Side Channel Attacks on Smartphones and Embedded Devices using Standard Radio Equipment

Gabriel Goller[1]* and Georg Sigl[2]

[1] Giesecke & Devrient, Munich, Germany
gabriel.goller@gi-de.com
[2] Technische Universität München, Institute for Security in Information Technology, Munich, Germany
sigl@tum.de

Abstract. Side Channel Attacks are a powerful instrument to break cryptographic algorithms by measuring physical quantities during the execution of these algorithms on electronic devices. In this paper, the electromagnetic emanations of smartphones and embedded devices will be used to extract secret keys of public key cryptosystems. This will be done using standard radio equipment in combination with far-field antennas. While such attacks have been shown previously, the details of how to find relevant emanations and the limits of the attack remain largely unknown. Therefore, this paper will present all the required steps to find emanations of devices, implement a side channel attack exploiting ultra high frequency emanations and discuss different test setups. The result is a test setup which enables an attacker to mount a side channel attack for less than 30 Euros.

1 Introduction

Side Channel Attacks (SCA) on processors of cryptographic algorithms, which are known for more than a decade now, are a very strong measure to break cryptographic algorithms. The basic idea of all side channel attacks is to measure a physical quantity of a processor during the processing of cryptographic algorithms and then extract information about the secrets of the algorithms out of these measurements. Such quantities can be the timing [1], the power consumption [2], electromagnetic emanations or even sound [3]. While most of these attacks require the attacker to have physical access to the device for these measurements (e.g. power consumption), recently also side channels were found where the attacker can make the measurements from a certain distance (e.g.

* This work has been partly supported by the German Bundesministerium für Bildung und Forschung as part of the project SIBASE with Förderkennzeichen 01IS13020E. Responsibility for the content of this publication lies with the authors.

sound, electromagnetic emanations, time). These attacks can be mounted remotely, so that the attacked device need not be in the possession of the attacker.

A side channel which offers a lot of possibilities is the electromagnetic emanation of a device. This is especially true for modern devices, with processors that run at frequencies in the high MHz or even GHz range. At these frequencies, each signal line which carries such high frequency components can act as an antenna, and possibly emanate secrets which can then be measured using antennas or near-field probes. This can be wires connected to the processor, or even signal lines inside the processor [5].

In this paper, it shall be researched if such emanations can be measured using standard radio equipment. The sensors connected to the radio receivers are primarily far-field antennas, but also near-field probes are considered. Although primarily a smartphone will be used during the experiments, other smartphones as well as single-board computers will be examined, too.

The possibility of side channel attacks using electromagnetic radiation, or more generally the possibility that circuits emanate high-frequency signals that possibly leak secret information is already known since 1982, when the NSA TEMPEST program internally published the "NACSIM 5000" handbook [4]. This classified handbook gives advice on the design of devices which are shielded against such attacks and describes the attacks themselves. The documents were released in December 2000, which led to numerous publications in the field of side channel attacks.

In 2003, Agrawal et al. published a comprehensive paper about the possibility to use electromagnetic leakage for side channel attacks (see [5]). They evaluated the emanations of several devices, including smartcards and a PCI bus based SSL accelerator. They found emanations using near-field probes as well as a far-field log-periodic antenna. Most of these signals were on frequencies which were harmonics of the clock frequency of the evaluated devices.

Aboulkassimi et al. showed in 2011 [6] and 2013 [7] that it is possible to extract the key of an AES encryption executed on a Java-based mobile phone using an electromagnetic near-field probe. They used a differential side channel analysis approach and their attack succeeded with only 250 traces.

In 2013, Montminy et al. [8] succeeded in extracting the key of an AES encryption running on a 32-bit processor with a clock frequency of 50 MHz using a setup consisting of a near-field probe and a software defined radio. Using a differential side channel attack, they were able to extract all keybits using 100000 traces.

In 2012, Jun et al. and Kenworthy et al. introduced the possibility to attack smartphones and tablets using near-field and far-field probes in combination with radio receivers, software defined radios and oscilloscopes. They succeeded in extracting keys of RSA and ECC and showed the possibility of a differential side channel attack against AES (see [9–11]).

This paper will introduce several approaches for mounting a side channel attack using standard radio equipment with different types of test setups. The different components of the test setups are introduced in section 2, which is followed by section 3 where we explain how to find the right frequencies where signals are emanated. In section 4, a practical attack on a smartphone using a far-field antenna is implemented, evaluated and also tested with different devices. This is followed by section 5, where a very low-cost setup for mounting the presented attack is evaluated.

2 Experimental Setup

In general, the different hardware-setups used for finding emanations and conducting the attack are based on the same layout (see Fig. 1). This layout consists of an antenna/near-field probe to receive the signal, a radio device which translates the analog signals into digital samples and a laptop which is responsible for signal and data processing. This makes it possible to scan a wide range of frequencies, use different antennas or sensors for different experiments, quickly change parts of the signal processing structure and save data for later analysis.

