Differential Power Analysis under Constrained Budget: Low Cost Education of Hackers

Filip Štěpánek, Jiří Buček, Martin Novotný
Czech Technical University in Prague, Faculty of Information Technology
Thákurova 9, 160 00 Prague, Czech Republic
Email: {filip.stepanek, jiri.bucek, martin.novotny}@fit.cvut.cz

***Abstract*—The differential power analysis is popular technique in exploiting weaknesses of the embedded systems — mostly of the smart cards. This approach is understandable as the DPA does not require expensive equipment or strong theoretical background on the device under attack. Therefore it is ideal for education of beginners or students in the field of computer security.**

The aim of this paper is to describe the economy of obtaining the basic equipment for the education of the differential power analysis and to share the experience with its teaching.

***Keywords*-Differential Power Analysis, education, low costs, cryptanalysis, smart card**

I. Introduction

Cryptography finds its application area in many devices of everyday life. For example, smart cards are used for public transport, hotel keys, payphones, building access, personal identification, etc. Such large field of applications induces dangers, like falsification of documents, unauthorized access to services/buildings, impersonating of someone else's identity, stealing sensitive information or some other form of piracy.

To prevent this unauthorized access to secret information the devices like smart cards use some layers of security — for example encryption algorithms like AES, 3-DES, and others. These algorithms, although already proven to be mathematically unbreakable by common means, can be exploited due to their implementation in form of embedded system [1]. The popular technique of exploiting this weakness is called Differential Power Analysis (DPA) and was first published by Kocher et al. in 1998 [2].

There are already ways to defend the embedded systems against the DPA [3]. Such countermeasures include e.g. hiding or masking the true power trace [4], thus the processed data cannot be easily revealed. However, to demonstrate the power of DPA and the necessity of implementing countermeasures in cryptographic devices, the students must be provided with their own hands on experience with DPA applied to devices without countermeasures. In this paper we describe our solution practicable under constrained budget.

II. Differential Power Analysis

The differential power analysis is a technique that exploits the dependency of the processed data on the power consumption of the device executing some (mostly cryptographic) operation. The DPA is non-invasive method which means that no modifications are done to the target device but some form of modification must be done to the connection of the communication equipment like described in [5].

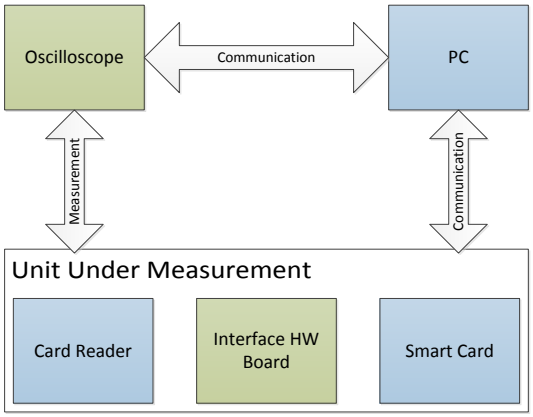

Figure 1. Connection schematic for the measurement of the power traces. Apart from the ordinary connection (PC, card reader, smart card) the oscilloscope and interface HW board are added.

This technique in exploiting the weaknesses of embedded systems is relatively obtainable. It does not place high demands on the expertise of the person that operates the attack and is easy to implement — therefore excellent for educational purposes. To perform DPA the student (attacker) uses a modified card reader or any other communication device — in our case an interface HW board inserted into the card reader, as shown in Figures 1 and 3.

The interface HW board provides measuring pins for the oscilloscope (measurement of the power consumption and the optional trigger signal) and the ordinary contact interface for the smart card to forward the communication. The communication is served by the PC like during normal operation, but in this case PC concurrently controls the oscilloscope and receives the data from it.

III. Previous form of education

In the last years, students did not perform the measurements. They were given the measured data (package of traces) and they analyzed this data using some sort of algebraic system (Matlab or Mathematica). This solution was impractical, but was necessary due to time requirements, insufficiency of measuring equipment, and its cost. As we were equipped with just 2 oscilloscopes, we were not able to provide sufficient working conditions to every student. Moreover, as the oscilloscopes were for about $25,000 each, we would have to apply extra security arrangements.

