Cryptographic Key Based Information Hiding Using FPGA in AES

Sagar V. Dalal
Department of Electrical and Electronics Engineering
Prof RamMeghe College of Engineering&mangement
Badnera, India
sagardalal1987@gmail.com

Dr. Ms. K.N.Kasat
Department of Electronics and Telecommunication
Prof RamMeghe College of Engineering&mangement
Badnera, India
mailtoknk@rediffmail.com

Abstract—We are living in the information age.We need to keep information about every aspect of our lives & hence to protect sensitive data transfers against malicious attacks; it is necessary to encrypt data before transmission.Study of techniques needed to protect information is the field of cryptography.Cryptography is a science of secret writing.The purpose of this paper is to implement a mechanism to hide information using cryptography.Advanced encryption standard is a type of symmetric cryptography standard which can be used to transfer a block of information securely during transmission.

Keywords-*FPGA,Cryptography,AES*

*****

I. INTRODUCTION

In traditional (symmetric-key) cryptography,sender and receiver of a message know and use the same secret key. Main challenge is getting sender and receiver to agree on secret key without anyone else finding out. If they are at differentlocations, they must rely ontransmission medium to prevent disclosure of secret key. Anyone who overhears key can later read, modify messages authenticated using that key.Sosecret-key cryptography often has difficulty providing secure key management. To solve this problem, Whitfield Diffie and Martin Hellman introduced concept of public-key cryptography in 1976. Public-key cryptography requiring two separate keys,secret and public. Two parts of key pair are mathematically linked.Algorithms used for public key cryptography are based on mathematical relationships.It is easy for receiver to generate public and private keys, to decrypt message using private key, and easy for sender to encrypt message using public key, it is extremely difficult anyone to derive private key, based only on their knowledge of the public key.Unlike symmetric key algorithms,public key algorithm does not require a secure initial exchange of one or more secret keys between sender and receiver. In practice, only hash of message is typically encrypted for signature verification purposes. Public-key cryptography is fundamental&widely usedtechnology.

II. RELATED WORK

Methodology proposed by F.X.Standaert [2] to implement block cipher in FPGA and it is applied to design AES Rijndael which is improves previouslyresults in terms of hardware cost, or efficiency.FPGAs is attractive options for hardware implementations of algorithms, as it provides physical security,andhigher performance than software solutions. Rijndael algorithm was found to yield best results when operating in feedback mode[3].U.S. National Institute of Standards and Technology (NIST) conducted a competition to develop replacement for DES.Rijndael algorithm was winner and destined to become new AES. In last phase of the selection, there were five finalist algorithms: Mars, RC6, Rijndael, Serpent and Twofish. All algorithms were considered secure.But hardware efficiency was given great importance in selecting Rijndael as winning algorithm.This algorithm is documented in US government publication, FIPS-197[4].Among manyalgorithms, most popular is Data Encryption Standard (DES) algorithm.DES could not keep up with advancement in technology.Triple DES takes three times as much CPU power but AES outperforms 3 DES [8].

III. PURPOSE OF CRYPTOGRAPHY

Cryptography is important when communicating over untrusted medium.Functions of cryptography are:

1. *Confidentiality:* Ensuring messageread by the intended receiver.
2. *Authentication:*Proving one'sidentity.
3. *Integrity:* Assuring received message has not been altered in any way from the original.
4. *Non-repudiation:* Mechanism for proving that the sender really sent message.
5. *Key exchange:* Method of crypto keys are shared between sender and receiver.

Cryptographic process have four basic parts:
Plaintext - Unscrambled information to be transmitted. It could be a simple text document, a credit card number, a password, a bank account number, or sensitive information such as payroll data, personnel information, or a secret formula being transmitted between organizations.
Ciphertext- Represents plain text rendered unintelligible by the application of a mathematical algorithm. Ciphertext is the encrypted plain text that is transmitted to the receiver. **Key**-Itdetermines how a plaintext message is encrypted or decrypted. Key is the only way to decipher the information.
Cryptographic Algorithm –Mathematical formula used to scramble the plain text to ciphertext.Using samealgorithm converting plain text to ciphertextis called encryption, and converting ciphertext back to plain text is called decryption.

