocess is also used to provide a trigger signal to the oscilloscope for collecting power traces.

Having a tunable field strength is important when taking contactless power measurements. Lowering the field strength to a level where the smart card has just enough power to operate can greatly improve the SNR of the measurements. For all our measurements the field strength is reduced as much as possible while ensuring proper operation of the card.

E. BasicCards

The smart cards used to evaluate the measurement methods are BasicCards ZC7.5 rev B [4]. They are dual interface cards that can be freely programmed by the user using the BASIC language. The cards are compliant with the ISO 14443 standard [2] and thus use a carrier frequency of 13.56 MHz. The BasicCards come with co-processors and libraries for different cryptographic primitives such as AES, RSA and SHA-256. The BasicCards are internally clocked at 18 MHz.

III. Measurement Quality Assessment

The goal of the evaluation is to compare the measurement quality of two different measurement setups, not to evaluate the security of a certain smart card. We use the BasicCards for our study because of their ease of use but we do not make any claims about their security.

Power traces taken by different measurement setups can look very different visually. However, simple visual inspection does not allow to quantify the performance of a measurement setup.

We define the measurement quality of a setup as its ability to remove noise from the measurement while retaining the side channel signal related to the targeted operation. The largest noise source in the signal is the reader's carrier field. This can easily be seen in Figure 2, which shows the frequency spectrum of a captured measurement without analog processing. Large peaks are visible at the carrier frequency, i.e. 13.56 MHz, as well as its third harmonic.

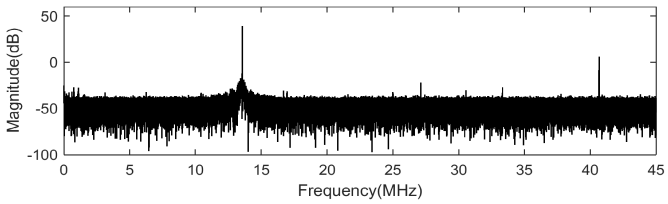

Fig. 2. Single antenna frequency spectrum of a smartcard in operation without analog post-processing.

The frequency spectrum of measurements obtained with our test experimental setups are able to partially remove the carrier field from the raw signal. This is illustrated in Figure 3, which show a clear reduction of the peak at the carrier frequency. The frequency spectra plot however only show the setups ability to remove noise, but give no indication to the amount of side channel information that is still present in the measured signal. For that we need another metric.

Different measures can be used to quantify the quality of a measurement method, such as the correlation coefficient, difference of means, signal to noise ratio, etc. All these measures use in essence the same statistical properties of the collected measurements. Therefore, in order to compare the different power measurement methods, a single measure was chosen namely the signal to noise ration (SNR) as given by equation (1) (see also [13], [14]).

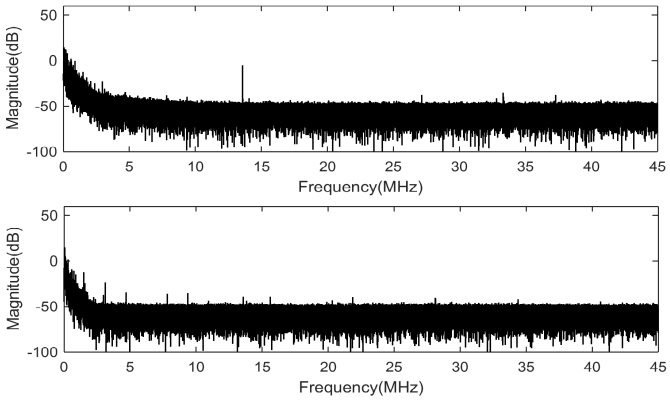

Fig. 3. Frequency spectrum of a smartcard in operation for the single antenna (top) and balanced (bottom) setup with analog post-processing.

