IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 01, August 2018)

Area Efficient AES SBOX Architecture

Swati Kukde
Swami Vivekanad college of Engineering, Indore, M.P. (India)
skswati.kukde@gmail.com

***Abstract* — As the Technology advances day by day, there is an essential need of a secured data transmission for exchanging information from one user to the other. The access of objects in data security is based on key properties that are the root for communication and authentication. Advanced Encryption Standard is specified by National Institute of Standards in 2001 as the specifications for encryption in electronic communication. It is also known as symmetric key algorithm as the encryption and decryption both are formulated using this single standard. From the family of ciphers NIST selected three members of Rijndael family, each with key length 128, 192 and 256 bits for each 128 bit block size. In this research, AES 128 bits has been designed and implemented. This paper presents an area efficient S-BOX structure based on Galois Field arithmetic which is also used for optimizing the speed. The proposed SBOX is very attractive for their extremely small sizes are described in hardware using the HDLs. These VHDL RTL models are simulated on Modelsim 6.5e to check area efficiency.**

***Keywords* — Advanced encryption standard, Encryption, composite field arithmetic, Galios field, Multiplicative inverse.**

I. INTRODUCTION

In the rapid increase in importance of information society is increasing the need for secured communication, especially data transmission. Its forms are different, but increasingly, the more it promotes communication via public data networks, primarily the Internet. This method is convenient, flexible and inexpensive. A fundamental disadvantage stemming from the fact that the network is public is that anyone can listen to everyone and therefore we need to count when communicating with the fact that someone captures our communication.

Even if private network (access to the transmission medium is not public), it is not always ensure the physical safety of the media. Much cheaper and more effective solution is to encrypt transmitted data.

In our present day society more exercises come to depend on telecom systems. It is normal and can as of now be watched today, that this mechanical unrest will influence numerous parts of human connection. The new innovation has offered ascent to imperative new ideas, for example, advantageous programming and time allocation of CPU.

At present, a paramount part is played by numerous sorts of paper reports, for example, worth archives, organization records, ID reports, contracts and arrangements. Effective application of correspondence and computer innovation requests the treatment of records that are no more interwoven from their physical carrier, yet are equivalent to concentrate series of symbols. Furthermore, technical movements are making it less complex and less requesting to physically produce customary paper documents. Such types of advancements bring with them an intense requirement for security systems.

Contracts, distinguishing proof records and worth reports are samples of responsibility transporters. Some affiliation, individual or social affair of individuals presents herself to particular results if not ready to keep certain insurances. The confirmation of these customary papers is still recognized by physical means, for instance, marks or inventive printing procedures that are seen as tough to fake. Clearly, the confirmation of dynamic computer archives must be acknowledged adequately at the sensible level.

In eye to eye correspondence it is generally simple to make circumstances in which listening stealthily is infeasible. In telecommunication applications (correspondence) messages go over effortlessly available channels and their security can never again be underestimated. Eye-to-eye correspondence has the inalienable part of genuineness. It could be confirmed by tactile recognition that the communication accomplice is the individual he or she claims to be and that the expressions ascribed to him or her are truth be told his or hers. In telecom applications the credibility of received messages is no more self-evident. Messages could be altered

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 01, August 2018)

amid transmission or an attacker can make messages that are wrongly credited to the honest to goodness correspondence accomplice.

Encryption is the methodology of changing data (alluded to as plaintext) to make it incoherent to anybody with the exception of those having exceptional information, normally alluded to as a key. The aftereffect of the methodology is encoded data (in cryptography, alluded to as cipher text). In numerous settings, the statement encryption likewise verifiable alludes to the opposite methodology [5].

Encryption has long been utilized by militaries and governments to encourage secret correspondence. Encryption is currently utilized as a part of ensuring data inside numerous sorts of non-military personnel frameworks, for example, machines, systems (e.g. the Internet e-trade), cellular phones, remote mouthpieces, ATMs (Automatic Teller Machines) and Bluetooth gadgets. Encryption is likewise utilized within computerized rights administration to confine the utilization of copyrighted material and to diminish the piracy.

Incomprehensible ciphertext to the plaintext conversion is called decryption. It is in essence that the encryption method operates in inverse and the inputs for this technique are cipher text and secret key. The output comes as the first plain text [5].

