ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

A new modified RC6 algorithm for cryptographic applications

P.Sritha[1], R.Ashokkumar[2], S, Bhuvaneswari[3], M.Vidhya[4]

Assistant Professor, Dept of EEE, Bannari Amman Institute of Technology, Anna University-Chennai, India[1,2,3,4]

Abstract: Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography finds its application in the areas of Wireless Sensor Network, Smart Card, Identification, and Security**.** With the ever increasing growth of data communication in the field of ecommerce transactions and mobile communication data security has gained utmost importance. However the conflicting requirements of power, area and throughput of such applications make hardware cryptography an ideal choice. In this context, the RC6 algorithm plays a major role in the hardware cryptography. The conventional RC6 algorithm has difference structure of encryption and decryption. So that the algorithm occupies separate space for encryption and decryption unit which leads to increase in area. Here algorithm is devised by inserting a symmetric layer in which the half of whole RC6 rounds uses encryption procedure and the rest of process employs decryption one. Thus it leads to reduce in area and it has made compromise of speed also.

Keywords: Cryptography, Wireless Sensor networks, RC6 algorithm, encryption, decryption

I.INTRODUCTION

RC6 algorithm requires 128-bit and variable-length block cipher encryption algorithm. It has a modified Feistel structure and a disadvantage that it has different algorithm between encryption and decryption. Thus, the RC6 algorithm needs double space compared with the same structure of encryption and decryption when it is implemented on hardware.In the proposed system a symmetric layer is inserted between the encryption and decryption process which has reduced the rounding operations to half thereby reducing the complexity of the algorithm. In this method also the proposed system consist of three major steps such as Encryption, key scheduling and decryption process. It inserts encryption procedure into first half of the rounding operations and rest of rounding employs decryption process.

II.SURVEY

Following are the algorithms used in the encryption and decryption process.

A.RC2

RC2 is an algorithm for which little cryptanalysis is available. However, it is known to have two weaknesses.

First, RC2 is vulnerable to differential attacks. An implementation with r mixing rounds (including the accompanying mashing rounds) will require at most 24r chosen plaintexts for a differential cryptanalysis attack. Commonly, the RC2 runs with 16 mixing rounds, making this attack less feasible than it may seem.

Second, the algorithm is vulnerable to a differential related-key attack requiring only 234 chosen plaintexts and one related-key query.

B.RC4

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent

of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table.

C.RC5

RC5 is a fast block cipher designed to be suitable for both software and hardware implementation. It is a parameterized algorithm, with a variable block size, a variable number of rounds, and a variable-length secret key. This provides the opportunity for great flexibility in both the performance characteristics and the level of security.

D.RC6

RC6 is a symmetric key block cipher derived from RC5. It was designed by Ron Rivest, Matt Rob shaw, Ray Sidney, and Yiqun Lisa Yin to meet the requirements of the Advanced Encryption Standard (AES) competition. RC6 encryption algorithm was selected among the other finalists to become the new federal Advanced Encryption Standard (AES).

III.PROPOSED SYSTEM

This improved RC6 algorithm is also a 128 bit block cipher symmetric key algorithm. Here the128 bit is subdivided into 32 bits and it is stored in four registers A, B, C, D and it undergoes encryption process in first 10 rounds by the use of symmetric layer and it undergoes decryption process in next 10 round.

A.BASIC BLOCK DIAGRAM

The basic block diagram of improved RC6 algorithm is shown in Figure 1.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

