International Journal of Electrical and Computer Engineering (IJECE)
Vol.8, No.6, December 2018, pp. 5144~5152
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i6.pp5144-5152

Revealing AES Encryption Device Key on 328P Microcontrollers with Differential Power Analysis

Septafiansyah Dwi Putra[1], Adang Suwandi Ahmad[2], Sarwono Sutikno[3], Yusuf Kurniawan[4], Arwin Datumaya Wahyudi Sumari[5]
[1]Management of Informatics, Politeknik Negeri Lampung, Indonesia
[2,3,4,5]School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Indonesia

Article Info

Article history:

Received Feb 3, 2018
Revised Jul 19, 2018
Accepted Aug 2, 2018

Keyword:

AES
DPA
SCA
Encryption Attack
Secure Device
IoT

ABSTRACT

This research demonstrates the revealing of an advanced encryption standard (AES) encryption device key. The encryption device is applied to an ATMEGA328P microcontroller. The said microcontroller is a device commonly used in the internet of things (IoT). We measured power consumption when the encryption process is taking place. The message sent to the encryption device is randomly generated, but the key used has a fixed value. The novelty of this research is the creation of a systematic and optimal circuit in carrying the differential power analysis or difference of means (DPA/DoM) technique, so the technique can be applied in key revealing on a microcontroller device by using 500 traces in 120 seconds.

Corresponding Author:

Adang Suwandi Ahmad,
CAIRG- Research Group,
School of Electrical Engineering and Informatics, Institut Teknologi Bandung,
Jl. Ganesha No. 10, Lebak Siliwangi, Coblong, Lb. Siliwangi, Coblong, Kota Bandung, 40132, Indonesia.
Email: adangSahmad@yahoo.com

1. INTRODUCTION

The increasing number of complex systems in computer applications increases the need for a secure data exchange inside them. Those applications use the internet as the media for the private exchange of information or data. Cryptology is a science about data safety. The use of the cryptographic application is increasing over the year. This increasing number is followed by the need for data movement in the internet, among mobile systems, andamong the Internet of Things (IoT). The improvement of cryptographic functionsis not limited to the confidentiality and the concealment of information by unauthorized parties. Cryptographic functions advance itself in becoming the instrument for verifying the authenticity, integrity, and digital signature of a data or information. The advancement in cryptographic functions is considered as an interesting research object whether from the application side, the strength, or the technique of attacking the said cryptographic application on hardware or software.

In the past, the attack on a cryptographic system is viewed only theoretically. A conventional cryptanalyst generally uses linear, differential, and brute force technique to analyze and obtain the vulnerabilities of an encryption algorithm [1], [2]. The cryptanalyst represents the cryptographic algorithm as a mathematical object.

The attacking technique of cryptography on hardware or embedded platform is a very interesting topic and very important matter to be researched especially in this modern day. According to statistics in 2018, the number of IoT devices or pervasive hardware computing is projected to hit as high as 75.4 billion devices in 2025. But, there are some potential errors and threat models on those IoT systems. The main problem with the error model is that IoT is a new object so that the security of such objects is not much considered in the design phase. IoT products that are available now, such as a microprocessor or microcontroller with embedded software, are very vulnerable to become an attack surface. IoT is very dependent on the development of a microcontroller unit (MCU) technology. MCU with low power and cost will be massively used especially as the main component in IoT devices. These MCUs contain a flash memory that carries a relatively-sized program (at least 64 kB). But, the shortfall of the usage of MCU is that there is no special peripheral such as true random number generator (TRNGs) or cryptographic coprocessors that is needed to improve the security. By that reason, we see a need of an examination on the vulnerabilities and the points of attacks of the MCU devices which will be used on the IoT devices.

However, in fact, when a cryptographic algorithm implemented in hardware will produce high performance, it can be mass produced and low costly [1], [2], [3]. Common forms of cryptographic devices are universal serial bus (USB) tokens, smart card [4], chips, field programmable gate array FPGA [5], [6], and micro-controllers [7]. These cryptographic devices have small dimensions and low power consumption. However, unnoticed by IC cryptanalyst and IC designers, cryptographic devices are more vulnerable and easily accessible by physical attack techniques [8]. So, the underlying assumption of classical cryptanalysis is no longer possible to be adapted.

The existence of a side channel attack (SCA) attacks on the security of cryptographic devices needs in-depth research. Some concrete characteristic leaks are occurring. Some side channel information, such as time [9] [10], sound [11], electromagnetic fields [12] and power consumption [13] can be used by an adversary to obtain the masterkey stored in the device. These leaks are unavoidable, and it is easy for an attacker to measure the value of such side information such as a probe and a high-frequency oscilloscope. Side channel analysis is an innovative new research area and very different from the classical cryptanalysis approach. Therefore, now, it not only focuses on the security of cryptographic algorithms but also on the security of the whole system that is a cryptographic device that implements a cryptographic algorithm [13].