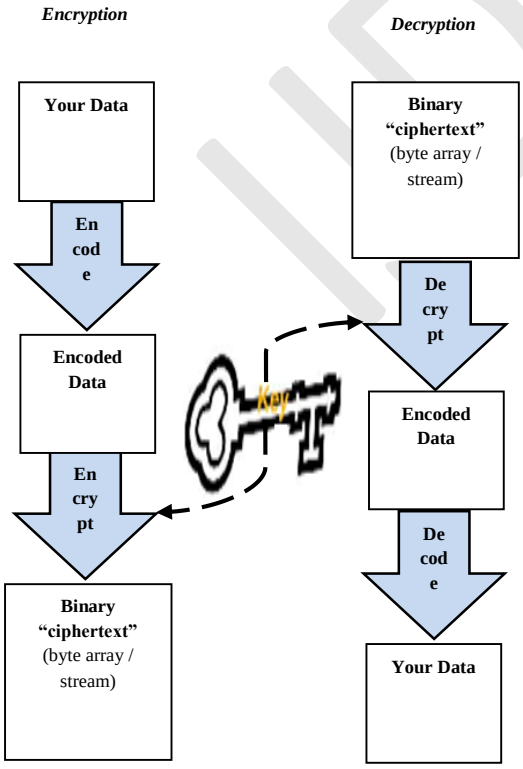

Figure 1: Block Diagram of Encryption and Decryption

II. Review

Plenty of literature has been reviewed in connection with the different cryptographic techniques regarding the present problem and the significantly related ones.

This paper exhibits a rapid structural engineering for composite field arithmetic based S-box utilized as a part of AES system. This construction modeling is determined by expanding the pre-computation procedure to an as of late proposed structural planning of AES S-box.

This paper have been picked a structure such that, with the exemption that diverse key sub-blocks are utilized, the encryption procedure is indistinguishable to the decryption methodology. This paper portrays the configuration and execution of secure information encryption calculation (S-IDEA) convention, the span of the key has been expanded from 128 bits to 256 bits. This expanded key size will expand the multifaceted nature of the calculation. To build the measure of dissemination, two multiplicative added (MA) blocks are utilized within a solitary round of IDEA as contrasted with one MA block utilized a while ago as a part of a solitary round, with these changes in this technique will expand the cryptographic quality.

III. Proposed Methodology

Cryptography is a Greek word that actually implies the "art of writing secrets" [6]. It gives the systems essential to give responsibility, exactness and privacy in innately open correspondence mediums, for example, the Internet. In preparation, cryptography is the errand of changing data into a structure that is unimaginable, yet in the meantime permits the planned beneficiary to recover the right information by method for a secret key. Ciphers are unique programs intended to ensure sensitive data on open correspondence systems. Amid encryption, original plaintext message is transformed to garbled ciphertext with the help of ciphers. The process of recovering plaintext from ciphertext is called decryption. Two manifestations of cryptography are ordinarily utilized within data structures these days: secret key ciphers and public key ciphers. Secret key ciphers utilize a solitary private key to encode and decode as demonstrated in Figure 3.2. Public key ciphers use a common open key to encode and oblige an exchange private key to decode. The procedure might likewise be turned around to deliver what is known as a digital sign which accept the sender. Since just the individual holding the private key knows its esteem, just that individual can make a digital sign that others can decode with public key. Public key ciphers have the profit of

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 01, August 2018)

having the ability to make a safe correspondence channel without dangerous exchange of keys. Private-key ciphers, of course, oblige an imparted private key before secure correspondence can begin. The scattering of the imparted private key is the fundamental deterrent in making secret key ciphers secure. Solid Public key ciphers can reach to a great degree on the basis of computation.

A. AES Algorithm

The Encryption procedure of Advanced Encryption Standard technique is intruded underneath, in figure 2. The block diagram demonstrated in figure 2, is bland for AES details. It involves different unique progressions associated successively over the information block bits, in an altered number of cycles, called rounds. The measure of rounds depends on upon the length of the key used for the encryption process.

