ASIC IMPLEMENTATION OF SWITCHABLE KEY AES CRYPTOPROCESSOR

Divya A.G[1], Srividya p[2]

[1]*PG ,Department Of ECE, Sjbit/ Vtu, Bangalore ,India*

[2]*Asso prof, Department Of ECE, Sjbit/ Vtu, Bangalore ,India*

ABSTRACT

This paper presents the ASIC implementation of switchable key Advanced Encryption standard algorithm Encryption and decryption with power gating. The implementation supports 128 bits, 192 bits and 256 bits key. The implementation is described in verilog HDL , simulated in VCS synopsys, Synthesized in Design Compiler (DC) using Nangate 45nm open cell library, Physical Design and power gating is performed in ICC of Synopsys. With the use of power gating power consumption can be reduced by 40%.

Keywords- *ASIC, power gating, AES, 45nm Cmos Technology, Key Expansion.*

1. INTRODUCTION

The special needs for secure communications are triggered not only in traditional sectors such as military and government services but also in all aspects of everyday life, in both business and private transactions. The large and growing number of internet and wireless communication users has led to an increasing demand of security measures and devices for protecting the user data transmitted over the open channels.

The AES algorithm comes from the cipher "Rijndael"[1]. It had been announced as the federal information processing standard (FIPS) by National Institute of standards and Technology (NIST) in late 2001 replacing DES [2]. Two types of cryptographic systems are mainly used for security purpose, one is symmetric-key crypto system and other is asymmetric-key crypto system. Symmetric key cryptography (DES, 3DES,AES) uses same key for both encryption and decryption.The asymmetric-key cryptography(RSA and Elliptic curve cryptography) uses different keys for encryption and decryption. The major disadvantage of DES is its key length is small.

The AES encryption is considered to be efficient both for hardware and software implementations. Compared to software, hardware implementations are more reliable. some works have been presented on the hardware implementations of AES using ASIC in[3], [4], [5], [6] .

The power gating enables to shut off the blocks which are not being using at a point of time. The work on power gating is presented in [7], [8] .

The remainder of this paper is organized as follows. It begins with describing basic AES algorithm in Section II. Sections III describes novel on the fly key expansion module. Section IV brief about AES crypto-processor. Section V describes power gating. Finally i concluded the paper in section VII.

2. AES ALGORITHM

The AES algorithm is a symmetric block cipher that processes data blocks of 128 bits using a cipher key of length 128,192 or 256 bits. In addition, the AES algorithm is an iterative algorithm. Each iteration can be called a round, and the total rounds,Nr is 10,12, or 14 , when the key length is 128, 192, or 256 bits respectively. Table 1 shows the number of rounds as a function of key length. TABLE 1 shows the number of rounds as a function of key length.

Table 1: Rounds vs key length

	Key Length Nk Words	Block Words NB words	Number of rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

The 128 bit data block is divided into 16 bytes. These bytes are mapped to a 4x4 array called state and the state undergoes all the internal operation of the AES algorithm. Every byte in the state is denoted by Si,j (o≤ I, j<4), and is considered as an element of GF(28). Although different irreducible polynomials can be used to construct GF(28),the irreducible polynomial used in the AES algorithm i.e, p(x) =x8+x4+x3+x+1. Block diagram of the AES encryption and the equivalent decryption structures are shown in Fig 1.

After an initial round key addition, a round function consisting of four different transformations sub-bytes, shift-rows, mix-columns and add -round-key are applied to the data block in the encryption procedure and in reverse order with inverse transformations in decryption procedure. But last round in encryption and decryption doesn't contains mix columns and inv-mix columns. Four transformations in a round function are examined and optionally designed to achieve efficient implementation.