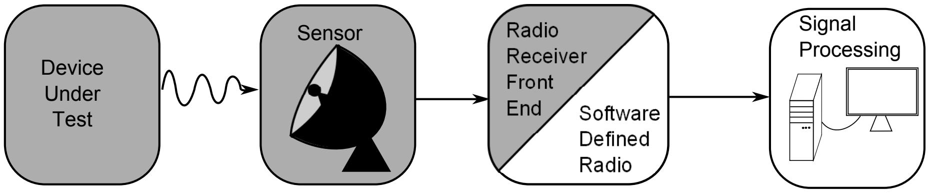

Fig. 1. Layout of the test setup (gray elements signify analog parts of the setup)

2.1 Sensors

Depending on the experiment, different antennas with different characteristics have to be used. To evaluate the emanations of the device under test (DUT), the antenna has to offer a high antenna gain over a large bandwidth, which can be achieved with a log-periodic antenna such as the HyperLOG 4025 by Aaronia AG. For the evaluation of the found emanations, the antenna should have a high antenna gain, but the bandwidth only needs to cover the found emanations. A high-gain-narrow-bandwidth antenna like a bi-quad type offer a good performance for these tasks, and can be built with very basic components.

Alternatively, near-field probes can be used to capture emanations. While the far-field antennas in general have to be specifically designed for a certain bandwidth, these probes work over a very large range of frequencies. However, they have to be placed very near to the device, and the emanations can only be measured if the probe is directly above the source. Since this paper is focused on attacks using far-field antennas and at the frequencies at which the device under test is running, a near-field probe was only used to find emanations. The probe used was a Langer ICR HV 150-27 with a frequency range from 1.5 MHz to 6 GHz.

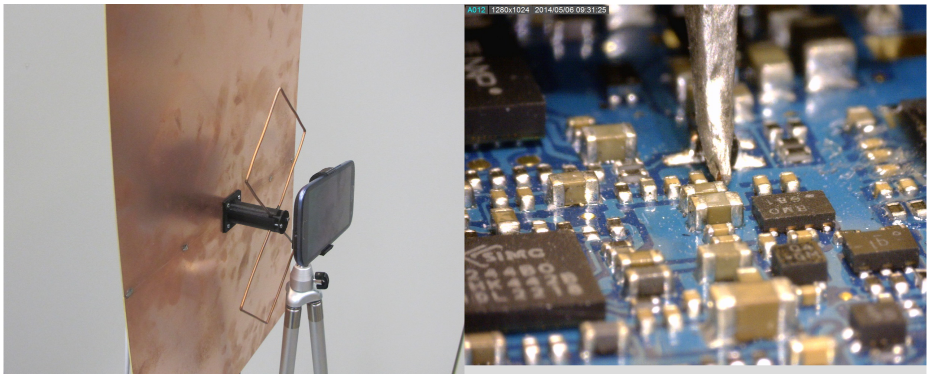

Fig. 2. Different sensors: Bi-Quad Antenna and Langer ICR HV 150-27

2.2 Radio Device

There are two devices responsible for the radio reception, an analog radio receiver and a software defined radio (SDR). A SDR is a radio device where most of the signal processing is done using digital algorithms rather than analog filters. By combining it with a high-end analog radio receiver, the advantages of both systems can be taken. For the analog part, a ESN test receiver by Rohde & Schwarz was used. It offers a frequency range from 9 kHz to 1 GHz and tools to analyze the signals within this spectrum. To combine this receiver with a digital signal processing system, a USRP N210 software defined radio was connected to the IF output of this receiver. The N210 is able to sample an analog signal with 100 MSps with a resolution of 14 Bit. With this measuring system, the high bandwidth of the test receiver can be combined with the advantages of a digital signal processing system. To further increase the signal strength, a PA 303 30 dB preamplifier from Langer was inserted between the antenna and the test receiver.

An alternative reception system (presented and only used in section 5) uses a standard DVB-T stick from Gixa Technology as an alternative to the ESN, the USRP and the preamplifier from above, which drastically reduces the price as well as the size of the measuring equipment, even compared to a setup for measuring power consumption. Furthermore, since no alteration of the hardware of the DUT is required and most of the signal processing is happening in software, it is possible to mount an attack even with little knowledge about hardware designs or measurement engineering. Internally, the DVB-T stick consists of two chips which roughly do the same job as the ESN radio receiver and the USRP software defined radio. A R820T chip by Rafael Microelectronic is used to tune in and downconvert a radio signal, which is then converted to a digital I/Q signal by a RTL2832U chip by Realtek. There exist numerous DVB-T sticks with this hardware combination, and a list of compatible sticks can be found at the project website [15].

Both systems can be seen in Fig. 3, which also shows the far smaller size of the DVB-T stick compared to the ESN-USRP combination.

