Research Paper

Volume : 2 | Issue : 11 | November 2013 • ISSN No 2277 - 8179

An Evaluation of Power Analysis Attacks on Asynchronous Substitution Box

Engineering

KEYWORDS : Differential power analysis, Side channel attack, correlation power analysis, substitution box and null convention logic.

S. Muhammad Jakheer	Department of Electronics & Communication Engineering, M.Tech Scholar of Madina Engg College Kadapa, INDIA.
Shaik Jaffar	Professor in ECE Dept, Madina Engg College Kadapa,INDIA
Syed Jahangir Badashah	Assoc Professor in ECE Dept, Madina Engg College Kadapa,INDIA

ABSTRACT

In this paper we demonstrate implementation of less-power asynchronous Advanced Encryption Standard substitution box design capable of being resistant to the side channel attack. A specified side channel attack standard evaluation field-programmable gate array board is used to implement both asynchronous and synchronous substitution box designs. This asynchronous substitution box, is based on a self-time logic referred as null convention logic which supports beneficial properties for resisting side channel attack dual-rail encoding, clock free and monotonic transitions. These properties make it difficult for an attack to decipher secret keys embedded in the cryptographic circuit of FPGA board. Comparisons on the resistance to side channel attack of both the original and proposed substitution box design are presented, using correlation power analysis and differential power analysis attacks. The power measurement results showed that the null convention logic substitution box had 24%–28% lower than total power consumption, was effective against differential power analysis and correlation power analysis attacks. An important factor of successfully implementing differential power analysis or correlation power analysis attacks, the number of power traces, are also analyzed in the paper.

I.INTRODUCTION

Security in mobile applications is very importance because a large number may be exposed in a hostile environment. Cryptographic services are required for these applications, provide solutions for data protection and also self- implementation concerns. If are captured by attackers, side-channel information leakages, such as power consumption, timing and electromagnetic radiation, are monitored for cryptanalysis. Among them, differential power analysis creates a high threat to the different cryptographic implementations due to it is practical, power attacks are divided into singlebit DPA and multibit DPA. In singlebit DPA attack, a certain bit of intermediate results are predicted. This is used to split the power measurements into two sets, are computed and subtracted. In multibit DPA, multiple bits of intermediate results are predicted.

In the two contexts, we had verified the peaks of bias signal by observing DPA traces. It is often subjective. The CPA is presented with a correlation factor between the output of power model and real power trace is shown. The correlation factors can be compared in different CPA trace at cost of computational complexity. Our improved DPA approach overcomes these drawbacks in the following analyses. Accurate measurement and estimation of these outputs are the key points of a successful attack. Sub Bytes step is the first step of AES round. Each byte in the array is updated by a 8-bit substitution box, derived from the multiplicative inverse over GF(28). AES S Box is constructed by the combination of inverse function with an invertible affine transformation in order to avoid attacks based on mathematics.

The attack is based on the fact that logic operations have power characteristics that depend on the input data. Its statistical analysis is to extract the information from the power consumption that is correlated to the secret key. Usually, there are four methods to conduct the power measurement experiments:

- using regular field-programmable gate array board,
- using computer-aided design tools,
- using the SASEBO-GII FPGA board and
- using a taped-out application-specific integrated circuit chip.

The procedures of taping out a chip include the frontend verification using CAD tools and an FPGA board. They are complicated and time-consuming. Therefore, in order to prove the proposed idea in a more effective way, the first three methods have been tried, and the experimental results show that the third method is the most effective one. The ration behind this lies as follows. First, while CAD-tool-based simulation shows that the synchronous S-Box design is indeed vulnerable to the DPA attacks, the DPA attacks could not be successfully implemented on the NCL S-Box by such simulation due to too much regularity in the power traces. The reason is that the CAD tools approximate the simulation results. Second, there are many constraints using regular FPGA board for this paper. However, the bandwidth of current probes is usually lower than that of voltage probes, which might not be able to capture the high-frequency alternating-current variations caused by data transients. Third, a stable power supply is critically important for power analysis experiments.

II.LITERATURE SURVEY

Power-Analysis Attack on an ASIC AES implementation,J.Kocher, and B. Jun, San Francisco, CA, 1998,Tech. Rep. The Advanced Encryption Standard, a new block cipher standard published by US government in 2001. As a consequence, the growing interest in efficient implementations of the AES, these implementations are to be resistant against side channel attacks, it should not be easy to extract information from physical measurements of the device. This article presents the first result on the feasibility of power analysis attack against an AES hardware implementation.