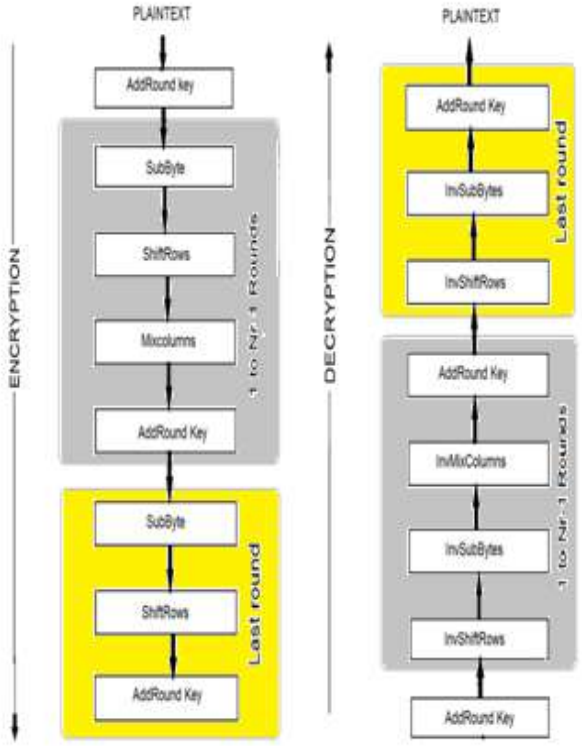

fig 1: encryption and decryption algorithm

1.1 Sub bytes/ Inv Sub Byte transformations

Sub byte transformations are a non-linear byte substitution. This can be done by using two methods. One is by using lookup tables(LUT);other is by using a combinational logic. The LUT approach is used in this design. In the sub Byte step, each byte in the matrix is updated using an 8-bit substitution box, the Rindael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over GF(28), known to have good non-linearity properties. To avoid attacks based on the simple algebraic properties, the S-box is constructed by combining the inverse function with invertible affine transformations. The S-box is also chosen to avoid any fixed points, and also any opposite fixed points. In the inverse Sub byte step, each byte in the matrix is updated using an inverse 8 bit substitution box.

1.2 Shift Rows/ InvShift Rows

Shift Rows is a simple shifting operation. First row is kept as it is, while the second, third and forth rows cyclically shifted by one byte, two bytes and three bytes to the left respectively. In the InvShiftRows, the first row of the state doesn't change, while the rest of the rows are cyclically shifted to the right by the same offset as in the shift rows.

1.3 Mix Column/InvmixColumn transformation

The Mix Columns() transformations operate on the state column by column, treating each column as a four term polynomial. The columns are considered as polynomials over GF(28) and multiplied modulo x4+1 with a fixed polynomial a(x), given by a(x) ={03}x3 +{01}x2 +{01}x + {02}. The function xtime is used to represent the multiplication with 02,moduo the irreducible polynomial m(x) =x8+x4+x3+x+1. Implementation of function xtime() includes shifting and conditional xor with 1B.

The InvMixColumns multiplies the polynomial formed by each column of the State with a-1(x) modulo x4+1, where

a-1(x) = {0b}x3 + {0d}x2 + {09}x + {0e}.

1.4 Add Round key

Add Round key involves only bit-wise XOR operation. After every round output of the mix column is added with round key. By inverting the encryption structure one can easily derive the decryption structure. However the sequence of the transformations will be different from that in encryption. This feature prohibits resource sharing between encryptors and decryptors.

3. KEY EXPANSION

In the AES algorithm, the key expansion module is used for generating round keys to provide for every round. There are two approaches to provide round keys. One is to precompute and store all the round keys and the other one is to produce them on the fly. First approach consumes more area. In second approach, the initial key is divided into NK words. With the help of these initial key is divided into NK words(key0, key1….keyNk-1) which are used as initial words. With the help of these initial words rest words are generated . It can be computed that is 4,6 or 8, when the key length is 128,192 or 256 bit, respectively. Each round key has 128 bits, and is formed by concatenating four words:

The key expansion procedure can be described by the pseudo code listed below and shown in Fig 2.

