FPGA Implementation of AES Algorithm Using Cryptography

Sagar V. Dalal **Dr.Ms.K.N.Kasat**

***Abstract*—Nowdays information storage became electronic. However three security requirements did not change. The files stored in computers require confidentiality, integrity and availability. Implementation of these requirements, is different and more challenging. Protecting information by transforming it into an unreadable format in which a message can be covered from the casual reader and only the intended recipient will be able to convert it into original text is known as cryptography. It is a technique of hiding the plain information. The content like text, image, audio and video files converted to unreadable form by hiding data within it is the way of data cryptography scrambling. Cryptography main goal is to keep the data secure from unauthorized access. Advanced encryption standard is an algorithm of cryptography used to transfer information securely.**

***Key Words* —AES, Cryptography, FPGA, Hiding**

I. INTRODUCTION

New varieties of cryptography came shortly when the widespread development of pc communications.A useful means of classifying security attacks, is in terms of passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation. There are three primary goals in any security service. These are confidentially, integrity and availability. The principle of confidentiality is that only the sender and the intended recipient should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the message.When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. The principle of availability is that resources should be available to authorized parties at all times.

II. RELATED WORK

Yang Jun,Ding Jun Li, Na Guo Yixiong [2] conferred the system aims at reduced hardware structure. Compared with the pipeline structure, it has less hardware resources and it is high cost-efficient.AES system may be wide employed in the terminal equipments.AES algorithm includes key expansion and encryption process .Advantage of this is that we tend to don't got to store the round key since they're presently calculated. Adam J. Elbirt, W. Yip, B. Chetwynd, and C. Paar [3] conferred the Advanced coding rule includes potency testing of each hardware and software system implementations of candidate algorithms. Reprogrammable devices like field-programmable gate arrays (FPGAs) enticing choices for hardware implementations of coding algorithms, as they provide physical security, and probably a lot of higher performance than software system solutions. U.S. National Institute of Standards and Technology (NIST) conducted a contest to develop replacement for DES.Rijndael rule was winner and destined to become new AES. In last section of the choice, there have been 5 challenger algorithms: Mars, RC6, Rijndael, Serpent and Twofish. All algorithms were thought of secure, hardware potency was given nice importance in choosing Rijndael as winning rule.This rule is documented in U.S. publication, FIPS-197[4]. William Stallings [5] AES may be a block cipher supposed to exchange DES. It uses a 128-bit block size and a key size of 128, 192, or 256 bits. AES doesn't use a Feistel structure. Instead, every full round consists of 4 separate functions:byte substitution, permutation, arithmetic operations over a finite field, and XOR with a key. AES was revealed by the National Institute of Standards and Technology (NIST) in 2001.

III. TYPES OF CRYPTOGRAPHIC ALGORITHMS

Types of algorithms that will be discussed are (Figure 1):

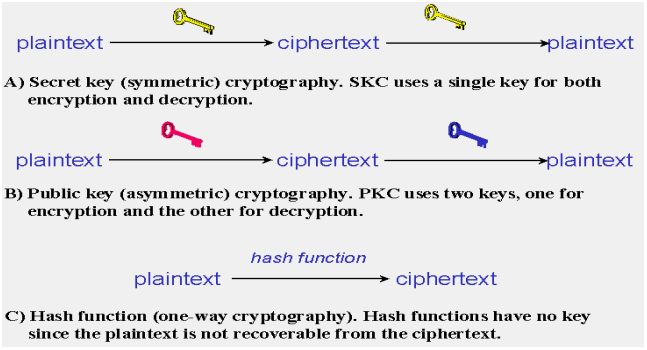
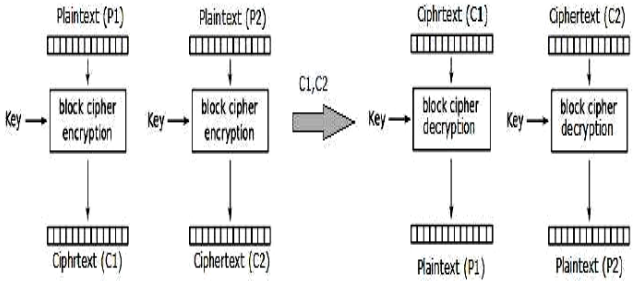


FIGURE 1: Three types: secret-key, public key and hash function.

In Hash functions changes made to the contents will result in the receiver calculating a different hash value than one placed by the sender.Secret key cryptography is applicable to encrypting messages.Public-key cryptography used to encrypt messages but this is oftenly done because secret-key cryptography works about 1000 times faster than public-key cryptography.

