Differential Power Analysis Attack on ARM based AES Implementation without Explicit Synchronization

Martin Petrvalsky, Milos Drutarovsky
Dept. of Electronics and Multimedia Communications
Technical University of Kosice
Kosice, Slovakia
Email: {martin.petrvalsky,milos.drutarovsky}@tuke.sk

Michal Varchola
Dept. of Electronics and Multimedia Communications
Technical University of Kosice
ELIT SYSTEMS, s. r. o.
Kosice, Slovakia
Email: michal@varchola.com

***Abstract*—This paper presents Differential Power Analysis (DPA) attack on 32-bit ARM Cortex-M3 microprocessor. Attacked algorithm is unprotected Advanced Encryption Standard (AES) with 128-bit key. DPA attack is deployed on the ARM processor by measuring its instantaneous power consumption during encryption algorithm. Analyzed power consumption traces obtained from the measurement are out-of-sync as they would be during the realistic DPA attack without using trigger to synchronize the traces. Unaligned traces or regular methods of static alignment are inappropriate for further analysis. In this paper elastic alignment methods are used for the trace synchronization. Dynamic Time Warping (DTW) and its fast algorithm FastDTW are deployed in order to match similar patterns in reference and misaligned power consumption traces. Output of DTW - optimal path is then used for the alignment process. Aligned traces are used for further processing and evaluation of the DPA attack. The result is successful DPA attack on misaligned power consumption traces and recovery of the secret 128-bit key. Results are comparable with DPA attack using trigger to align power traces during measurement.**

Keywords*—*Differential Power Analysis, ARM processor, AES, elastic alignment, Dynamic Time Warping

I. Introduction

Differential Power Analysis (DPA) attack [1] was published in 1999 [2]. Nowadays, it still poses a threat for cryptographic devices. It is common side-channel attack. Multiple power consumption traces are required for successful attack. The traces are measured during execution of cryptographic algorithms. Afterwards they are used for correlation analysis. The data analysis needs to have the power consumption samples of corresponding data operations aligned.

Preparation of DPA laboratory [3] for new further research in field of the side-channel attacks leads us to solve realistic scenario of DPA implementation. The scenario does not use explicit synchronization of traces. In [4] we presented attack on 8051-based microcontroller using synchronization impulse during measurement. In this paper we present successful DPA attack on ARM Cortex-M3 microprocessor without embedded synchronization signal. Our contribution is the usage of elastic alignment to solve problems connected to realistic scenario.

Synchronization of the traces is often achieved by using an auxiliary trigger signal embedded in cryptographic algorithm. In real scenario of DPA application, the trigger signal can not be deployed. Misalignment of traces measured without triggering can be caused by different start time of the measurement (can be triggered only by sending input data), by jitter of the oscillator [5] which provides clock for the cryptographic device, by various execution time of processor instructions which depend on input data (e.g. SMULL operation for ARM Cortex-M3 [6]) or it can be done intentionally as DPA countermeasure [7], [8] by inserting random delay while executing cryptographic algorithm.

There are two main approaches in power trace alignment. First is static alignment proposed in [9]. It finds a reference samples (e.g. rising edge) in measured power consumption traces and matches the same references by shifting the traces. The second approach is elastic alignment [10], [11], [12] which uses linear resampling of the traces. Elastic alignment is more efficient method than static alignment. On the other hand, it requires more computational power. One of the approach of elastic alignment is DTW [13] which is widely used in speech recognition [14].

The paper is organized as follows. Brief information about DPA attack will be provided in section II. In section III, the measurement setup and hardware will be introduced. The results will be presented in section IV and the last section V is dedicated to conclusion of this paper.

