INTERNATIONAL JOURNAL ★ ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

2017 IJIEMR. Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 8 June 2017. Link :

http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-4

Title: DESIGN OF AES USING REGIONAL THRESHOLD IMPLEMENTATION

Volume 06, Issue 04, Pages: 768 - 774

Paper Authors

***K.SIREESHA, N. GOPI CHAND**

* Dept. of E.C.E, V.N.R COLLEGE OF ENGINEERING, PONNUR.

Engineering and Management Research ★ International Journal for Innovative

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DESIGN OF AES USING REGIONAL THRESHOLD IMPLEMENTATION

*K.SIREESHA, **N. GOPI CHAND

*PG SCHOLAR Dept. of E.C.E, V.N.R College Of Engineering. Ponnur, Guntur Dt.

**Associate Professor Dept. of E. C.E, V.N.R College Of Engineering. Ponnur, Guntur Dt.

ABSTRACT:

This work proposes a novel scheme for encryption algorithm based data security hiding. In the first work, a content owner encrypts the original uncompressed text using an encryption key. Then, it may compress the least significant bits of the encrypted text using a data-hiding key to create a sparse space to accommodate some additional data. The communication processes are still used in many applications today. The existed system we have three based encryption and decryption but not having capable for international system and flat encryption process is used. When we are using flat encryption we do not provide either high security to international system or loss the encryption process for local level. So to overcome this we provide different key selection for different encryption process is proposed. There are four stages one for local, national, international and special case depends on their length. As the number of hackers are less. So, we provide less bits to choose combination cases. This process of security will be high in national, higher in international, very high in special case.

I. INTRODUCTION

Due to the increasing use of computers, security is an important issue for digital information. Intruder is anunwanted person who reads and changes the information while transmission occurs. This activity of intruder is called intrusion attack. To avoid such attack data may be encrypted to some formats that is an unreadable by an un authorized person.

Most of the work on reversible data hiding focuses on the data embedding/extracting on the spatial domain. But, in some applications, a channel administrator hopes to append some additional message, such as the origin information, text notation or authentication data, within the encrypted text though he does not know the original text content.

It is also hopeful that the original content should be recovered without any error after text decryption and message extraction at receiver side. Reference presents a practical scheme satisfying the above-mentioned requirements. The owner of the information encrypts the original text using an encryption key, and a data hacker can embed additional data into then crypted text using a data-hiding key though he does not know the original content. With an encrypted text containing additional data, a receiver may decrypt it according to then cryption key, and then take the embedded data and recover the original information according to the data-hiding key. Encryption has long been used by militaries and governments to facilitate secret communication.

II. RELATEDWORKS

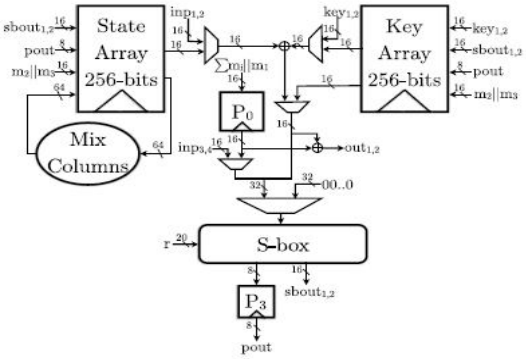


Fig. 1. Schematic of the serialized TI of raw AES-128.

1) Raw Implementation: We use two sets of state registers, each consisting of sixteen 16-bit registers, corresponding to the two shares of the state. The Mix Columns and the Key XOR operations are also performed with two shares. This can be seen in Fig. 1, as the key and the state registers are 256 bit simplying the two shares.

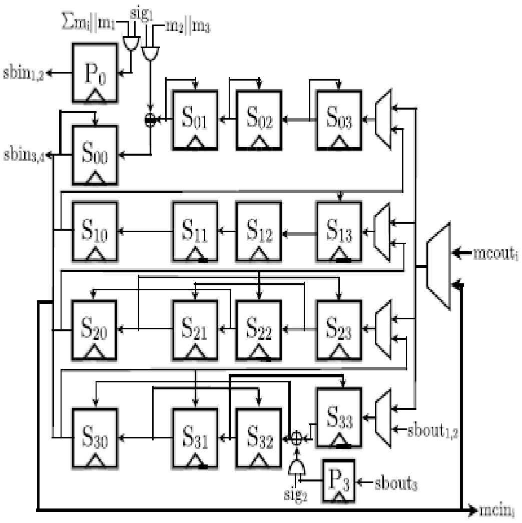
This TI of the S-box (details will be given in the following section) requires four input shares, therefore, we initially sharethe plaintext in four shares. We share the key in two shares and XOR them with two of the plaintext shares before the S-box operation. More details about the key scheduling will be given later in this section.