This solution seemed to be only possible compromise, however, as a result, the students got no real experience with the DPA attack. They were unable to obtain the power traces themselves and therefore their understanding of the technique or background on the DPA/security matter was inadequate.

IV. Low cost education

In order to improve the students' understanding of the differential power analysis, we needed to acquire new measuring equipment that would be available for all students in groups of two. In other words, we needed to purchase at least 10 oscilloscopes and sufficient amount of smart cards, card readers, programmers and measuring adapters. The oscilloscopes are the most cost intensive equipment and also the most tricky part to select. The following part describes the selection criteria.

A. Equipment requirements

The main requirements for oscilloscopes were as follows:

- Bandwidth at least 100 MHz — attacking mainly smart cards clocked at units of MHz,
- enough memory depth — at least 1 MSa,
- good sensitivity — lowest voltage range better than 10 mV/div with 8 bit sampling,
- good connectivity — preferably USB high speed,
- fast data transfer — at least 300 kSa/s,
- good stability — several hundred measurements must be attainable without problems with reliability,
- responsive user interface, well arranged and simple to use controls,
- two channels — one for measuring power consumption, one for trigger.

The main challenge in selecting the right oscilloscope is mainly in the data transfer speed. This figure is rarely given in data sheets (actually, we did not encounter it even once), and therefore we needed to test it on real hardware before purchase.

We contacted several test equipment providers for samples of oscilloscopes that would fit our requirements and meet the price range up to ca. $2,000. We tested the measurement on a preliminary test setup with a microcontroller performing AES encryption and connected to the PC via serial line.

Although several oscilloscope models fulfill our requirements according to their specifications, there were substantial differences in user interface responsiveness and (more importantly) data transfer speed. We tested oscilloscopes from Agilent (DSO-X3104A), GW Instek (GDS1152A), Hameg (HMO1024) and Tektronix (MSO2024). We tried to get a sample from Rigol (but did not succeed in time). We derived our test code from our reference measurement with a Picoscope 5204.

The most important criterion, as already mentioned, proved to be the data transfer speed. With DPA, we needed to perform approx. 500 measurements with 1 MSa each during the time frame of a normal laboratory class, that is 90 minutes. This corresponds to approx. 10 seconds per measurement, not accounting for the time needed for measurement setup, debugging and analysis. Therefore we set our criterion on data transfer speed at 300 kSa/s or better. This way, with 1 MSa trace, we could transfer at 3.3 s per trace, and have enough time for the rest of the class. Measured data transfer speeds are presented in Table I.

Table I
Data transfer speed of tested oscilloscopes.

Tested model (alphabetical order)	**Memory [MSa]**	**Transfer speed [kSa/s]**	**Target model**
Agilent DSO-X3104A	2	2060	DSO-X3012A
GW Instek GDS1152A	2	67	GDS1152A
Hameg HMO1024	2	77	HMO1022
Tektronix MSO2024	2.5	312	MSO2012

From our testing, it is clear that of the limited set of oscilloscope models, only Agilent DSO-X3104A and Tektronix MSO2024 could be considered usable for DPA education in normal laboratory class time frame. Agilent DSO-X3104A was the fastest by a large margin. It should be noted that we tested only the oscilloscopes that we were offered by the test equipment providers with the provision that a model from the same family would fulfill our requirements including our price limit. We cannot rule out that a different model, perhaps from a higher level family, would be better, if a sufficient discount from the price would be possible.

B. Design of the measuring equipment

The simplest way of measuring the power consumption of a smart card is inserting a current-sensing resistor in the power supply path. The resistor is usually inserted into the ground path. This way, normal oscilloscope probe can be used (no differential probe is needed). The measuring fixture must provide the signal from this resistor as well as communication signals and auxiliary signals that are used to simplify triggering. This can be done either as a modification of a smart card reader, or as a special HW interface board that fits between an unmodified reader and the analyzed card.