for *i* = 0 to Nk-1

wi = *keyi*

end for *i* = Nk to 4(Nr + 1)-1

temp = *wi-1*

if (I mod Nk = 0)

temp = SubWord(RotWord(*wi-1*)) XOR Rcon(*i*/Nk)

else if

wi = *wi-Nk* XOR temp

end

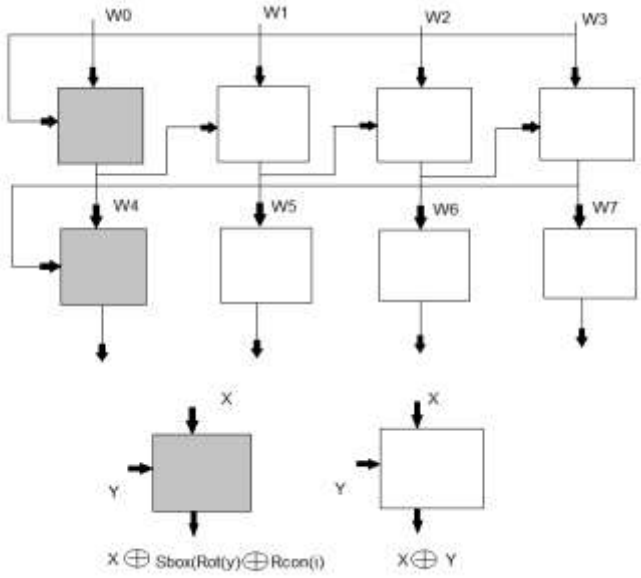

fig 2. data path for key generator

4. AES CRYPTOPROCESSOR

The AES crypto-processor is capable of performing both encryption and Decryption simultaneously for different data inputs at a given time. It takes 14 clock cycles for the processor to produce the output data. In the first 14 clock cycles the encryption is being performed the decryption block is idle, after the encrypted data is produced the decryption block is enabled to perform and simultaneously next data can be fed into the encryption block. Fig 3 depicts the AES cryptoproceoor.

4.1 Encryption

Encryption process includes the sub bytes, shift rows, mix column and Add round key steps. The input data is 128 bit and the input key can be 256 or 128 or 192. The key stored is used in every clock cycle to perform the add round key step.

A Multiplexer and a counter are used as a part of the control unit. The counter used is a 15bit one hot counter and depending upon the value of the counter the operations for 14 rounds are performed as in the last round the mix column step is not required. The F/F ensures that the fed back data is available at the next clock cycle. Fig 4 shows the encryption process containing the control unit and the other main blocks

