Bit-level Differential Power Analysis Attack on implementations of Advanced Encryption Standard software running inside a PIC18F2420 Microcontroller

K. Mpalane*
Department of Computer Science
North West University
Private Bag X2046,Mafikeng
2745, South Africa
kmpalane@csir.co.za

H.D. Tsague
Council For Scientific and Industrial Research
P.O Box 395,Pretoria
0001, South Africa
HDjononTsague@csir.co.za

N. Gasela and B.M. Esiefarienrhe
Department of Computer Science
North West University
Private Bag X2046,Mafikeng
2745, South Africa
naison.gasela@nwu.ac.za and
esiefabukohwo@gmail.com

***Abstract*—Small embedded devices such as microcontrollers have been widely used for identification, authentication, securing and storing confidential information. In all these applications, the security and privacy of the microcontrollers are of crucial importance. To provide strong security to protect data, these devices depend on cryptographic algorithms to ensure confidentiality and integrity of data. Moreover, many algorithms have been proposed, with each one having its strength and weaknesses. This paper presents a Differential Power Analysis(DPA) attack on hardware implementations of Advanced Encryption Standard(AES) running inside a PIC18F2420 microcontroller.**

***Index Terms*—Differential Power Analysis, Power Attacks, AES, Microcontroller, Side Channel Attacks;**

I. Introduction

Cryptographic devices are widely used in different applications that require strong security protection. Therefore, security of these devices are of crucial importance. To protect these devices, cryptographic device developers rely on cryptography to secure their data [1]. Consequently, cryptographic devices depend on cipher algorithms to ensure confidentiality and integrity of data. The goal of cryptography is to use cryptographic algorithms to protect data from unintended individuals by converting it into a non-recognizable form which cannot be read or understood by anyone except the intended party [2].

Cryptographic devices have been known for protecting secret information. However, cryptanalysts are still able to break the security of most cryptosystems by studying and analyzing the information system in an attempt to recover its hidden characteristics [3], [4].This happened after the introduction of Side Channel Attacks (SCA) in 1998 by Paul Kocher [5]. Since then, microcontrollers have been targets of security attacks.
Microcontrollers are implemented using Complementary metal-Oxide Semiconductor (CMOS) technology. CMOS circuits consumes electric power by charging load capacitances every time they are switched [6]. This consumed power can be used as leaked information that attackers can use to break the system in the sense that the consumed power depends on the operations performed by the computing device [7], [8]. Examples of leaked information include electromagnetic radiations, power consumption, and timing information measurements leaks [9]. This information is used to obtain the secret key or other information stored on the device.

In [5], it was shown that Power Analysis Attacks (PAA) can reveal secret information of a device by using its leaked information. There are two kinds of PAA, Simple Power Analysis (SPA) and Differential Power Analysis (DPA). Both attacks are based on statistical methods established by Kocher et.al [10], [11]. DPA is much more powerful than SPA and more difficult to prevent [12], [13]. For an attacker to run DPA, s/he do no not need any extensive knowledge of how the algorithm was implemented. Most cryptographic systems use the implementations of Advanced Encryption Standard (AES) algorithm because it is believed to be mathematically strong [5] . However, AES can be broken by using PAA.
The authors of [8], [14] showed that power consumption measurements of a device measured while performing multiple algorithmic operations can be used to extract the secret key of AES implementation. DPA is the most used technique against cryptographic algorithms implemented in cryptographic devices [14].
This paper presents DPA attack in a PIC18F2024 running an implementation of AES algorithm which is used as a target for the attack. DPA will be used because it is the most practical and inexpensive physical attack [14]. It uses statistical methods to extract private information from the power consumption of the cryptographic device under attack [8] [5].
The remaining sections of the paper are organized as follows.