II. Attack specification

A. Vulnerable part of AES

Advanced Encryption Standard (AES) [15] is widely used algorithm in embedded cryptographic applications with symmetric key. It consists of rounds which number depends on the key size. Each round is composed by four steps:

1) SubBytes
2) ShiftRows
3) MixColumns
4) AddRoundKey

AES algorithm is typically attacked on first or last round of the encryption. We choose byte substitution operation (SubBytes) of the first round. SubBytes is often implemented using a lookup table which consists of 256 byte elements. Reading

978-1-4799-3715-8/14/$31.00

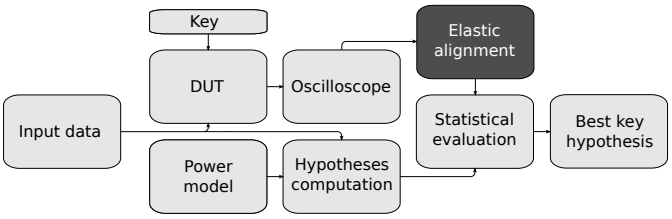

Figure 1. Diagram of DPA attack. It has two branches. The upper one represents measurement of the power consumption. New block of the workflow is elastic alignment which allows DPA attack without explicit synchronization. The lower branch illustrates creation of the consumption hypothesis. The final block compares measured traces with hypothesis. Hypothesis with the highest correlation leads us to secret key.

from this table leaks information into the side channel - in our case it is instantaneous power consumption. Thereafter, this leaked information during first SubBytes is used to perform DPA attack.

B. DPA principles

DPA attack works in three basic steps. Full workflow of DPA is depicted in Fig. 1. Firstly, attacker sends set of known data to Device Under Test (DUT) and measures instantaneous power consumption while the device is performing cryptographic algorithm. Secondly, attacker creates hypothesis of power consumption for all possible key parts (usually bytes) using input data from the first step. Finally, the hypothesis which has the highest correlation with measured power consumption can lead to the secret key - for statistical evaluation we use Eq. (1)

$$r_{H,T}(n) = \frac{\sum_{i=1}^{numt} [(T_i(n) - \bar{T}(n))(H_i - \bar{H})]}{\sqrt{\sum_{i=1}^{numt} [T_i(n) - \bar{T}(n)]^2 \sum_{i=1}^{numt} (H_i - \bar{H})^2}} \quad (1)$$

where $r_{H,T}(n)$ is Pearson's correlation coefficient for n-th sample (measured during execution of cryptographic algorithm), $numt$ is number of measured traces, $T_i(n)$ is value of n-th sample measured during i-th measurement (i-th trace), $\bar{T}(n)$ is mean value of corresponding n-th samples (from all traces), H_i is hypothesis of power consumption for one value of input data corresponding with i-th measurement (i-th trace) and $\bar{H}$ is mean value of all hypotheses H_i.

III. Workbench description

A. Attacked hardware

The chosen target for the DPA attack is microcontroller STM32F103 (STM32 family [16]) with 32-bit ARM Cortex-M3 core [6]. It uses a 8 MHz crystal with on-chip PLL generating core clock up to 72 MHz. Selected features are:

- Instruction set Thumb2
- 20 kB RAM, 128 kB Flash
- ADC, USB, RTC, USART, 7 timers, ...

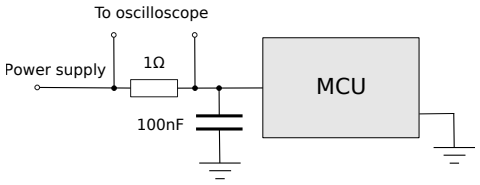

Figure 2. Measurement point uses common way to measure power consumption. It measures voltage drop on resistor inserted in power supply branch. The voltage drop can be measured using two channels of oscilloscope or with a differential probe.

The STM microcontroller is fitted on the custom evaluation board. This board is equipped with serial port connector for sending and receiving data. It also has prepared various measure points with SMA connectors for oscilloscope probes in order to measure power consumption traces. For purposes of this paper we used measurement point depicted in Fig. 2.

B. Measurement setup

The main part of the workplace is an oscilloscope Agilent Technologies DSO9404A [17]. It is a combination of oscilloscope and PC. The main features are:

- 4 analog channels, 4 GHz @ 50Ω, 500 MHz @ 1MΩ
- Max F_s - 20 GS/s, 500 MHz probes Agilent N2873A
- Vertical resolution 8 bits, ≥12 bits with averaging
- PC - 1.7 GHz CPU, 2 GB RAM, 250 GB HDD

We take all measurements with 2 GS/s sampling frequency (2 GHz is more than sufficient in order to test filtering and resampling). Probes are connected to SMA connectors on the evaluation board. Power consumption traces acquisition is described in Fig. 3. Process of measurement is controlled through VISA interface by custom software which runs on PC (in oscilloscope or external PC). It sends input data to the board, receives acknowledgment from the board and controls how the oscilloscope measures and stores the power consumption traces. We use set of 1000 traces. These traces are ready for further processing.