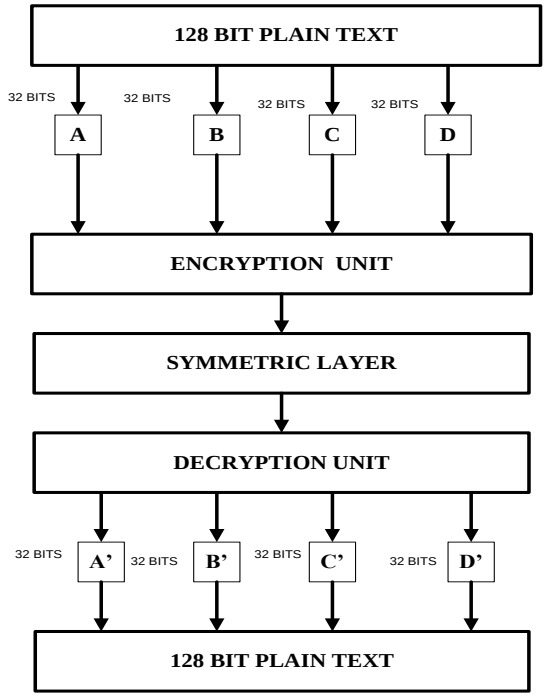

Fig 1.Basic Block Diagram of Improved RC6 Algorithm

B. KEY SCHEDULING ALGORITHM

The user supplies a key of b bytes. Sufficient zero bytes are appended to give a key length equal to a non-zero integral number of words; these key bytes are then loaded in little-endian fashion into an array of c w-bit (w = 32 bits in our case) words L [0]… L [c - 1]. Thus the first byte of key is stored as the low-order byte of L [0], etc., and L [c - 1] is padded with high-order zero bytes if necessary. The number of w bit (32 bit) words that will be generated for the additive round keys is 2r + 4 and these are stored in the array S [0, … ,2r +3]. The constants P32 = B7E15163 and Q32 =E3779B9 (hexadecimal) are the same "magic constants" as used in the RC6 key schedule.

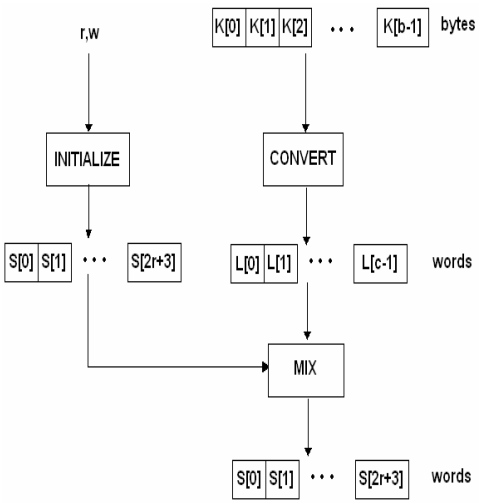

Fig 2.Key Scheduling Algorithm

C. ENCRYPTION

The encryption process involves taking each character of data and comparing it against a key

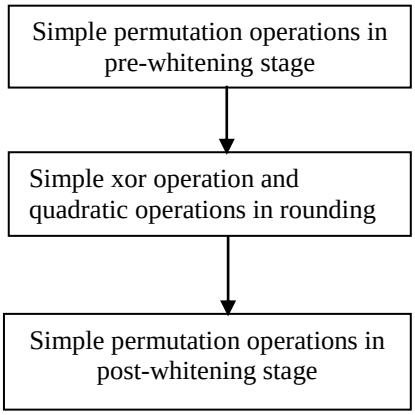

Fig 3.Basic Steps in Encryption Process

Here the encryption process consists of three stages. They are followed as

i. Pre whitening

ii. Round operations

iii. Post whitening

In RC6 encryption process the 128 bits is first subdivided into 32 bits and it is stored in 32 bit registers A, B, C, D. Next the data stored in the B and D undergoes pre whitening operations as follows

$$B=B+S[0] \quad (1)$$

$$D=D+S[1] \quad (2)$$

Here the data stored in the registers B and D is permuted with the round keys S [0] and S [1] The main purpose of pre whitening is to remove inference of part of the input to the first round of encryption.

Next it undergoes rounding operations, the steps in rounding operations can be explained as

i. A 32-bit addition can be computed using four 8-bit additions with carry.

ii. A 32-bit exclusive-or can be computed using four 8-bit exclusive-ors.

iii. A 32-bit squaring can be computed using six 8-bit by 8-bit multiplications and eleven additions with carry. Note that six multiplications are enough since we only need the lower 32 bits of the 64-bit product.

$s= (B \times (2B + 1))<<<\lg w \quad (3)$

$t = (D \times (2D + 1))<<<\lg w \quad (4)$

iv. Rotating a 32-bit word left by five bit positions can be computed by rotating the word right by one bit position three times and then permuting the four bytes. Note that rotating the word right by one bit position can be done using four byte rotations with carry.

v. Rotating a 32-bit word left by r can be computed by rotating the word left or right by one bit position r0 times and then permuting the four bytes appropriately. The five least-significant bits of r are used to determine r0 and the permutation which can be controlled using jumps.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

Next it undergoes post whitening steps, i.e. the data stored in registers A and C undergoes post whitening steps. Post whitening removes inference of part of the input to the last round of encryption.