978-1-4673-9795-7/15 $31.00 © 2015 IEEE
DOI 10.1109/CSCI.2015.115

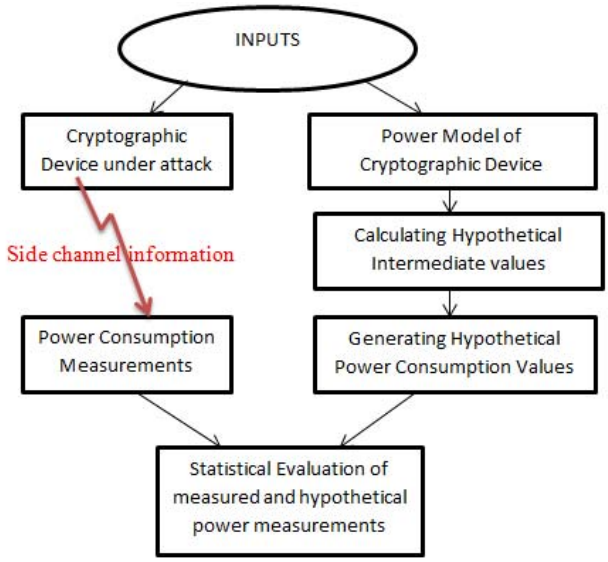

Fig. 1. DPA flow chart.

Section 2 presents DPA techniques. Section 3 describes the method applied to acquire data and addresses the description of the experimental set-up. Section 4 describes the attack method applied to the acquired data. Experimental results and discussion are provided in Section 5. Section 6 concludes the paper.

II. DPA Execution

DPA attacks are the most widely used type of power analysis attacks which is widely used to extract the secret keys for encryptions or decryptions executed on cryptographic devices. DPA require a large number of power traces measured while the device encrypt or decrypt different data blocks. One of the advantages of using DPA is that the secret key of the device can be revealed even when the measured traces are extremely noisy. In addition, a DPA attacker do not require detailed knowledge about the cryptographic device but adequate knowledge of the cryptographic algorithm executed by the device is essential.

Figure 1 above illustrates the principle that DPA follows:

- Firstly the attacker input known data to the device under attack and measure its power consumption while it is performing encryption or decryption operations.
- Secondly, they use a power model to calculate the hypothetical power consumption for all possible values of the secret key.
- Thereafter, they compared the hypothetical power consumption and the measured power consumption values.
- Lastly, the correct key byte is revealed by correlating the hypothetical power consumptions with the measured power consumption. In a successful attack, the correct key byte hypothesis will show a significantly high peak relative to other key bytes hypotheses.

III. Data Acquisition

To show that cryptographic devices are not secure against DPA attacks, we apply general principles to attack AES software implementation data kindly provided by [15]. The target device is PIC18F2420 microcontroller by Microchip Technology Inc. The microcontroller has an 8-bit architecture, 16kB program memory size, 256B EEPROM, 768B RAM and 40MHz CPU frequency. The microcontroller was running an unprotected AES-128 software implementation. The environmental setup used is shown in Figure 2. As depicted by the diagram, the communication between the PC and the target device was realized by RS-232 serial port interface.

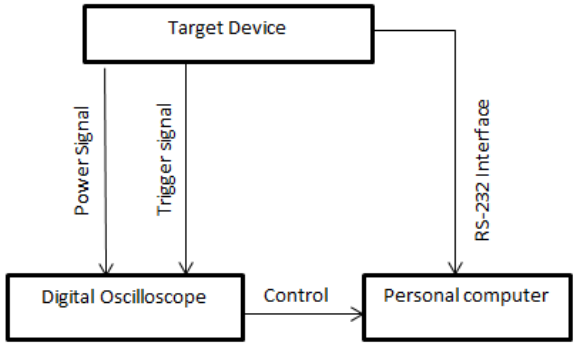

Fig. 2. Experimental setup.

A set of 1000 power traces were collected while the microcontroller was encrypting 1000 random generated plaintexts using the same key throughout. The microcontroller generated a trigger signal to make the oscilloscope aware of the start of the encryption operations. During this time, the power consumption of the microcontroller was measured. For this purpose, a 10Ω serial resistor was inserted in the power line of the microcontroller and the voltage drop (power consumption) along this resister was measured. The measurements retrieved were transformed to the PC with the help of LeCroy WavePro oscilloscope.