The signal in side channel analysis is due to the data we want to retrieve. This can be for instance the output of an AES

S-box operation. The targeted data has a discrete number of possible values i (equation (1)). Every value i will yield a signal according to a leakage function such as the Hamming weight or distance, and has a certain power consumption. In practice measurements of this power consumption are noisy. The mean power consumption of a value i is given by μ_i. The variance of the means of all $i's$ is a measure for the distinguishability of the $i's$ and thus for the signal related to the data. The variance of the power consumption of a value i is given by σ_i^2. The mean of all variances σ_i^2 is a measure for the noise in the measurements. The SNR is then

$$SNR = \frac{Var(\{\mu_i\})}{Mean(\{\sigma_i^2\})}\,. \tag{1}$$

The most prominent noise sources are the noise introduced by other components of the microcontroller that perform data independent operations $P_{electronic}$ and the noise caused by the carrier field $P_{carrier}$. The noise $P_{electronic}$ can be approximated as white Gaussian noise. $P_{electronic}$ can therefore not be filtered out. The noise introduced by $P_{carrier}$ on the other hand is situated mostly at the carrier frequency and at higher harmonics of the carrier frequency. This noise can therefore be reduced using filtering techniques and specialized measurement methods. The measurement method able to reduce $P_{carrier}$ most will have the best overall SNR.

The SNR is strongly influenced by every component in the measurement setup. The targeted device, measurement method, analog post-processing, sample rate and quantization noise introduced by the oscilloscope all contribute to the SNR. In order to only measure the impact of the measurement method on the SNR we keep all the other components such as the target, analog postprocessing and oscilloscope settings constant during the experiments.

IV. Experimental Results

In this section we present the outcome of our experiments. We provide results for two different applets programmed in the BasicCard: Applet #1 executes a simple substitution operation corresponding to the AES S-box, while Applet #2 performs a message digest by leveraging on the built-in SHA-256 hash function from the BasicCard API. For each experiment we collect a set of 50 000 measurements. This number is determined experimentally, and corresponds to the amount of observations necessary for the estimated SNR value to be stable.

We note that our experimental setups contain several configurable parameters that can influence the final value of the SNR, e.g. from the sampling rate of the oscilloscope to the settings of the filters/amplifiers in the analog demodulation stage. The reported experiments represent a small set of such parameter values. The only aspect we investigate is whether disabling the first low pass filter in the ADL5511 envelope detector yields any improvements. For the sake of comparability, we opt to keep the rest of parameter values constant for all experiments.

A. Applet #1: AES Sbox Substitution

Our first applet is a software implementation of the AES S-box look-up table. Its functioning is very simple: it receives an 8-bit input value in, performs a memory look-up, and returns an 8-bit output value $out = Sbox(in)$.

An example of a measurement obtained for each setup when using a 2 MHz low pass filter in the ADL5511 is shown in Figure 4 (top and middle). The highly varying peaks at the beginning (resp. end) of the measurement indicate communication operations, i.e. data reception (resp. data transmission) of the 8-bit value. The window of interest where computations take place lies thus somewhere in this interval.

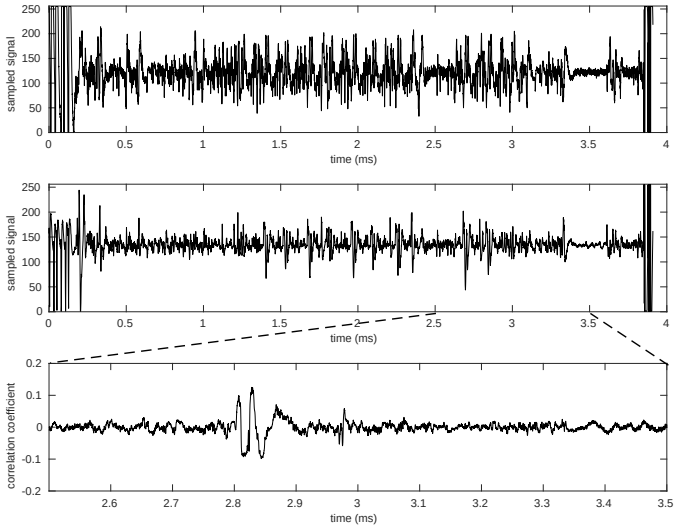

Fig. 4. Measurement of Applet #1 for the single antenna setup (top) and balanced setup (middle). Outcome of CPA attack for the single antenna setup targeting the Hamming weight of output value (bottom).

Two practical problems appear at this stage. First, the power measurements for different executions of the applet are strongly desynchronized in the time domain. And second, it is not obvious in the measurements the time sample(s) where the actual substitution operation takes place. In order to overcome these effects, we need to align all measurements horizontally at the point where the target operation is executed. This can be done by iterative testing, i.e. by performing a rough alignment at certain patterns in the measurement and checking for the presence of a signal. The latter can be done for instance by computing the correlation coefficient between the measurements and the Hamming weight of the output value, i.e. HW(out). This is similar to what would be computed in a real CPA [5] attack. After some trials, we determine the interesting operations take place in the pattern starting after time instant $2.6\ ms$. This is verified by looking at the correlation trace in Figure 4 (bottom). Results for the balanced setup are similar, so The peaks at $2.8\ ms$ indicate that the output value is computed and/or manipulated at these instants.