 ISSN: 2321-8169
25 – 30

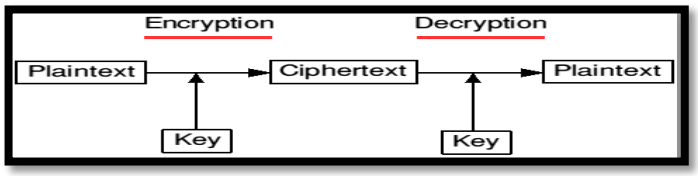


Figure 1 Cryptography

IV. TYPES OF ALGORITHMS

Three cryptographic algorithmswill be discussed are:

- Secret Key Cryptography for privacy and confidentiality .
- Public Key Cryptography for authentication, non-repudiation, and key exchange.
- Hash Functions for message integrity.

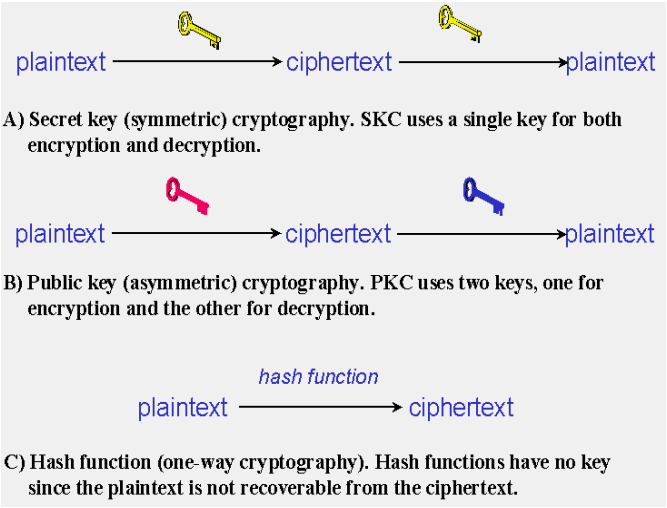
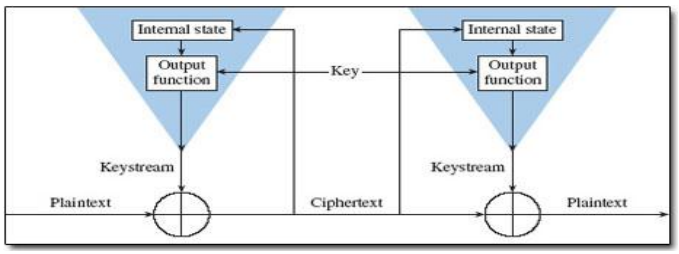


Figure 2: Three types of cryptography

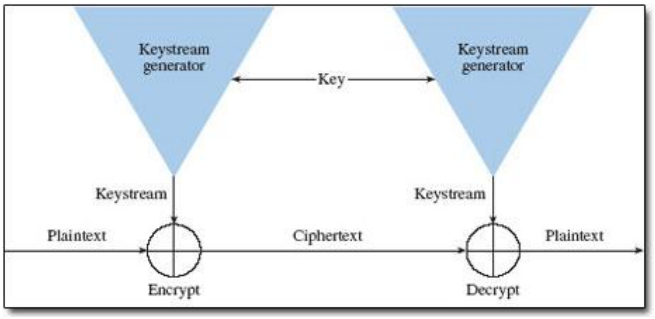
A. *Secret Key Cryptography*

Single key is for encryption and decryptionprocess.In Figure (a), sender useskey to encrypt plaintext and sends ciphertext to receiver.Receiver applies same key to decrypt message and recover plaintext.Secret key cryptography is also called *symmetric encryption*.Difficulty with this is the distribution of the key.Theyare categorized as *block ciphers*.