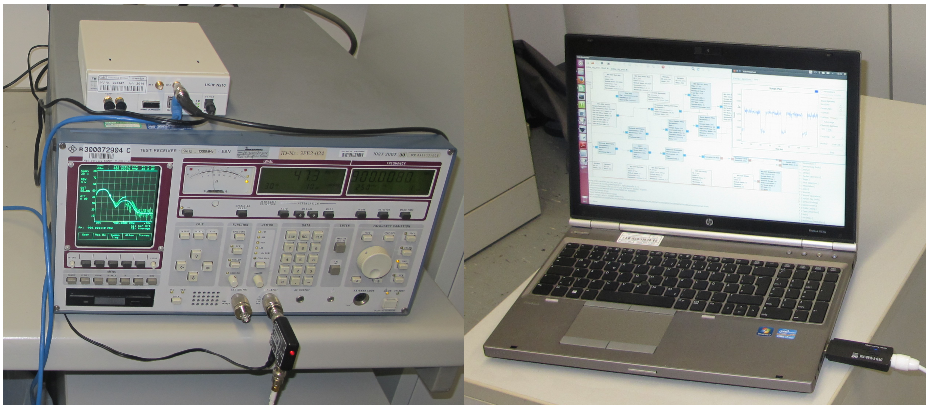

Fig. 3. ESN test receiver with USRP N210 and preamplifier (left), compared to the DVB-T stick (plugged into Laptop, right)

2.3 Software Components

To process the digital signals, the open source software GNU Radio was used. This makes it possible to test whether relevant signals are emanated, be it directly or in a modulated way. Further processing was done using GNU Octave, an open source tool for numerical computations [12].

2.4 Device under Test (DUT)

Though in section 4.4 several other devices will be examined, the primary research was conducted on an Android-based smartphone. The only alteration of the hardware was to remove a shielding plate above the main circuit to make it easier to find and measure emanations (see Fig. 4). However, in section 4.3 the attack will also be tested with the shielding plate. Software-wise, the system was rooted to be able to influence the CPU clock frequency. The app which computes the cryptographic algorithms was written in Java, with the cryptographic parts written in C using the Android Native Development Kit.

Positioning of Near-field Probes To get good results with the near-field probes, the probe has to be near the source of the emanations. Therefore the first step is to find a position where emanations take place. Such a position can be found by connecting the probe to a oscilloscope, then produce a processor load and change the position of the probe until a signal is received. By doing this, a position was found directly above a capacitor next to the main CPU where a signal is emitted by the smartphone (see Fig. 4).

2.5 Software on DUT

To evaluate the possibility of a side channel attack, a square and multiply algorithm was implemented on the device. This algorithm, which is one of the

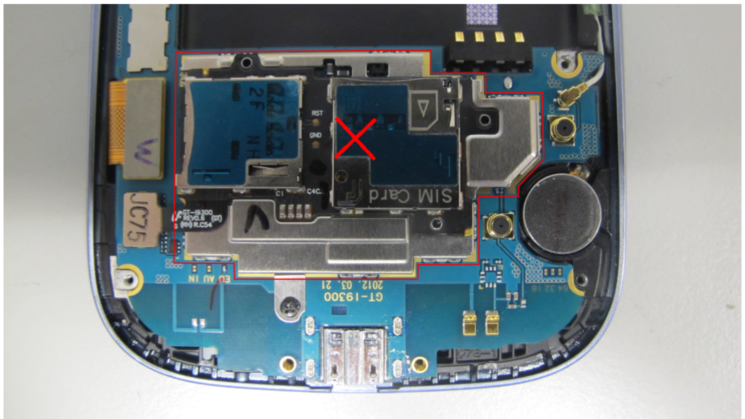

Fig. 4. DUT, with shielding plate (red frame) and position where the near-field probe captured signals (red cross).

standard algorithms for implementations of RSA, can be used to calculate the result of the equation

$$m = c^d \bmod N, \tag{1}$$

with m being the decrypted message, c the encrypted message, d the secret key and N a publicly known integer. The algorithm can be described by the following pseudo-code:

```
function square-and-multiply(Number c, Integer d, Modulus N)
    result = 1
    for each bit(d) from (number_of_bits(d) - 1) downto 0
        result = square(result) mod N //square operation
        if bit(d) == 1
            result = (c * result) mod N //multiply operation
        end if
    end for
    return result
end function
```

For the implementation, the OpenSSL library was used. This was done in such a way that the algorithm itself was a custom C implementation, but the square and the multiply operations were taken from the OpenSSL library.

3 Emanations of Smartphones

The first challenge when trying to implement a side channel attack is to find appropriate signals which contain information correlated to the activity of the processor of the device. This can be very difficult when the sensor is a far-field antenna, because there are many other signals caused by terrestrial radio stations, such as mobile phone networks, DVB-T and others. Therefore, it is easier to use a near-field probe as a sensor to find the emanations of a device. During research, 3 approaches to find the relevant frequencies where the smartphone emanates signals were developed, one using an antenna, one using a near-field-probe and one by making an educated guess.

