Attacking AES-Masking Encryption Device with Correlation Power Analysis

Septafiansyah Dwi Putra, Adang Suwandi Ahmad, Sarwono Sutikno, Yusuf Kurniawan

School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung, Indonesia

Abstract: Cryptography is the science and art of hiding and securing information. There is a new vulnerability in a cryptographic algorithm implemented on a hardware device. This vulnerability is considered capable of uncovering secret key used in a cryptographic algorithm. This technique is known as Side channel attack (SCA). Previous and other research introduces countermeasure to countering this new vulnerability. Some researchers suggest using logic level with encoding the AES. The countermeasure using logic is very low cost and efficient. The contribution of this paper is to analyze CPA on encryption device that has been given logic level countermeasure. Our finding of this paper is the use of encoding with one-hot masking technique does not provide the maximum countermeasure effect against CPA-based attacks. In this research CPA attack can be successfully revealing the AES secret-key.

Keywords*:* AES, CPA, SCA, Attack

1. Introduction

Cryptography is the science and art of hiding and securing information. A cryptographic algorithm uses a mechanism function known as a secret key. This function is used to open encoded information. Without having knowledge of secret key, it is impossible to open encoded information in modern cryptographic algorithms today[1], [2]. An attack on a cryptographic algorithm is processed or means of encryption and decryption without using a secret key. Process of attacking a cryptographic algorithm is known as "breaking an algorithm". In recent years, there have been many researches in attacking cryptographic algorithm such as AES[3], DES[4], ECC[5], and other cryptography algortihm. Until now, those techniques has not been significantly able to uncover secret key used. It can be seen that enormous use of computation and time can only reveal and analyze a few key spaces. Secret key disclosure process of cryptographic or encryption algorithms is still a huge research opportunity, especially in terms of computing and time usage efficiency.

In general, techniques used to attack encryption algorithms are known-plaintext attacks called differential cryptanalysis [2, 13], linear cryptanalysis [19], and bruteforce analysis. In results shown by previous researchers, outcome of those attacks have not been significantly able to reveal the use of a secret key. There is a new vulnerability in a cryptographic algorithm implemented on a hardware device. This vulnerability is considered capable of uncovering secret key used in a cryptographic algorithm. This technique is known as Side channel attack (SCA). SCA is one of attack models that utilizes side informations to obtain the secret key. A cryptographic device is a device that implements cryptographic algorithms on a hardware[6–8]. Power analysis is a type of SCA attacks that can reveal confidential information[9]. Here, confidential information is secret key used in cryptographic algorithms on a hardware device. Process of acquiring a confidential information is obtained by analyzing various information leaks. The earliest known attack techniques were SPA (simple power analysis) and differential power analysis (DPA) introduced by Paul Kocher (1999) and formalized by Thomas Messerges (1999)[10]. This attack technique has shown the overall outcome of both SPA and DPA[11]. Results shown in DPA technique show 48 bits of secret key value from 64 bits of correct whole key (75%). SPA and DPA attack techniques have been proven to get 75% of secret key and the remaining bits are obtained by bruteforce technique. A second technique has been proposed in various papers, which is using the correlation factor between traces and hamming weights of the processed data[12]. In some previous studies a subkey has been obtained from secret key of AES and DES cryptographic algorithm with relatively high trace number [13][14]. Previous DPA attack patterns use a lot of trace resources (> 1000 traces) to get 75% of true bit value from masterkey. There is an improvement of the previous attack model when traces and hamming weights factor of the processed data is correlated. However, in correlation assessment, attacks must have ability to fully control plaintext value that will be encrypted on cryptographic devices. Some researchers propose approach to DPA / SCA attacks by using encoding at logic levels. The contribution of this paper is to analyze DPA on encryption device that has been given logic level countermeasure. We try to revealing AES encryption device and compare CPA attack on AES without countermesure and AES with logic countermeasure.

2. Related Research

2.1 AES Algortihm

AES algorithm consist of cipher module and key expansion module. Cipher module performs data encryption or decryption. In an AES algorithm with a 128-bit key, cipher module does ten rounds of substitutions and permutations to

encrypt data input (plaintext). This cipher module consists of SubByte, ShiftRow, MixColumn, and AddRoundKey operations. AES key generation module is derived from AES MasterKey, sometimes called as key schedule function. This module consists of two main components: the MasterKey Expansion and the SubKey Selection. Details and specifications related to implementation of AES algorithm in hardware system can refer to our related publication in. Figure 1 shows standard structure of AES-128 algorithm. This figure also shows iterative process in combining different functions of each module with cipher key expansion module.