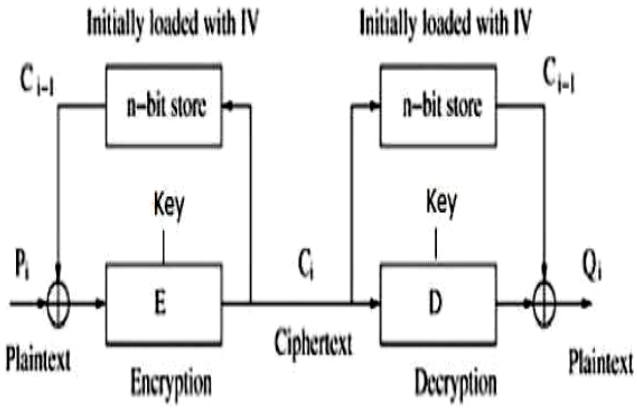
Block ciphers following modes are most important:

Simplest of the coding modes is the Electronic Codebook (ECB) mode .Message is split into blocks, and every block is encrypted severally.Drawbacks of this technique is that identical plaintext blocks encrypted into identical ciphertext blocks. In some senses, it does not give serious message confidentiality.



a) Electronic codebook (ECB) Mode

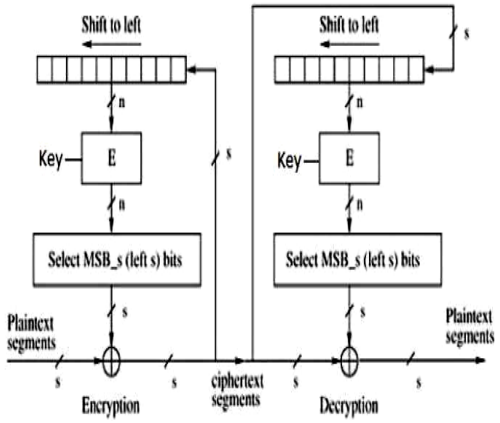
In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. In this way, each ciphertext block depends on all plaintext blocks processed up to that point.For making each message unique, an initialization vector must be used in first block. CBC has been the most commonly used mode.Its main drawbacks are that encryption is sequential and that the message must be padded to a multiple of the cipher block size.



b) Cipher Block Chaining(CBC) Mode

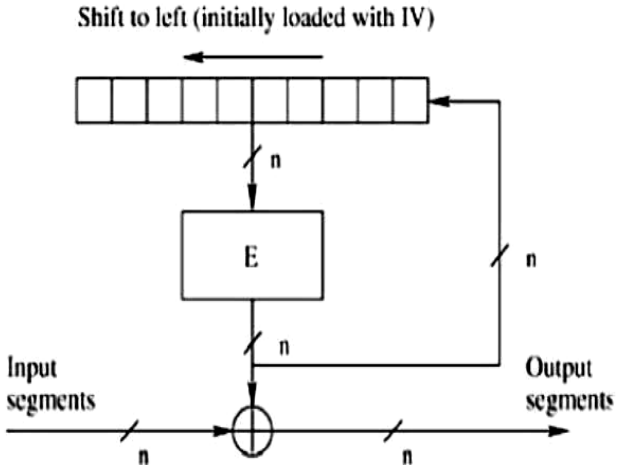
One way to handle this last issue is through the method known as ciphertext stealing.One-bit change in a plaintext or IV affects all following ciphertext blocks.

In Cipher *Feedback* (CFB) mode,decryption performed is almost similar to CBC encryption performed in reverse. Like cipher block chaining mode, changes in the plaintext propagate forever in the ciphertext,& encryption cannot be parallelized.Like cipher block chaining mode decryption can be parallelized.In decrypting, one-bit change in the ciphertext affects two plaintext blocks: one-bit change in the corresponding plaintext block, and complete of the following plaintext block.Next plaintext blocks are decrypted normally.Advantages are: the block cipher is only ever used in the encrypting direction, & the message doesn't need to be padded to a multiple of the cipher block size.



c) Cipher Feedback(CFB) Mode

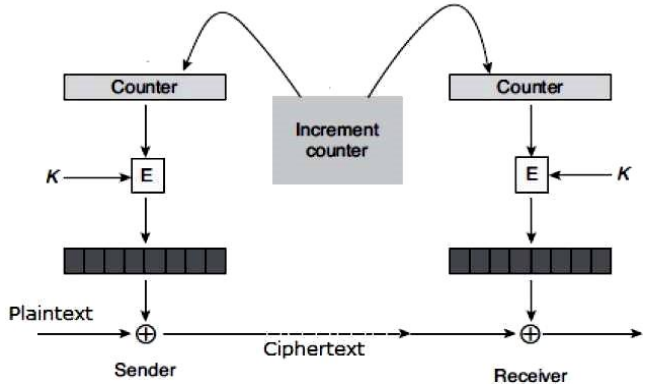
In *Output Feedback* (OFB) mode generation of keystream blocks due to the making of a block cipher into a synchronous stream cipher by OFB mode is done,that are XORed with plaintext blocks to get ciphertext. Like with other stream ciphers, flipping bit in the ciphertext makes flipped bit in the plaintext at the same position. This makes many error correcting codes to function normally even when applied before encryption.



d) Output Feedback(OFB) Mode

CTR mode has same characteristics to OFB, but also allows an property of random access during decryption. It uses different key inputs to 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.It allows blocks to be processed in parallel thus offering performance advantages. CTR mode is

well suited to operate on a multi-processor machine where blocks can be encrypted in parallel.It does not suffer from the short-cycle problem that can affect OFB.



e) Counter(CTR) Mode

Secret key cryptography algorithms include:

Data Encryption Standard (DES): DES was based on an earlier cipher from Feistel called Lucifer which had a 112-bit key. This was rejected, partially in order to fit the algorithm onto a single chip and partially because of the National Security Agency (NSA).NSA also proposed a number of tweaks to DES that many thought were introduced in order to weaken the cipher, but analysis in the 1990s showed that the NSA suggestions actually strengthed DES.DES was defined in American National Standard X3.92 and three Federal Information Processing Standards (FIPS), all withdrawn in 2005:

Two important variants that strengthen DES are:

- *Triple-DES (3DES):* A variant of DES that employs up to three 56-bit keys and makes three encryption/decryption passes over the block; 3DES is the recommended replacement to DES.
- *DESX:* A variant devised by Ron Rivest. By combining 64 additional key bits to the plaintext prior to encryption, effectively increases the keylength to 120 bit.

Public-key cryptography algorithms include:

- *RSA:* Developed by Ronald Rivest, Adi Shamir, and Leonard Adleman.Used for key exchange, digital signatures, or encryption of small blocks of data and uses variable size encryption block and variable size key.Key-pair is derived from very large number, *n*, that is the product of two prime numbers choose according to special rules.Public key information includes *n* and a derivative of one of the factors of *n;* an attacker cannot determine prime factors of *n* therefore that makes this algorithm secure.
- *Diffie-Hellman:* Diffie and Hellman algorithm which is not for authentication or digital signatures.It is used for secret-key key exchange only.

Hash Functions

They also called *message digests*.They use no key, but a fixed-length hash value is computed here based upon the plaintext that makes these algorithm impossible to detect.These algorithms are used to provide *digital fingerprint* , often used to ensure that the file has not been altered by an intruder. Hash functions are employed by many operating systems.Primarily used for message integrity.

IV. ADVANCED ENCRYPTION STANDARD:

AES became official successor to DES in 2001. AES uses an SKC scheme called Rijndael, designed by Belgian cryptographers Joan Daemen and Vincent Rijmen.It uses a variable block length and key length; the specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits. NIST initially selected Rijndael in October 2000 but formal adoption came in December 2001.It's an iterated block cipher and undergoes multiple rounds of transformation before giving output. Each intermediate cipher is called a *State*.

Block and cipher key are presented as array of columns. Each array has 4 rows and each column represents 8 bits (single byte).Number of columns in an array representing state can be calculated as the key length divided by 32 (32 bits = 4 bytes). Array representing a State will have **Nb** columns.In this **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.In this **Nk** values of 4, 6, and 8 correspond to a 128-, 192-, and 256-bit key.

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

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

Number of transformation rounds (**Nr**) is a function of the block length and key length, and 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 Rijndael transformation operates on each of the State bytes separatly 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.

If in SubBytes 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-box	====>	$s'_{0,0}$	$s'_{0,1}$	$s'_{0,2}$	$s'_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$				$s'_{1,0}$	$s'_{1,1}$	$s'_{1,2}$	$s'_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$				$s'_{2,0}$	$s'_{2,1}$	$s'_{2,2}$	$s'_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$				$s'_{3,0}$	$s'_{3,1}$	$s'_{3,2}$	$s'_{3,3}$

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 Rijndael transformation 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 $0 \le i \le 3$ 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.

APPLICATIONS :

Used for security of Smart cards, wireless sensor and mesh networks. Usable in broad band links.Suited for restricted-space environments where either encryption or decryption is implemented.Web servers that need to handle many encryption sessions.

CONCLUSION

Size matter in cryptography.The strength of cryptography is in the choice and management of the keys; longer keys will resist attack better than shorter keys. The purpose of this paper is to implement a mechanism to hide information (image) 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.

ACKNOWLEDGMENT

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

REFERENCES

[1] Ahmad, N.; Hasan, R.; Jubadi, W.M; "Design of AES S-Box using combinational logic optimization", IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 2010.

[2] Yang Jun ;Ding Jun Li; Na Guo Yixiong School of Information Science and Engineering, Yunnan University Kunming, China - "FPGA based design and implementation of reduced AES algorithm"(IEEE 2010).

[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] William Stallings,"Cryptography and Nework Security",Third Edition, Pearson Education, 2003.

[6] 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.

AUTHOR'S PROFILE

Sagar V. Dalal
currently pursuing M.E (EEE) from Prof Ram Meghe College Of Engineering And Management, Badnera, affiliated to Sant Gadge Baba Amravati University, Maharashtra. He did B.E in EXTC from Prof Ram Meghe Institute Of Technology & Research, Badnera in 2013. His interested research areas are Network Security, Information Security System.

Dr.Ms.K.N.Kasat
Working as a HOD at Electronics & Telecommunication department of Prof. Ram Meghe college of Engineering &Management,Badnera-Amravati.Had completed her B.E.(Industrial Electronics) and M.E.(Electronics and telecommunication) from Dr. B.A.M university, Aurangabad in 1999 and 2009 respectively.Had completed her Ph.D. degree in (Electronics and telecommunication) in 2016. Her research interests are Artificial Intelligence, Power Electronics.