The first approach was done with a wide-band antenna and consists of filtering the external disturbances from the signal, so that only the signals emanated by the DUT remain. The idea is that the signal s measured by the antenna at a certain frequency consists of two components: The signals emanated by the DUT s_{DUT} and the signal emanated by other sources s_{others}, which can be written as

$$s = s_{\text{DUT}} + s_{\text{others}}. \tag{2}$$

In this equation, s and s_{others} can be measured by measuring two times in a row, one time with and one time without the DUT enabled. That way, s_{DUT} can be calculated by computing

$$s_{\text{DUT}} = s - s_{\text{others}}. \tag{3}$$

While it is not possible to filter all the external signals using this system, because s_{others} is not constant, the search space is reduced to a few frequencies at which the DUT possibly emanates signals, which can then be checked manually. The results of this approach for a frequency range from 400 MHz to 1 GHz can be seen in Fig. 5.

The second approach is done by measuring with a small near-field probe directly above the main processor. The near-field probe is not affected by the disturbing radio signals, and thus the measured signals are directly emanated by the smartphone. Since the emanations found by the near-field probe are only magnetic fields, it is necessary to check in a second step whether the emanations can also be measured with the far-field antenna. During this experiment, the clock frequency of the smartphone was set to a fixed frequency of 900 MHz. As it can be seen in Fig. 6, at this frequency signals were emanated by the device.

The third approach is done by making an educated guess to find the relevant frequencies. This can be done without any sensors by studying the manual of the device to find out which clock frequencies exist. Since the emanations are caused by coupling of high frequency signal generators with other parts of the circuit [4], there is a high probability that there are signals emanated on the frequencies used by the active high-frequency elements of a smartphone, e.g. clock generators.

Using these 3 approaches, several signals emanated by the smartphone were found. These signals could be categorized into signals emanated by the main processor and, far stronger, signals emanated by the display. The signals emanated by the display are only measurable when the touchscreen is turned on, while the signals emanated by the main processor can be always measured when the processor is doing work. However, to be able to capture the processor signals, the smartphone has to be configured so that the CPU clock is kept at a distinct rate, because otherwise the frequency is changed depending on the workload. This is also the reason why the far-field antenna did not receive a signal at

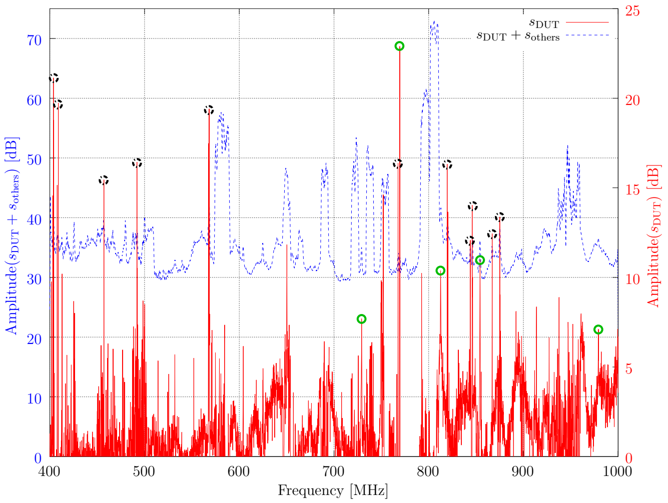

Fig. 5. Results of the antenna measurements: Received signal strength of the DUT and disturbances (blue, dashed line), calculated emanations of only the DUT (red, solid line). Signals really emanated by the DUT are marked with a green circle, false positives are marked with a dashed black circle

900 MHz, because during this experiment the device was not running at a fixed clock frequency.

4 Side Channel Attack using Far-Field-Antennas

4.1 Correlation to Computations

To successfully mount a side channel attack, it is crucial to find out which of the signals contain information about the main processor. To do this, during the measurements, a periodical workload is executed. This way, if there is a correlation of the processor load with the signals, the emanations should also contain a periodical component. Doing this, the two categories of signals were analyzed, which led to two different results.

It is not possible to extract information of the main processor from the signals emanated by the display. However, these signals contain information about changes in the display content and the state of touchscreen. In a first experiment, it was possible to measure the blinking of a cursor and the signal when a finger touches the display from a distance as far as 3 m. However, since the focus of this paper are side channel attacks on cryptographic algorithms, these signals were not further considered.

The emanations of the main processor however are correlated with the data and instructions processed there. Every time the processor is working, the am-

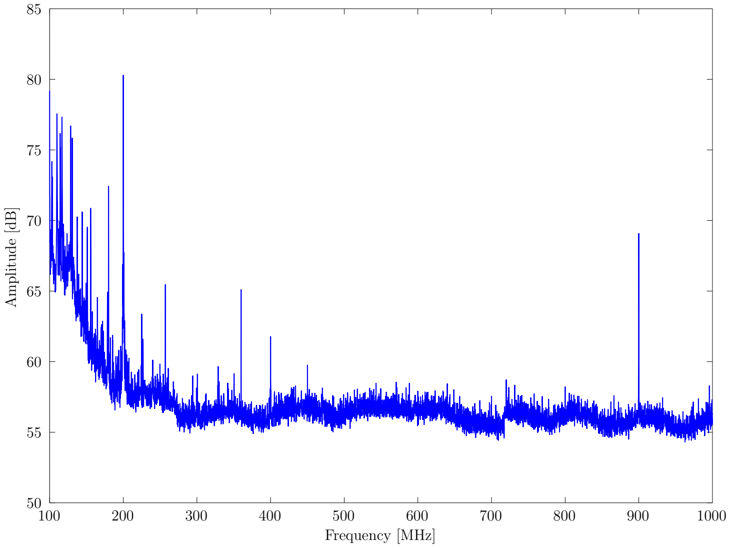

Fig. 6. Results of the near-field measurements: Emanations on several frequencies, especially 900 MHz, the CPU clock frequency.

