Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 1, Number 3; November, 2014 pp. 123-127

http://www.krishisanskriti.org/acsit.html

FPGA Implementation of Cryptographic Algorithms: A Survey

Mr. Narendra Sharma M[1], Mr. Praveen Kumar Bhati[2] and Mr. Manjunath Rao BM[3]

[1]BE(EC), MVJCE #14 7th Cross D Street Magadi Road Bangalore-23, India
[2]BE(CS), MJVCE # 163/9 shop no.1 Ramesh steel Kumbarpet B'lore-002,India
[3]BE(EC), MVJCE #408 6th main HRBR 2nd Block Bangalore-560043, India
E-mail: [1]narendragem32@gmail.com, [2]cool.praveenkumar24@gmail.com, [3]manjunath452266@gmail.com

Abstract: *Cryptography was and still is one of the hot research areas. With the development of Computer Network and Communication Technology, a great mass of data and information need to be exchanged by public communication networks. High efficiency and high safety of data transmission become much more important. There are several information encryption algorithms of which, Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) are widely used two algorithms. The existing -AES algorithm provides high speed stream for large data and uses less amount of computer resources but induces less degree of security in large amount of data. The RSA is more secure comparatively, but it is much slower and uses a huge amount of computer resources. In order to cope up with these short comings, a hybrid encryption scheme was done, which is a combination of Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) with cross encrypted keys for secure key exchange and hybrid encryption for enhanced cipher-text security. This is an attempt, to survey in detail. The prime focus is on the FPGA implementations of cryptographic algorithms.*

Index Terms: *Advanced Encryption Standard (AES), FPGA, hybrid encryption, Rivest Shamir Adleman (RSA).*

1. INTRODUCTION

Cryptography is the art and science of achieving security by encoding messages to make them non-readable. The Cryptographic technique consists of encryption & decryption methods. These are the principal means to provide information security. Encryption method transform plain text message into cipher text, whereas decryption method transforms a cipher text message back into plain text. Not only has it to ensure the information confidential, but also provides digital signature, authentication, secret sub-storage, system security and other functions. Therefore, the encryption and decryption solution can ensure the confidentiality of information, as well as the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting. Encryption and decryption algorithm's security depends on the algorithm while the internal structure is the rigor of mathematics and also depends on the key confidentiality. Key in the encryption algorithm has a pivotal position, once the key is leaked, it means that anyone can be in the encryption system to encrypt and decrypt information; it means the encryption algorithm is useless.

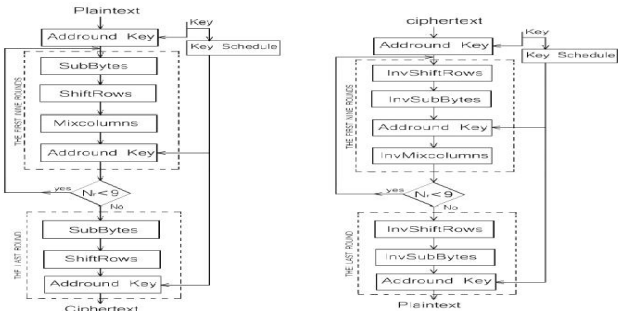
Therefore, what kind of data you choose to be a key, how to distribute the private key, and how to save both data transmission keys are very important issues in the encryption and decryption process. There are several information encryption algorithms of which Advanced Encryption Standard (AES) and Rivets Shamir Adleman (RSA) are considered as the best two algorithms of symmetric encryption technology and asymmetric encryption technology respectively. The existing symmetric scheme-AES algorithm provides high speed stream for large Data and uses less amount of computer resources but induces less degree of security of data. In turn, the asymmetric cryptographic algorithm or a public key cryptographic algorithm-RSA is more secure, as it has two keys one for encryption and another one for decryption, but is much slower and uses a huge amount of computer resources. So to overcome these disadvantages the Hybrid encryption scheme was done, which is a combination of Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) with cross encrypted keys for secure key exchange and hybrid encryption for enhanced cipher-text security.