The security of Rijndael is evaluated with respect to all types of attacks. While being resistant to the classical cryptanalytic methods, it turned out that so-called implementation attacks are a serious threat of the Rijndael algorithm.

Power analysis attacks are passive implementation attacks. Computer security aspects in industrial instrumentation and measurements, M. Lazzaroni, V. Piuri, and C. Maziero, in Proc. IEEE I2MTC, May 2010. Industrial Control Systems (ICS), formerly isolated proprietary systems, are giving place to highly-connected systems, implemented using widespread operating systems and network tools on public networks.

As computer systems become more pervasive and connected, their security-related aspects should receive increasing attention.

Industrial Control Systems, formerly isolated proprietary sys-

tems, are giving place to highly-connected systems, implemented using widespread operating systems and network protocols in public networks.Such standardization trend is imposed by interoperability and cost reduction needs.

However, it also opens the door to security threats previously restricted to the corporate and personal computing areas.

Measurement of power consumption in digital systems, V. Konstantakos, K.Kosmatopoulos, S. Nikolaidis, and T. Eliopoulos, IEEE Trans. A study on measurement configurations for the estimation of power consumption of processing systems is presented in this work. The problem addressed is to measure the energy that a digital system consumes for a numerous number of clock cycles and to assign this consumption to a specific group of instructions.

The increasing popularity of low-power applications drives the need for analyzing and optimizing power consumption in all parts of a micro-processing system.

Accurate measurement and analysis of the power consumption is essential in order to evaluate the hardware and software related power consumption of a processing system.

The main reason for searching for information about power consumption is mainly the verification of the overall system's power budget.

III.PROPOSED SYSTEM

The AES algorithm consists of a number of rounds that are dependent on the key size. For both cipher and inverse cipher of the AES algorithm, each round consists of linear operation and nonlinear operation. SUBBYTES step is the first step of AES round. Each byte in the array is updated by an 8-bit S-Box, which is derived from the multiplicative inverse over GF(28).A block diagram of the AES S-Box is shown in Fig. The affine transformation and inverse affine Transformation components follow a series of Boolean equations given in Table where i and q. Represents the 8-bit input and output, respectively. Both transformations require many XOR gates. First, map operation converts the 8-bit input into elements of GF (24) (i.e., ah and al). Second, calculate the square of ah and al. It should be noticed that multiplication in GF (24) is done by multiplying the polynomial ah(x)ah(x) followed by a modular reduction. Third, a series of multiplication and XOR operations were implemented to extend the field GF(24) to the field GF(28). To implement this conventional S-Box using NCL, the XOR, AND, and MUX operations in dual-rail NCL gates are required.

We can find that the dual-rail encoding, with the pre charge method, spacers, or return-to zero protocols, is frequently used in both synchronous and asynchronous designs. The dual-rail encoding provides better data in dependence with the power consumption since the Hamming weights (HWs) of each data set are the same. An RTZ protocol, a spacer, or the precharge method was used to achieve the monotonic transition to enhance the security. Our proposed null-conventional-logic-based substitution box design essentially matches all these important security properties: asynchronous, dualrail encoding, and an intermediate state.Unlike other asynchronous designs, NCL adheres to the monotonic transitions between DATA and NULL, which utilizes dual-rail and quadrail signaling methods to achieve the delay insensitivity. This would significantly reduce the design complexity. With the absence of a clock, the NCL system is proved to reduce the power consumption, noise, and electromagnetic interference. Furthermore, we have demonstrated that NCL can also resist SCAs without worrying about the glitches and power supply variations. This paper provides an extension to what has been presented. In addition to the DPA attack, a CPA attack has also been applied to both synchronous and NCL S-Box design to demonstrate that the proposed NCL S-Box is capable of resisting CPA attack as well

IV. METHODS AND SOLUTIONS

Power analysis attacks exploit the correlation between the data and the instantaneous power consumption of cryptographic devices. As this correlation is usually very small, statistical methods should be used to exploit it efficiently. In a power analysis attack, an attacker first creates a hypothetical power model of the cryptographic device at a very abstract level. In practice, each cryptographic algorithm designed operates only small parts of the secret key, called sub key, at certain period. In order to set up the correlation, predictions from different power models and statistical methods must be tested. An important improvement has come with the appearing of high-order DPA. There are two basic attack scenarios we consider: collision attacks without pro-filing and collision attacks with profiling. A collision attack without profiling consists of an online stage and an offline stage, while a collision attack with profiling additionally contains a profiling stage. In the optional profiling stage, the device is triggered to perform a number of cryptographic operations with some unknown profiling inputs for some unknown keys. The profiling traces are acquired by the measurement equipment. The profiling stage takes place before the online stage and can be reused by several attacks on the same implementation. The offline stage recovers the key. This occurs in two steps. First, collisions are detected in the online traces Ti by means of signal processing. The collision detection with profiling additionally uses the profiling traces. Second, an AES key candidate is obtained using the detected collisions and the corresponding inputs Pi. Note that one or several plaintext-cipher text pairs produced with the attacked key may be needed to identify the correct key candidate in the offline stage. If averaging is applied, the attacker has to be able to send several unknown equal inputs to the device and to fix some unknown key for these measurements in the profiling stage.