plitude of the signals is higher than in an idle mode, where the amplitude goes down to nearly zero (e.g. during the call of the standard C-function "sleep()"). To check if this behavior can be used for a side channel attack, the signal was evaluated during the execution of the Square-and-Multiply algorithm from section 2.

4.2 Square-and-Multiply algorithm

Using OpenSSL, a Square-and-Multiply algorithm was implemented. If it is possible to distinguish square and multiply operations, the secret exponent d can be extracted during calculation of Equ. 1.

By isolating the single operations from each other with a *sleep()*-function, it can be checked if they cause different signals and can be distinguished that way. As it can be seen in Fig. 7, this is not the case. The operations can not be distinguished on first sight, and further investigations showed that this is not even possible by using statistical tools like the cross-correlation of the signal. This is probably due to the low sampling rate and the low signal-to-noise ratio.

When the *sleep()*-functions are removed, the single signals of the operations melt into a big block with a high amplitude, and thus the operations can neither be seen nor distinguished in the final signal. However, this can be improved by a common technique from the field of signal processing, which is to record the same signal several times in a row and then compute the average of these recorded signals [13, page 367]. This way, it is possible to extract the key, because the

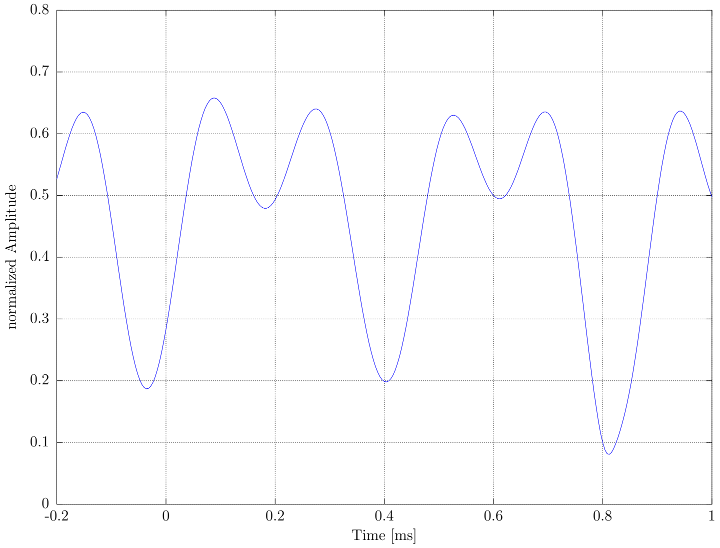

Fig. 7. A square (0–0.4 ms) and a multiply (0.4–0.8 ms) operation, not distinguishable.

signal of a 1-bit (square and multiply) can be distinguished from the calculation of a 0-bit (square only). This can also be seen in Fig. 8.

4.3 Evaluation of Attack

After proving that an attack using a far-field antenna is possible, a few parameters of the attack shall be evaluated here.

Number of Traces. Since for a successful attack it is necessary to average several traces (with a single trace being the recorded curve of a single execution of the algorithm), it is convenient to find the minimal number of traces for a successful attack. The challenge is however that the result of the attack is not computed by an algorithm, but by a human which interprets the results, which is highly subjective. To find an objective measure for the minimum number of traces, a property of the averaging was used. Since the average of many traces converges to a unique solution where the keybits can be extracted, an objective measure is to compare the average of i traces with the converged solution, and then see how much alike the curves are. A tool for such an analysis is the correlation coefficient, which can be used to compare two digital waveforms x and y with each other. It is defined as

$$\mathrm{corr}(x,y) = \frac{\mathrm{cov}(x,y)}{\mathrm{std}(x)\mathrm{std}(y)}, \tag{4}$$

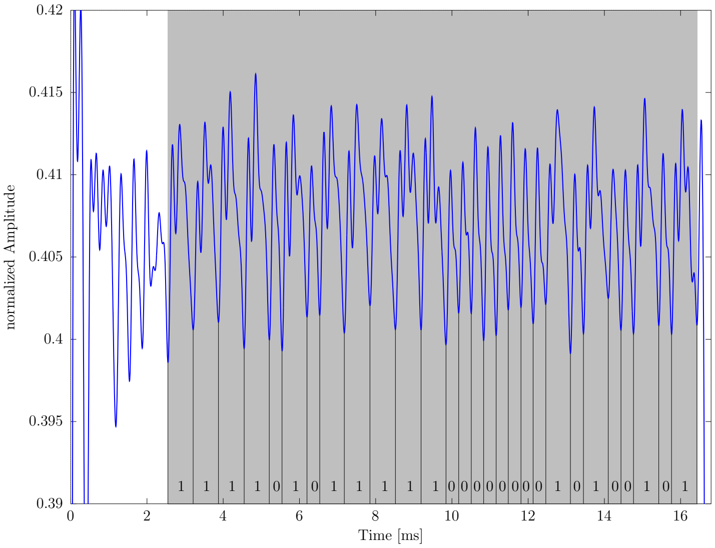

Fig. 8. Average of 1063 traces of a Square-and-Multiply algorithm (execution marked gray, key: 1010 0101 0000 0000 1111 1010 1111, computed backwards).