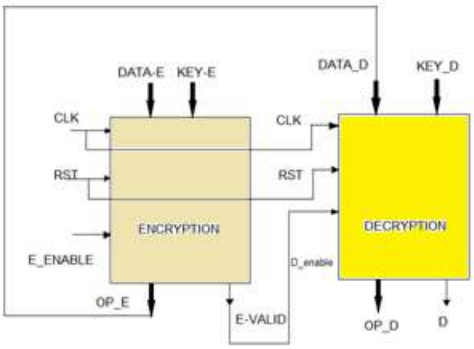

fig. 3. aes crypto-processor

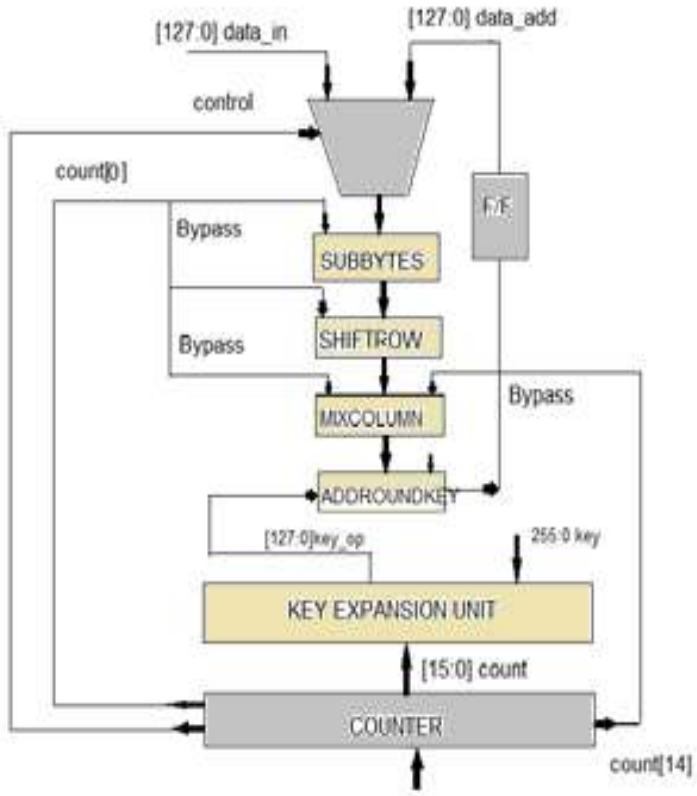

fig .4. internal block diagram of encryption

4.2 Decryption

The decryption block is not the exact inverse of the encryption block but it is similar to the encryption steps. The decryption block describes the inverse sub bytes, inverse-shift-rows and the inverse-mix –column steps. The control unit works in a similar manner. Counter output is used to bypass the inverse mix column step that is used in the final round of the operation and only add-round key operation is performed in the first stage. Fig 8 shows the decryption process containing the control unit and the other main blocks.

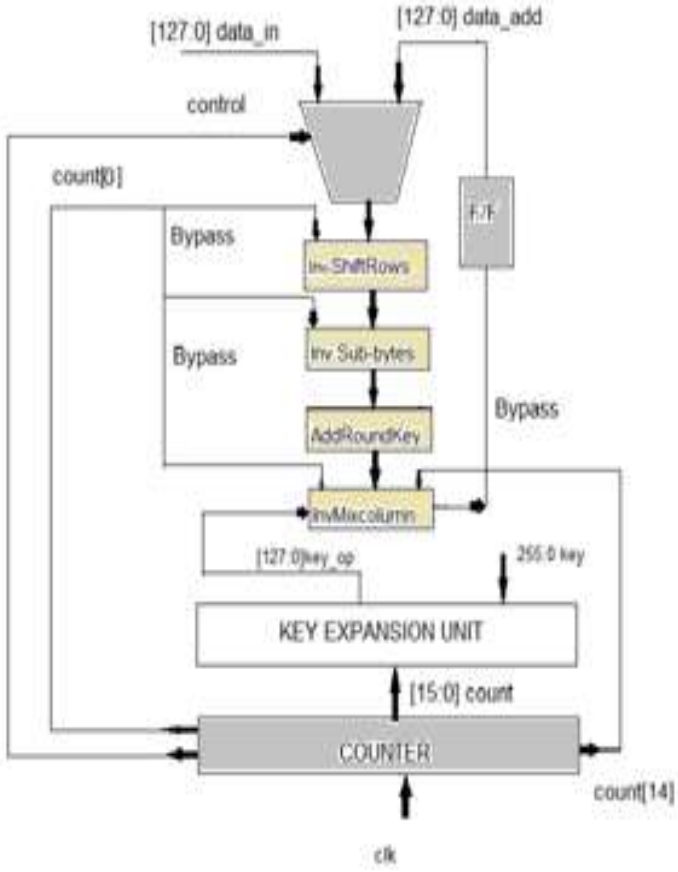

fig.5. internal block diagram of decryption

5. POWER GATING

Power gating is the technique wherein circuits blocks that are not in use temporarily turned off to reduce the overall leakage power of the chip. This temporary shutdown time can also be called as “low power mode” or “inactive mode”. When circuit blocks are required for operation once again they are switched at the appropriate time and in the suitable manner to maximize power performance while minimizing impact to performance

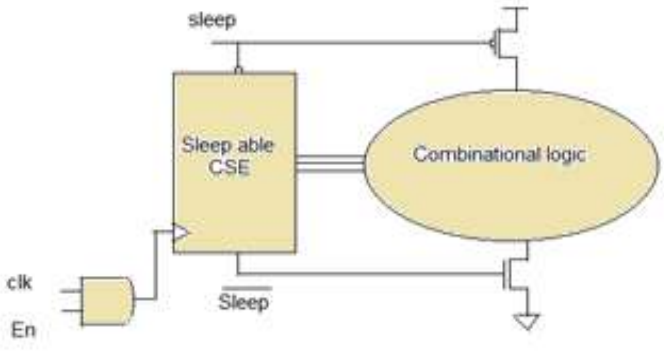

fig.6. analysis setup-power gated cs

Power gating can be applied in this context by shutting down power to the encryption block while performing decryption. The encryption block consists of an enable pin and by adding a switch to the enable pin we can switch between the active mode and sleep mode. The encryption block can be put to sleep while performing decryption. Power gating is performed using the ICC synopsys tool. A region/ boundary can be chosen with in which the cells of the encryption block are placed. The placed cells are connected to the output of the switch and taken forward to the routing stage.