The above encryption process can be explained as follows

TABLE I: ENCRYPTION OUTPUT

KEY	000000000000000000000000abcdef
INDATA	00000000000000000000001234567890
OUTDATA	d2638f95a73947660084459b8457a73

If the given input as in the above form and it undergoes the following above mentioned steps and it is converted into cipher text in first ten rounds of encryption

D. ADVANCED SYMMETRIC LAYER STRUCTURE

The advanced proposed symmetry layer is made faster by consisting of logical block operations and fixed rotate operation when implemented via hardware and software. The half of whole RC6 round uses encryption procedure and the rest of it employ decryption one, and symmetry layer has been put into the middle of encryption and decryption. Therefore the algorithm between encryption and decryption has become same, and the performance of RC6 has been improved.

The logical block consist of XOR and AND operations. It consists of all the bit wise logical operations.

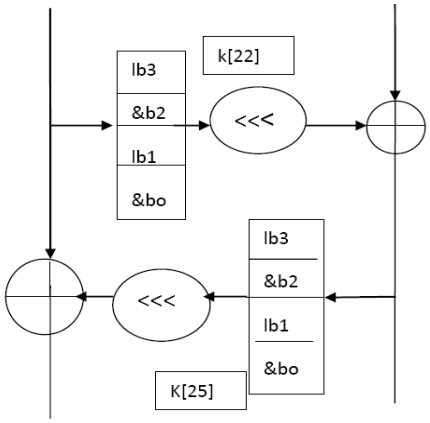

Fig 4. Structure of logical block

F.IMPLEMENTATION OF ADVANCED SYMMETRIC LAYER IN RC6 ALGORITHM

When applying the symmetry layer into RC6 algorithm, this algorithm use operations in the original round functions without modification. However it inserts encryption algorithm into the half of the whole progress rounds, applies decryption algorithm into the rest of it, and inserts symmetry layer in the middle of encryption and decryption algorithm. First of all, encryption executes 15 rounds encryption after executing round keys and XOR operations as whitening stage before round functions.

Each round operations use two 32bits round key to XOR operation. In the next, the application of the symmetry layer is executed as the explanation of the symmetry layer and uses four 32bits round keys. The rest 10 rounds apply the decryption algorithm of RC6, and after the execution of subtract operation of two 32bits round keys in each round and the last whitening process, finally 128bits cipher-text is created. The decryption of the proposed algorithm is executed and the application of round keys is the inverse of the process.

G.DECRYPTION

The process of converting the cipher text into plain text is called decryption. In this proposed system the decryption process is just inverse of the encryption process. The decryption process also undergoes three stages as similar to encryption process.In the whitening stage the registers A and C undergoes pre whitening stages

$$C = C + S\,[2r+3] \qquad (5)$$
$$A = A + S\,[2r+2] \qquad (6)$$

Here the register values are permuted with the round keys just in inverse of encryption process.Next it undergoes rounding operations, the steps in rounding operations can be explained as

i. A 32-bit subtraction can be computed using four 8-bit additions with carry.

ii. A 32-bit exclusive-or can be computed using four 8-bit exclusive-ors.

iii. A 32-bit squaring can be computed using six 8-bit by 8-bit multiplications and eleven additions with carry. Note that six multiplications are enough since we only need the lower 32 bits of the 64-bit product.

$$t = (D \times (2D + 1))\lll \lg w \qquad (7)$$
$$s = (B \times (2B + 1))\lll \lg w \qquad (8)$$

iv. Rotating a 32-bit word right by five bit positions can be computed by rotating the word right by one bit position three times and then permuting the four bytes. Note that rotating the word right by one bit position can be done using four byte rotations with carry.

Rotating a 32-bit word right by r can be computed by rotating the word left or right by one bit position r0 times and then permuting the four bytes appropriately.

Next it undergoes post whitening steps, i.e. the data stored in registers Band D undergoes post whitening steps. Post whitening removes inference of part of the input to the last round of encryption.