This attacking technique has shown the overall result of simple power analysis (SPA) and DPA [14]. The result produced from DPA revealed correct 48 bit from 64 bit of the overall key (75%). The SPA and DPA have proved that both of them can recover 75% of the secret key and the rest could be obtained by using bruteforce. The second technique has been proposed in many articles that is by using the correlation factor between the traces and the hamming weight of the processed data [15], [16]. In some previous research, subkey and a secret key of AES and data encryption standard (DES) have been recovered by using a quite large number of traces [17–19]. Previous DPA attacking pattern used a large quantity of traces (>1000 traces) to get 75% correct bit of the master key. There are some improvements from the previous attacking model by calculating the correlation coefficient of the trace and the hamming weight of the processed data. However, when calculating the correlation coefficient, the attack must have the capability to fully control the value of the plaintext that is to be encrypted by the cryptographic device [20], [21]. The DPA flowis is shown in
Figure 1.

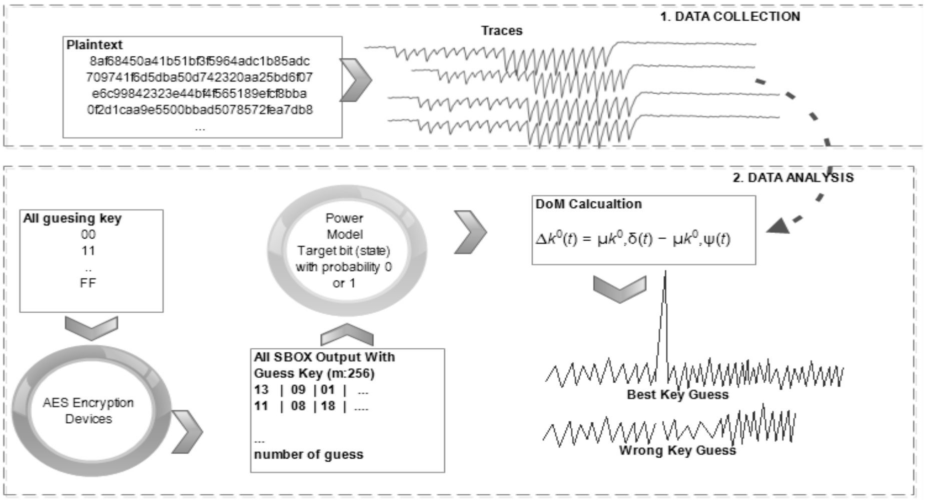

1. DATA COLLECTION
Traces
Plaintext
8af68450a41b51bf3f5964adc1b85adc
709741f6d5dba50d742320aa25bd6f07
e6c99842323e44bf4f565189efcf8bba
0f2d1caa9e5500bbad5078572fea7db8
...
2. DATA ANALYSIS
All guesing key
00
11
..
FF
AES Encryption Devices
Power Model Target bit (state) with probability 0 or 1
All SBOX Output With Guess Key (m:256)
13 | 09 | 01 | ...
11 | 08 | 18 | ....
...
number of guess
DoM Calcualtion
$\Delta k^0(t) = \mu k^0,\delta(t) - \mu k^0,\psi(t)$
Best Key Guess
Wrong Key Guess

Figure 1. DPA Flow

Unlike traditional cryptanalysis, SCA targets physical cryptographic system implementation. Power analysis attacks are one type of SCA that exploit power information changes. Power analysis attacks can be launched with simple equipment and attacks in a short time. Power analysis is a potent and useful attack against the actual implementation of the cryptographic algorithm on the hardware. From the various sources of the side channel information mentioned earlier, such as time measurement, electromagnetic radiation, error message; information derived from power consumption may be the most difficult matter to be controlled by the cryptographic designer. All calculations performed by encryption devices operate on zero and one logic gates. The process of computing encryption and decryption will lead to changes in power form and more specifically the logic gate. Attacker encryption devices can monitor power differences and get useful side channel information in key space searches. ~~(~~DPA~~)~~, introduced by Kocher et al. is a statistical approach to monitorsuch power signals.

Specific DPA attack forms against encryption devices running DES algorithms are contained in their DPA study [19]. Based on the results of the study, it was confirmed that DPA attacks are very potent and can even be used to monitor thedifference of every single bit of transistors in encryption devices. The paper will show how this attack can be used against the AES encryption algorithm and what factors cause the vulnerability to occur.

The purpose of this research is to investigate SCA and to develop a DPA based attack on an MCU target that applies AES-128. In this article, readers will be introduced to the idea of SCA in searching for the key. Next, we will introduce the power analysis technique with DPA-DoM (difference of means) on an MCU. The least significant bit (LSB) model of intermediate value is introduced as a partial means in executing DPA. Finally, we made some conclusions about thersefindings and comments about some future worksbased on the research results. One topic regarding the future works is about finding the best approach in mitigating DPA attack on an MCU.