IV. Attack Methodology

The analysis was performed by using the technique similar to that of Figure 1. This was realized by using a MATLAB script. Firstly, an output byte of Substitution Box(Sbox) in the first round was chosen as our key-dependent value. This output value is a point in the algorithm that depends on the plaintext and on a byte of the secret key. Secondly, the hypothetical

intermediate values of the target bit were computed using the plaintexts and the measured traces. Instead of calculating the power consumption of hypothetical intermediate values by targeting only one bit(LSB of the intermediate value), we performed separate attacks for each of the eight bits of the first byte. We repeated the attack for the other 15 bytes.

Algorithm 1: Algorithm for performing DPA attack using Hamming-weight as a power model and DoM as a correlation method.

Input: Plaintexts, traces
Result: Results matrix of size 256*100002

```
1  for key byte position b=0:16 do
2      get key byte position b for each plaintext;
3      Predict the intermediate values;
4      for key guess k=0 to 256 do
5          for plaintext p=1 to 1000 do
6              Predict the power consumption;
7              PowerConsumption = bitget(AfterSbox,bit);
8          end
9          for trace no.i=1 to 1000 do
10             Correlate the predicted power consumption with
               the traces;
11             Generate difference traces;
12         end
13     end
14     return Results
15 end
```

It is believed that the power consumption of the target device depends on all bits of the output byte at some moment in time. Hamming weight power model was used to generate the hypothetical power consumption. Finally, Difference of Means (DoM) method was used to measure the statistical dependency between the measured power consumption and the hypothetical power consumption. The results based on 1000 traces generated a $Results$ matrix which generated graphs for every key byte hypotheses. The graph with the highest peak was taken as the correct key byte. As illustrated in Algorithm 1, line 7 was used to guess the instantaneous power consumption values for all the encryption runs for all key hypotheses, bit is the target bit number, and $bitget$ returns the bit value at position bit in the integer array AfterSbox. To correlate the hypothetical power consumption with the measured power consumption (Algorithm 1, line11), Difference of Means (DoM) statistical method was used and can be calculated as shown in (1) through (5).

$$mean_{1i,j} = \frac{1}{n_1 i} \times \sum_{l=1}^{n} HT_{l,i} \times MT_{l,j} \tag{1}$$

$$mean_{0i,j} = \frac{1}{n_0 i} \times \sum_{l=1}^{n} (1 - HT_{l,i}) \times MT_{l,j} \tag{2}$$

$$n_{1i} = \sum_{l=1}^{n} HT_{l,i} \tag{3}$$

$$n_{0i} = \sum_{l=1}^{n} (1 - HT_{l,i}) \tag{4}$$

$$Results = MEAN_1 - MEAN_0 \tag{5}$$

HT denotes hypothetical power consumption, MT denotes measured power traces and n denotes the number of power traces used for the attack. The inputs used for the algorithm are:
Plaintexts: AES inputs bytes of size (1000x16)
Traces: power traces of an AES microcontroller implementation of size (1000x10002) corresponding to plaintexts.

V. Attack Results

The measurement samples stored in Matlab were divided into two samples of the same plaintext. Equation 1 and 2 were used to calculate the average of each sample to get two average power traces. Equation 1 shows the power trace were the intermediate bit value was one and Equation 2 shows the case were the intermediate bit was zero. Equation 5 was used to subtract the two power traces to test whether there were significant peaks in the subtracted means or not. It created the subtracted graphs for all 256 key byte hypothesis.

The experimental results of Figure 3 shows key byte plots for bit 1, 2, 3 and 4 of byte 1 and as depicted by the figure,all the four bits revealed the key byte with bit1 revealing most of the information about the key. Although bit 2 did not reveal much, the information was enough to reveal the key byte. It can be concluded that different bits in the same micro-controller register leaks different amount of information.

