MNK Publication

International Journal of Latest Research in Science and Technology **ISSN (Online):2278-5299**
Vol.1,Issue 2 :Page No.137-140 ,July-August 2012
https://www.mnkpublication.com/journal/ijlrst/index.php

USING SYNCHRONOUS AND ASYNCHRONOUS SYSTEMS AS A COUNTER-MEASURE FOR POWER ATTACKS ON ADVANCED ENCRYPTION SYSTEM

S.Mohamed Salhian
Research Scholar Singhania University.
msalhian@hotmail.com

Abstract*— The selection and widespread usage of the cryptographic algorithm Advanced Encryption Standard by the US Government has made this as the de-facto standard worldwide. This popularity of AES had invited various cryptanalysts to try to break this standard. Though officially it was not broken, many researchers had predicted and in-fact documented methods to prove that it can be broken. One such method is Differential Power Analysis attack which is powerful and expected to give out the secret keys. Here we have given a method using Synchronous communication and asynchronous communication for within the module and between the modules of AES algorithm. This modification acts as a counter-measure and gives improved strength against the power attack.

Keywords— Advanced Encryption Standard(AES), Cryptanalysis, Differential Power Analysis attack, Synchronous, Asynchronous

I. INTRODUCTION

Modern cryptographic algorithms are designed to be secure against all known mathematical cryptanalysis techniques. Due to the length of key and current computer processing power, cracking them using brute force takes a considerably long amount of time.

Apart from brute force attack, there is another group of attacks called *side channel attacks,* which rely on the fact that a cryptographic device is not a 'black box' where the plaintext goes in and the cyphertext comes out, but a complex physical device that leaks information on its internal actions through other channels like the power consumption, timing and electromagnetic emissions. This is indicated in Fig.1.

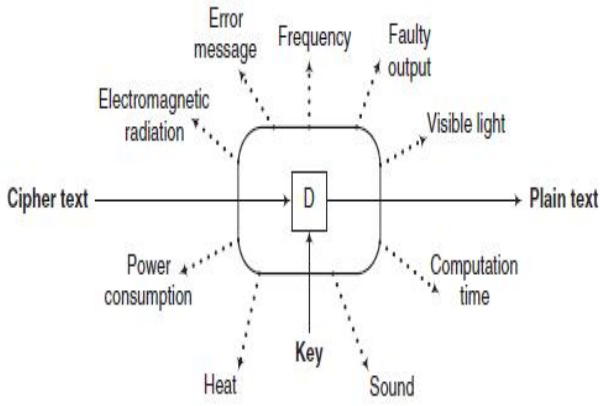

Fig. **1** **Decryption process using the Crypto-engine.**

(Dotted lines are side channels)

It is not the standard that is weak but the implementation of the standard is weak, emenating various informations leading to the cracking of the whole process by way of the secret key knowledge.

The progressively strong physical attack referred to as side channel or covert channel attack takes advantage of implementation specific characteristics to recover the secret parameters involved in the computation. Normally a crypto-graphic scheme is developed against traditional algebraic attacks. The VLSI designer optimizes the hardware with respect to time, area and power only [1]. But the crypto-processor releases several unwanted information through covert channels which are normally neglected by the design engineers. These hidden side channels could be exploited to perform an attack on the decryption function.

This side channel attacks can be divided in two groups as *active* and *passive* attacks depending on the ability of the attack. In active attack, the attacker has to enter the internal circuit of the cryptographic device. The passive attack uses the standard functionality like physical and electrical effects during implementation of the algorithm. Different types of passive attacks are Timing attacks-exploiting the timing information, Power attacks- using the dynamic power consumption, Electromagnetic attacks-using the EM radiation and Acoustic attacks-using the sound coming out of the cryptographic hardware during the execution of the cryptographic algorithm. All the groups of passive attacks have two types namely *simple* and *differential analysis* attacks.

From the long list of Cryptographic algorithms, the Rijndael ciper algorithm developed by Rijmen and Daemen was selected as the Advanced Encryption Standard (AES)

Publication History
Manuscript Received : *25 July 2012*
Manuscript Accepted : *15 August 2012*
Revision Received : *20 August 2012*
Manuscript Published : *31 August 2012*

by the US government body (NIST) in 2000 [2]. AES was analyzed extensively and is used now worldwide.

In this paper a new method of implementation of AES making use of two types of communication systems, namely asynchronous system for intercommunication between different modules and synchronous system for communication within the module is presented. Also the clock for the synchronous system was made random by the use of a random number generator. The combined effect of both modifications has resulted in high resistance towards the power analysis attack.