2. RESEARCH METHOD

This section introduces the performed and lab setup for DPA attacks in this research. Figure 2 as shown the research steps used in this paper. The research steps used in this paperwas done by setting them in a systematic meansfor reviewing the SCA technique on an encryption device. The test will make a DPA attack on an AES encryption device by using a laboratory-testing environment. The environment itself is shown in Figure 3.

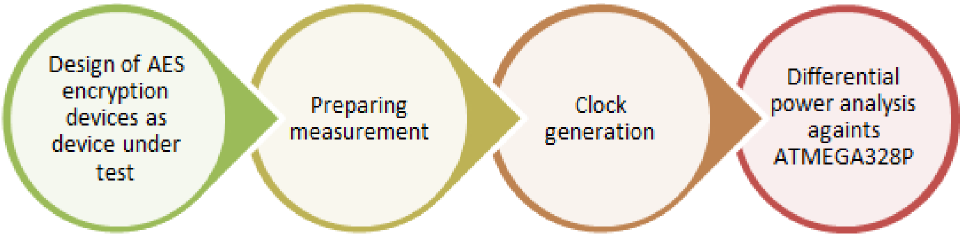

Design of AES encryption devices as device under test
Preparing measurement
Clock generation
Differential power analysis againts ATMEGA328P

Figure 2. Research Method

The expected main result of this research is to recover the secret key after the encryption process is finished. More comprehensively, the design step ofencryption device will produce an AES128 device that runs on an ATMEGA328P microcontroller. After the encryption device is obtained, the method of measurement is designed by making a circuit with a series resistor on the V_{ground}. The next step is to generate the clock by sending ciphertext to the encryption device previously obtained. The last part of the second test is to do a DPA attack so the characteristics and the model can be obtained and be further analyzed.

Table 1 lists the main components and setting for the testing. To run and simulate this attack technique we build the device under test (DUT). The system's design architecture is shown in Figure 3. This DUT environmentisconsisted ofat least three connected components: AES crypto processor, a personal computer (PC), and digital sampling oscilloscope (DSO). The crypto processor is the DUT from which side channel information would be harvested by the DSO, creating a traces curve. The PC collects the traces and performs statistical analyses to find the key by modeling the traces curve using key guesses. The DUT and the oscilloscope communicate using USB and RS232.

Table 1. Lab Setup for DPA-DoM

Variable	Description
Algorithm and length of the key Sample frequency	AES -128 bit 1Gsample/s
FPGA architecture	Xilinx Artix-7
Trigger signal	Header pin with SMA connectors
Shunt resistor	500mOhm- Stackpole
VCC-External	5 Volt -2A
Secret key	00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
PC – sampling	Intel i5 with 8G RAM

The differential power analysis attack was used in this study is a difference of means approach (DoM) was proposed by Kocher at 1999 [19]. However, the Kocher publication implements the attack on a DES algorithm that is located in an FPGA. In this research, we focused on a DPA attack on an AES encryption device. Specifically, the device is an AES encryption system implemented in a microcontroller device. The basic idea of DPA is to make one hypothesis one by one bit of the whole key bits. Next, we select a function known as function selection. The selection function gets the input value of the key guess k_g, where $k_g = (k_{g1}, k_{g2}, ... k_{g255})$.

This technique will divide several curves of traces (encryption device measurement result) into two sets $S_{\delta} \equiv m_i(t) |L_{k0,i}= 0$ and $S_{\psi} \equiv m_i(t) |L_{k0,I}$=1’ and the traces are adjusted to the leakage values of hypothetical keys $L_{k0,i}$. The adversarywill focus on one LSB bit (a least significant bit) $L_{k0,i}=\in \{0,1\}$ then the output of the bit determines where the position of the traces curve is placed. Laying the traces done by looking at if LSB = 0 will be placed on set 0 ($L_{k0,i} = 0$)or otherwise set 1 ($L_{k0,i} = 1$) [18], [22]. Furthermore, both sets of traces are mutually reduced or to obtain the difference between the two curves calculated. In the correct hypothetical key that is $k^0 = k$, then the true predictive value will be separated from the shape of the whole curve. At the technical end of this attack produces a peak on the differential trace curve and the point in time when the targeted operation is calculated $\Delta k^0(t)$. In other hypotheses the k^0, k curve traces will look flat. The correct k_g values can be identified by looking at the different peaks on the curves of the table (DoM traces). Formally, DoM calculations are indicated by:

$$\Delta k^0(t) = S_{\delta} - S_{\psi} \qquad (1)$$

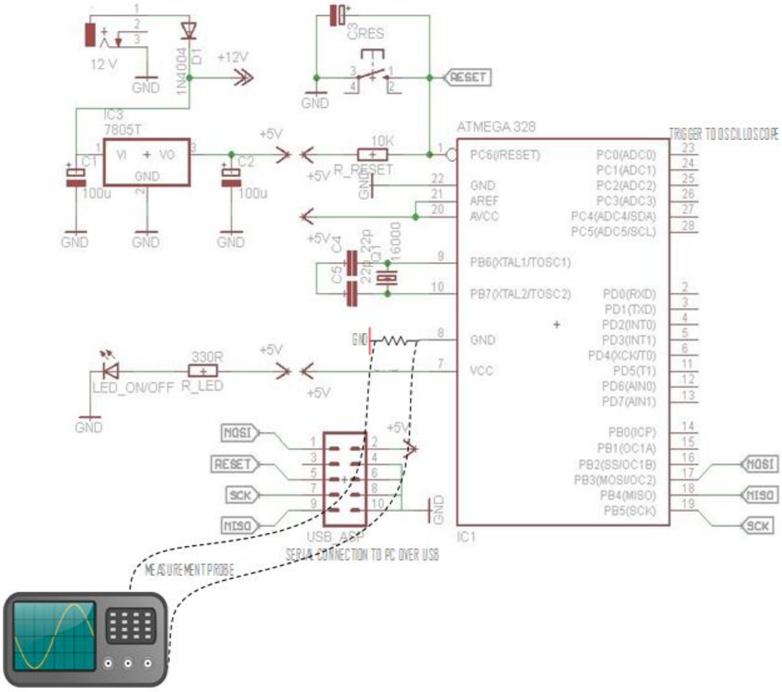


Figure 3. Setup architecture for attack against ATMEGA328P

In this paper, DPA attack techniques use the DPA AES128 bit attack. The number of traces data is 500 curve traces with information about the plaintext and the resulting cipher-text. The stages in carrying out the DPA attack on this report are to observe the first round of the AES-128 encryption protocol. The DPA attacks targetis outbreak from AddRoundKey and SubBytes on AES round operations.

***Algorithm 1. DPA DoM for 1st subkey** k_1*

```
Input : N pairs traces with plaintext and $k_g$ = key guess
Output: Recovered key fo$k_1$
for$k_g$ = 0 to 255 do
    fori = 1 to N do
        $Matrixdata(i,k_g) \leftarrow$ LSB of(Sbox (Ci[0] $\oplus k_g$));
    end for
    for each sample point p = 1, 2, . . , M of power trace do
        DoMp, $k_g \leftarrow (S_\delta \equiv m_i(t)\ |L_k0,_i = 1) - (S_\psi \equiv m_i(t)\ |L_k0,_i = 0)$;
    end for
    DoMtrace, $k_g \leftarrow$ {DoM$_{1,}k_g$ , DoM$_{2,}k_{g\,....}$ DoM$_{M,}k_g$};
end for
$k_1[0] \leftarrow$ absmax | DoMtrace, $k_g$ |
end
```

In each trace$i$, I_i, a 16byte is an intermediate state of the output value of the cipher after SubBytes operation is performed in the first round. Then, as many as n bytes of each state ∈ {0...15} is denoted by $I_{i,n}$. The key value used in the first round is denoted as K, andthe value of n of each byte will be denoted by Kn. The plaintext used on each trace is denoted as Xi,n. Therefore, the mathematical model of the first round observation can be:

$$I_{i,n} = S[x_{i,n} \oplus K_n] \qquad (2)$$

$$D = LSB\ (I_{i,n}) \qquad (3)$$

From the equation, the value of X_i,n is a known variable: one byte of plain-text. K_n is the secret key constants. The S variable is the default value of the AES substitution table. While the output of the S function is $I_{(}i,n)$ an unknown variable whose value depends on a 1-byte secret key and a known variable such as plain-text, use of tough tests can crack AES passwords easily if found the value of a key guess is correct. More specifically K_n is an 8-bit value, so at least 256 tests will be performed to confirm the correct K_n value. In the 16 bytes of K_n that make up all AES-128 keys can be found only by splitting for each byte separately. The flowchart DPA-DOM on AES as shown in Figure 4.