The above Decryption process can be explained as follows

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

TABLE II: DECRYPTION OUTPUT

KEY	000000000000000000000000abcdef
IN DATA	d2638f95a73947660084459b8457a73
OUT DATA	00000000000000000000001234567890

If the given input as in the above form and it undergoes the following above mentioned steps and it is converted into cipher text in first ten rounds of Decryption

IV. RESULT AND ANALYSIS

In this paper, the RC6 algorithm which applies the proposed symmetry structure has been checked up regarding the correct execution of encryption and decryption in the environment of Verilog. The speed of the original RC6 algorithm and the proposed one has been tested with normal text.

TABLE III. RESULT OF THE SPEED TEST (UNIT: SEC)

Time Algorithm	Encryption	Decryption
RC6	10.156 (90.00%)	10.147 (90.00%)
Proposed Algorithm	11.531 (97.54%)	11.438 (96.78%)

The result is shown as Table III, and the execution time of the proposed algorithm is about 7% increase than original one. It comes to conclusion that the simple logical operation applied in the stage of symmetry layer doesn't affect the whole process of encryption and decryption. Because of this symmetric process the proposed RC6 algorithm is made more secure and it is less attacked by the linear and differential cryptanalytic attacks. . The diffusion process is also increased which made the security of the proposed system. It made the whole process faster by the byte logical unit.

The symmetric layer process consists of simple shifting and XOR operations. Here the four keys are separately used for the symmetric layer alone. The symmetric layer has made the hardware implementation of the whole process simpler when compared to the existing system. Furthermore the synthesis report which is done in Xilinx software is given in TABLE IV.

TABLE IV SYNTHESIS REPORT

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	10643	3584	296%
Number of Slice Flip Flops	495	7168	6%
Number of 4 input LUTs	20291	7168	283%
Number of bonded IOBs	257	141	182%
Number of MULT18X18s	12	16	75%
Number of GCLKs	1	8	12%

V. CONCLUSION

The proposed advanced symmetry layer has been put into the middle of the whole rounds of the algorithm which made different algorithm of encryption and decryption has been implemented to have the same algorithm between encryption and decryption. When symmetry layer is put into the half of the rounds, the security of the core system is improved and the proposed algorithm has the speed variation than the original algorithm by the percentage of 7.The area occupied by the algorithm has reduced by the factor of 60%

REFERENCES

[1] "Report on the Development of the Advanced Encryption Standard(AES)." http://www.csrc.nist.gov/encryption/aes/round2/r2report.pdf.
[2] "New European Schemes for Signatures. Integrity. and Encryption(NESSIE)." http://cryptonessie.org/.
[3] "Cryptography Research and Evaluation Committees(CRYPTREC)." http://www.cryptrec.go.jp/.
[4] H. Feistel, "Cryptography and Computer Privacy," Scientific American, Vol.228, No.5, pp. 15-23, 1973.
[5] C. E. Shannon, "Communication theory of secrecy system," *Bell System Technical Journal*, Vol.28, No.4, pp. 656-715, 1949.
[6] S. Contini, R.L. Rivest, M.J.B. Robshaw, and Y.L. Yin, "The security of RC6", http://www.rsasecurity.com/rsalabs/aes.
[7] Y. L. Yin, "A Note on the Block Cipher Camellia"
[8] E. Biham and A. Shamir, "Differential cryptanalysis for DES-like cryptosystem", Journal of Cryptology 4(1): 3-17, 1991.
[9] M. Matsui, "Linear cryptanalysis method for DES cipher", In TorHelleseth, editor, Advances in Cryptology-Eurocrypt `93, LNCSVol.765, pp. 386-397, 1994.
[10] L. R. Knudsen, "Truncated and higher order differential", Fast Software Encryption-Second International Workshop, LNCSVol.1008, pp. 196-211, 1995.
[11] William Stallings, "Cryptography and network security: Principles and practice" , Prentice Hall, Upper Saddle River, New Jersey, 2003
[12] An improved RC6 algorithm with the same structure of encryption and decryption Gil-Ho Kim*, Jong-Nam Kim*, Gyeong-Yeon Cho**Dept of Computer Engineering PuKyong National Univ.