The rest of the paper is organized as follows. Section II describes the normal AES implementation in brief, whereas one of the side-channel attack namely differential power analysis attack has been explained in section III. The section IV gives the details of modification to counter the effects of attacks and the next section V gives the effects of modifications. This is followed by conclusion and bibliography in the last sections VI and VII.

II. ADVANCED ENCRYPTION STANDARD (AES)

AES is an iterated block cipher with a block length of 128 bits and with variable key lengths of 128, 192 and 256 bits. Along-with security, the major advantage of AES is its efficient implementation on various platforms. It is suitable for small 8-bit microprocessor platforms, common 32-bit processors and dedicated hardware implementations that can reach throughput rates in the gigabit range.

The several operations that are implemented in this algorithm are listed below:

**Key Schedule*: It is an array of 32-bit words that is initialized from the cipher key. The cipher iterates through a number of cycles or rounds, each of which uses *Nk* words from the key schedule. This is considered as an array of round keys, each containing *Nk* words.

***Finite Field Operations*: In this algorithm, finite field operations are carried out, which refers to operations performed in the finite field resulting in an element within that field. Finite field operations such as addition, multiplication, inverse multiplication, multiplications using tables and repeated shifts are performed.

***Rounds*: At the start of the cipher the inputs message and key are copied into the internal state. An initial round key is then added and the state is then transformed by iterating a round function in a number of cycles. On completion, the final state is copied into the cipher output. The round function is parameterized using a key schedule that consists of a one dimensional array of 32-bit words for which the lowest 4, 6 or 8 words are initialized with the cipher. There are several steps carried out during this operation:

***Sub-Bytes*: It is a non-linear substitution step where each of the byte replaces with another according to a lookup table.

***Shift-Rows*: This is a transposition step where each row of the state is shifted cyclically a certain number of steps.

***Mix-Columns*: This is a mixing operation which operates on the columns of the state, combining the

***Add-Round-Key*: Here each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

***Final-Round*: The final round consists of the same operations as in the Round function except the Mix-Columns operation.

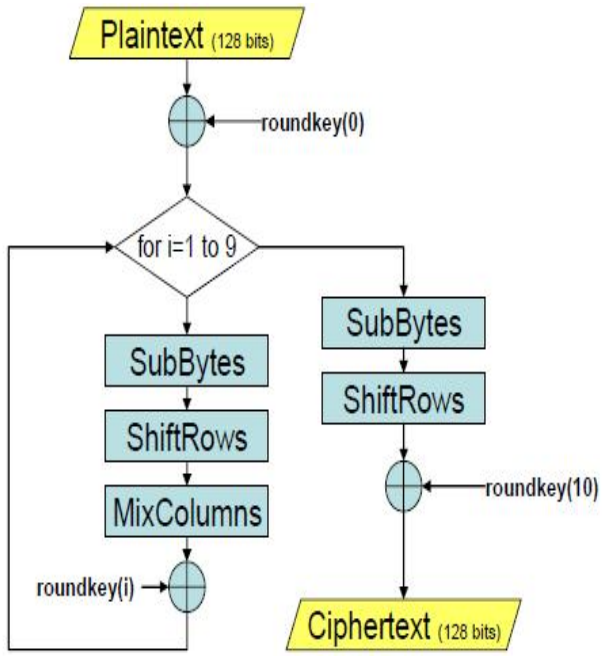

Fig 2. AES Algorithm (encryption)

III.DIFFERNTIAL POWER ANALYSIS ATTACK

Power analysis is a type of side channel attack that was first developed by Kocher in 1996 [3]. It uses the fact that in digital circuits, Complementary Metal Oxide Semiconductor (CMOS) technology, there is a significant data dependence in the power consumption, due to the large amount of current flowing when a bit changes value compared to the small amount when it does not. Differential Power Analysis (DPA) is a type of power analysis that applies statistical tests to the power consumption data from large number of encryptions in order to determine the most probable key value from a set of hypotheses.