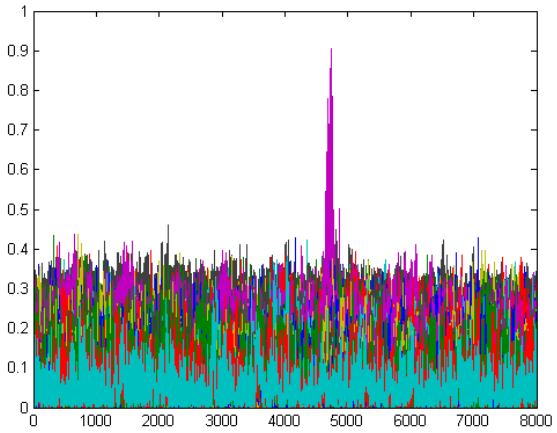

Figure 2. Calculation of the correlation coefficient

Figure 3. Smart card connected to the card reader through the interface HW board

We have decided to create the HW interface board, as this solution is non-invasive and can be used with any reader provided that the physical dimensions allow inserting a larger card into the reader. The resulting mechanical construction is depicted in Figure 3. The interface board is a double-sided 0.8 mm thick board with gold plating of the contact area.

The attacked smart card can be practically any card, but not every smart card is suitable for teaching the DPA attack. For beginners, it is better to work with cards that do not implement any countermeasures against DPA. There are several types of programmable smart cards with microcontrollers like Atmel AVR and Microchip PIC. At our faculty, students are accustomed to program AVR processors. Therefore, we chose to use AVR smart cards — firstly, a PCB with ATmega32A, and secondly, an off-the-shelf integrated smart card with ATmega163 ("ATmega163 Card").

For programming cards with AVR processors, we created a programming adapter to the AVR Dragon programmer [9].

V. The measuring exercise

During the laboratory session the students use the DPA to extract the key or some other secret information from their implementation of the AES encryption algorithm on the smart card with ATmega163 micro-controller.

First, the students implement AES algorithm in a smart card. In the next phase, several successful implementation of AES are selected. The keys in these implementations are changed by teachers, and preprogrammed smart cards with unpublished keys are distributed among all students.

Students task consists of following phases:

1) Getting acquainted with the firmware of the embedded device and communication over the T=1 protocol,
2) modification of the firmware and implementation of the cipher,
3) measurement of the power traces,
4) extracting the secret key using algebraic systems.

Let describe these phases in more detail.

A. Getting acquainted with the FW

First, students need to get acquainted with the firmware of the embedded device (smart card) and then they try to communicate with the card by connecting it to the computer using the standard card reader as shown in the Figure 3 (note: in this phase the interface HW board is not necessary). The FW communicates over the T=1 protocol for the smart cards specified by [6]. To communicate with the smart card some simple software like JSmartCardExplorer [7] is used — students can encrypt/decrypt some data using a prepared dummy cipher that XORs the plain-text with the stored key and inverts the positions of the bytes of the text.

B. Modification of the FW

The next step is to let the students to modify the FW. Adding a new instruction seemed to be a good start. Then the students implement the cipher and prove its correctness by means of some cryptographic software like Cryptool [8].

During the laboratory sessions the students had no problems with implementation of new instruction or the cipher in the prepared FW.

C. Measurement of the power traces

Students begin the exercise by connecting the card reader and the oscilloscope to the PC using the USB cable. After that the client application (already prepared for the students) is used to communicate with the oscilloscope/smart card — students just confirm the correct selection of the oscilloscope and then they start sending continuous stream of data to be able to correctly observe the encryption cycle as shown in Figure 4. The cycle is easy to obtain as the smart card sets

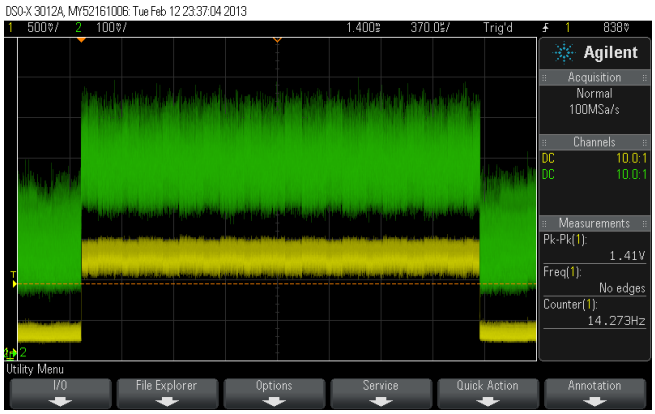

Figure 4. Measuring the power traces using the Agilent Technologies InfiniiVision DSO-X 3012A oscilloscope. Above - the power trace of the AES algorithm, below - the trigger signal

the trigger signal outside the call of the desired operation and therefore it eliminates the traces for communication etc.

