ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

High Performance Hardware Implementation of AES Using Minimal Resources

I.Rama Devi
M.Tech Student,
Department of ECE,
KITS for Women's, kodad, T.S, India.

Mr.M.Narasimha Rao
Associate Professor,
Department of ECE,
KITS for Women's, kodad, T.S, India.

ABSTRACT:

The increasing need for protecting data communication in computer networks has led to development of several cryptography algorithms. The Advanced Encryption Standard (AES) is a computer security standard issued by the National Institute of Standards and Technology (NIST) intended for protecting electronic data. Its specification is defined in Federal Information Processing Standards (FIPS) Publication 197. The AES cryptography algorithm can be used to encrypt/decrypt blocks of 128 bits and is capable of using cipher keys of 128 bits wide (AES128).In this project, a hardware implementation of the AES128 encryption algorithm was proposed. A unique feature of the proposed pipelined design is that the round keys, which are consumed during different iterations of encryption, are generated in parallel with the encryption process. This lowers the delay associated with each round of encryption and reduces the overall encryption delay of a plaintext block. This leads to an increase in the message encryption throughput.

1. INTRODUCTION:

AES is short for Advanced Encryption Standard and is a United States encryption standard defined in Federal Information Processing Standard (FIPS) 192, published in November 2001. It was ratified as a federal standard in May 2002. AES is the most recent of the four current algorithms approved for federal us in the United States. One should not compare AES with RSA, another standard algorithm, as RSA is a different category of algorithm. Bulk encryption of information itself is seldom performed with RSA.RSA is used to transfer other encryption keys for use by AES for example, and for digital signatures.

AES is a symmetric encryption algorithm processing data in block of 128 bits. A bit can take the values zero and one, in effect a binary digit with two possible values as opposed to decimal digits, which can take one of 10 values. Under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for security is the key. AES may configured to use different keylengths, the standard defines 3 lengths and the resulting algorithms are named AES-128, AES-192 and AES-256 respectively to indicate the length in bits of the key. Each additional bit in the key effectively doubles the strength of the algorithm, when defined as the time necessary for an attacker to stage a brute force attack, i.e. an exhaustive search of all possible key combinations in order to find the right one.

2. METHODOLOGY:

2.1 Some background on AES:

In 1997 the US National Institute of Standards and Technology put out a call for candidates for a replacement for the ageing Data Encryption Standard, DES. 15 candidates were accepted for further consideration, and after a fully public process and three open international conferences, the number of candidates was reduced to five. In February 2001, the final candidate was announced and comments were solicited. 21 organizations and individuals submitted comments. None had any reservations about the suggested algorithm. AES is founded on solid and well-published mathematical ground, and appears to resist all known attacks well. There's a strong indication that in fact no back-door or known weakness exists since it has been published for a long time, has been the subject of intense scrutiny by researchers all over the world, and such enormous amounts of economic value and information is already successfully protected by AES. There are no unknown factors in its design, and it was developed by Belgian researchers in Belgium therefore voiding the conspiracy theories sometimes voiced concerning an encryption standard developed by a United States government agency. A strong encryption algorithm need only meet only single main criteria: There must be no way to find the unencrypted clear text if the key is unknown, except brute force, i.e. to try all possible keys until the right one is found.

A secondary criterion must also be met:

The number of possible keys must be so large that it is computationally infeasible to actually stage a successful brute force attack in short enough a time. The older standard, DES or Data Encryption Standard, meets the first criterion, but no longer the secondary one – computer speeds have caught up with it, or soon will. AES meets both criteria in all of its variants: AES-128, AES-192 and AES-256.

2.2Encryption must be done properly:

AES may, as all algorithms, be used in different ways to perform encryption. Different methods are suitable for different situations. It is vital that the correct method is applied in the correct manner for each and every situation, or the result may well be insecure even if AES as such is secure. It is very easy to implement a system using AES as its encryption algorithm, but much more skill and experience is required to do it in the right way for a given situation. No more than a hammer and a saw will make anyone a good carpenter, will AES make a system secure by itself. To describe exactly how to apply AES for varying purposes is very much out of scope for this short introduction.