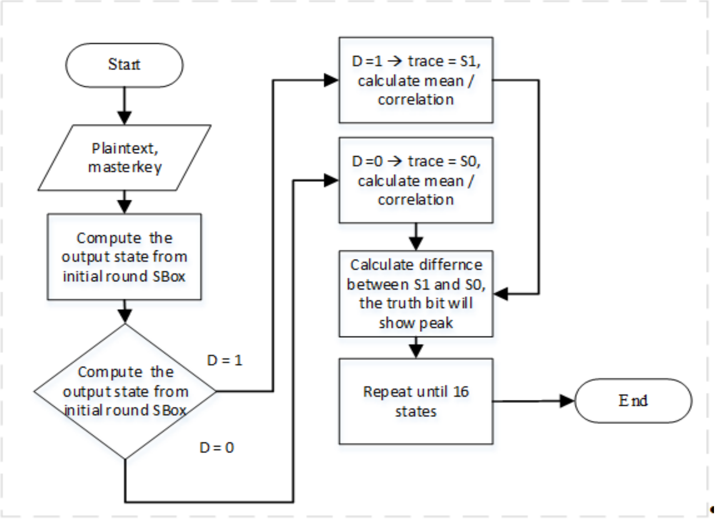

Start
Plaintext, masterkey
Compute the output state from initial round SBox
Compute the output state from initial round SBox
D = 1
D = 0
D =1 → trace = S1, calculate mean / correlation
D =0 → trace = S0, calculate mean / correlation
Calculate differnce between S1 and S0, the truth bit will show peak
Repeat until 16 states
End

Figure 4. Flowchart DPA-DOM on AES

3. RESULTS AND DISCUSSION

MCUs vulnerability with DPA attack is proved in this work. In our test, we have succeeded in designing an attacking environment that runs on an ATMEGA328P microcontrolleras shown in Figure 5. The DPA technique needs an input of some power trace and public data such as the ciphertext to carry the recovering key algorithm. The researchers made a correlation between secret key, public data, and measurement traces to recover the secret key. The calculation is made for every key guess. If the key guess is correct, it will be shownin the form of a graph similar to the one in Figure 6.

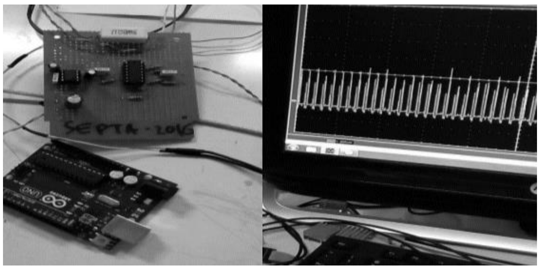


Figure 5. AES DUT and Traces

DPA is a practical way of testing whether the value of the Kn guessing process is closer to the truth. The Kn candidate is used with the equation above to obtain the value I(i,n) for each X(i,n) trace. A selection function can be made based on the process of calculating the value I(i,n). In this study, the one-bit value of I(i,n) (LSB) is used as the output of the selection function. Each trace is searching the value of one bit LSB then divided into two groups based on the output of the selection function. The average difference between each subset is then observed. If the output value of the S-boxes estimated by the selection function has a small correlation value for the traces, the DPA technique will show the spikes of the traces average indicating that the guess value of Kn is true. For every wrong Kn, the prediction of I(i,n) values would not be related to the data being processed by the target device.

Figure 6 shows the distribution of key guessing for the the16th state. It is visible that the key guesses index number 61 has a significant difference in data distribution compared to key guess index number 50 to 60. The large difference is assumed as the correct key guess. The test result shows that the attack has succeeded in recovering the whole 128-bit key (100% key recovery). The attacking simulation test is done by using 1,050 traces and takes 16 minutes of execution. The key can be directly recovered because of the AES algorithm vulnerability in initial AddRoundKeyoperation, which is, basically, an XOR operation of plaintext and masterkey. The result produced the key used, and the key guesses from the simulation correspond the sequence of the simulated states (43 126 21 22 40 174 210 166 271 247 21 136 9 207 79 60).

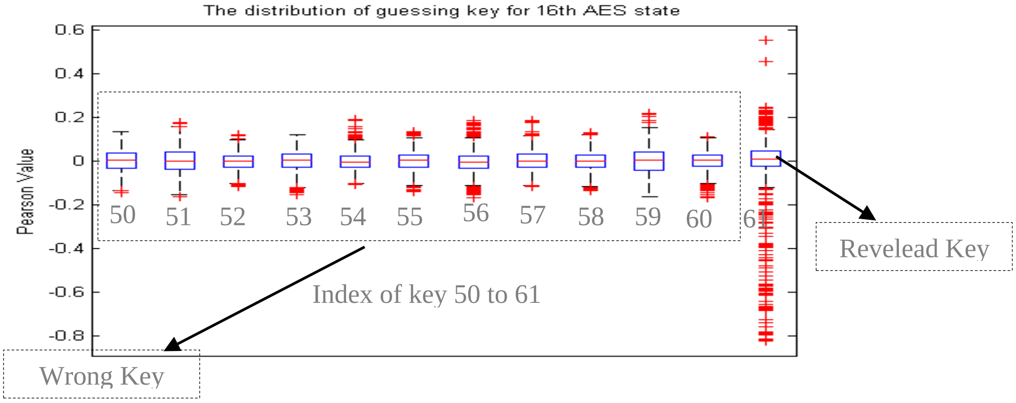
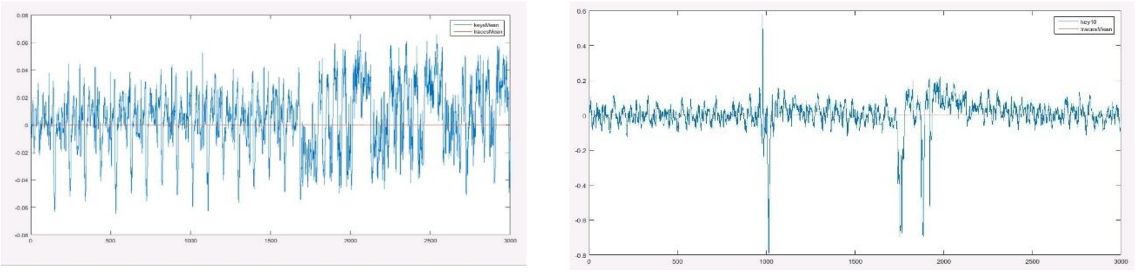