AFFINE TRANSFORM AND INVERSE AFFINE TRANSFORMATION

The affine transformation and inverse affine transformation components follow a series of Boolean equations given in Table I, where i and q represents the 8-bit input and output, respectively. Both transformations require many XOR gates.

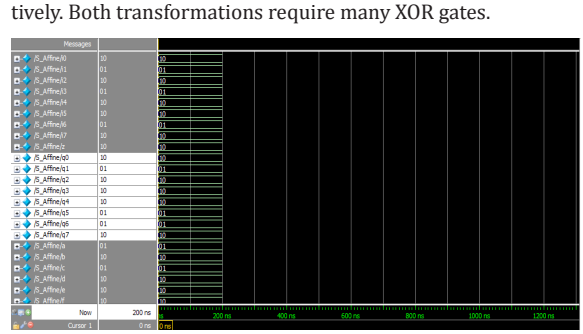

Figure 1 Affine Transformation NCL

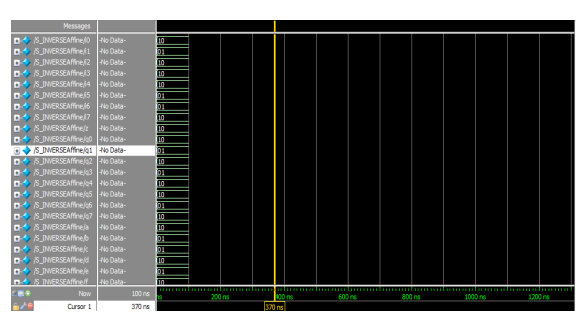

Figure 2 Inverse Affine Transformation NCL

Volume : 2 | Issue : 11 | November 2013 • ISSN No 2277 - 8179

TABLE I BOOLEAN EQUATIONS FOR AFFINE TRANSFORMATION AND INVERSE AFFINE TRANSFORMATION COMPONENTS

q=a f f_trans(i)	q=a f f_trans^{-1}(i)
$q_0=(i_0 \oplus i_4) \oplus (i_5 \oplus i_6) \oplus (i_7 \oplus 1)$	$q_0=i_2 \oplus i_5 \oplus i_7 \oplus 1$
$q_1=i_1 \oplus i_5 \oplus i_6 \oplus i_7 \oplus i_0 \oplus 1$	$q_1=i_0 \oplus i_3 \oplus i_6$
$q_2=i_2 \oplus i_6 \oplus i_7 \oplus i_0 \oplus i_1$	$q_2=i_1 \oplus i_4 \oplus i_7 \oplus 1$
$q_3=i_3 \oplus i_7 \oplus i_0 \oplus i_1 \oplus i_2$	$q_3=i_2 \oplus i_5 \oplus i_0$
$q_4=i_4 \oplus i_0 \oplus i_1 \oplus i_2 \oplus i_3$	$q_4=i_1 \oplus i_3 \oplus i_6$
$q_5=i_1 \oplus i_5 \oplus i_2 \oplus i_3 \oplus i_4 \oplus 1$	$q_5=i_2 \oplus i_4 \oplus i_7$
$q_6=i_6 \oplus i_2 \oplus i_3 \oplus i_4 \oplus i_5 \oplus 1$	$q_6=i_0 \oplus i_3 \oplus i_5 \oplus 1$
$q_7=i_7 \oplus i_3 \oplus i_4 \oplus i_5 \oplus i_6$	$q_7=i_1 \oplus i_4 \oplus i_6$

B. MULTIPLICATIVE INVERSE BLOCK

The multiplicative inversion in GF (28) follows the procedure shown in Figure 1.