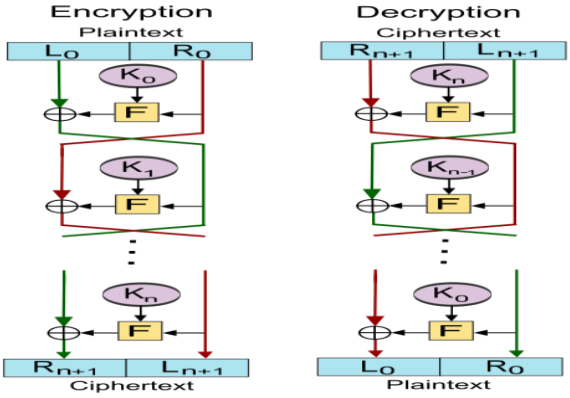
a) Self-synchronizing stream cipher

Stream ciphers implement feedback mechanism so that key is constantly changing.They are operate on single bit at a time.*Self-synchronizing stream ciphers* calculate each bit in the keystream as a function of the previous *n* bits in the keystream.It is termed "self-synchronizing" because decryption processcan stay synchronized with encryption process and nothing more by knowing how far into the *n*-bit keystream it is.Hereproblem is error propagation;garbled bit in transmission will resultin *n*garbled bits at the receiving side. *Synchronous stream ciphers*keystream is independent of the message stream but uses the same keystream generation function at sender and receiver.Stream ciphers do not propagate transmission errors, theyare periodic so keystream will repeat.



b)*Synchronous stream cipher*

In Block cipher scheme encrypts one block of data at a time using same key on each block.Same plaintext block will always encrypt to same ciphertext when using same key in a block cipher whereas same plaintext will encrypt to different ciphertext in a stream cipher.Common construct for block encryption algorithms is Feistel cipher, named for Horst Feistel (IBM).In Figure(c),Feistel cipher combines elements of substitution, permutation and key expansion.InFeistel design encryption and decryption stages are similar,requiring only reversal of the key operation,thus reducing size of the code or circuitry.

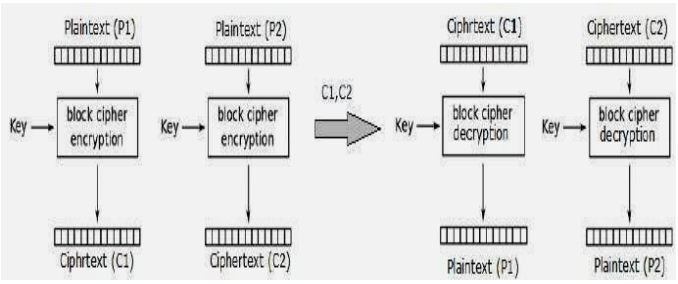


c) Feistel cipher

Block ciphers operates infollowing modes:

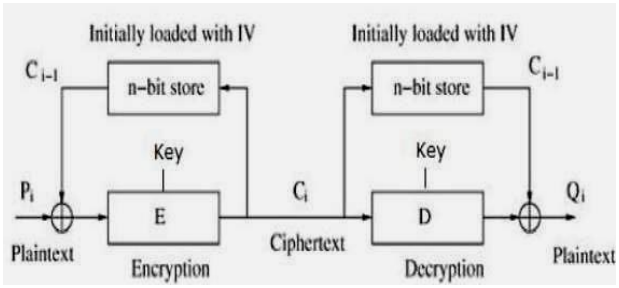
Electronic Codebook (ECB) mode:Secret key is used to encrypt plaintext block to form a ciphertext block. Two identical plaintext blocks will always generate same ciphertextblock.It is susceptible to variety of brute-force attacks and insertion attacks.

 ISSN: 2321-8169
25 – 30



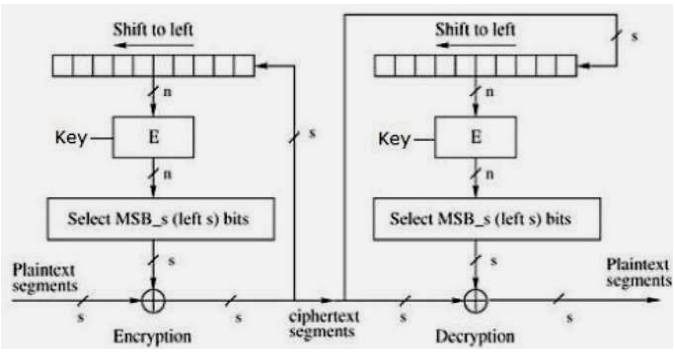
d)Electronic codebook (ECB) Mode

Cipher Block Chaining (CBC) mode adds feedback mechanism to encryption process; plaintext is exclusively-ORed with previous ciphertext block so that two similar plaintext blocks will encrypt differently.It protects against many brute-force, deletion, and insertion attacks.