Figure 6. Global Success Rate AES128 for state number 16

The same analysis can be repeated for all 16-byte states (n = 0,..., 15) in obtaining all of 128-bit AES cipher keys from the encryption device. The value of the success of this attack is shown in Figure 7. The x-axis shows the number of traces and the y-axis indicates the key obtained.



(a) (b)

Figure 7. The comparison of trace averages for false and correct state guesses

Figures 7.a and 7.b show a very significant difference between the right guess (blue line) and the wrong key guess (red line) against power consumption. The graph in both images measures the value of DoM (Y-axis) with trace number (X-axis). The correctkey guesses have the highest level of trace graph difference when compared to the average trace graph. The test results shownin Table 2 represent the attack succeeds in an overall 128-bit key (100% key acquisition). Testing of attack simulation used 500 traces and ittook 120 seconds. The key can be directly obtained because of the weakness of the AES algorithm found in the initial AddRoundKey operation which is basically the XOR plaintext operation against the master key directly.

Table 2. The result of a DPA attack

No	Variable Testing	Results
1.	The number of traces needed	500
2.	Execution time	120 seconds
3.	A number ofkey bits gained	128bits
4.	Some missing key bits	0bits

4. CONCLUDING REMARKS

The implementation of an AES encryption system in anMCU has a high vulnerability to the master key of the AES encryption device itself. A DPA attack is a statistical attack based on the power usage analysis required by the encryption device. We already get the main problem of this power-based attack. After analysing the DPA on the DUT, we obtained an attack surface on the AES encryption device. The main susceptibility of AES128 lies in a predictable power estimation value after the SubBytes function in each round. We have succeeded demonstrating it by using a minimum trace and timenamely, only 500 traces and it took 120 seconds. The main vulnerability of AES to DPA is in the first roundof attack (after SBOX operation). The vulnerability is when the XOR of plaintext and the master key followed by a non-linear substitution of SubBytes function (SBOX). The attacker can easily make the empirical computation in determining the intermediate value. This value is essential in recovering the secret key. We believe that this vulnerability can be solvedby hiding and masking the intermediate value. As Figure 8 shows, we could obtain the intermediate value modelled as haming weight (8 bit) for every message. In future research, we will try to randomize the intermediate value by using ***information fusion*** [23–31] and ***constant weight encoding*** [27], [32] approach. Those approaches could deceive attackers in recovering AES encryption device's secret key. We proposed that method called as **cognitive-masking**. Cognitive-masking is built on the most significant power usage analysis affecting a single message encryption process. Cognitive-masking is a concept developed from information fusion. The concept of information fusion is to combine two information quickly and accurately to get the best value of masking decisions.