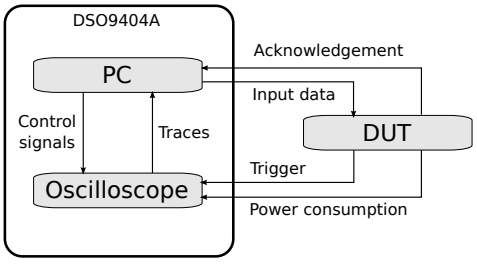

Figure 3. Workflow of the workplace. Oscilloscope Agilent Technologies DSO9404A is used for measurements. It also contains PC which runs software that controls the whole process. First it initializes oscilloscope and then input data are transfered to DUT through UART. DUT rises trigger (optional) and starts ciphering the data. Oscilloscope measures power consumption during that process. When finished, PC sends command to store measured power consumption trace to hard disk. Depending on desired number of traces, we repeat the measurement process.

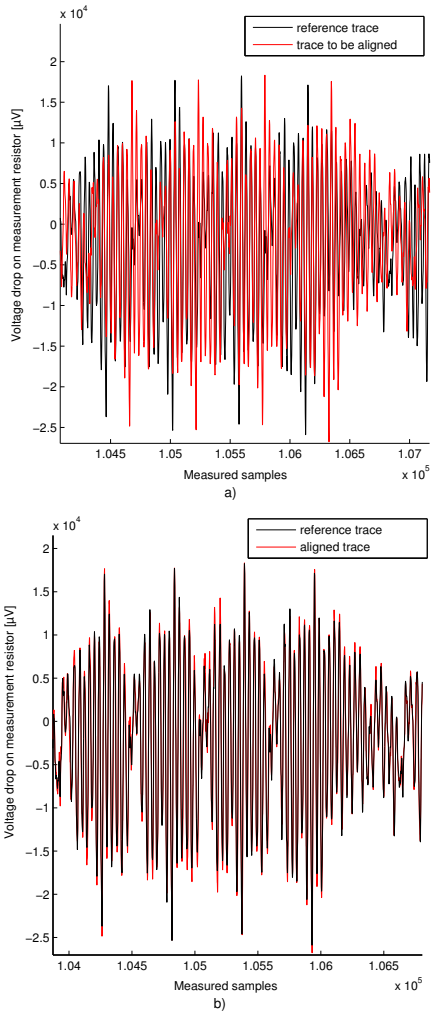

Figure 4. Comparison of misaligned traces on figure a) and aligned traces needed for successful DPA attack - figure b). Traces was measured on Cortex-M3 based microcontroller STM32F103 with core clock 72 MHz. We used 2 GS/s sampling frequency. Misalignment was achieved by special implementation of CRC code. Alignment was done by FastDTW algorithm.

IV. Experimental results

First step is trace filtering. Bands around core frequency and its harmonic components contain the most of information leaking from microprocessor [18]. For our purpose low-pass filter with cutoff frequency 300 MHz is sufficient (core clock frequency, 1st, 2nd, 3rd and 4th harmonic components). There is no significant additional information in higher frequency spectrum.

In realistic attack the traces are misaligned as shown in Fig. 4. During our measurement we simulate attack without explicit synchronization by using operations with various time duration (special implementation of CRC algorithm). We use auxiliary trigger signal generated by MCU before execution of CRC in order to have traces synchronized prior to simulated misalignment (we have common point to observe delays for each measurement). This implementation simulates misalignment caused by oscillator jitter, measurement without trigger and random delay insertion countermeasure.

Second step after filtering is trace alignment. Static alignment are insufficient for real scenario attack so we chose elastic alignment - Dynamic Time Warping (DTW) algorithm (Fig. 5). Each of the measured traces consists of 150,000 samples (75 μs @ 2 GS/s - 5,400 instruction cycles @ 72 MHz core frequency). Using regular algorithm of DTW is infeasible with such high amount of samples (22.5 GB RAM used, time for one trace alignment on Intel Core i7 CPU - 4 hours). We chose FastDTW [19] algorithm for more effective calculations.