A field-programmable gate array (FPGA) is an integrated circuit designed to be configured by a customer or a designer after manufacturing hence "field-programmable". Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs) provide different values to designers, and they must be carefully evaluated before choosing any one over the other. Information abounds that compares the two technologies. While FPGAs used to be selected for lower speed/complexity/volume designs in the past, today's FPGAs easily push the 500MHz performance barrier. With unprecedented logic density increases and a host of other features, such as embedded processors, DSP blocks, clocking, and high-speed serial at ever lower price points, FPGAs are a compelling proposition for almost any type of design.

2. EXISTING AES AND RSA CRYPTOGRAPHY ALGORITHM

The AES is a cryptographic algorithm that is used to encrypt (encipher), and decrypt, (decipher), information. Key Expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedures. Cipher and Inverse Cipher are composed of specific number of rounds (Table 1). For the AES algorithm, the number of rounds to be performed during the execution of the algorithm is dependent on the key length. Table I Comparison of block size, key length and number of rounds in AES

Type	Block Size Nbwords	Key Length Nkwords	Number of Rounds Nr
AES -128 bits key	4	4	10
AES -192 bits key	4	6	12
AES -256 bits key	4	8	14



a. Encryption **b. decryption**

Fig. 1 block diagram of AES algorithm.

2.1 Aes operation

Following indicates the transformation in AES algorithm based on the structure in Fig. 1.The brief introduction is listed as below**:**

1. *The SubBytes operation*: The SubBytes operation is a non-linear byte substitution, operating on each byte of the state independently [8]. The substitution table (S-Box) is invertible and is constructed by the composition of two transformations: Take the multiplicative inverse in Rijndael's finite field .Apply an affine transformation which is documented in the Rijndael documentation. Since the S-Box is independent of any input, pre-calculated forms are used. Each byte of the state is then substituted by the value in the S-Box whose index corresponds to the value in the state is a(i,j) = SBox[a(i,j)]
2. *Shift row transform:* Cyclically shifts the rows of the State over different offsets[4]. The operation is almost the same in the decryption process except for the fact that the shifting offsets have different values. The goal of this transformation is to scramble the byte order inside each 128-bit block.
3. .*Mix column transform:* This process is for mixing up of the bytes in each column separately during the forward process. The corresponding transformation during decryption is denoted Inv Mix Columns and stands for inverse mix column transformation. The goal is here is to further scramble up the bit input block.
4. *Add round key and key expansion:* In this operation, the round key is applied to the State by simple bit by bit XOR. Basically Key Expansion unit is used to generate the next round key as for three different key size, AES consist of 10,

or 14 rounds. So after every round a new round key need to be produced. So this unit produces that round key for each round. This unit also utilizes the concept of shifting the bytes and substitution of bytes which were used in data processing unit.

Key Schedule: Key scheduling is a critical process in AES that generates (Nr+1) round keys based on an external single key. The Key expansion process of AES algorithm uses a Cipher Key K to generate a key schedule. This generates Nb(Nr+1) words, of which the algorithm requires initial Nb words and each of the Nr rounds, require Nb words of Key Data. Key scheduling can produce keys either on the fly or store them in an internal key memory the key setup phase and then read them from this memory whenever required by the encryption/decryption unit. The critical path of Key Expansion is shorter than that of any round, speed of the system can't be enhanced by reducing the critical path of Key expansion. Keys on the fly eliminate the requirement for key storage, but brings overhead for decryption since decryption begins after the last round key is generated.

2.2 B.The RSA Algorithm

The RSA algorithm is used for both public key encryption and digital signatures. It is the most widely used public key encryption algorithm [6]. The basis of the security of the RSA algorithm is that it is mathematically infeasible to factor sufficiently large integers.