6. RESULTS

The proposed AES architecture is described in Verilog HDL at the register-transfer level. Synthesizing the RTL into the gate level is done by using Synopsys DC compiler using 45 nm standard-cell CMOS technology. Back-end design has been carried out using ICC of Synopsys. The simulated waveforms for both encryption and decryption process with 256-bit,128 bit and 192 bits key are verified with expected results. The comparison results of the proposed implementation with and without power gating is presented in Table 2. The final layout of the proposed configurable AES processor is shown in Fig 7.

Table 2. Power Results at 1.25v

power Parameter	Before power gating	After power gating
Switching power	27.3mW	17.01mW
Internal Power	15.93mW	7.79mW
Leakage Power	665.1mW	347.60mW
Net power	700mW	372mW

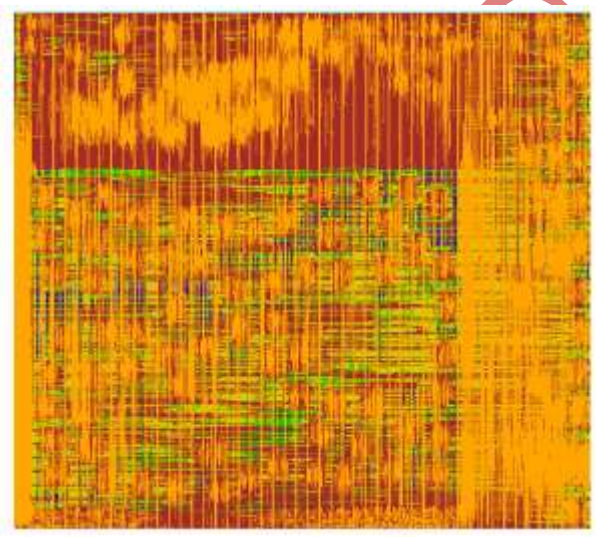

fig.7. final chip layout

7. CONCLUSION

In this paper, I've presented a hardware implementation of an switchable key AES crypto-processor with power gating to achieve the low power. The design is modeled using verilog HDL and simulated with the help of VCS of synopsys , synthesys is done using Dc compiler and physical design and power gating is done using ICC of synopsys. With the proposed low power design technique power consumption can be reduced by 40%.

REFERENCE:

[1] J.Daemen and V.Rijmen, ―AES Proposal: Rijndael, AES algorithm submission, September 3, 1999, available: http://www.nist.gov/CryptoToolkit.

[2] Draft FIPS for the AES available from: http://csrc.nist.gov/encryption.aes , February 2001.

[3] C.-P. Su, T.-F. Lin, C.-T. Huang, and C.-W. Wu, ―A high-throughput low-cost AES processor, IEEE Commun. Mag., vol. 41, no. 12, pp. 86–91, Dec. 2003

[4] huang Yin, hedebiao, kang yong and fei Xiande , ―High speed ASIC implementation of AES supporting 128/192/256 bits, International conference on test and Measurement, 2009.

[5] I. Verbauwhede, P. Schaumont and H. Kuo, ―Design and Performance Testing of a 2.29-GB/s Rijndael Processor, IEEE Journal of Solid State Circuits, Vol. 38, No. 3, March 2003, pp. 569-572 .

[6] T. Ichikawa, T. Kasuya, and M. Matsui, ―Hardware Evaluation of the AES Finalists, in Proc. 3rd AES Candidate Conference, pp. 279-285, New York, April 2000.

[7] H. Jiang, M. Marek-Sadowska, S. R. Nassif, "Benefits and Costs of Power-Gating Technique," *ICCD-05*, pp. 559-566, Oct. 2005.

[8] R. Bhanuprakash, Manisha Pattanaik, S. S. Rajput and Kaushik Mazumdar, " and Reduction of Ground Bounce Noise and Leakage Current During Mode Transition of Stacking Power Gating logic circuits" ,IEEE 2009 .