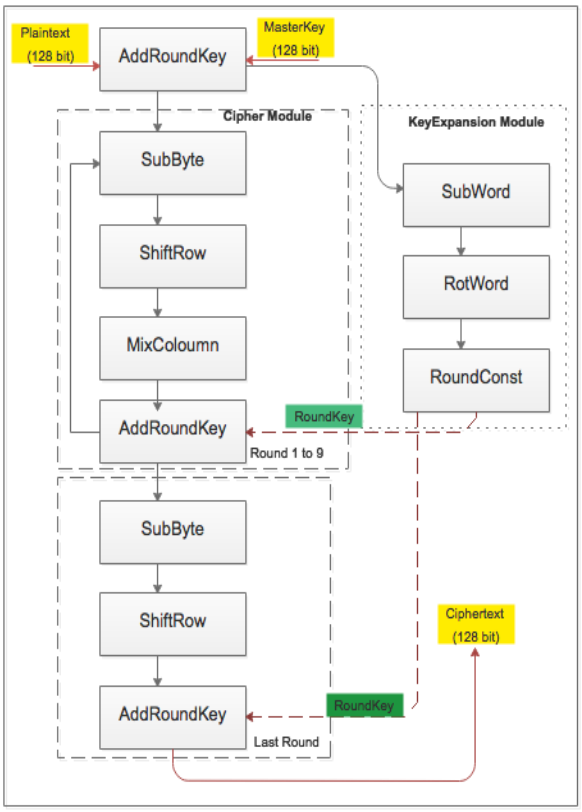

Figure 1. AES-128 Algortihm

2.2 SCA and DPA Attack Techniques

Attack technique on side channel attack is an attack based on using "side information"[15]. This side information is generated by any noise produced when encryption devices perform computations. For example, microprocessor consumes time and power to perform each task instructed. Here, side information is information that can be retrieved from encryption machine which can be either plaintext to be encrypted or ciphertext to be decrypted. This side information is acquired when encryption devices perform computational encryption, that is changing plaintext to ciphertext and vice versa. When this happens, SCA and CPA attacks can be done. Currently not only plaintext and ciphertext are produced by encryption machine, but also additional information that can be measured such as time, power, and so on. Side channel attacks utilize this information to obtain main information, i.e. plaintext, and also get secret key[16]

Side-channel analysis attacks are attacks that belong to passive and non-invasive attacks. Modern cryptographic modules are all based on digital computing that takes place inside physical devices. When computing, cryptographic devices consume electrical power and cause heat, electromagnetic radiation, and so on. It encourages opening of new information channels to attackers from manipulation and physical interaction of cryptographic devices. This leak passes on physical information. The information leakage channel is called a side-channel. Since side-channel informations depend on the value of the data being processed (intermediate value), sensitive informations associated with the key can be extracted by analyzing side-channel informations. Analogical physical leakage in devices such as power consumption or electromagnetic radiation is called as side-channel information.

Side-channel analysis has two goals. First is for designers to verify security of their devices. Another goal is for attackers to break into cryptographic systems. Chip designers, in designing their chips, try to minimize leakage of side-channel information that can be used to obtain keys. On the other hand, attackers try to find side-channel information and useful analysis methods to maximize the value of side-channel information leakage. Architecture of DPA attack technique is shown in Figure 2, which in this paper is referred as DUT (device under test) enviroment.