Once the window of interest is located, we perform a second fine horizontal alignment taking as reference the samples

containing the correlation peaks. After this, we perform the SNR calculations as described in Section III on the window where the correlation has been observed. The results are summarized in Table I. The SNR values for both setups are very similar, indicating that the removal of $P_{carrier}$ for this experiment is equally effective independently of how the raw measurements are obtained.

TABLE I
SNR FOR APPLET #1: ADL5511 WITH 2 MHZ LOWPASS FILTER

Target variable	Single antenna setup	Balanced setup
HW(out)	0.0663	0.0623

B. Applet #2: SHA-256 digest

Our second applet is an implementation of a message digest using the SHA-256 hash function. The applet receives a 32-byte random input string, computes its hash using the built-in SHA-256 routine, and returns the corresponding 32-byte output string.

Figure 5 shows an exemplary power measurement obtained with the single antenna setup (top) and the balanced setup (bottom). In both cases, measurements are obtained when enabling a 2 MHz low pass filter in the ADL5511 envelope detector. Similar to Applet #1, the beginning (resp. ending) dense patterns correspond to communication operations. In this case however, the actual computations are clearly visible in the measurement, i.e. both signals contain a particular pattern that repeats 64 times. This is consistent with the functioning of the SHA-256 algorithm, whose compression function consists of 64 iteration rounds. Each round applies a transformation to the internal SHA-256 state, which consists of 8 32 bit values denoted as (a, b, ... ,f, g). More formally: the state at the end of Round #i is computed as: (a_i, b_i, ... ,f_i, g_i) = f(a_{i-1}, b_{i-1}, ... ,f_{i-1}, g_{i-1},m), where f is the transformation function and m is a 32 bit value which depends on the input message.

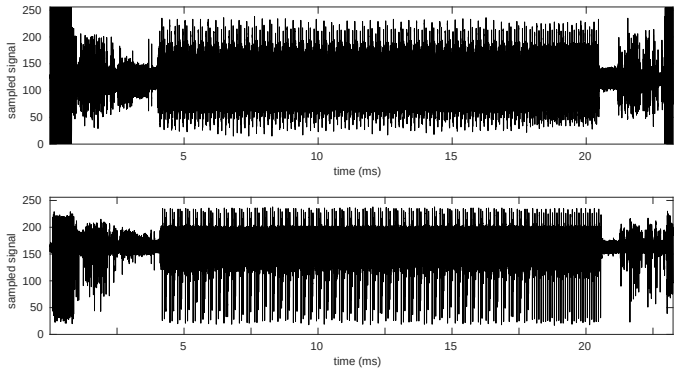

Fig. 5. Measurement of Applet #2 for the single antenna setup (top) and balanced setup (middle).

A close-up view of the power measurements during the first 5 rounds is shown in Figure 6 (top and middle). In order to verify the presence of a signal we can compute the correlation coefficient between the measurements and the Hamming weight of the state update from a_{i-1} to a_i during Round #i. More specifically, we compute four correlation traces when targeting ($a_{i-1,j} \oplus a_{i,j}$), where $1 \leq j \leq 4$ denotes each byte of the 32-bit word a. The reason why we target individual bytes rather than complete words is that the implementation operates at byte level. We speculate this is simply because the internal processor has an 8-bit architecture.

The results of this test after aligning all measurements at the start of the first pattern (beginning of Round #1) are shown in Figure 6 (bottom). Each trace corresponds to the outcome of a correlation test when targeting ($a_{0,j} \oplus a_{1,j}$) $1 \leq j \leq 4$. The plot shows that each variable update leaks very similarly. The main difference is a horizontal shift, which indicates each byte is manipulated at a different clock cycle.