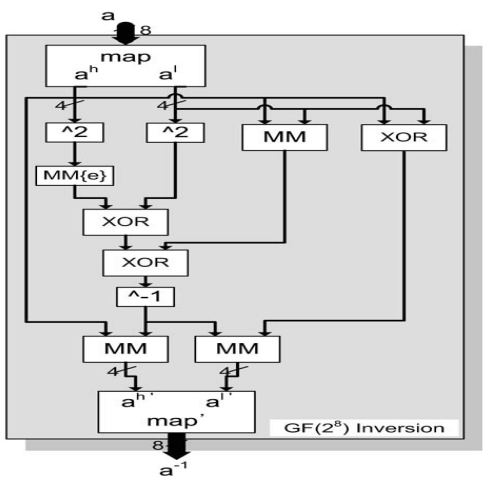

Figure 3. Multiplicative inverse

ADDITION IN GF (2^4)

Addition of 2 elements in Galois Field can be translated to simple bitwise XOR operation Addition of 2 elements in Galois Field can be translated to simple bitwise XOR operation .

GF (2^4) MULTIPLIER

Sub Bytes are a nonlinear transformation that uses 16 byte substitution tables. An S-Box is the multiplicative inverse of a Galois field GF(2^4) followed by an affine transformation. Although two Galois Fields of the same order are isomorphic, the complexity of the field operations may heavily depend on the representations of the field elements. Composite field arithmetic can be employed to reduce the hardware complexity.

Three multipliers in GF (24) are required as a part of finding the multiplicative inverse in GF(2^8). Figure 3. shows the GF (2^4) multiplier circuit. As can be seen from the figure the GF(24) multipliers consist of 3 GF(22) multipliers with 4 XOR Gates and with constant multiplier θ. This constant multiplier which has 2 bits input extracts the lower bit output as the higher bit input, while the higher output bit will be the result of XOR operation between the 2 input bits. Full derivation of this multiplier circuit can be found.

GF (2^2) MULTIPLIER

While each finite field is itself not infinite, there are infinitely many different finite fields; their number of elements of the form p^n where p is a prime number and n is a positive integer.

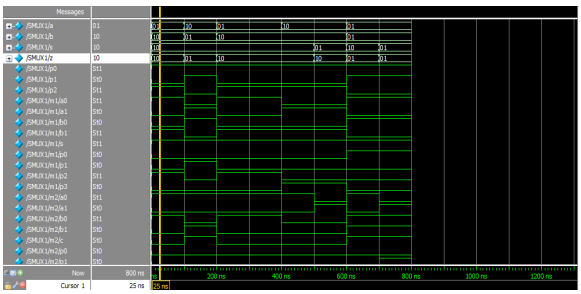

Figure 4 NCL Multiplexer

GF (2^4) SQUARER

It consists of bitwise xor operation. A bitwise operation operates on one or more bit atterns or binary numerals at the level of their individual bits. It is a fast; primitiveaction directly supported by the processor, and is used to manipulate values for comparisons and calculations. On simple low-cost processors, typically, bitwise operations are substantially faster than division, several times faster than multiplication, and sometimes significantly faster than addition. While modern high-performance processors usually perform addition and multiplication as fast as bitwise operations, the latter may still be optimal for overall power/performance due to lower resource use.

MULTIPLIER GF (24):

This is derived a formula to compute the inverse multiplier of q (where q is an element of GF (24)) such that q-1 = {q3-1,q2-1,q1-1,q0-1}. The inverses of the individual bits can be computed from the equation below.

q3-1= q3⊕ q3q2q1⊕ q3q0⊕q2

q2-1= q3q2q1⊕ q3q2q0⊕ q3q0 ⊕ q2⊕ q2q1

q1-1 = q3⊕ q3q2q0⊕ q3q1q0⊕ q2⊕ q2q0⊕ q1

q0-1= q3q2q1⊕ q3q2q0⊕ q3q1 ⊕ q3q1q0 ⊕ q3q0⊕ q2q1⊕ q2q1q0⊕ q3⊕

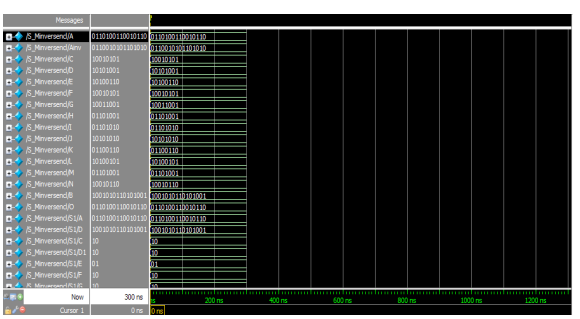

Figure 5 Multiplicative Inverse NCL

V. SIMULATION IMPLEMENTATION

Verilog HDL is a Hardware Description Language (HDL). A Hardware Description Language is a language used to describe a digital system, for example, a computer or a component of a

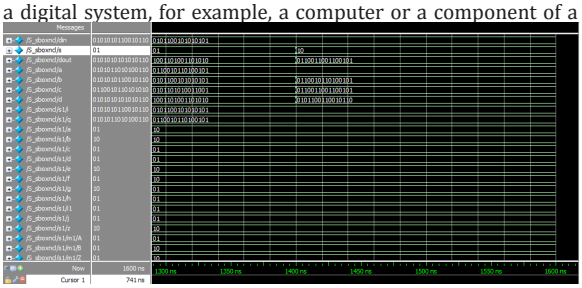

Figure 6.Combinational S-BOX architecture with encryption and decryption.