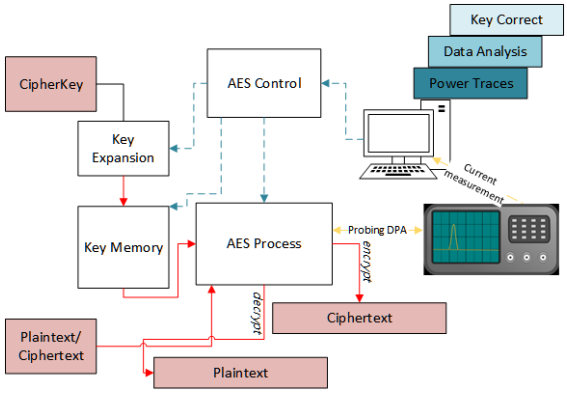

Figure 2. AES Device Under Test Architecture

Figure 2 shows main components and settings for the architecture. To run and simulate this attack technique we build DUT (device under test). This DUT environment consists of at least three connected components: AES cryptoprocessor, personal computer, and digital sampling oscilloscope (DSO). The cryptoprocessor is the DUT from which side channel information would be obtained by DSO, creating trace curves. The PC collects traces and performs statistical analyses to find key by modeling trace curves using key guesses. The DUT and the oscilloscope communicate using USB and RS232.

2.3 Countermeasure Technique at Logic Level

In designs using standard cells, RTL code will be synthesized and mapped into an embedded technology. This standard cell is also known as logic gate. In CMOS technology, power consumption of a logic gate depends heavily on data being processed. Calculating estimated value of power consumption determines the success of DPA attacks. In general, power consumption value (P_{tot}) is sum of changes in static power (P_{stat}) and dynamic power (P_{dyn}).

$$P_{tot} = P_{stat} + P_{dyn}$$

Where static power (P_{stat}) is obtained from power that a device uses during computation process multiplied by supply voltage V_{DD}.

$$P_{stat} = I_{leak}. V_{DD}$$

Change in dynamic power consumption is the most dominant factor in overall power consumption. Dynamic power consumption value depends on data processed by CMOS circuit. P_{dyn} consists of variables, including voltage (V_{DD}), frequency (f), switching activity (α) and load capacitance (C).

$$P_{dyn} = \alpha C_{load} V_2^{dd} f$$

Table 1 shows change in bit values affecting power consumption in CMOS circuits.

Tabel 1. Power consumption change and type

Bit value transition	Power consumption	Power consumption type
0 → 0	P_{00}	Static
0 → 1	P_{01}	Static + dynamic
1 → 0	P_{10}	Static + dynamic
1 → 1	P_{11}	Static

3. Security Evaluation

3.1. Side Channel Attacks

As described in previous section, there are currently many researchers beginning to address problem of physical attacks. Systems that rely on encryption devices to provide security are of considerable concern. In such systems, encryption devices are often viewed as safe tamper-resistant devices against all attacks. Anderson et al. indicate that this dependence on tamper resistance needs to be investigated in depth.

Encryption devices produce not only cipher-text output data but also some additional information such as power, time, and electromagnetic radiation, referred to as side channel information [17]. Side channel information can be exploited by attackers to extract secret informations involved in cryptographic calculations. This type of attack is known as side channel analysis [18]. Unlike traditional cryptanalysis, side channel attacks target physical cryptographic system implementations. Power analysis attacks are one type of side channel attack that exploits power information changes. Power analysis attacks can be launched with low-cost equipment and executed in short time. Power analysis is a potential and useful attack against actual implementation of cryptographic algorithms on the hardware.

From various sources of side channel information mentioned earlier, such as time measurement, electromagnetic radiation, error message, information derived from power consumption may be most difficult information to control by cryptographic designers. All calculations performed by encryption devices operate on zero and one logic gates. Process of computing encryption and decryption will lead to changes in power form and more specifically the logic gate.

3.2. Design of AES-Masking

In this section, we conducted a design proposed by other researchers before. Previous researchers have proposed use of encoding as a form of DPA countermeasure.

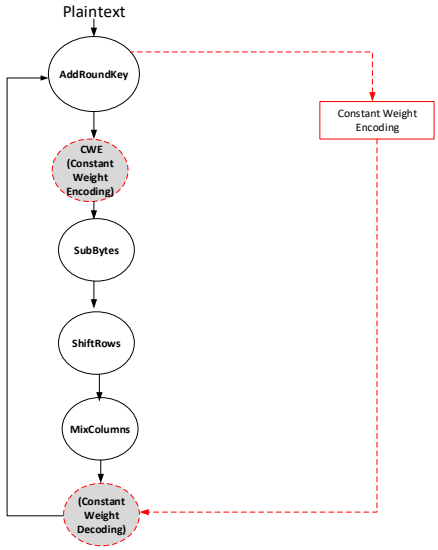

Figure 3. AES With Constant Weight Encoding

In above architecture, encoding is done to input value before SubBytes function with parameters shown in Table 2 below. Then after process SubBytes, decoding process is done and produces output value to be used in next process. Encoding and decoding processes are done based on number of rounds used. In case of AES-128, encoding and decoding process were performed for 10 iterations.