where x and y are the waveforms to compare, $\operatorname{std}(\cdot)$ is the standard deviation and $\operatorname{cov}(x, y)$ is the sample covariance of the waveforms x and y defined as

$$\operatorname{cov}(x, y) = \frac{1}{n-1} \sum_{j=1}^{n} (x_j - \mu_x)(y_j - \mu_y), \tag{5}$$

with μ as the mean value of a waveform, x_j and y_j as the j–th element of the waveforms x and y and n as the total number of elements of the waveforms. Using these definitions, the following formula was used to calculate the correlation between the average of $i = 1 \ldots q$ traces t_i with the converged solution, which is the average of q traces:

$$y(i) = \operatorname{corr}(\operatorname{mean}(t_1, t_2, \ldots, t_i), \operatorname{mean}(t_1, t_2, \ldots, t_q)). \tag{6}$$

$\operatorname{mean}(\cdot)$ computes the average curve c of multiple traces t. Each point c_j of the curve c is defined by

$$c_j = \frac{1}{i} \sum_{p=1}^{i} t_{p,j} \tag{7}$$

with $t_{p,j}$ being the j-th element of the p-th trace t_p.

As it can be seen in Fig. 9, the correlation is already higher than 0.999 when more than 170 traces are averaged. This means that with 170 traces it should still be possible to extract the key, which was also confirmed by experimental results.

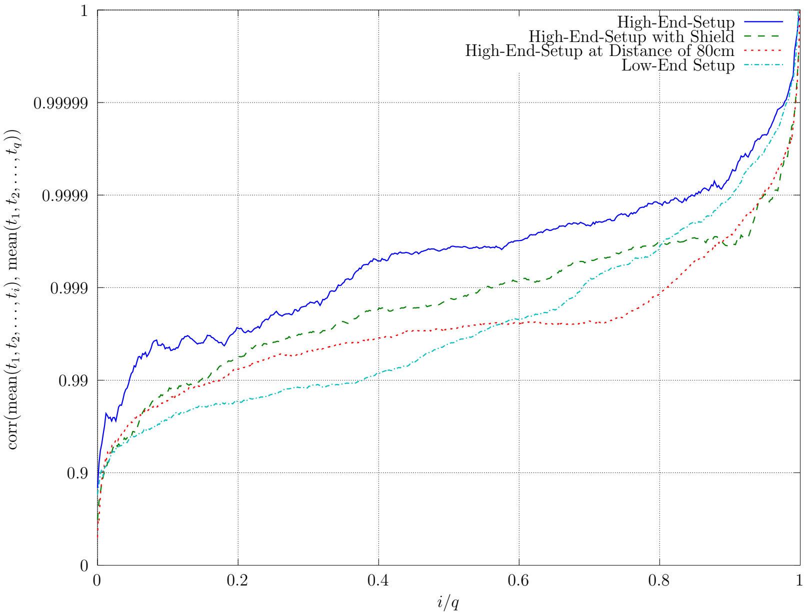

Fig. 9. Correlation of the average of i traces with the average of q traces ($q = 1894$ for high-end setup at distance of 80 cm and $q = 500$ for the other experiments.)

Maximum Distance. So far, the device was placed directly in front of the antenna. Increasing the distance decreases the quality of the signal in several ways. Obviously, the amplitude of the signal is reduced, which worsens the signal-to-noise ratio. Subsequently, the synchronization of the traces gets more difficult, which means that more traces are needed and even with more traces, it is harder to identify the different operations in the signal. However, it is still possible to extract the key from a distance of 80 cm using 1894 traces, but it is very hard to identify the different operations, even when comparing the curve with the result of the attack from a distance of 2 cm (see Fig. 10). As it can be seen in Fig. 9, when applying the correlation experiment from above to the data acquired at a distance of 80 cm, the average of 1530 traces is needed to get a correlation of 0.999 with the average curve of the 1894 traces shown in Fig. 10.