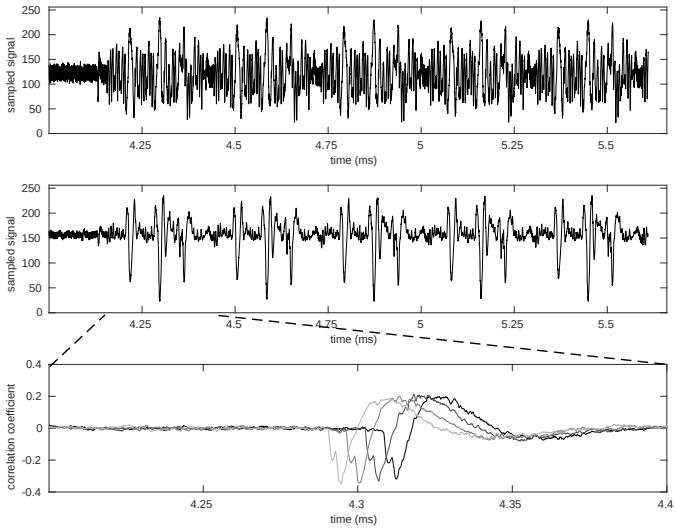

Fig. 6. Close-up view of measurement of Applet #2 for the single antenna setup (top) and balanced setup (middle). Outcome of CPA attack for the single antenna setup when targeting the different HD($a_{0,j} \oplus a_{1,j}$) (bottom).

Based on this result, we can calculate the SNR for each of the four byte transitions of a for a given round. The results when using a 2 MHz low pass filter during envelope detection are shown in Table II.

The upper four rows show the results for the SNR at the output of Round #1. We use the same measurements as for the calculation of the correlation traces, i.e. aligned at the first repeating pattern. The results are once again quite similar for both setups, although it appears that for certain bytes the single antenna setup performs slightly better than the balanced setup.

For completeness, the lower four rows show the SNR results at the output of Round #2. In this case, we need to re-align all measurements at the beginning of the second repeating pattern. In this case we observe that the single antenna setup performs consistently better for all tests, i.e. the SNR value is roughly 30% higher than the result obtained for the balanced setup

We presume that this difference in SNR is an artifact of the alignment, i.e. it might indicate that measurements of the single antenna setup can be better aligned than measurements of the balanced setup.

TABLE II
SNR FOR APPLET #2: ADL5511 WITH 2 MHZ LOW PASS FILTER

Target variable	Single antenna setup	Balanced setup
HW($a_{0,1} \oplus a_{1,1}$)	0.1683	0.1604
HW($a_{0,2} \oplus a_{1,2}$)	0.2723	0.2307
HW($a_{0,3} \oplus a_{1,3}$)	0.1456	0.1432
HW($a_{0,4} \oplus a_{1,4}$)	0.1661	0.1415
HW($a_{1,1} \oplus a_{2,1}$)	0.1174	0.0908
HW($a_{1,2} \oplus a_{2,2}$)	0.1276	0.0969
HW($a_{1,3} \oplus a_{2,3}$)	0.1306	0.1128
HW($a_{1,4} \oplus a_{2,4}$)	0.1336	0.0934

In addition to these results, we also evaluated the SNR when removing the low pass filter in the ADL5511 envelope detector. Results are provided in Table III. Two observations can be made. First, disabling the filtering stage results in a degradation of the SNR for both setups (around 50% compared to the case with 2 MHz filtering). And second, the single antenna setup appears once again to perform better than the balanced setup. Surprisingly, the difference in SNR for some target variables (e.g. $a_{1,4} \oplus a_{2,4}$) is almost a factor 4 worse.

Removing the low pass filter in the envelope detector leads to more noisy measurements. We presume that the more noisy measurements are more difficult to align, which may explain the observed differences.

TABLE III
SNR FOR APPLET #2: ADL5511 WITHOUT LOW PASS FILTER

Target variable	Single antenna setup	Balanced setup
HW($a_{0,1} \oplus a_{1,1}$)	0.0755	0.0652
HW($a_{0,2} \oplus a_{1,2}$)	0.0855	0.0647
HW($a_{0,3} \oplus a_{1,3}$)	0.0576	0.0437
HW($a_{0,4} \oplus a_{1,4}$)	0.0576	0.0294
HW($a_{1,1} \oplus a_{2,1}$)	0.0488	0.0427
HW($a_{1,2} \oplus a_{2,2}$)	0.0416	0.0186
HW($a_{1,3} \oplus a_{2,3}$)	0.0487	0.0307
HW($a_{1,4} \oplus a_{2,4}$)	0.0462	0.0180

In addition, the outcome of all experiments is strongly influenced by the target device and the setup. Choices for the analog post-processing components, the targeted smart card, the frequency at which the smart card operates might all influence the SNR. Further investigation is needed.