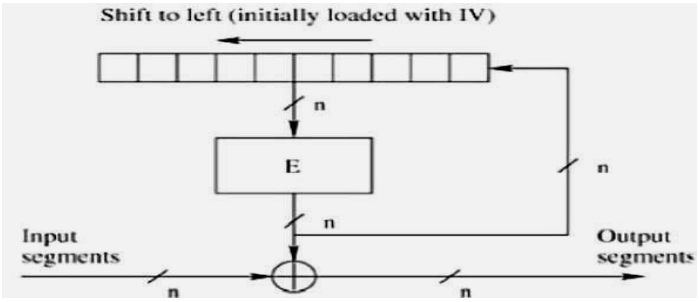
e) Cipher Block Chaining(CBC) Mode

*Cipher Feedback (CFB) mode*as a self-synchronizing stream cipher is block cipher implementation. It allows data to be encrypted in units smaller than block size,which is helpful in encrypting interactive terminal input.In one-byte CFB mode,incoming character is placed into shift register the same size as the block, encrypted, & the block transmitted.In receiving side,ciphertext is decrypted & the extra bits in the block are discarded.



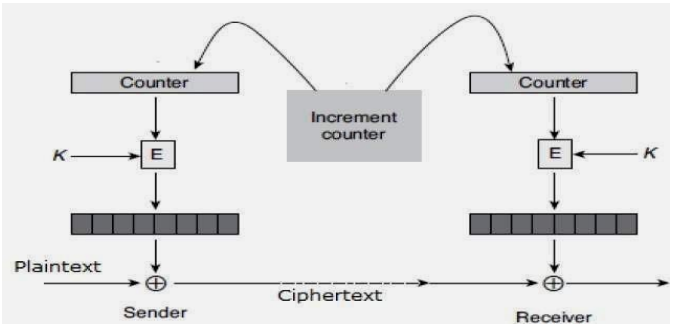
f) Cipher Feedback(CFB) Mode

Output Feedback (OFB) mode is block cipher implementation similar to synchronous stream cipher.Itprevents same plaintext block from generating same ciphertext block by using internal feedback mechanism that generates keystream independently of both bitstreams.In OFB,single bit error in ciphertext yields single bit error in the decrypted plaintext.



g)Output Feedback(OFB) Mode

Counter (CTR) mode:Itoperates on the blocks as in a stream cipher.Itoperates on the blocks independently.Ituses different key inputsto different blocks so that two identical blocks of plaintext will not result in the same ciphertext. Finally, each block of ciphertext has specific location within the encrypted message.Itallows blocks to be processed in parallel thus offering performance advantages.Onebit of plaintext message is corrupts, only that one corresponding output bit is corrupt as well.one should change secret key after using for a number of sent messages.It provides security and secret key needs to be changed less often.



h) Counter(CTR) Mode

Secret key cryptography algorithmsinclude:*DataEncryption Standard (DES)*designed by IBM in the 1970s and adopted by National Bureau of Standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 for commercial and unclassified government applications.DES is Feistel block-cipher employing a 56-bit key that operates on 64-bit blocks.It has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations.Two important variants that strengthen DES are:

*Triple-DES (3DES):*3DES employs up to three 56-bit keys & makes three encryption/decryption passes over the block; 3DES is also described in FIPS 46-3&is the recommended replacement to DES.

DESX: A variant devised by Ron Rivest.Combining 64 additional key bits to the plaintext prior to encryption, effectively increases the keylength to 120 bit.

Advantages of Symmetric Key Cryptography: Quick recitation.Rapid check authenticity of key recipients.To get a

 ISSN: 2321-8169
25 – 30

plain texts same key is required as used at message encrypt time.

Disadvantages of Symmetric Key Cryptography: Unauthorized person can get whole information without any effort if gets secrete key. This technique not provide digital signatures that cannot be repudiated .

B. Public-Key Cryptography

Public-key cryptography algorithms include:

*RSA:*Named for the three mathematicians who developed it Ronald Rivest, Adi Shamir, and Leonard Adleman,used for key exchange, digital signatures, or encryption of small blocks of data.It uses variable size encryption block and size key.Key-pair is derived from very large number, *n*, is the product of two prime numbers chosen according to rules; these primes may be hundread or more digits in length, yielding an *n* with roughly twice as many digits as the prime factors.Public key information includes a derivative of one of the factors of *n*; an mugger cannot determine prime factors of *n* therefore private key from this information alone and that makes this algorithm secure.