2.3 Strong keys:

Encryption with AES is based on a secret key with 128, 192 or 256 bits. But if the key is easy to guess it doesn't matter if AES is secure, so it is as critically vital to use good and strong keys as it is to apply AES properly. Creating1 good and strong keys is a surprisingly difficult problem and requires careful design when done with a computer.

The challenge is that computers are notoriously deterministic, but what is required of a good and strong key is the opposite – unpredictability and randomness. Keys derived into a fixed length suitable for the encryption algorithm from passwords or pass phrases typed by a human will seldom correspond to 128 bits much less 256. To even approach 128--bit equivalence in a pass phrase, at least 10 typical passwords of the kind frequently used in day-to-day work are needed. Weak keys can be somewhat strengthened by special techniques by adding computationally intensive steps which increase the amount of computation necessary to break it. The risks of incorrect usage, implementation and weak keys are in no way unique for AES; these are shared by all encryption algorithms. Provided that the implementation is correct, the security provided reduces to a relatively simple question about how many bits the chosen key, password or pass phrase really corresponds to. Unfortunately this estimate is somewhat difficult to calculate, when the key is not generated by a true random generator.

2.4 Security is relative:

Security is not an absolute; it's a relation between time and cost. Any question about the security of encryption should be posed in terms of how long time, and how high cost will it take an attacker to find a key? Currently, there are speculations that military intelligence services possibly have the technical and economic means to attack keys equivalent to about 90 bits, although no civilian researcher has actually seen or reported of such a capability. Actual and demonstrated systems today, within the bounds of a commercial budget of about 1 million dollars can handle key lengths of about 70 bits. An aggressive estimate on the rate of technological progress is to assume that technology will double the speed of computing devices every year at an unchanged cost.

If correct, 128-bit keys would be in theory be in range of a military budget within 30-40 years. An illustration of the current status for AES is given by the following example, where we assume an attacker with the capability to build or purchase a system that tries keys at the rate of one billion keys per second. This is at least 1 000 times faster than the fasted personal computer in 2004. Under this assumption, the attacker will need about 10 000 000 000 000 000 000 000 years to try all possible keys for the weakest version, AES-128.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The key length should thus be chosen after deciding for how long security is required, and what the cost must be to brute force a secret key. In some military circumstances a few hours or days security is sufficient – after that the war or the mission is completed and the information uninteresting and without value. In other cases a lifetime may not be long enough.

3. IMPLEMENTATION:

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. It has been adopted by the U.S. government and is now used worldwide. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.In the United States, AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a five-year standardization process in which fifteen competing designs were presented and evaluated before it was selected as the most suitable (see Advanced Encryption Standard process for more details). It became effective as a Federal government standard on May 26, 2002 after approval by the Secretary of Commerce.

It is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information (see Security of AES, below). Originally called Rijndael, the cipher was developed bytwo Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted by them to the AES selection processtwo Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted by them to the AES selection process. The name Rijndael (Dutch pronunciation: [ˈrɛindaːl][5]) is a play on the names of the two inventors.Strictly speaking, AES is the name of the standard, and the algorithm described is a (restricted) variant of Rijndael. However, in practice the algorithm is also referred to as “AES” (a case of totum pro parte).

3.2 Description of the cipher:

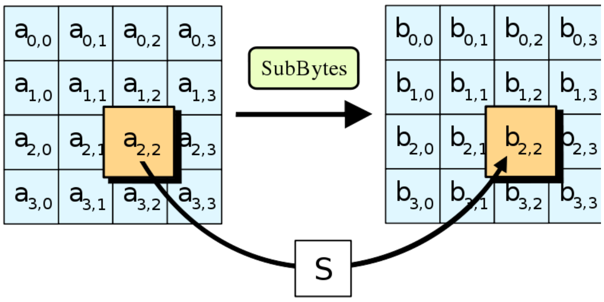
AES is based on a design principle known as a substitution-permutation network. It is fast in both software and hardware.[6] Unlike its predecessor, DES, AES does not use a Feistel network.

AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The blocksize has a maximum of 256 bits, but the keysize has no theoretical maximum.AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field.The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

4. DISCUSSION:

The SubBytes step:

In the SubBytes step, each byte in the matrix is updated using an 8-bit substitution box, the Rijndael 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 simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen The S-box is also chosen to avoid any fixed points (and so is a derangement), and also any opposite fixed points.

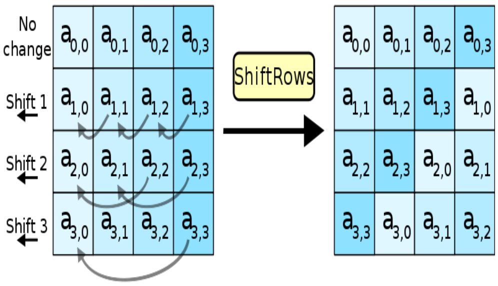

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

The ShiftRows step:

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first ro33w is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

For the block of size 128 bits and 192 bits the shifting pattern is the same. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state. (Rijndael variants with a larger block size have slightly different offsets). In the case of the 256-bit block, the first row is unchanged and the shifting for second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively—this change only applies for the Rijndael cipher when used with a 256-bit block, as AES does not use 256-bit blocks.


No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Brief Description of Rijndael Algorithm:

Rijndael algorithm consists of encryption, decryption and key schedule algorithm. The main operations of the encryption algorithm among the three parts of Rijndael algorithm include: bytes substitution (SubBytes), the row shift (ShiftRows), column mixing (MixColumns), and the round key adding (AddRoundKey). It is shown as Fig. 1.

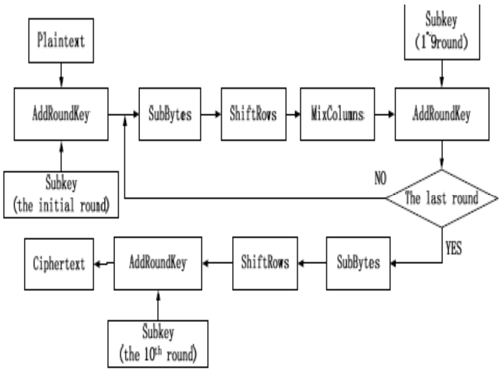


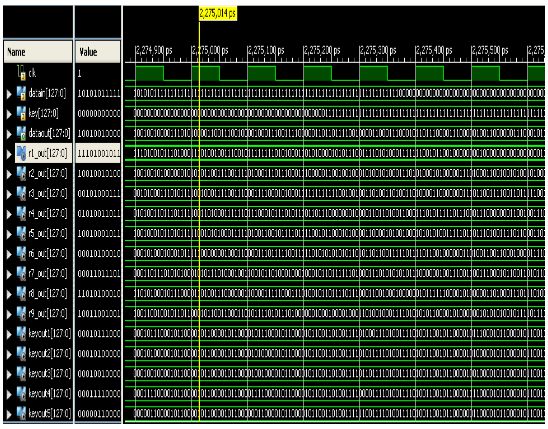
Figure. The structure of Rijndael encryption algorithm

5. Concluding Remarks :

AES-128 algorithm for encryption and decryption is implemented in Virtex-5 FPGA. With the designing of all the operations as LUTs and ROMs, the proposed architectureachieves a throughput of 3.74 Gbps and thereby utilizing only 1% of slices in the targeted FPGA. Since the speed is higher than the already reported systems, hence the proposed design serves as the best high speed encryption algorithm and is thus suitable for various applications. Moreover with less area utilization, the proposed design can be embedded with other larger designs as well.