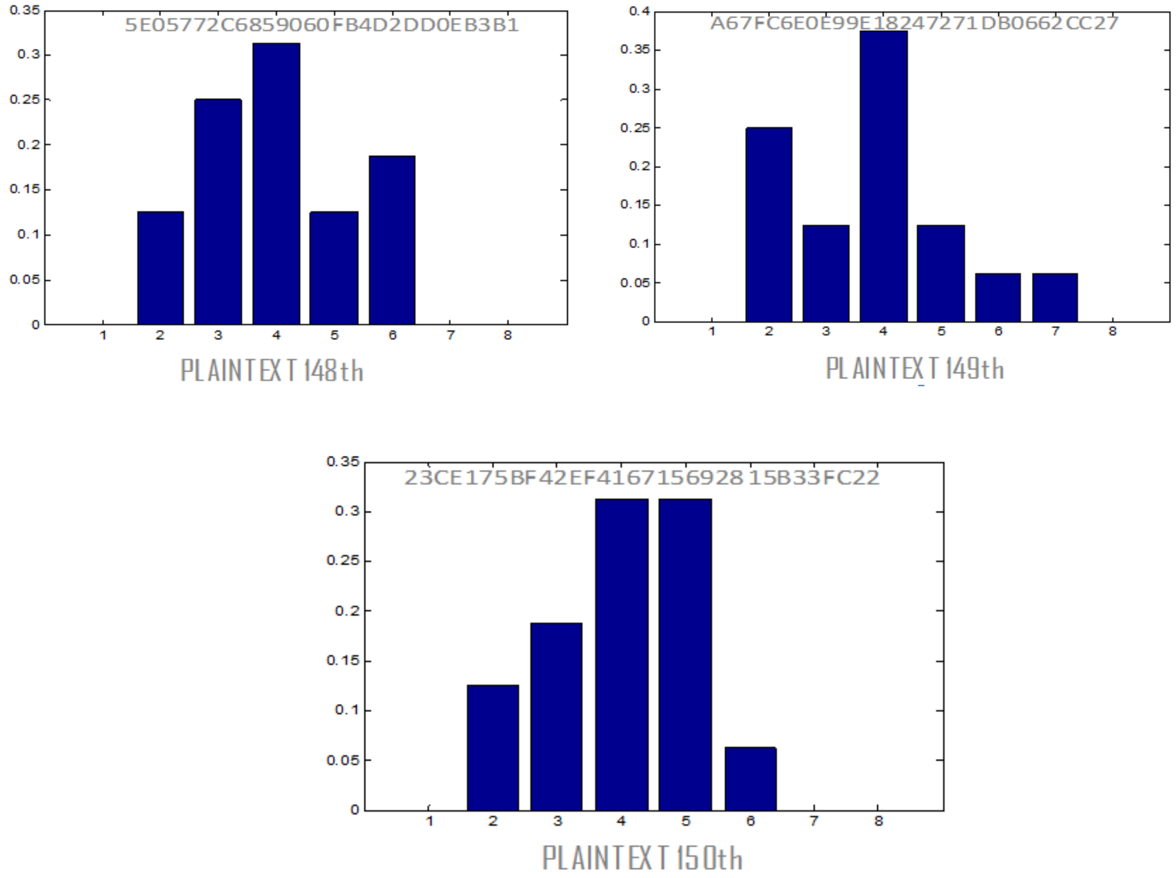


Figure 8. Hamming weight distribution for plaintext number 148, 149, and 150

ACKNOWLEDGEMENTS

The first author acknowledges support from the Indonesia Endowment Fund for Education (LPDP - Lembaga Pengelola Dana Pendidikan) scholarship, Ministry of Finance, The Republic of Indonesia. The authors gratefully knowledge the anonymous reviewers for their valuable comments.

REFERENCES

[1] S.D. Putra, A.S. Ahmad, and S. Sutikno, “Design of an AES Device as Device Under Test in a DPA Attack”, in *International Journal of Network Security*, 2018.

[2] S.S. Chawla and N. Goel, “FPGA implementation of an 8-bit AES architecture: A rolled and masked S-Box approach”, in *2015 Annual IEEE India Conference (INDICON)*, 2015, pp. 1–6.

[3] H. Chen, Y. Chen, and D.H. Summerville, “A survey on the application of FPGAs for network infrastructure security”, *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 4, pp. 541–561, 2011.

[4] T.S. Messerges, E. Dabbish, R.H. Sloan, and others, “Examining smart-card security under the threat of power analysis attacks”, *Computers, IEEE Transactions on*, vol. 51, no. 5, pp. 541–552, 2002.

[5] A. Arivazhagan and others, “RTL Modelling for the Cipher Blcok Chaining Mode (Cbc) for Data Security”, *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 8, no. 3, 2017.

[6] S. Oukili and S. Bri, “High throughput FPGA Implementation of Data Encryption Standard with time variable sub-keys”, *International Journal of Electrical and Computer Engineering*, vol. 6, no. 1, p. 298, 2016.

[7] P. Saravanan, N. Rajadurai, and P. Kalpana, “Power analysis attack on 8051 microcontrollers”, in *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*, 2014, pp. 1–4.

[8] F. Koeune and F.X. Standaert, “A tutorial on physical security and side-channel attacks, Foundations of Security Analysis and Design III: FOSAD 2004/2005 tutorial lectures”, Springer-Verlag, Berlin, Heidelberg, 2005.

[9] D.R. Rani and S. Venkateswarlu, “Security against Timing Analysis Attack”, *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 5, no. 4, p. 759, 2015.

[10] P.C. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems”, in *Advances in Cryptology—CRYPTO’96*, 1996, pp. 104–113.

[11] G. Deepa, G. Sri Teja, and S. Venkateswarlu, “An Overview of Acoustic Side-Channel Attack”, *International Journal of Computer Science & Communication Networks*, vol. 3, no. 1, p. 15, 2013.

[12] M. Masoumi and M.H. Rezayati, “Novel approach to protect advanced encryption standard algorithm implementation against differential electromagnetic and power analysis”, *Information Forensics and Security, IEEE Transactions on*, vol. 10, no. 2, pp. 256–265, 2015.