Table 2. Encoding Rule With One Hot

No	Decimal	Hex	Binary One Hot Encoding
1	0	0	0000000000000001_2
2	1	1	0000000000000010_2
3	2	2	0000000000000100_2
4	3	3	0000000000001000_2
5	4	4	0000000000010000_2
6	5	5	0000000000100000_2

No	Decimal	Hex	Binary One Hot Encoding
7	6	6	0000000001000000_2
8	7	7	0000000010000000_2
9	8	8	0000000100000000_2
10	9	9	0000001000000000_2
11	10	A	0000010000000000_2
12	11	B	0000100000000000_2
13	12	C	0001000000000000_2
14	13	D	0010000000000000_2
15	14	E	0100000000000000_2
16	15	F	1000000000000000_2

Every m bit codeword ranges from zero to 15. That is, total number of m bit codewords ranges. This encoding rule is required to get a constant value of hamming weight. For this encoding rule, the result of hamming weight is 1. The main reason for using constant values in hamming weight is a very close association of information leakage on side channel. Details of this encoding rule are shown by:

$$EncodingR_{(n,1,16)} : \{0,1\}^n \rightarrow \{z \in \{0,1\}^n \mid HW(z)= 1\}$$

Where HW is hamming weight function, and $EncodingR_{(n,1,16)}$ is one-hot encoding function. N represents value to be encoded.

4. Research Result and Analysis

In this paper we conduct DPA analysis with supporting equipments which have following specifications:

Table 3. Lab Setup for DPA-DoM

Algorithm and length of key	AES -128 bit
Sample frequency	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

Differential power analysis attack used in this study is correlation power analysis (CPA). Basic idea of CPA is to make one hypothesis from correlation value of key guess and traces. Next, we create a special function known as selection function. This selection function gets input value of the key guess $KeyGuess_j$, where $KeyGuess_j = (k_{g1}, k_{g2}, ... k_{g255})$.

Algorithm 1. CPA for HD AES Last Round

Input: N pairs traces with ciphertext C_i and KeyGuess = key guess
Output: Recovered key for K

```
for state = 1 to 16 do
    for i = 1 to number of traces do
    for j = 1 to 256 do
    inv_sbox[i,:] = (bitxor(Ciphertext, KeyGuess))
    reg_after[i,:]=InvSbox(Invshiftrow(bitxor(CTi,KeyGuessj)))
    power_consumption = HD(inv_sbox[i,:],reg_after[i,:])
    cmatrix[:]¬absolute(Pearson_Correlation(traces,power_consu
    mption[:, j]));
    end
    End
     K[state] ← rowNumber(max(cmatrix)
   End
```

CPA analysis process begins by initializing required variables. Simulation will then load trace and plaintext that will be used for each ongoing encryption process. Key logging is done in iteration representing state. This attack targets AES devices that have been given constant weight encoding. Attacking process is done by guessing the key used in initial AddRoundKey operation or before entering encryption rounds. Predictable keys are 8-bit size for every single state. In that iteration, key hypothesis will be calculated by simulating or calculating intermediate value in first two stages of AES algorithm (AddRoundKey before first round and SubBytes of first round).

We manage to get whole 128 bits of key from AES divided into 16 states. In that test, we used 2000 pieces of traces. We use Correlation Power Analysis (CPA) to measure connection between power consumption model and trace used. Since power consumption model and trace can have a proportional or reverse relationship, value sought in DPA attacks is absolute value of PCC. In first test we used a CPA with a Hamming Weight approach on its leakage model. However, these results do not show success in attack techniques. Then, in second test we used Hamming Distance (HD) approach in last round of AES encryption. Excellent results are shown on HD usage. The formula of CPA is shown in the following equations:

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i}-\bar{h}_i).(t_{d,j}-\bar{t}_j)}{\sqrt{\sum_{d=1}^{D}(h_{d,i}-\bar{h}_i)^2.\sum_{d=1}^{D}(t_{d,j}-\bar{t}_j)^2}} \quad ...(2)$$