The power traces were partitioned based on the predicted value of a bit on the output of an S-box[4], the groups of traces are then averaged and one is subtracted from the other. When the hypothesis is correct there will be a large peak in the differential trace. The technique was improved by Brier[5] to use an optimal statistical test. Under the following assumptions the power consumption of a device can be modelled as:

i) The energy required for switching a bit from 0 to 1 and the energy required for switching a bit from 1 to 0 are the same.

ii) Remaining changes in the circuit can be modelled as noise with a normal distribution

This leads to equation (1) for the power consumption of a device:

$$W = aH\ (Ri \oplus R_{i-1}) + b \qquad (1)$$

Where *W* is the power consumption, *R*i is the current register value, *Ri-1* is the previous register value, *a* is the linear scaling factor and *b* is noise, the contribution from the rest of the circuit. Based on a known plaintext and the assumed value of a byte of the key, it is possible to predict the value inside a register. This is then repeated for several plaintexts. A statistical test is then used to compare the predictions to the power consumption in order to determine the most likely value for the key byte.

There are several different tests that were used for this and the correlation coefficient is the best of these. As the correlation coefficient determines the strength and direction of the linear relationship between two variables it is an ideal test for this situation. The value varies between -1 and 1. A value of 1 means there is a perfect linear relationship between the two variables, -1 means there is a perfect inverse relationship and 0 means there is no linear relationship, although this does not always mean that there is no relationship at all. In practice it is not possible to know the true values for the covariance or standard deviation of variables, only calculations of approximations of them based on the values discovered through experiments.

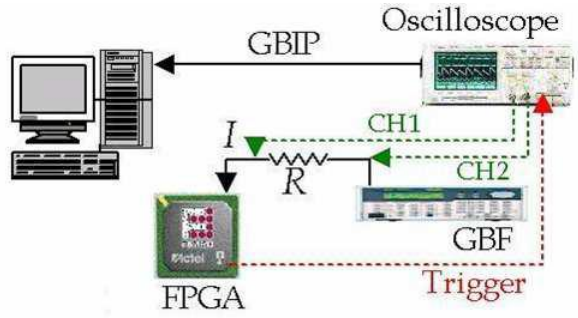

Fig. 3. Experimental configuration for Differential Power Analysis Attack on a FPGA board

The DPA algorithm used here is implemented in three steps.

A. Prediction

B. Measurement

C. Correlation.

The first, prediction step uses the plaintext and a guess of one byte of the key to predict the number of bits that change in one intermediate byte in a register. This is repeated for all plaintexts and all possible values of the key byte, and then entered in the prediction matrix.

The second step is to measure the instantaneous power consumption during the encryption of the plaintext and put into the measurement matrix.

The final step is to calculate the correlation between each column in the measurement matrix and each column in the prediction matrix. The resulting highest value represents the correct key guess and time when the value in the targeted register changes.

The DPA attack is basically targeting a specific operation of the algorithm of the cryptographic system, that gives out the more useful information about the cypher key as much as possible. For an AES implementation the Sub-Bytes operation during the first or last of the encryption round is normally targeted. DPA attacks normally target a small portion of the cipher key namely sub-key of 8 to 16 bits typically[8]. As the attacks on keys are independent, the same procedure can be repeated on remaining portions with-out much difficulty.

Based on the available circuit model knowledge, the attacker devises a simple model of the chip. Using this simple model, the hypothetical power consumption for all the permutations of the sub-key is estimated with a large number of plain-texts. Later measurements were taken for the device under attack while it encrypts the same set of plain-texts. The DPA attack is successful if and only if one of the sub-key permutations shows a distinctively higher correlation to the actual power measurement.

IV. SYNCHRONOUS & ASYNCHRONOUS DESIGNS

A global clock is used in synchronous design methodology whereas in asynchronous no such clock driving large on-chip load is used. This results in the power spectrum of an asynchronous circuit more uniform. Here the advantage of asynchronous design with the convenience of synchronous design is used to reduce the vulnerability of cryptographic hardware to the differential power attack [6].

For the small modules local synchronous circuits with the standard design provide the functionality. These local modules are formed by encapsulating with individual self-timed clock along with an asynchronous port controller that governs the communication between these modules. The communication between these modules is fully asynchronous[7]. For communication between modules the asynchronous port controllers can momentarily pause the local clock so that the concerned communication partners can be synchronized for the data transfer.

If we analyse the AES functions, the round function is divided between two data paths. The Sub-Bytes and Mix-Columns operations are performed in a unit called ‘A’. This unit ‘A’ takes a 32 bit word and using two parallel look-up tables (LUT’s), applies four Sub-Byte transformations and the Mix-Column operation following this. The rest two operations Add-Round key and Shift-Rows along with the Round-Key generation are performed in another unit called ‘B’. As we can expect the total system consists of single ‘B’ unit and two identical units of ‘A’. All three units are equipped with the addition of local clock generator and asynchronous port controllers.