1. Key Generation Algorithm

The RSA Cryptosystem requires the use of a public key and a private key. Both these keys must fulfill certain conditions to ensure the integrity of the system. The following steps illustrate the key generation**:**

Choose two large prime numbers of approximately the same size, namely p and q.

i. Compute the product of these two primes, n = pq.
ii. Also, compute the value of φ(n) = (p-1)(q-1).
iii. Choose an integer e between 1 and φ (n) such that gcd (e, φ (n)) = 1.
iv. Finally, compute d whereby $d = e^{-1} \bmod (\varphi(n))$**.**

The public key is (n, e) whereas the private key is (p, q, and d)**.**

2. Encryption and Decryption

When Bob intends to send an encrypted message to Alice, these are the steps to be taken**:**

i. Obtain Alice's public-key (n,e), which should be listed in a public directory.
ii. Represent the plaintext message as a positive integer x, whereby x < n.
iii. Compute the ciphertext using the encryption function: $y = e_K(x) = x^e \bmod n$
iv. Transmit the ciphertext to Alice.

Upon receiving the encrypted message, there are several steps to be taken by Alice:

i. Compute the integer representation of the plaintext using the decryption function: $x = d_K(y) = y^d \bmod n$ and her own private key (p,q,d).
ii. Decode the corresponding plaintext from its integer representation, x.

3. HYBRID ENCRYPTION CRYPTOSYSTEM

A hybrid cryptosystem that utilizes benefits of both symmetric key and public key cryptographic methods. Symmetric key algorithm (aes) is used in the crypto system to perform data encryption and decryption. Public key algorithm (rsa) is used in the crypto system to provide key encryption before key exchange. Combining both the symmetric-key and public-key algorithms provides greater security and some unique features which are only possible in the hybrid system shown in Fig. 2. The implementation has various modules of aes and rsa.

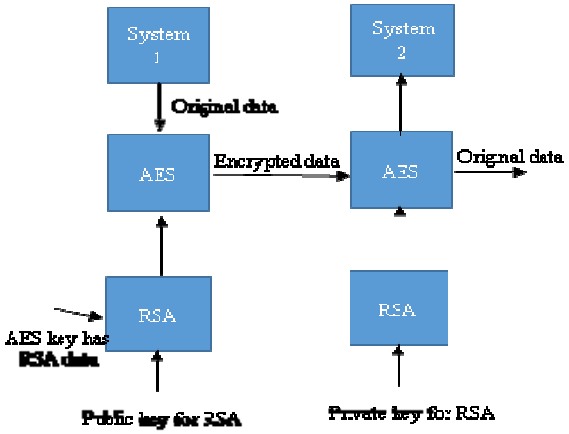


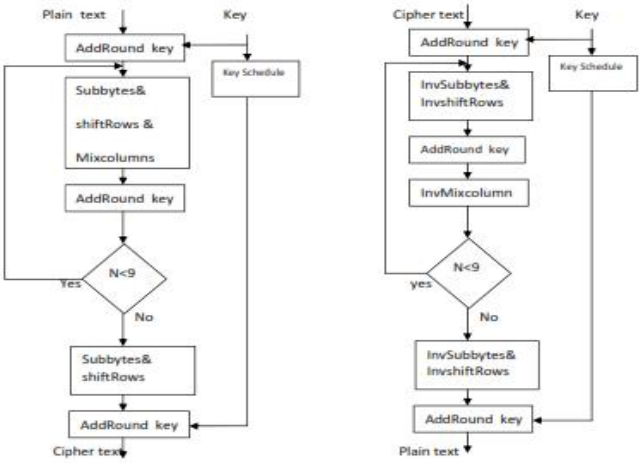
Fig. 2.Proposed Hybrid cryptography

Modified block description

The original data/message is sent for encryption using AES. The key used for the AES algorithm is further encrypted as a RSA data by the RSA algorithm using recipient's public key. Both the encrypted secret key and the encrypted message are then sent to the recipient. The recipient decrypts the secret key first, using its own private key, and then uses that key to decrypt the message.