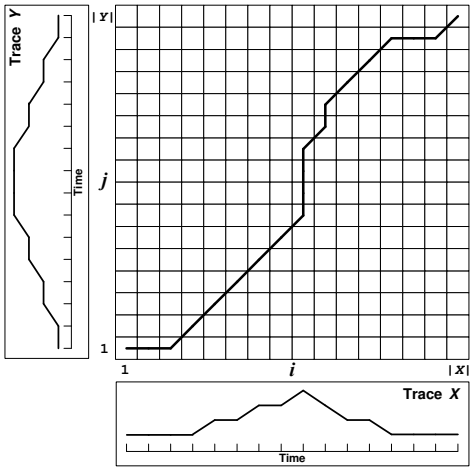

Figure 5. Principle of DTW algorithm. In first step it constructs cost matrix (differences between reference trace X and misaligned trace Y). Then it searches for the shortest path in the cost matrix. The results of DTW are length of the shortest path (used in speech recognition) and its coordinates (used for our purpose - trace alignment).

Last step is a correlation analysis of the filtered and aligned traces based on Pearson correlation coefficient. We gathered results from two measurements. First measurement was done by using simulation of realistic attack. Second measurement was common way of attack with trigger impulse placed near attacked instruction and without trace alignment. Comparison of results of the analysis can be found in Fig. 6.

V. Conclusion

In this paper we presented method of DPA attack on first SubByte operation of AES algorithm. We used microcontroller STM32F103 as attacked device. The main contribution is proposed method of trace alignment using elastic alignment based on DTW algorithm. The method we use is applied for attacks without explicit synchronization of the measurement which is often case in real application of DPA attack. Deployment of DTW algorithm in trace alignment can also be used for traces misaligned by jitter or countermeasures as mentioned in [13].

Our implementation of the synchronizing of misaligned traces (as shown in Fig. 6) is comparable with implementation with explicit synchronization. The resulting values of correlation coefficients for correct and also for wrong hypotheses are about same level. This fact allows us using further steps of analysis as in implementation with regular trigger. The last outcome is the amount of traces needed for successful attack on ARM Cortex-M3 microprocessor. Proposed attack needs only 40 traces for correct key extraction.

The results presented in this paper are important for future research in which we want to focus on different cryptographic

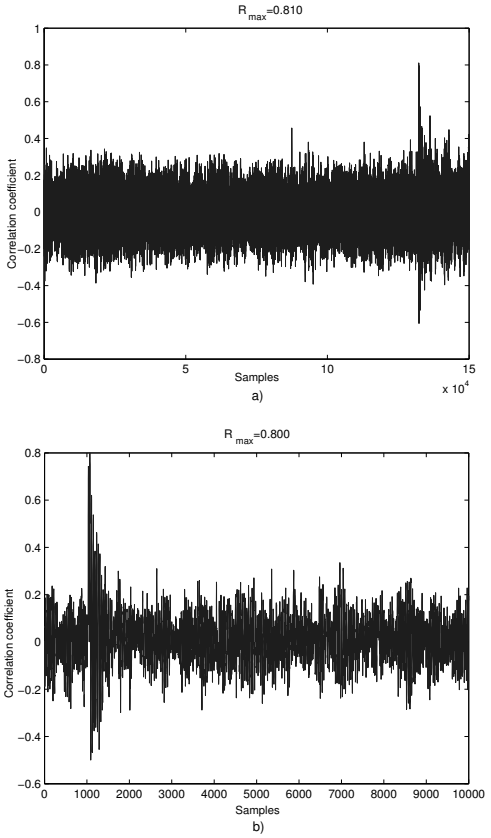

Figure 6. Comparison of correlation analysis of the realistic scenario DPA - figure a) and the attack with synchronized races by trigger - figure b). We use analysis of correct key byte hypothesis. The attack without synchronization was done with 150,000 samples (75 μs @ 2 GS/s) and usage of CRC in order to misalign traces - execution time of our implementation of CRC algorithm is dependable on input data so the traces after CRC are misaligned. The attacked instruction (SubByte) and also correlation peak is located around sample 130,000 on the figure a). The second (reference) attack was done by explicit synchronization impulse just before SubByte with 10,000 samples (5 μs @ 2 GS/s) per trace as seen in figure b) (the scales of the figures are not the same). The correspondent correlation peak is located around sample 1,000. We can see that levels of peak correlation coefficients and noise (other correlation coefficients) are about the same level. In both attacks, we use set of 100 traces measured with 2 GS/s sampling frequency.

algorithms. We choose elliptic curve cryptography which is more complex compared to AES and elastic alignment will be essential for successful DPA attack.