The port controllers of ‘A’to‘B’ and ‘B’to‘A’ use a four phase handshaking protocol to control the data flow between ‘A‘ and ‘B’. Once ‘A’ is ready to accept the new data it signals the information by activating the port controller ‘A’to‘B’. ‘A’ then monitors the status of the port controller and waits until the data transfer is complete. For the other part, once ‘B’ is ready to send new data to ‘A’ it activates the port controller ‘B’to‘A’. As soon as the port is activated, it will send a data transfer request to the ‘A’to‘B’ controller. This controller if it has been activated, will pause the local clock of ‘A’ and acknowledge the request back to ‘B’to‘A’.

As soon as the acknowledge signal is received by 'B'to'A', the local clock of 'B' will also be paused. At this time the data can be transferred between two units reliably. Both controllers will inform their respective units, the successful data transfer and release their local clocks thus reverting their handshaking signals to their initial condition.

V. EFFECTS OF MODIFICATIONS

The various effects of the above-mentioned modifications are listed below.

i) Independent Clocks:

All three units of this system are having their own independent local clock generators. During data transfer alone, the phases of local clocks of the communicating devices are synchronized for a short time in the handshaking operation. Rest of the time the phase and frequency of the clock generators are fully un-related.

ii) Random Clock Periods:

The local clock generator used in this system was designed to run at different frequencies[9]. The various frequencies were selected using a pseudo random number generator. Depending on stored configuration settings it selects one of a fixed number of frequency settings for the next clock period. Of course the minimum clock period must be configured to match the critical path of individual units.

iii) Arbitrary order of execution:

For each encryption round, unit 'B' needs the result of four Mix-Columns operation, which are programmed on two instances of two of unit 'A'. Similarly for each Mix-Column operation, unit 'A' must programme four Sub-Bytes operations on two hook-up tables. In both above cases the ordering of these operations can be determined arbitrarily. This reordering of operations, without increasing the latency of the encryption adds a large amount of confusion in the execution time of the targeted operation.

The combination of all these effects presents a difficult challenge for the DPA arrack and increases the overall resistance.

VI. CONCLUSIONS

We have described how the use of synchronous communication for communication inside the module where a set of operation is expected to be carried out and asynchronous communication for communication outside the module where the modules are expected to deliver and receive the signals for again operations inside those concerned modules can present a difficult situation for the attacker. Here we have taken the scenario of the differential power analysis attack to precisely tune our counter-measures. The various measures indicated gives considerable strength for the modified algorithm in particular the AES to resist the DPA attack.

No doubt the additional modifications to the algorithm or in other words to the circuit will definitely increase the complication of the circuit. This in turn increases the area, power and to some extent the latency of the system. Hence it may not be compatible to the low power cryptographic devices in smart-card systems and the like.

An in-depth evaluation of the proposed DPA counter-measures will be the continuation of this project.

BIBLIOGRAPHY

[1] N. H. E. Weste and K. Eshraghian, *Principles of CMOS VLSI design*. Addison-Wesley Publishing Company, 1993.

[2] National Institute of Standards and Technology, *Advanced Encryption Standard (FIPS PUB 197)*, http://www.nist.gov/aes, 2001.

[3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology – Crypto '99*, ser. Lecture Notes in Computer Science, vol. 1666. Springer-Verlag, 1999, pp. 388–397.

[4] V. Rijnmen, "Effificient Implementation of the Rijndael S-box," http://csrc.nist.gov/CryptoToolkit/aes/

[5] E. Brier, C. Clavier and F. Olivier, "Correlation power analysis with a eakage model," in CHES 2004, LNCS 3156, 2004, pp 16-29.

[6] J. Sparsø and S. Furber, Eds., *Principles of asynchronous circuit design*. Kluwer Academic Publishers, 2001.

[7] G. Birtwistle and A. D. (Eds), *Asynchronous Digital Circuit Design*. Springer, 1995.

[8] S. B. Ors, F. Gurkaynak, E. Oswald, and B. Preneel, "Power analysis attack on an ASIC AES implementation," ITCC 2004, LV. NV

[9] Y. Zafar, J. Park, D. Har, "Random Clocking Induced DPA Attack Immunity in FPGAs," ICIT 2010, March 2010, pp 1068-1070. Family," Infineon Technologies AG 81726 Munich, Germany, Nov 2008.