1. Optimised AES Algorithm used in proposed hybrid cryptosystem

In standard AES algorithm, there are four steps like SubByte, ShiftRow, MixColumn and Add Round Key in normal rounds. this design highlights some following modification, Exclusion of Shift Row is performed through calling required shifted element from the data matrix, (instead of calling element one by one sequentially orderly from the data matrix); thus merging of the two steps SUB-BYTE and SHIFT ROW reduces one step. Further merged sub bytes and shift rows is combined with mix columns to form T box as shown in Fig. 3**.**



a. Encryption b.Decryption

Fig. 3 Optimized AES algorithm to be used in Hybrid cryptosystem

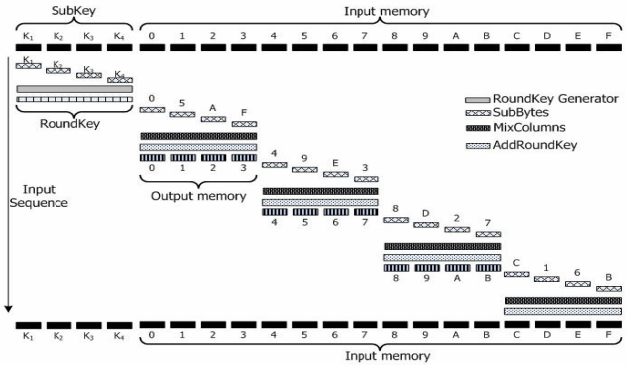


Fig. 4: The internal data flow of the optimized

AES architecture

In the proposed design, the entire round operation consists of five phases [1]. Each phase executes the four basic

transformations in sequence, as shown in Fig. 4. The first phase is executed to obtain the round key. Each of the remaining four phases performs the four basic transformations for the input block.

2. Modified RSA algorithm used in proposed hybrid system

i. Choosing the Modulus for the RSA Algorithm

With the definitions of d and e as presented earlier, the modulus m must be selected in such a manner that the

following is guaranteed:

$$(P^e)^d) \equiv P^{ed} \equiv P \pmod m \quad (1)$$

Since, $C = P^e \pmod m$**,** is the encrypted form of the message integer M and decryption is carried out by $P=C^d \pmod m$.It was shown by Rivest, Shamir, and Adleman that, n is a product of two prime numbers: $n = p \times q$ for some prime p and prime q[6].

ii. Choosing a Value for the Public Key Exponent e and N private key d.

Encryption consists of raising the message integer M to the power of the public exponent e modulo n. This step is referred to as modular exponentiation. The mathematical requirement one is

$$\gcd(e,\varphi(n)) \quad (2)$$

since otherwise multiplicative inverse mod wouldn't exist φ

(n).Since $n = p \times q$, this requirement is equivalent to the two requirements

$$\gcd(e, \varphi(p)) = 1 \text{ and } \gcd(e, \varphi(q)) = 1. \quad (3)$$

$$\gcd(e, p-1) = 1 \text{ and } \gcd(e, q-1) = 1. \quad (4)$$

Once a value for the public encryption exponent e is found, the next step is to calculate the private decryption exponent d from e and the modulus n. $d = e^{-1} \bmod \varphi(n)$.Calculating $e^{-1} \bmod \varphi(n)$' is referred to as modular inversion.

The table II shown below which shows the resources used in hybrid encryption cryptosystem.

TABLE II: Resources utilization of Hybrid cryptosystem

Logic Utilization	Used	Available	Utilized
Number of Slices			
	1269	3584	35%
Number of Slice Flip		7168	31%
Flops	2235		
Number of 4 input LUTs	495	7168	6%
Number of bonded IOBs	68	141	48%
Number of GCLKs	1	8	12%

Optimal architecture that permits to use 3589 CLBs (35%) and 48% Input/ Output Block of this circuit with a clock frequency of 87.704 MHz is used.