*Diffie-Hellman:*Theycame up with their own algorithm.D-H is used for secret-key key exchange only, and not for authentication or digital signatures.

Advantages of Asymmetric Key Cryptography**:**Overcome key distribution issues of symmetric key algorithms. Public-key cryptography is not meant to replace secret-key cryptography, but to supplement it. By using pair of keys it increases the level of security.Provide digital signatures that can be repudiated.

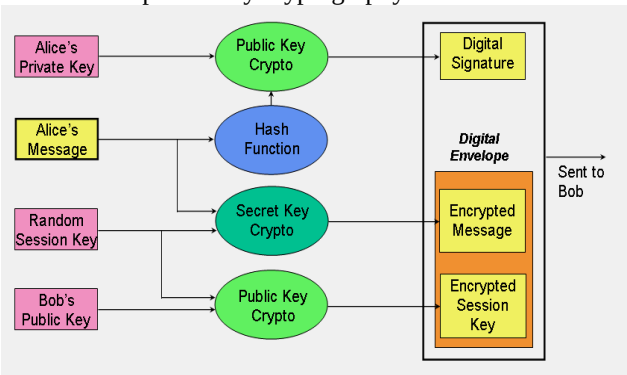
Disadvantages of Asymmetric Key Cryptography**:**Disadvantage is speed.Public-key cryptography may be vulnerable to impersonation, even if users private keys are not available.Certification Problems, Many public key systems use a third party to certify the reliability of public keys.

C. Hash Functions: It's computation based upon the plaintext. It is inaccessible for the length of the plaintext to be recovered.Used to provide a digital fingerprint of a file's contents,to ensure that the file has not been altered by an virus.They are employed to passwords.It includes:

Message Digest (MD) algorithms:Series of byte-oriented algorithms produced128-bit hash value.

*Secure Hash Algorithm (SHA):*SHA-1 produced160-bit hash value.SHA-2,described in FIPS PUB 180-2 and replaced by FIPS PUB 180-3 and 180-4.SHA-3 is current SHS algorithm.

In Hash functions change made to the contents of a message will result in the receiver calculating a different hash value than one placed in the transmission by the sender.Secret key cryptographyis suited to encrypting messages.Public-key cryptography used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography.



i)Use of three cryptographic techniques

Figure (i)shows how *hybrid cryptographic* scheme combines all of functions to form secure transmission comprising *digital signature* and *digital envelope*.Senderof message is Alice and receiver is Bob.Digital envelope comprises an encrypted message and an encrypted session key.Alice uses secret key cryptography to encrypt her message using *session key*, which she generates at random with each session. Alice then encrypts session key using Bob's public key.Encrypted message and encrypted session key together form the digital envelope.Upon receipt, Bob recovers session secret key using his private key and then decrypts encrypted message.Digital signature is formed in two steps.First,Alice computes hash value of her message; next, she encrypts hash value with her private key.Upon receipt of digital signature, Bob recovers hash value calculated by Alice by decrypting digital signature with Alice's public key.Bob can then apply hash function to Alice's original message,which he has already decrypted.Ifresultant hash value is not same as value supplied by Alice,then Bob knows that message has been altered; if the hash values are same,Bob should believe that message he received is identical to one that Alice sent.

V. AES IN FPGA

Rijndaelis designed by Joan Daemen and Vincent Rijmen.pronounced as rain doll, operate over a variable-length block.Block length can be extended in multiples of 32 bits.Designwas influenced by block cipher called *Square*.Works on principle ofSubstitution Permutation network.It doesn't use a Feistel network and is fast in both software and hardware.It operates on a 4×4 matrix of bytes termed as a state.It is specified as number of repetitions of transformation sounds that convert input plaintext into the final output of cipher text.It is an iterated block cipher and it's initial input block and cipher key undergoes multiple rounds of transformation before giving the output.Intermediate cipher output is called State.Block and cipher key are represent as an array of columns where each array has 4 rows and each column represents a single byte (8 bits).Number of columns in an array representing state calculated as key length divided by 32 (32 bits = 4 bytes). Array representing State will have Nb columns, Nb values of 4, 6, and 8 correspond to a 128-, 192-, and 256-bit block.Array representing a Cipher Key will have Nk columns, Nk values of 4, 6, and 8 correspond to a 128-, 192-, and 256-bit key.Used for security of Smart cards, wireless sensor.Inbroad band links.Suited for restricted-space environments.Web servers that need to handle many sessions.