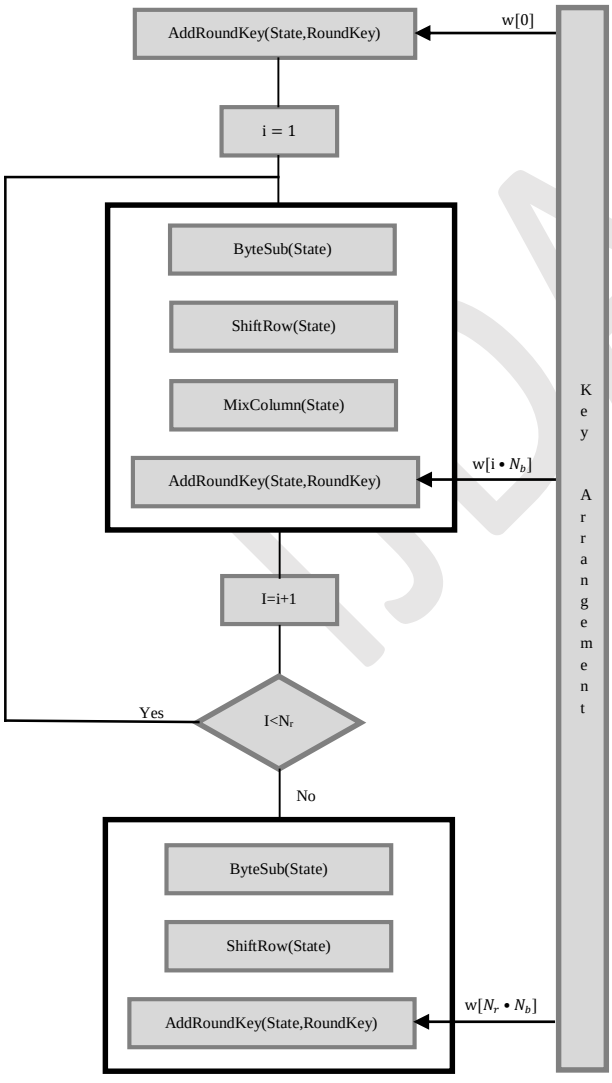

Figure 2: Encryption Process of AES Algorithm

B. Proposed S-BOX Design

The multiplicative inverse computation will be done by decomposing the more complex GF (2^8) to lower order fields of GF (2^1), GF (2^2) and GF$((2^2)^2)$. In order to accomplish the above, the following irreducible polynomials are used.

GF $(2^2) \rightarrow$ GF(2) : $x^2 + x + 1$
GF$((2^2)^2) \rightarrow$ GF (2^2) : $x^2 + x + \varphi$
GF$(((2^2)^2)^2) \rightarrow$ GF$((2^2)^2)$: $x^2 + x + \lambda$
Where $\varphi = \{10\}_2$ and $\lambda = \{1100\}_2$

Any arbitrary polynomial can be represented by $bx + c$ where b is upper half term and c is the lower half term. Therefore, from here, a binary number in Galois Field q can be spilt to $(q_H)_x + q_L$. For instance, if $q = \{1011\}_2$, it can be represented as $\{10\}_{2x} + \{11\}_2$, where q_H is $\{10\}_2$ and $q_L = \{11\}_2$. q_H And q_L can be further decomposed to $\{1\}_{2x} + \{0\}_2$ and $\{1\}_{2x} + \{1\}_2$ respectively. The decomposing is done by making use of the irreducible polynomials introduced at equation shown above. Using this idea, the logical equations for the addition, squaring, multiplication and inversion can be derived.

IV. Simulation Results

A. S-Box Simulation

ModelSim is used as simulation tool in our work below. While we used Xilinx for the reports regarding device utilization, power requirement, placement and routing of design etc.

B. S-BOX based on Galois Field Arithmetic: Proposed Method

The VHDL model of the S-BOX is prepared for AES based on Galois Field arithmetic (GF (2^4))using Xilinx Integrated Software Environment (ISE) and is implemented on Xilinx spartan-3 (Device: XC3S400) FPGA platform. The obtained results are shown in Table 1

Table 1: Result for S-BOX with GF (2^4)

FPGA Resources	Slices	LUT	Bonded IOBs	Slice MUXs
Proposed work	37	68	15	5

Table above showing the device utilization of SBOX, designed using Galois Field Arithmetic logics. The Schematic of possible inputs, outputs and detailed RTL schematic for S-BOX using Galois Field is shown in Figure 3 and Figure 4

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 01, August 2018)