VI. APPLICATIONS.

Digital Information Systems are decomposed in three main portions, hardware, software and communications with the purpose to identify and apply information security industry standards, as mechanisms of protection and prevention. Digital Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Image encryption is the process of transforming images using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted image. The reverse process, i.e., to make the encrypted information readable again, is referred to as decryption. S-box is used in the encryption and decryption of images.

Computer/Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

VII. CONCLUSIONS AND FUTURE ENHANCEMENT.

In this paper, a hardware implementation of the proposed low-power SCA resistant asynchronous S-Box design for the AES cryptosystem has been revealed to be successfully resisting DPA and CPA attacks. The asynchronous S-Box design is based on self-time logic referred to as NCL, which supports beneficial properties for resisting DPA clock free, dual-rail signal, and monotonic transitions. These beneficial properties make it difficult for an attacker to decipher secret keys embedded within the cryptographic circuit of the FPGA board. Utilizing the two FPGAs included in the SASEBO-GII board, the configuration and cryptographic functions are able to be separately performed to ensure that the power trace measurements for the analysis attacks do not interfere with each other. Experimental results of the original design against the proposed S-Box revealed that the asynchronous design decreased the amount of information leaked from both DPA and CPA attacks. Results also revealed that the proposed design showed of flatter power peaks and 24%–28% lower total power consumption during regular operation. The proposed DPA and CPA attacks procedure based on power measurement is comprehensive and general and not limited to the SASEBO-GII board. It can be revised and used for studying SCAs on other devices.

Our future enhancement is to implement our NCL S-box in Advanced Encryption Standard. AES is used for Encrypt the image in communication. Here we encrypt the image by AES with the help of our S-box. The input of AES is image pixels, which consist of 4x4 image applied to the both test and reference circuit. For encryption a specific key is required, in this encrypt key also we use 4x4 key which makes the better performance of the AES.

REFERENCE

[1] Jun Wu,Yiyu Shi,and Minsu choi, "Measurement and evaluation of power analysis attacks on asynchronous s-box,in IEEE Transactions on Instrumentation and Measurement,March 29,2012. | [2] M. Lazzaroni, V. Piuri, and C. Maziero, "Computer security aspects in industrial instrumentation and measurements," in Proc. IEEE I2MTC, May 2010, pp. 1216–1221. | [3]J. Kocher,P. Jaffe,and B. Jun, "Introduction to differential power analysis and related attacks," Cryptography Res. Inc.,San Francisco, CA, 1998, Tech. Rep. | [4] D. Macii and D. Petri, "Accurate software-related average current drain measurements in embedded systems," IEEE Trans. Instrum. Meas., vol. 56, no. 3, pp. 723–730, Jun. 2007. | [5] D. Macii and D. Petri, "An effective power consumption measurement procedure for bluetooth wireless modules," IEEE Trans. Instrum. Meas., vol. 56, no. 4, pp. 1355–1364, Aug. 2007. | [6] L. Angrisani, M. D'Apuzzo, and M. Vadursi, "Power measurement in digital wireless communication systems through parametric spectral estimation," IEEE Trans. Instrum. Meas., vol. 55, no. 4, pp. 1051–1058, Aug. 2006. | [7] T. Lopez and R. Elferich, "Measurement technique for the static output characterization of high-current powerMOSFETS," IEEE Trans. Instrum. Meas., vol. 56, no. 4, pp. 1347–1354, Aug. 2007. | [8] S. Ors, F. Gurkaynak, E. Oswald, and B. Preneel, "Power-analysis attack on an ASIC AES implementation," in Proc. Int. Conf. Inf. Technol.— Coding Computing, Apr. 2004, vol. 2, pp. 546–552. | [9] Y. Han, X. Zou, Z. Liu, and Y. Chen, "Improved differential power analysis attacks on AES hardware implementations," in Proc. Int. Conf. Wireless Commun., Netw. Mobile Comput., Sep. 2007, pp. 2230–2233. | [10] P. Kocher, "Design and validation strategies for obtaining assurance in countermeasures to power analysis and related attacks," in Proc. NIST Phys. Security Workshop, 2005, pp. 1–11. |