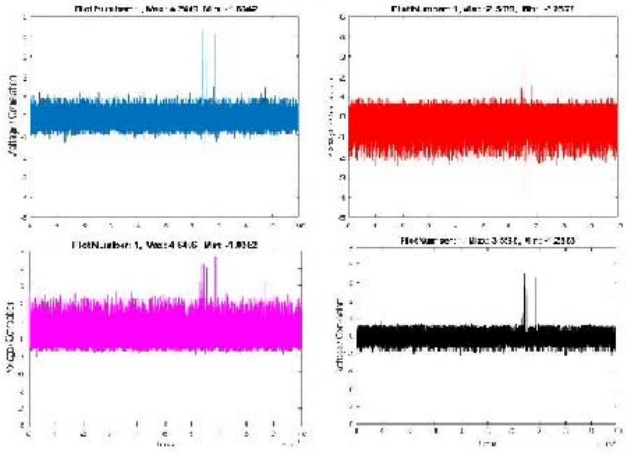

Fig. 3. Plots for first four bits of Byte1.

Figure 4 shows all the correct bits that revealed the key byte for byte1. All the bits except bit 7 revealed the key byte. The plots are overlapping, hence other plots are invisible.

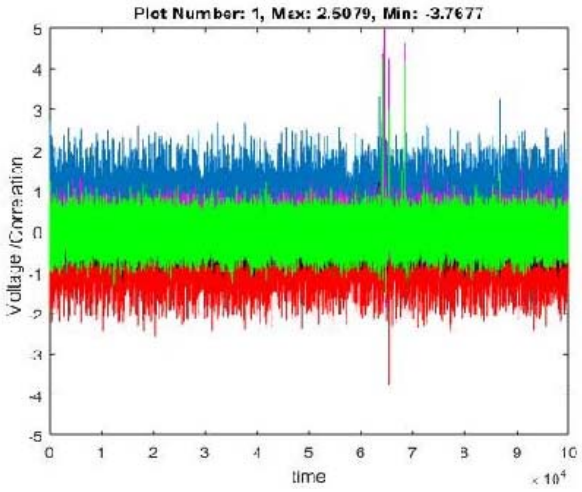

Fig. 4. All Correct bits of Byte1.

Figure 5 shows a plot for the incorrect key byte for byte 1. The target bit for this byte was bit7. The bit did not reveal any information and this is because leakage of each bit of the target intermediate value is different and each bit leaks independently.

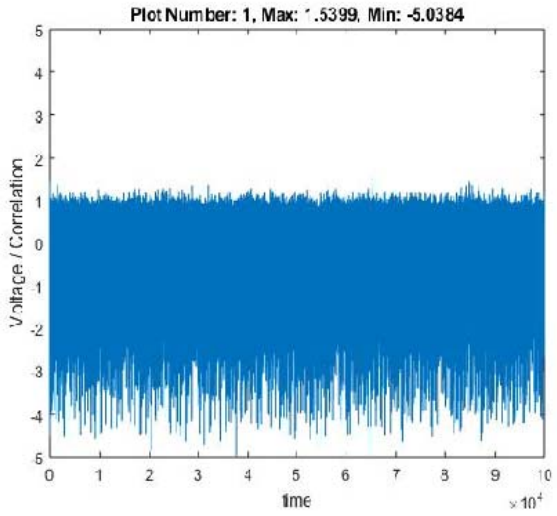

Fig. 5. Incorrect key byte for byte1.

TABLE I. Bytes Results for different Bits

	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7	Bit8
Byte1	✓	✓	✓	✓	✓	✓	×	✓
Byte2	✓	✓	✓	✓	×	×	×	✓
Byte3	×	×	×	×	×	×	×	×
Byte4	×	×	×	×	×	×	×	×
Byte5	×	✓	×	✓	✓	×	×	✓
Byte6	✓	✓	✓	✓	✓	×	✓	✓
Byte7	×	×	×	×	×	×	×	×
Byte8	×	×	×	×	×	×	×	×
Byte9	✓	×	✓	×	✓	×	✓	×
Byte10	×	✓	✓	✓	✓	✓	✓	✓
Byte11	×	×	×	×	×	×	✓	×
Byte12	×	×	×	×	×	×	×	×
Byte13	×	×	✓	✓	✓	✓	✓	✓
Byte14	✓	×	×	✓	✓	✓	×	✓
Byte15	×	×	×	×	×	×	×	×
Byte16	×	×	×	×	×	×	×	×