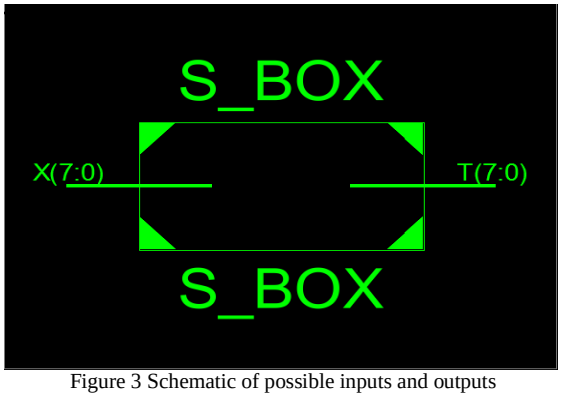

Figure 3 Schematic of possible inputs and outputs

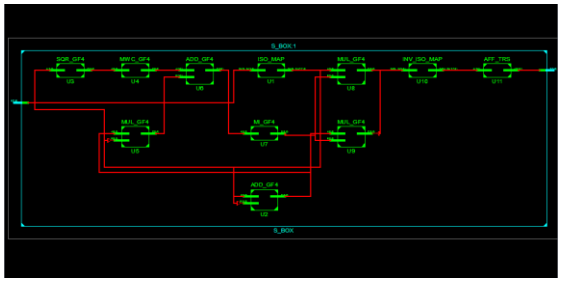
Figure 4: Detailed RTL Schematic of S- BOX with Galois Field

Figure 5 shows the simulation of GF based S-Box architecture. The input X is an 8 bit data to be transformed, which is fed to the S-Box. After a delay of 22.118 ns we get the transformed output.

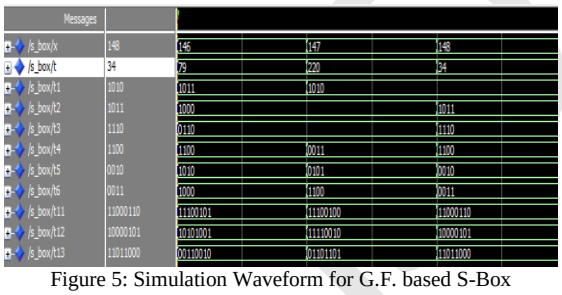

Figure 5: Simulation Waveform for G.F. based S-Box

V. Conclusion And Future Scope

S-BOX is the key element of Advance encryption standard algorithm. This paper presents an area efficient S-BOX structure based on Galois Field arithmetic. In this we presented the VHDL implementation of proposed S-BOX using ModelSim and Xilinx ISE tools. When compared to previous S-BOX architectures (Based on Pre-computation and ROM based architecture), it shows that proposed design is area efficient as well as optimized in speed.

Optimization of critical path using Dual-VT technology can be recommended as the future work for this paper in order to construct a low power design of SBOX for Advance encryption standards.

Acknowledgement

The path to the successful completion of this project has gone through various ups and downs. GF based multiplicative inverse and computation coupled with help and encouragement from several quarters have paved the path to success.

References

[1] National Bureau of Standards, Data Encryption Standard (DES), US Department of Commerce. Federal Information Processing Standards Publication 46 (FIPS PUB 46), 15 January 1977.
[2] Eli Biham, Adi Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Springer Verlag, 1993.
[3] A. Menezes, P. Van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
[4] Xuelija Lai, "On the Design and Security of Block Ciphers", Hartung-GorreVerlag Konstanz, 1992
[5] [5] VinodShokeen, NiranjanYadav, "Encryption and Decryption Technique for Message Communication", International Journal of Electronics & Communication Technology (IJECT), ISSN: 2230-7109, Vol. 2, Issue 2, June 2011.
[6] C. Kaufman, R. Perlman, and M. Speciner, "Network Security: Private Communication in a Public World", Prentice Hall PTR, 1995.
[7] An Introduction to Cryptography. Network Associates, Inc., 1999. .
[8] The SSL Protocol, version 3.0. Netscape, Inc., 1999.
[9] Ekta Agrawal, Dr. ParashuRam. Pal, "Refined Polygram Substitution Cipher Method: A Enhanced Tool for Security", International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume 2, Issue 1, July 2012.
[10] Schneier, Bruce, "Applied Cryptography. Protocols, Algorithms, and Source Code in C", New York: Wiley & Sons, 1996.