ACKNOWLEDGMENT

This research was supported by APVV-0586-11 grant.

REFERENCES

[1] P. C. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *J. Cryptographic Engineering*, vol. 1, no. 1, pp. 5–27, 2011.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *Lecture Notes in Computer Science*, vol. 1666, pp. 388–397, 1999.

[3] M. Varchola and M. Drutarovsky, "The differential power analysis laboratory setup," in *Radioelektronika (RADIOELEKTRONIKA), 2012 22nd International Conference*, April 2012, pp. 1–4.

[4] M. Petrvalsky, M. Drutarovsky, and M. Varchola, "Differential power analysis of advanced encryption standard on accelerated 8051 processor," in *Radioelektronika (RADIOELEKTRONIKA), 2013 23rd International Conference*, April 2013, pp. 334–339.

[5] P. Maffezzoni, Z. Zhang, and L. Daniel, "A study of deterministic jitter in crystal oscillators," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2013.

[6] *Cortex-M3 Technical Reference Manual*, ARM Limited, 2010.

[7] Y. Lu, M. O'Neill, and J. Mccanny, "FPGA implementation and analysis of random delay insertion countermeasure against DPA," in *ICECE Technology, 2008. FPT 2008. International Conference on*, 2008, pp. 201–208.

[8] J.-S. Coron and I. Kizhvatov, "Analysis and improvement of the random delay countermeasure of CHES 2009," in *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop*, ser. Lecture Notes in Computer Science, vol. 6225. Springer, 2010, pp. 95–109.

[9] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.

[10] J. Woudenberg, M. Witteman, and B. Bakker, "Improving differential power analysis by elastic alignment," in *Topics in Cryptology – CT-RSA 2011*, ser. Lecture Notes in Computer Science, A. Kiayias, Ed. Springer Berlin Heidelberg, 2011, vol. 6558, pp. 104–119.

[11] Q. Tian and S. Huss, "A general approach to power trace alignment for the assessment of side-channel resistance of hardened cryptosystems," in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on*, July, pp. 465–470.

[12] R. Muijrers, J. Woudenberg, and L. Batina, "RAM: Rapid alignment method," in *Smart Card Research and Advanced Applications*, ser. Lecture Notes in Computer Science, E. Prouff, Ed. Springer Berlin Heidelberg, 2011, vol. 7079, pp. 266–282.

[13] S. Salvador and P. Chan, "Toward accurate dynamic time warping in linear time and space," *Intell. Data Anal.*, vol. 11, no. 5, pp. 561–580, Oct. 2007.

[14] T. Bin Amin and I. Mahmood, "Speech recognition using dynamic time warping," in *Advances in Space Technologies, 2008. ICAST 2008. 2nd International Conference on*, 2008, pp. 74–79.

[15] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Berlin, Heidelberg, New York: Springer Verlag, 2002.

[16] ST Microelectronics, "STM32 product information, software and datasheets," http://www.st.com/web/en/catalog/mmc/FM141/SC1169, Online: 20/01/2014.

[17] Agilent Technologies, "DSO9404A datasheet and product information," http://www.home.agilent.com/en/pd-1632456-pn-DSO9404A/oscilloscope-4-ghz-4-analog-channels, Online: 20/01/2014.

[18] A. Barenghi, G. Pelosi, and Y. Teglia, "Improving first order differential power attacks through digital signal processing." in *SIN*, O. B. Makarevich, A. Elçi, M. A. Orgun, S. A. Huss, L. K. Babenko, A. G. Chefranov, and V. Varadharajan, Eds. ACM, 2010, pp. 124–133.

[19] "FastDTW," http://code.google.com/p/fastdtw/, Online: 20/01/2014.