Besides the shared input, the S-box needs 20-bits of randomness *r*. The first two output shares sbout1,2 are written to the state register S33 (Fig. 2)whereas the remaining share sbout3 is written to register P3.The

data in the state registers are shifted to the left for the following 16 cycles so that the next output of the S-box can be stored in the same registers. During this shift, the data inP3 (pout in Fig. 1) is XOR ed with the second share of the S-box output, which is in the state register S33, to reduce the number of shares from three to two. To achieve this signal,sig2 is active from the fourth to the 19th clock cycle.

The Shift Rows operation is performed in the 19th clock cycle with an irregular horizontal shift. In the next four clock cycles, the data in the registers S00, S10, S20, and S30 are sent to the Mix Columns operation, the rest of the registers are shifted to the left horizontally and the output of the Mix Columns operation is written to the registers S03, S13,S23, and S33. The Mix Columns operation is implemented column-wise as in [16] and with two shares working in parallel.

The registers except S10–S12 are implemented as scan flip-flops (SFF) that are D-flip-flops (DFF) combined with2-to-1 MUXes. They can operate with two inputs at reduced area cost. A single 2-to-1 MUX costs 3.33 GE and one bit register costs 5.33 GE whereas one bit SFF costs 6.33 GE in our library. In the following AES rounds, we increase the number of shares of the S-box input from two to four, using 24 bits of



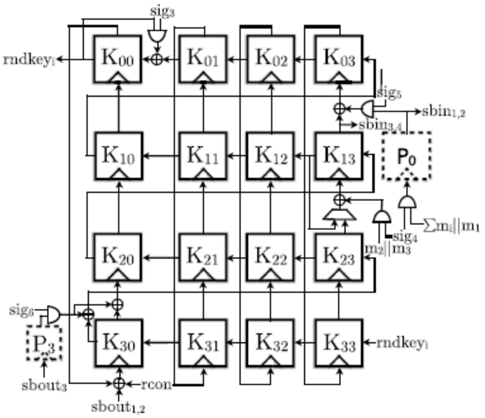


Fig. 2. Schematic BOX

Randomness (three bytes each of which is referred to as *mi* in the figures), one clock cycle before the S-box operation. To achieve this signal, sig1 is active for 16 clock cycles, starting from the last clock-cycle of each round. We separate the increase of the number of shares and the nonlinear operation with registers to achieve the non-completeness property.

The two additional shares are stored in P0. The two shares in S00are XORed with the two shares of the corresponding round key byte and sent to the S-box together with the two shares in P0.

The registers P0 and P3 are used for both round transformations and key scheduling. Similar to the state array, the key array also consists of sixteen 16-bit registers, implemented as SFFs, each corresponding to the two shares of a byte in the key schedule. The round key is inserted from the register K33 in the first 16 clock cycles of each round. For the next three clock cycles, the registers except the last column (K03, K13, K23, and K33) are not clocked. The registers K03, K23, and K33 are also not clocked in the 17th clock cycle. In that clock cycle, we increase the number of shares in the register K13.

In the following three clock cycles, this re sharing is done during the vertical shift from the register K23 to K13, i.e., the re sharing signal sig4is active from the 17th to the 20th clock cycle. Signal sig5is active from the 18th to the 21st clock cycle to reduce the number of shares back to two. The registers K03, K13, K23,and K33 are not clocked in the remaining two clock cycles of each round.

We choose this way of irregular clocking to avoid using extra MUXes in our design. Two shares of the S-box output are XORed to the data in K00 in the last four clock cycles of each round. In the 20th clock cycle, the round counter rcon is additionally XORed to one of these shares. The number of shares is reduced back to two by XORing the share in P3 to one of the shares in K30. Signal sig3 is active in the first 16 clock cycles except the 4th, 8th, 12th, and 16thclock cycles. The round key is taken from the register K00 to be XORed with the corresponding plaintext before going to the S-box operation.

2) Adjusted Implementation: This version works on three shares for both state and key schedule which increases the area significantly. The S-box still requires four input shares and outputs three shares, hence the register P0 is reduced to 8-bits(one share) and the register P3 is not required. Similar to the raw implementation, we use 24-bits of randomness to increase the number of shares from three to four one cycle before the S-box, i.e., each of the existing three shares is XORed with arandom byte and the sum of these random bytes is taken as the fourth share.

This also ensures uniformity of the S-box input. Together with the state, the number of shares for Mix Columns and Key XOR increases to three.

3) Nimble Implementation: Similar to the raw implementation, this one also uses two shares for the state and key arrays.

The main difference is that the S-box needs three input shares instead of four. Hence, the size of the register P0 is reduced to 8-bits (one share). As a result, we need only 16-bits of randomness to increase the number of shares from two to three before the S-box operation, i.e., each share is XORed with one byte of randomness and the XOR of the random bytes is taken as the third share.