Shielding Plate In the factory state the smartphone is equipped with a shielding plate which resides directly above the main circuits of the device. Since this does decrease the emanations of the device, it was removed so far. When putting it back into the device, the results are comparable to increasing the distance. The amplitude drops, resulting in a lower signal-to-noise ratio and thus requiring more traces than before. However, it was still possible to extract the secret of a Square-and-Multiply algorithm by averaging multiple curves. The maximum distance with the shielding plate is however drastically reduced, so that the an-

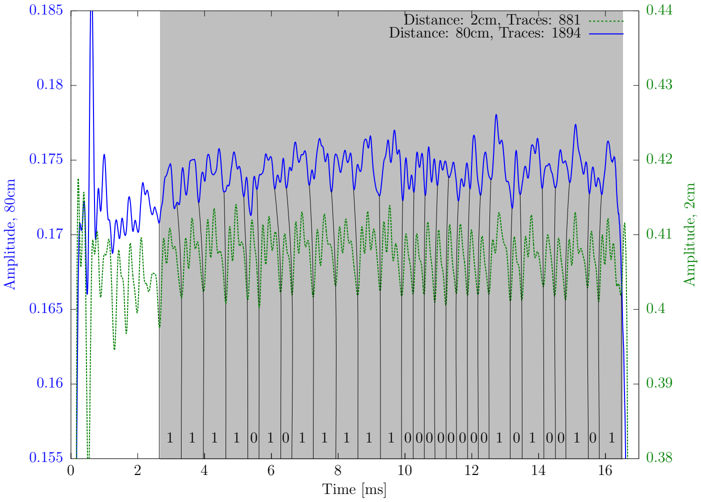

Fig. 10. Average of 1894 traces recorded at a distance of 80 cm.

tenna has to be directly next to the device during the attack. When applying the correlation experiment from above to 500 traces collected with the shielding plate installed and the antenna at a distance of 2 cm, it takes the average of 276 traces instead of 170 to reach a correlation of 0.999.

4.4 Other Devices

At first, the research was only conducted with a single smartphone. Since many more devices are based on the same processor architecture, it could well be that all these devices are vulnerable to the attack. Therefore, it was tested with different devices, not only in the area of smartphones, but also on single board computers. The results were that on all tested devices (3 smartphones and 2 single board computers) emanations were measurable at the clock frequency, and the attack could be performed successfully. While it was necessary to remove a shielding plate on two of the smartphones, this was not the case for one smartphone. Because the attack can also be mounted on single-board computers like the Raspberry Pi or the BeagleBone Black, it is unlikely that the phone-specific circuits (e.g. the antennas) are the reason for the emanations. Altogether, the results suggest that the emanations are not caused by an individual flaw in the circuit- or processor-design and could possibly affect many more devices.

5 A low-cost setup for EM analysis

Recently, a cheap alternative to radio receivers was introduced by making it possible to use DVB-T sticks as Software Defined Radios [15]. The sticks that can be used for this purpose offer a frequency range between 24 and 1850 MHz, a sampling rate of up to 2.5 MSps and a resolution of 8 Bit. While this is well below the parameters of the USRP, a working system could reduce the parts needed to mount the attack to only an own-built bi-quad antenna and a DVB-T stick, with total costs well below 30 Euros. Because of this, the attack was implemented with this setup as well.

5.1 Reproduction of the Far-Field Attack

The primary goal is to find out whether the DVB-T stick can compete with the performance of the system from above. The results are very promising: The attack works just like the attack with the system consisting of USRP and test receiver, however there are a few drawbacks.

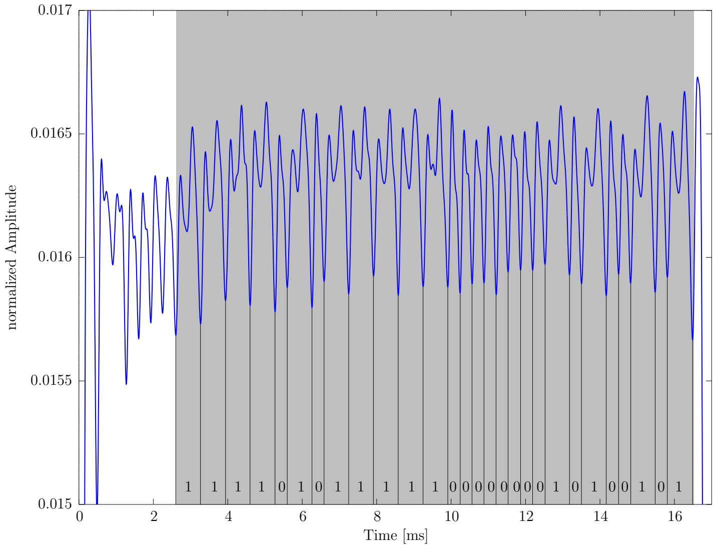

Fig. 11. Average of 1228 traces of a Square-and-Multiply algorithm recorded with a DVB-T stick (execution marked gray, key: 1010 0101 0000 0000 1111 1010 1111, computed backwards).