The results for other bytes are represented in Table I. Looking at the table, the rows highlighted in grey shows the byte whose bits did not reveal anything. As depicted by the table, all the bits for byte 3, 4, 7, 8, 12, 15 and 16 did not reveal any information. This is because the targeted bit did not have any conclusive impact in the measured traces. Furthermore, some data are slightly correlated with the target bit. In addition, there might have been a lot of noise when measurements were taken for these bytes.

VI. Conclusion

In this paper we have applied a DPA attack on AES software implementations running on PIC18F2420 micro-controller. Main contribution of this work is highlighting that different bits of the target intermediate values can be used to reveal information about the secret key. Experimental results showed that using different target bits leads to inconclusive results .For future work, its necessary to define countermeasures suitable for DPA attacks to protect the secret key.

VII. Acknowledgement

The authors would like to thank: Council for Scientific and Industrial Research (CSIR), Department of Science and Technology(DST), and North West University (NWU) for their financial support.

References

[1] Smid, M. E., and Branstad, D. K. ”Data encryption standard: past and future.” Proceedings of the IEEE 76.5 (1988): 550-559.

[2] Zaidan, B. B., et al. ”On the differences between hiding information and cryptography techniques: An overview.” Journal of Applied Sciences 10 (2010): 1650-1655.

[3] Diffie, W., and Hellman, E. M. ”New directions in cryptography.” Information Theory, IEEE Transactions on 22.6 (1976): 644-654.

[4] YongBin Z., and DengGuo F. ”Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing.” IACR Cryptology ePrint Archive 2005 (2005): 388.

[5] Kocher, P., Jaffe J. M, and Jun B. ”Differential power analysis.” Advances in CryptologyCRYPTO99. Springer Berlin Heidelberg, 1999.

[6] Tsague H. D., and Twala B. ”Simulation and Parameter Optimization of Polysilicon Gate Biaxial Strained Silicon MOSFETs ” The Fifth International Conference on Digital Information Processing and Communications (ICDIPC2015), Sierre, Switzerland 2015.

[7] Micali, S., and Reyzin L. ”Physically observable cryptography.” Theory of Cryptography. Springer Berlin Heidelberg, 2004. 278-296.

[8] Mangard, S., Oswald E., and Popp T. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer Science Business Media, 2008.

[9] Moabalobelo, T., Nelwamondo F., and Tsague H. D. ”Survey on the cryptanalysis of wireless sensor networks using side-channel analysis.” (2012).

[10] Kocher, P. C., Rohatgi P., and Jaffe J. M. ”Cryptographic device with resistance to differential power analysis and other external monitoring attacks.” U.S. Patent No. 8,707,052. 22 Apr. 2014.

[11] Mangard, S., Oswald E., and Standaert F-X. ”One for allall for one: unifying standard differential power analysis attacks.” IET Information Security 5.2 (2011): 100-110.

[12] Agrawal, D., et al. ”The EM sidechannel (s).” Cryptographic Hardware and Embedded Systems-CHES 2002. Springer Berlin Heidelberg, 2003. 29-45

[13] Messerges, T. S., Dabbish E. A, and Sloan R. H. ”Investigations of power analysis attacks on smartcards.” USENIX workshop on Smartcard Technology. Vol. 17. 1999.

[14] Kizhvatov, .I ”Physical Security of Cryptographic Algorithm Implementations.” Diss. University of Luxembourg, Luxembourg, Luxembourg, 2011.

[15] Breier, J., and Kleja M. ”On practical results of the differential power analysis.” Journal of Electrical Engineering 63.2 (2012): 125-129.