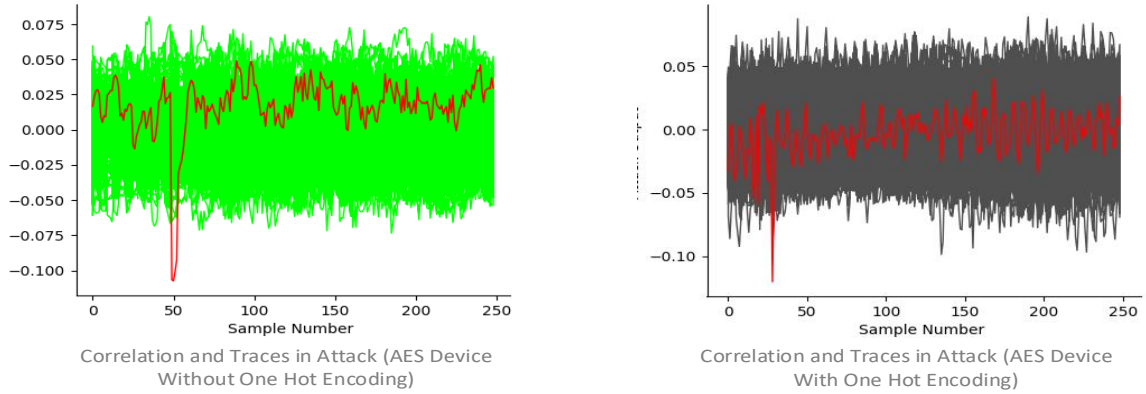

Figure 4. Comparison of CPA Attacks on AES Without Countermeasure and With Logic Countermeasure

In equation (2), $r_{i,j}$ is denoted as CPA value on key guess i and point j on the trace; D is number of traces and d is trace enumerator; $h_{i,j}$ is the power consumption hypothesis on key guess i and point j on the trace and $\bar{h}_i$ is average power consumption hypothesis on key guess i; and $t_{d,j}$ is d-th trace at j-th point and $\bar{t}_j$ is average of the trace at j-th point.

Table 5. Result for CPA attack

No	Variable Testing	Without Encoding	With Masking-Encoding
1.	The number of traces needed	2100	2500
2.	Execution time	300 seconds	360 seconds
3.	A number of key bits gained	128bits	128bits
4.	A number of missing key bits	0bits	0bits

5. Concluding Remarks

Use of encoding with one-hot masking technique does not provide maximum countermeasure effect against CPA-based attacks. Figure 4 show the comparison of CPA Attacks on AES without countermeasure and AES with logic countermeasure. From the above figure, CPA attack can be succesfully revealing the key.

Table 5 and Figure 5 show the Number Traces Needed for CPA Attacks on AES Without Countermeasure and With Logic Countermeasure. This small difference is assumed as the CPA attack can be successfull for AES with logic countermeasure . Test result shows that the attack has succeeded in recovering whole 128-bit key (100% key recovery). Attacking simulation test is done by using 2500 traces and take 6 minutes of execution. Comparison of DPA attacks on AES with countermeasure and countermeasure counts by simply adding the number of traces. The key can be directly recovered because of AES algorithm vulnerability in initial AddRoundKey operation which is, basically, an XOR operation of plaintext and masterkey. The result produced are okey used and key guesses of the simulation that correspond to sequence of simulated states (43 126 21 22 40 174 210 166 271 247 21 136 9 207 79 60).

6. References

[1] R. Thandeeswaran and M. S. Durai, "DPCA: Dual Phase Cloud Infrastructure Authentication," *International Journal of Communication Networks and Information Security*, vol. 8, no. 3, p. 197, 2016.

[2] M. Yuliana, S. Wirawan, and others, "Performance Improvement of Secret Key Generation Scheme in Wireless Indoor Environment," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 9, no. 3, 2017.

[3] NIST, *FIPS 197, Advanced Encryption Standard (AES)*, no. 197. 21: Federal Information Processing Standards Publications, 2001.