Quality of the signal The quality of the signal is drastically reduced. Although both signals are normalized (which means that the amplitude is between 0 and 1), the signal is one magnitude smaller (0.4 vs. 0.016) than with the high-end setup. However, the amplitude of the noise is also much smaller when measuring with the DVB-T stick compared to the setup from above (see Fig. 11). To compare both measurements, the amplitude of a signal has to be compared with the amplitude of the noise, which can be done by computing the signal-to-noise ratio [16]. It can be estimated as

$$\mathrm{SNR}_{\mathrm{dB}} = 20 \log_{10}\left(\frac{A_{\mathrm{signal}}}{A_{\mathrm{noise}}}\right), \tag{8}$$

where A_{noise} and A_{signal} are the root mean square amplitudes of the signal and the noise, respectively. This gives 11.82 dB for the DVB-T stick and 13.94 dB for the high-end system. This suggests that the low-end setup is not performing as bad as the small amplitude of the signal would suggest. The best comparison of the two systems however is the number of traces needed for a successful attack. Using the correlation technique from section 4.3, the DVB-T stick can be compared to the system from above, which can be seen in Fig. 9. As it can be seen, to get the same correlation as above (0.999), twice as many curves are needed (346 vs. 170).

Maximum Distance Another drawback is that the maximum distance is reduced due to the bad signal. Instead of 80 cm maximum distance with the other system, the low-cost system is not able to receive a signal when the distance is larger than ∼10 cm. Altogether, for the far-field attack the system does not perform as well as the original system, but the reduction of costs makes it a very good alternative, especially when the number of traces and the distance is not of vital importance.

6 Summary

In this paper, the already existing results on side-channel attacks on smartphones and embedded devices using electromagnetic emanations were further researched. This includes all parts of the experiment, starting with the search for emanated signals, continuing with the description and evaluation of the possible attacks and concluding with the development of a very low-cost test setup. It was shown that using a far-field antenna, it is possible to extract the secret key of a Square-and-Multiply algorithm by averaging several traces. While a lower distance is advantageous, the attack can also be conducted from a distance much larger than it is possible with the state of the art near-field probes. Finally, a very low-cost setup was implemented, which makes it possible to mount the attack with costs lower than 30 Euros, using a DVB-T stick and a self-built antenna. This enables even attackers with a very small budget to attack smartphones and embedded devices. The results of this paper show that hardware and software countermeasures have to be implemented in smartphones and embedded devices, or secure elements should be used for these cryptographic computations, especially since devices like smartphones and single-board computers tend to be used for more and more applications where security is vital, e.g. payment applications (smartphones) or industrial applications (embedded single-board computers).

References

1. Kocher, P.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Advances in Cryptology–CRYPTO'96, p. 104–113. Springer, 1996.
2. Kocher, P., Jaffe, J., and Jun, B.: Differential power analysis. In: Advances in Cryptology–CRYPTO'99. Springer Berlin Heidelberg, 1999.
3. Genkin, D., Shamir, A., and Tromer, E.: RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. IACR Cryptology ePrint Archive 2013 (2013): 857.
4. National Security Agency: NACSIM 5000 Tempest Fundamentals. Partially released in 12/2000, February 1982.
5. Agrawal, D., Archambeault, B., Rao, J., and Rohatgi, P.: The EM Side-Channel(s). In: Cryptographic Hardware and Embedded Systems-CHES 2002, pp. 29–45. Springer, 2003.
6. Aboulkassimi, D., Agoyan, M., Freund, L., Fournier, J., Robisson, B., and Tria, A.: Electromagnetic Analysis (EMA) of Software AES on Java Mobile Phones. In: Information Forensics and Security (WIFS), 2011 IEEE International Workshop on, pp. 1–6. IEEE (2011).
7. Aboulkassimi, D., Fournier, J., Freund, L., Robisson, B., and Tria, A.: EMA as a Physical Method for Extracting Secret Data from Mobile Phones. In: International Journal of Computer Science and Application (IJCSA) (2013).
8. Montminy, D., Baldwin, R., Temple, M., and Oxley, M.: Differential Electromagnetic Attacks on a 32-bit Microprocessor using Software Defined Radios. In: Information Forensics and Security, IEEE Transactions on , vol.8, no.12, pp. 2101–2114. IEEE (2013).
9. Kenworthy, G. and Rohatgi P.: Mobile device security: The case for side channel resistance. In: Proceedings of the 2012 Mobile Security Technologies Conference, California, USA (2012).
10. Jun B. and Kenworthy G.: Is your mobile device radiating keys? Presentation, held at RSA Conference (2012).
11. Kenworthy G. and Rohatgi P.: Mobile device security: The case for side channel resistance. Presentation, held at Mobile Security Technologies Workshop (2012).
12. Eaton, J., Bateman, D., Hauberg S., and Wehbring R.: GNU Octave Free Your Numbers, edition 3 for octave version 3.8.0 edition. (2011).
13. Swanson, D.C.: Signal Processing for Intelligent Sensor Systems with MATLAB, Second Edition. Taylor & Francis (2012).
14. The OpenSSL Project: OpenSSL: The Open Source Toolkit for SSL/TLS, `http://www.openssl.org` . Retrieved on: December 2014.
15. rtlsdr.org Wiki, `http://rtlsdr.org`. Retrieved on: December 2014.
16. Johnson, D.H.: Signal-to-noise ratio. In: Scholarpedia, 1(12):2088 (2006).