TABLE III: Hybrid Encryption and Decryption

Process	Clock	Delay (ns)
	frequency(MHz)	
Encryption		
	87.704	10.402
Decryption	87.704	11.23

We implemented our design for following optimised algorithm key bit lengths(K).Table 1V shows our results in terms of used CLBs (C),frequency F,clock cycle time (T) and the timearea product (TA).

TABLE IV: AES and RSA comparation

Algorithm	K	F	T	C	TA
		(Mhz)	(ns)		(C.ns)
AES	128	65	16.5	1207	19915.5
RSA	128	65	19.8	1122	22215.6

4. CONCLUSION

After seeing the clear results from tabular column we can say that the Hybrid encryption cryptosystem has overcome the disadvantages of AES and RSA algorithm. This Cryptosystem has encryption and decryption of any data has a secure key, which is used for data encryption and decryption. For this purpose asymmetric key is used. One of the approaches is to generate a random secret key of 128bits for a symmetric cipher-AES, and then encrypt this key via an asymmetric cipher-RSA, using the recipient's public key of 128 bits. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient. The recipient decrypts the secret key first, using his/her own private key,and then uses that key to decrypt the message .Thus providing higher degree of security to data transmission.There is a provision and flexibility to remove or add any other cryptographic standards in this system.

REFERENCES

[1] Ohyoung Son and Jiho Kim "Compact Design of the Advanced Encryption Standard Algorithm for IEEE 802.15.4 Devices "Journal of Electrical Engineering & Technology Vol. 6, 2013,

[2] Avi Kak , Avinash Kak, "Computer and Network Security on Public-Key Cryptography and RSA" May 15, 2013 Purdue University

[3] N.Singh, G .Raj. "Security on bccp trough AES encryption technique",Special Issue of INTERNATIONAL journal of engineering science & advanced technology (22503676) Jul-Aug.2012.

[4] Jeneba mary.B "hybrid cryptography by the implementation of rsa and aes"international Journal of Current Research, Vol. 3, Issue, April, 2011

[5] Alan Daly and William Zhenzhen Liu. "Implementation of AES Encryption based on FPGA". Modern electronic technology.

[6] Marnane "Efficient Architectures for implementing Montgomery *Modular Multiplication and RSA Modular Exponentiation on Reconfigurable Logic*". -University College Cork Ireland 2010.

[7] Yu; Tong Li; Na Zhao; Fei Dai "*Design and implementation of an improved RSA algorithm*", April 2010

[8] Song J. Park "Analysis of AES Hardware Implementations" Department of Electrical & Computer Engineering Oregon State UniversitCorvallis,

[9] Tim Good and Mohammed Benaissa. "*AES on FPGA from the Fastest to the Smallest"*.

[10] Panu Hämäläinen, Marko Hännikäinen, Timo Hämäläinen, and Jukka Saarinen. "*Hardware implementation of the improved wep and rc4 encryption algorithms for wireless terminals*" ,2010

[11] Tim Güneysu. J Cryptogram Eng "*Utilizing hard cores of modern FPGA devices for high-performanc*e *cryptography*". 2011

[12] Benjamin Leperchey, Charles Hymans "FPGA *implementation of the Rijndael algorithm"* June 9, 2009

[13] Shanxin Qu,Guochu Shou,Yihong Hu,Zhigang Guo,Zongjue Qian. "*High Throughput Pipelined Implementation of AES on FPGA*". International Symposium on Information Engineering and Electronic Commerce.2009

[14] M.N. Praphul, K.R.Nataraj, FPGA Implementation of Hybrid Cryptosystem International Journal of Emerging Science and Engineering (IJESE) ISSN: 23196378, Volume-1, Issue-8, June 2013

Behrouz A.Forouzan "*Cryptography and network security "*TATA Mcgraw hill publication 2007 edition.