After the oscilloscope is correctly aligned the client application is used to extract the power traces — the basic setting extracts 200 power traces which seemed to be adequate on the device that is not secured against DPA but experience shows that 70 traces led to successful key extraction. The key extraction was also tried with 65 traces but this amount was not sufficient to calculate correct key.

The application returns collection of traces (70 MB containing 200 traces) and all corresponding plaintexts and ciphertexts that can be loaded for example into Matlab.

The size of the measured traces (or the probability of success in finding the correct key) is dependent on the length of the one encryption or decryption cycle (that means on the length of the segment) and number of traces where each sample of the trace is stored as 8 bit unsigned integer (uint8) — this data-type proved to be sufficient for this kind of measurement.

D. Extracting the secret key using algebraic systems

When the power traces have been measured the corresponding data are analyzed using algebraic system (in this case we use the Matlab 2012a or Mathematica 8). These systems contain functions for loading the data in a correct format. The students task is to program the application analyzing obtained data and finding the correct key.

VI. Conclusion

The final results of the laboratory sessions met with our expectations — the set-up of the equipment was without problems or any risk of damage to the equipment. The speed of the measurement was satisfactory and the traces were sampled within the interval of 2 minutes. Also the preparation of the software that communicates with the oscilloscope and firmware for the smart card helped students to focus on implementation of the cipher and extracting the secret key using algebraic systems. The results of the laboratory sessions were 100% successful in implementing the cipher, measuring the power traces and extracting the key.

Our experience shows that differential power analysis is feasible even with a very limited budget. Total expenses were below $23,000, i.e. just $2,300 per one measuring set (oscilloscope, programmer, smart cards, card reader, interface HW board, etc.). The key can be found even with the oscilloscope having just 8 bit resolution. On the other hand, communication speed over USB showed to be crucial for breaking the system in reasonable time.

All software — client (PC) application for the communication with the oscilloscope/smart card and the firmware for the smart card have been created with the usage of open materials for the purpose of education, research and non-profit activities. They are available for consulting/sharing upon request by contacting the authors.

Acknowledgement

This work has been partially supported by FRVS grant no. 1154/2012 and FRVS grant no. 1160/2012. We also appreciate help of Timo Kasper from Ruhr-University Bochum, who significantly influenced our effort.

References

[1] C. Paar, J. Pelzl, *Understanding Cryptography*, 2nd corrected printing Springer, 2010.

[2] Kocher, P., Jaffe, J., Jun, B. *Differential power analysis*, In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)

[3] Cryptography Research, *http://cryptography.com/*, company's website, March 28, 2013.

[4] S. Mangard, E. Oswald, T. Popp, *Power Analysis Attacks*, Springer, 2007.

[5] C. Paar, *Implementation of Cryptographic Schemes 1*, version 1.8.1 Ruhr-University at Bochum, Germany, January 18, 2012.

[6] INTERNATIONAL STANDARD, *ISO/IEC 7816-3: Cards with contacts — Electrical interface and transmission protocols*, 3rd edition, ISO/IEC, 2006.

[7] P. Tucci,*http://www.primianotucci.com/default.php?view=112*, Java (cross-platform), graphical, low level (APDU) smart card tool aimed to help developing of smart card applications and understanding of ISO-7816 protocol March 28, 2013

[8] The CrypTool Portal, *http://www.cryptool.org/en/*, The most-widespread free e-learning programs in the area of cryptography and cryptanalysis, March 28, 2013

[9] AVR Dragon programming and debugging platform, *http://www.atmel.com/tools/avrdragon.aspx*, manufacturers' website March 28, 2013