 ISSN: 2321-8169
25 – 30

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$	$k_{0,4}$	$k_{0,5}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$	$k_{1,4}$	$k_{1,5}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$	$k_{2,4}$	$k_{2,5}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$	$k_{3,4}$	$k_{3,5}$

Number of rounds (**Nr**) is given by:

No. of Rounds Nr		**Block Size**		
		128 bits Nb = 4	**192 bits Nb = 6**	**256 bits Nb = 8**
Key Size	**128 bits Nk = 4**	10	12	14
	192 bits Nk = 6	12	12	14
	256 bits Nk = 8	14	14	14

Nb, **Nk**, and **Nr** values supported are:

	Parameters		
Variant	**Nb**	**Nk**	**Nr**
AES-128	4	4	10
AES-192	4	6	12
AES-256	4	8	14

It has three operational stages:

- AddRound Key transformation
- **Nr**-1 Rounds comprising:
  - SubBytes transformation
  - ShiftRows transformation
  - MixColumns transformation
  - AddRoundKey transformation
- A final Round comprising:
  - SubBytes transformation
  - ShiftRows transformation
  - AddRoundKey transformation

Arrays *s* and *s'* refer to the State before and after a transformation.Rijndael specification uses the array nomenclature a and b for before and after States.For indicating byte locations within the State array the subscripts *i* and *j* are used.

The SubBytes transformation

ByteSub in Rijndaeltransformation operates on each of the State bytesseparatly and changes the byte value. An S-box, controls the transformation.Characteristics of the S-box transformation as well as a compliant S-box table are provided in the specification.InSubBytes transformation a given byte in State s is given a new value in State s' according to the S-box. The S-box, is a function on a byte in State s:

$s'_{i,j} = \text{S-box}\ (s_{i,j})$

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

== S-box ====>

$s'_{0,0}$	$s'_{0,1}$	$s'_{0,2}$	$s'_{0,3}$
$s'_{1,0}$	$s'_{1,1}$	$s'_{1,2}$	$s'_{1,3}$
$s'_{2,0}$	$s'_{2,1}$	$s'_{2,2}$	$s'_{2,3}$
$s'_{3,0}$	$s'_{3,1}$	$s'_{3,2}$	$s'_{3,3}$

The ShiftRows transformation

ShiftRow in Rijndael transformation cyclically shifts the bytes in the bottom three rows of the State array.Rows 2, 3, and 4 are cyclically left-shifted by C1, C2, and C3 bytes, respectively:

Nb	C1	C2	C3
4	1	2	3
6	1	2	3
8	1	3	4

Effect of the ShiftRows transformation on State s:

State s					State s'			
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$	---------- no shift ----------	$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	----> left-shift by C1 (1) --	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$	----> left-shift by C2 (2) --	$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$	----> left-shift by C3 (3) --	$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$

The MixColumns transformation

MixColumn in Rijndaeltransformation uses a mathematical function to transform values of a given column within a State.MixColumns as a function,could be written:

$s'_{i,c} = \text{MixColumns}\ (s_{i,c})$

for $0 \leq i \leq 3$ for some column, c. The column position doesn't change, only the values within the column.

Round Key generation and the AddRoundKey transformation

Cipher Key can be 128, 192, or 256 bits in length.It is used to derive a different key to be applied to the block during each round of the encryption operation.Cipher keys are called Round Keys and each will be the same length as the block, i.e., **Nb** 32-bit words.Words are denoted by W. Key schedule by which the original Cipher Key (of length **Nk** 32-bit words) is used to form an *Expanded Key*is defned. Expanded Key size is equal to the block size times the number of encryption rounds plus 1, which will provide **Nr**+1 different keys. There are **Nr**encipherment rounds but **Nr**+1 AddRoundKey transformations.

alternative to custom and semicustomApplication Specific Integrated Circuits (ASICs).Integrated circuits that must be designed all the way fromthe behavioral description to the physical layout are sentfor an expensive and time-consuming fabrication.AES algorithm based on FPGA deviceshas the following advantages:

· Lower cost of the computer-aided design tools, verificationand testing.