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

[5] H. Li, K. Wu, G. Xu, H. Yuan, and P. Luo, "Simple power analysis attacks using chosen message against ECC hardware implementations," in *Internet Security (WorldCIS), 2011 World Congress on*, 2011, pp. 68–72.

[6] 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.

[7] H. S. Deshpande, K. J. Karande, and A. O. Mulani, "Area optimized implementation of AES algorithm on FPGA," in *Communications and Signal Processing (ICCSP), 2015 International Conference on*, 2015, pp. 10–14.

[8] O. S. Dhede and S. Shah, "A review: Hardware Implementation of AES using minimal resources on FPGA," in *Pervasive Computing (ICPC), 2015 International Conference on*, 2015, pp. 1–3.
[9] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO'99*, 1999, pp. 388–397.
[10] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Investigations of Power Analysis Attacks on Smartcards.," *Smartcard*, vol. 99, pp. 151–161, 1999.
[11] L. Goubin and J. Patarin, "DES and differential power analysis the "duplication"? method," in *Cryptographic Hardware and Embedded Systems*, 1999, pp. 158–172.
[12] 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.
[13] R. Mayer-Sommer, "Smartly analyzing the simplicity and the power of simple power analysis on smartcards," in *Cryptographic Hardware and Embedded Systems—CHES 2000*, 2000, pp. 78–92.
[14] W. Shan, X. Fu, and Z. Xu, "A Secure Reconfigurable Crypto IC With Countermeasures Against SPA, DPA, and EMA," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 34, no. 7, pp. 1201–1205, 2015.
[15] J.-Y. Park, D.-G. Han, O. Yi, and J. Kim, "An improved side channel attack using event information of subtraction," *Journal of Network and Computer Applications*, vol. 38, pp. 99–105, 2014.
[16] P. C. Kocher, J. M. Jaffe, and B. C. Jun, "Differential power analysis." Google Patents, 2009.
[17] 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.
[18] 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.

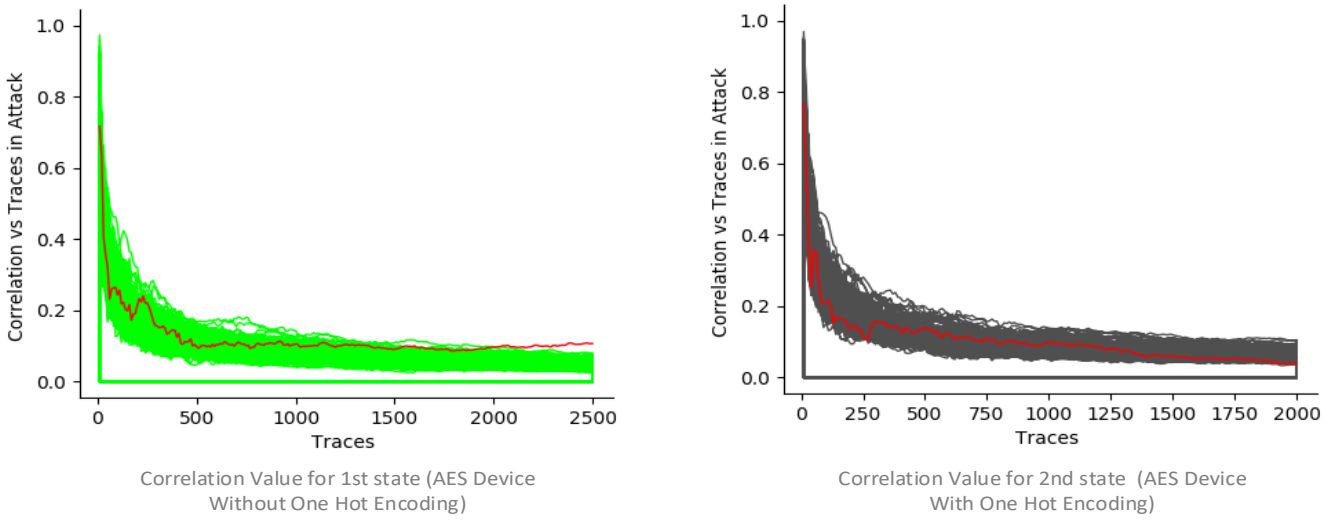

Figure 5. Comparison of Traces Needed For CPA Attacks on AES Without Countermeasure and With Logic Countermeasure