[13] P. Kocher, R. Lee, G. McGraw, A. Raghunathan, and S. Moderator-Ravi, “Security as a new dimension in embedded system design”, in *Proceedings of the 41st annual Design Automation Conference*, 2004, pp. 753–760.

[14] L. Goubin and J. Patarin, “DES and differential power analysis the “duplication ? method”, in *Cryptographic Hardware and Embedded Systems*, 1999, pp. 158–172.

[15] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model”, in *Cryptographic Hardware and Embedded Systems-CHES 2004*, Springer, 2004, pp. 16–29.

[16] H. Li, K. Wu, B. Peng, Y. Zhang, X. Zheng, and F. Yu, “Enhanced correlation power analysis attack on smart card”, in *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for*, 2008, pp. 2143–2148.

[17] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems”, in *Advances in Cryptology-CRYPTO*, 1991, vol. 90, pp. 2–21.

[18] S. Guilley and R. Pacalet, “SoCs security: a war against side-channels”, in *Annales des télécommunications*, 2004, vol. 59, no. 7–8, pp. 998–1009.

[19] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis”, in *Advances in Cryptology—CRYPTO’99*, 1999, pp. 388–397.

[20] S.D. Putra, A.S. Ahmad, and S. Sutikno, “Power analysis attack on implementation of DES”, in *Information Technology Systems and Innovation (ICITSI), 2016 International Conference on*, 2016, pp. 1–6.

[21] Y. Souissi, S. Guilley, S. Bhasin, and J.L. Danger, “Common framework to evaluate modern embedded systems against side-channel attacks”, in *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, 2011, pp. 86–91.

[22] B. Gierlichs, E. De Mulder, B. Preneel, and I. Verbauwhede, “Empirical comparison of side channel analysis distinguishers on DES in hardware”, in *Circuit Theory and Design, 2009. ECCTD 2009. European Conference on*, 2009, pp. 391–394.

[23] A.S. Ahmad and K.O. Bachri, “Cognitive artificial intelligence method for measuring transformer performance”, in *2016 Future Technologies Conference (FTC)*, 2016, pp. 67–73.

[24] K.O. Bachri, A.D.W. Sumari, B.A. Soedjarno, and A.S. Ahmad, “The implementation of A3S information fusion algorithm for interpreting Dissolved Gas Analysis (DGA) based on Doernenburg Ratio”, in *2017 International Symposium on Electronics and Smart Devices (ISESD)*, 2017, pp. 335–340.

[25] L. Goeirmanto, R. Mengko, and T.L. Rajab, “Direction of ventricle contraction based on precordial lead ECG signal”, in *2016 4th International Conference on Cyber and IT Service Management*, 2016, pp. 1–3.

[26] S.D. Putra, A.S. Ahmad, and S. Sutikno, “DPA-countermeasure with knowledge growing system”, in *2016 International Symposium on Electronics and Smart Devices (ISESD)*, 2016, pp. 16–20.

[27] S.D. Putra, M. Yudhiprawira, Y. Kurniawan, S. Sutikno, and A. S. Ahmad, “Security analysis of BC3 algorithm for differential power analysis attack”, in *2017 International Symposium on Electronics and Smart Devices (ISESD)*, 2017, pp. 341–345.

[28] C.O. Sereati, A.D.W. Sumari, T. Adiono, and A.S. Ahmad, “Cognitive artificial intelligence (CAI) software based on knowledge growing system (KGS) for diagnosing heart block and arrythmia”, in *2017 6th International Conference on Electrical Engineering and Informatics (ICEEI)*, 2017, pp. 1–5.

[29] C.O. Sereati, A.D.W. Sumari, T. Adiono, and A.S. Ahmad, “Implementation Knowledge Growing System Algorithm using VHDL”, in *2016 International Symposium on Electronics and Smart Devices (ISESD)*, 2016, pp. 7–10.

[30] A.D.W. Sumari, A.S. Ahmad, A.I. Wuryandari, and J. Sembiring, “Brain-inspired Knowledge Growing-System: Towards A True Cognitive Agent”, *International Journal of Computer Science & Artificial Intelligence (IJCSAI)*, vol. 2, no. 1, pp. 26–36, 2012.

[31] H.R.A. Talompo, A.S. Ahmad, Y.S. Gondokaryono, and S. Sutikno, “NAIDS design using ChiMIC-KGS”, in *2017 International Symposium on Electronics and Smart Devices (ISESD)*, 2017, pp. 346–351.

[32] S.D. Putra, A.S. Ahmad, S. Sutikno, and Y. Kurniawan, “Attacking AES-Masking Encryption Device with Correlation Power Analysis”, in *International Journal of Communication Networks and Information Security (IJCNIS)*, 2018, pp. 397–402.