The S-box requires 16-bits of extra randomness per iteration and outputs three shares. Hence, the logic of the register P3 to reduce the number of shares back to two stays the same.

III. PROPOSED SYSTEM

In proposed system we are using user, role and attribute they have their own disadvantages. To overcome this we introduced proposed system in that we divide key-selection into four sub dividing. Key- one used for local level encryption with limited number of bits. This encryption is combination of multiplication and addition. The total probability of chances depends on the number of bits. As the bits are changing we are getting the number of combination. In local level the total channels are low. So we are using key-one as limited number of bits. Key-two used for national level encryption with more number of bits compared with local level. The total wanted channels in national level is more compared with local level. So we use more bit length than local level. Key-three used for international level with high security. So here we have high bit length compared with national level. Key-four used for VIP-level encryption with more number of bits compared with international level to provide very high security for their data. The total description of key-selections depends on their register use. The key is given to key-register to store the key and that key is encrypted with data and gives the output. The output of the encryption is taken as input for decryption part.

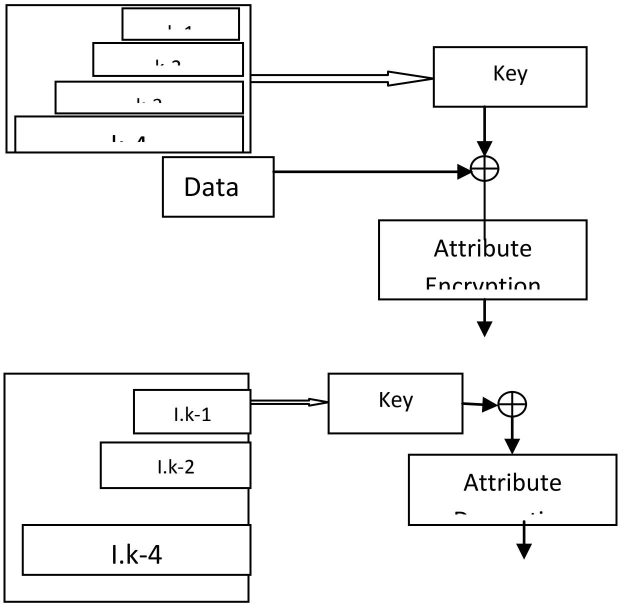


FIG. 3: PROPOSED SYSTEM

In decryption the receiver key-selection is selected with synchronization with encryption key. The recover key-selection is stored in key register and that key is decrypted the input data which is taken as decryption input and that decryption data is taken as finalized output.

IV. RESULTS

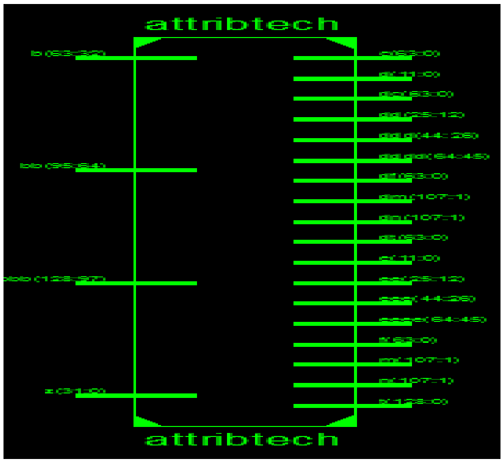
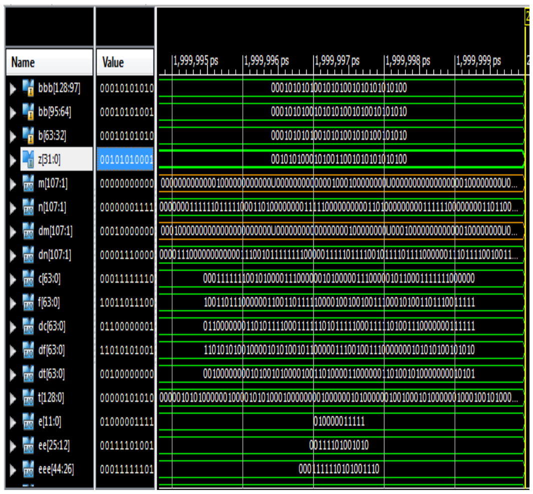