· Potential for fast, low-cost multiple reprogramming andexperimental testing of a large number of various architecturesand revised versions of the same architecture.

· Higher accuracy of comparison.

The input from the keyboard is considered to beencoded in ASCII.The input from the keyboard is considered to beencoded in Hexadecimal, thus the only validcharacters are 0-9, A-F.Device is configured to receive data and outputcipher text.Device is configured to receive cipher text andoutput data.Mix Columns and the Inverse Mix Columns instructions, operate column by column on the state array.Each column is replaced after being multiplied by a constantarray. The operation is reduced to simple shift and XOR operationswhile writing the source code.Thus the Encryption process of Advanced Encryption Standardalgorithm is summarized as; each round of AES (except thelast round) for encryption consists of four stages. a) Sub-Bytes - a non-linear substitution step where each byte isreplaced with another according to a lookup table (known as S-Box). b) ShiftRows - transposition step where eachrow of the state is shifted cyclically a certain number ofsteps. c) MixColumns - a mixing operation which operateson the columns of the state, combining the four bytes ineach column using a linear transformation. d) AddRoundKey- each byte of the state is combined with theround key; each round key is derived from the cipher key using a key schedule.Anmodule decodes the scan codes generated by the keyboardinto ASCII or hexadecimal format. LCD displays the input and output of the core.

VI. CONCLUSION

Cryptography is an essential field because of amount of task or work i.e, by unavoidably,done in secret. Disregardingmathematical theory behind an algorithm,best Applications :Used for security of Smart cards, wirelesssensor and mesh networks. Usable in broad band links.Well suited for restricted-space environments where either encryption or decryption is implemented.Web servers that need to handle many encryption sessions.

Field Programmable Gate Array (FPGA) is an integrated circuit consists of thousands of universal building blocks, knownas configurable logic blocks (CLBs), connected using programmableinterconnects. Reconfiguration is able tochange a function of each CLB and connections amongthem, leading to a functionally new digital circuit.For implementing cryptography in hardware, FPGAsprovide the only major algorithms are those that are well known and documented because they are well tested and studied!Scheme that stays in use year after year is most likely a good one.The AES cipher is implemented on the FPGA provides an excellent platform for high security applications.

ACKNOWLEDGMENT

The authors would like to thank the members of the Dept. of EEE , Amravati University and all the people who helped in preparing and carrying out the data collection.

REFERENCES

[1] Aliwa Mehemed Bashir, El-Tobely Tarek EI-Ahmady,Fahmy Mahmood M., Nasr Mohamed EL Said and EI-Aziz Mohamed Hashem Abd;(2010) "A NewNovel Fidelity Digital Watermarking Based on Adaptively Pixel-Most-SignificantBit-6in Spatial Domain Gray Scale Images and Robust",American Journal of Applied Sciences 7 (7): 987-1022.

[2] F.X.Standaert, "A Methodology to implement block ciphers in reconfigurable hardware and as application to fast and compact AES Rijndael. "The field programmable logic array conference, Monterey, California, pp.216-224. 2003.

[3] Adam J. Elbirt, W. Yip, B. Chetwynd, and C. Paar- "An FPGABased Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists" (IEEE 2001).

[4] National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publications – FIPS 197.

[5] J.R. Hernandez, M.Amado, and F. Perez-Gonzalez,(2000) "DCT-DomainWatermarking Techniques for Still Images:Detector Performance Analysis And a New Structure", in IEEE Trans. Image Processing, vol. 9, pp 55-68.

[6] Mohanty S. P.,(1999) :Watermarking of Digital Images.M.S. Thesis, IISc, Bangalore, India.

Article in a journal:

[7] P.T.Thasneem Salim, T.Vigneswaran, "FPGA Implementation of Hiding Information using Cryptography ",Indian Journal of Science and Technology, vol 8(19),August 2015 , ISSN 0974-6846.

[8] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbirand Y. Al-Nabhani, "New Comparative Study between DES, 3DES and AES within Nine Factors", Journal of Computing, Volume 2, Issue 3, March 2010, ISSN 2151-9617.

Article in a conference proceedings:

[9] Bharathiraja Nallathambi, Karthigaikumar P, (2014) International Conference on Electronics and Communication Systems (lCECS -2014), Feb.13-14,2014,Coimbatore,India.