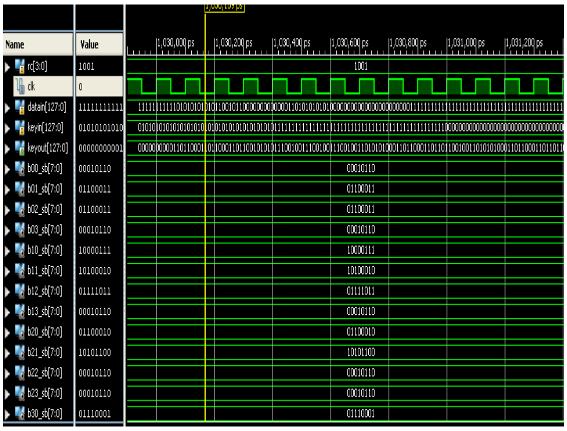
6. Experimental Results:

Simulation For Aes



```
Name              Value
clk               1
datain[127:0]     10101011111
key[127:0]        00000000000
dataout[127:0]    10010010000
r1_out[127:0]     11101001011
r2_out[127:0]     10010010100
r3_out[127:0]     00101000111
r4_out[127:0]     01010011011
r5_out[127:0]     10010001011
r6_out[127:0]     00010100010
r7_out[127:0]     00011011101
r8_out[127:0]     11010100010
r9_out[127:0]     10011001001
keyout1[127:0]    00010111000
keyout2[127:0]    00010100000
keyout3[127:0]    00010010000
keyout4[127:0]    00011110000
keyout5[127:0]    00000110000
```

Simulation For Rounds



```
Name              Value
rc[3:0]           1001
clk               0
datain[127:0]     11111111111
keyin[127:0]      01010101010
keyout[127:0]     00000000001
b00_sb[7:0]       00010110
b01_sb[7:0]       01100011
b02_sb[7:0]       01100011
b03_sb[7:0]       00010110
b10_sb[7:0]       10000111
b11_sb[7:0]       10100010
b12_sb[7:0]       01111011
b13_sb[7:0]       00010110
b20_sb[7:0]       01100010
b21_sb[7:0]       10101100
b22_sb[7:0]       00010110
b23_sb[7:0]       00010110
b30_sb[7:0]       01110001
```

7. ACKNOWLEDGMENTS:

I am I.Ramadevi and would like to thank the publishers, researchers for making their resources material available. I am greatly thankful to Associate Prof: Mr.M.Narasimharao for their guidance. We also thank the college authorities, PG coordinator and Principal for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members

8.REFERENCES:

1] M. C. C¸ avu¸so˘glu. Telesurgery and Surgical Simulation: Design, Modeling, and Evaluation of Haptic Interfaces to Real and Virtual Surgical Environments. PhD thesis, University ofCalifornia, Berkeley, August 2000.

[2] M. C. C¸ avu¸so˘glu, F. Tendick, M. Cohn, and S. S. Sastry. A laparoscopic telesurgical workstation. IEEE Transactions on Robotics and Automation, 15(4):728–739, August 1999.

[3] E. Graves. Vital and Health Statistics. Data f rom the National Health Survey No. 122. U.S. Department ofHealth and Human Services, Hyattsville, MD, 1993.

[4] J. W. Hill, P. S. Green, J. F. Jensen, Y. Gorfu, and A. S. Shah. Telepresence surgery demonstration system. In Proceedings of the IEEE International Conference on Robotics and Automation, pages 2302–2307, 1994.

[5] A. J. Madhani. Design of Teleoperated Surgical Instruments for Minimally Invasive Surgery. PhD thesis, Massachusetts Institute ofTechnology, 1998.

[6] A. J. Madhani, G. Niemeyer, and J. K. Salisbury. The black falcon: a teleoperated surgical instrument for minimally invasive surgery. In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS'98), volume 2, pages 936–944, 1998

.

[7] J.W.Hill, P. S. Green, J. F. Jensen,Y. Gorfu, and A. S. Shah, "Telepresence surgery demonstration system," in Proc. IEEE Int. Conf. Robot. Autom.,San Diego, CA, May 1994, vol. 3, pp. 2302–2307.

[8] P. Dario, E. Guglielmelli, B. Allotta, and M. C. Carrozza, "Robotics for Medical applications," IEEE Robot. Autom.Mag. vol. 3, no. 3, pp. 44–56, Sep. 1996.

Author's Details:

Ms. I.RAMADEVI. MTech student, in M.Tech Student, Dept of ECE in KITS for women's,kodad, T.S, India.

Mr.M.Narasimha Rao working as a Associate at ECE in KITS for women's,kodad, T.S, IndiaJNTUH Hyderabad. he has 6 years of UG/PG Teaching Experience