FIG. 4: RTL SCHEMATIC



```
Name         Value
bbb[128:97]  00010101010   000101010100101010100101010101010100
bb[95:64]    00010101001   00010101001010101010010100101010101010
b[63:32]     00010101010   0001010101001010101001010101001010101010
z[31:0]      00101010001   00101010100010100110010101010101010100
m[107:1]     00000000000   000000000000010000000000000U00000000000000100010000000U000000000000000000100000000U0...
n[107:1]     00000001111   0000000111111011111000110100000000111110000000000110100000000111111000000001101100...
dm[107:1]    00010000000   0001000000000000000000000000U00000000000000000010000000U00010000000000000100000000U0...
dn[107:1]    00001110000   000011100000000000011100101111111100000111110111100101111011110000001110111100100 11...
c[63:0]      00011111110   0001111111001010000111000000101000001110000010110001111111000000
f[63:0]      10011011100   1001101110000001100110111110000100100100111000101001101110011111
dc[63:0]     01100000001   0110000000110101110001111110101111000111110100111000000011111 1
df[63:0]     11010101001   1101010100100001010100101100000111001001110000000101010100101010
dt[63:0]     00100000000   0010000000010100101000010011010000110000001101001010000000010101
t[128:0]     00000101010   0000010101000000100001010100010000000010000001010000001001000101000000100010010100 0...
e[11:0]      01000001111   010000011111
ee[25:12]    00111101001   00111101001010
eee[44:26]   00011111101   0001111111010 1001110
```

FIG. 5: OUTPUT WAVEFORM

V. CONCLUSION

The existed system we have encryption and decryption but not having capable for international system and flat encryption process is used. When we are using flat encryption we do not provide either high security to international system or loss the encryption process for local level. So to overcome this we provide different key selection for different encryption process is proposed. There are four stages one for local, national, international and special case depends on their length. As the number of hackers are less. So, we provide less bits to choose combination cases. This process of security will be high in national, higher in international, very high in special case. So finally I am concluding that proposed system provides different security level depends on application and it is better than Existed system.

V. REFERENCES

[1] A. Sahai and B. Waters, "Fluffy personality based encryption," in Progresses in Cryptology EUROCRYPT 2005, ser. Address Notes in Software engineering, R.Cramer, Ed. Springer Berlin Heidelberg, 2005, vol. 3494, pp. 457–473.

[2] D. Boneh, A. Sahai, and B. Waters, "Utilitarian encryption: Definitions what's more, difficulties," In principle of Cryptography, ser. Address Notes in Software engineering, Y. Ishai, Ed.Springer Berlin Heidelberg, 2011, vol. 6597, pp. 253–273.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Trait based encryption for fine-

grained access control of scrambled information," in Procedures of the thirteenth ACM meeting on PC and correspondences security, ser. CCS '06. New York, NY, USA: ACM, 2006, pp 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Figure content approach trait based encryption," in Procedures of the 2007 IEEE Symposium on Security and Protection, ser. SP '07. Washington, DC, USA: IEEE PC Society, 2007, pp. 321–334.

[5] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the unscrambling of ABE figure writings," IN: Procedures of the twentieth USENIX Meeting on Security, SEC 2011. San Francisco, CA, USA: USENIX Affiliation, Berkeley, 2011.

[6] E. Fujisaki and T. Okamoto, "Secure combination of unbalanced what's more, symmetric encryption plans," in Advances in Cryptology - CRYPTO '99, ser. Address Notes in Software engineering, M. Wiener, Ed. Springer Berlin Heidelberg, 1999, vol. 1666, pp. 537–554.

[7] R. Canetti, O. Goldreich, and S. Halevi, "The arbitrary prophet system, returned to (preparatory rendition)," in Procedures of the Thirtieth Yearly ACM Symposium on Hypothesis of Figuring, ser. STOC '98. New York, NY, USA: ACM, 1998, pp. 209–218.

[8] J. Lai, R. Deng, C. Guan, and J. Weng, "Property based encryption with obvious outsourced unscrambling," IEEE Exchanges on Data Legal sciences and Security, vol. 8, no. 8, pp. 1343–1354, Aug 2013.

[9] B. Waters, "Figure content strategy characteristic based encryption: an expressive, proficient, and provably secure acknowledgment," in Procedures of the fourteenth global meeting on Practice and hypothesis out in the open key cryptography gathering on Open key cryptography, ser. PKC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.

[10] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "Bland developments for picked ciphertextecure quality based encryption," Out in the open Key Cryptography - PKC 2011, ser. Address Notes in Software engineering, D. Catalano, N. Fazio, R. Gennaro, also, A. Nicolosi. Ed. Springer Berlin Heidelberg, 2011, vol. 6571, pp. 71–89.

AUTHORS

KONIDALA SIREESHA studied B.Tech at chintalapudi engineering collegeand present she is pursuing M.Tech at V.N.R College of engineering. Her area if interest is V.L.S.I DESIGN.

N. GOPI CHAND studied M.Tech at Andhra University and pursuing PH.D at SATYABHAMA UNIVERSITY. He has 9 years of teaching experience. At present he is working as associate professor at V.N.R College of engineering. His area of interest V.L.S.I design.