Besides the comparison between setups the results also show the importance of having a proper analog post-processing setup when taking contactless power measurements. Not filtering out $P_{carrier}$ properly results in a significantly worse SNR. The analog post-processing stage is constant for the AES S-box and the SHA-256 from tables I and II and yet their SNR is significantly different. Also between SHA-256 rounds and even between the state bytes of a single SHA-256 round there is a variance in the SNR. This indicates that also $P_{electronic}$ has a relatively strong influence on the SNR.

V. CONCLUSION

We described and compared two measurement setups for contactless power measurements: the balanced measurement setup and the single antenna setup. We compared the measurement quality of both setups by calculating the SNR of the power measurements for two different applets run on a BasicCard. First results indicate that both setups perform similar with a slight advantage for the single antenna setup. The obtained results however were only obtained for a small set of the parameter space. Further investigation is needed into the influence of the target device and the analog post-processing in order to draw a more definitive conclusion on how the two measurement setups compare.

The experimental results, besides comparing both setups, also highlight the importance of careful analog post-processing of side-channel measurements especially in the case of contactless power measurements.

ACKNOWLEDGMENT

We would like to thank Brightsight for supplying us with the test equipment. This work was supported in part by the Research Council KU Leuven: C16/15/058 and through the Horizon 2020 research and innovation programme under Cathedral ERC Advanced Grant 695305.

REFERENCES

[1] Brightsight. http://www.brightsight.com.
[2] ISO/IEC 14443, Identification cards Contactless integrated circuit cards Proximity cards, 2000.
[3] ADL5511 rectifier board. http://www.analog.com, December 2017.
[4] Zeitcontrol basic card. http://basiccard.com/, December 2017.
[5] E. Brier, C. Clavier, and F. Olivier. Correlation power analysis with a leakage model. In M. Joye and J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, volume 3156 of *LNCS*, pages 16–29. Springer, 2004.
[6] D. Carluccio, K. Lemke-Rust, and C. Paar. Electromagnetic side channel analysis of a contactless smart card: First results. In E. Oswald, editor, *RFID Security and Privacy - RFIDSec 2005*, pages 44–51, 2005.
[7] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel. Mutual information analysis. In E. Oswald and P. Rohatgi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2008*, volume 5154 of *LNCS*, pages 426–442. Springer, 2008.
[8] M. Hutter, S. Mangard, and M. Feldhofer. Power and EM attacks on passive 13.56 mhz RFID devices. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 4727 of *LNCS*, pages 320–333. Springer, 2007.
[9] T. Kasper, D. Oswald, and C. Paar. EM side-channel attacks on commercial contactless smartcards using low-cost equipment. In H. Y. Youm and M. Yung, editors, *Information Security Applications Workshop - WISA 2009*, volume 5932 of *LNCS*, pages 79–93. Springer, 2009.
[10] T. Kasper, D. Oswald, and C. Paar. Side-channel analysis of cryptographic rfids with analog demodulation. In A. Juels and C. Paar, editors, *RFID Security and Privacy - RFIDSec 2011*, volume 7055 of *LNCS*, pages 61–77. Springer, 2011.
[11] P. C. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. J. Wiener, editor, *Advances in Cryptology - CRYPTO '99*, volume 1666 of *LNCS*, pages 388–397. Springer, 1999.
[12] T. Korak and T. Plos. Applying remote side-channel analysis attacks on a security-enabled NFC tag. In E. Dawson, editor, *Topics in Cryptology - CT-RSA 2013*, volume 7779 of *LNCS*, pages 207–222. Springer, 2013.
[13] S. Mangard. Hardware countermeasures against DPA ? A statistical analysis of their effectiveness. In T. Okamoto, editor, *Topics in Cryptology - CT-RSA 2004*, volume 2964 of *LNCS*, pages 222–235. Springer, 2004.
[14] S. Mangard, E. Oswald, and T. Popp. *Power analysis attacks - Revealing the secrets of smart cards*. Springer, 2007.
[15] D. Oswald and C. Paar. Breaking mifare desfire MF3ICD40: power analysis and templates in the real world. In B. Preneel and T. Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011*, volume 6917 of *LNCS*, pages 207–222. Springer, 2011.