ISSN No. 0976-5697

Volume 2, No. 6, Nov-Dec 2011

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Analysis of RC6 Symmetric Encryption Algorithm

Rutuja R.Yawale*
Student (ME), Electronics Department
Sipna's College of Engg. & Technology
Amravati, Maharashtra, India
yawale.rutuja@yahoo.com

Prof. S.V. Rode
Professor, Electronics Department
Sipna's College of Engg. & Technology
Amravati, Maharashtra, India
sandeeprode30@yahoo.com

Abstract: Internet and networks applications are growing very fast, so the needs to protect such applications are increased. Cryptography refers to the science and art of transforming messages to make them secure and immune to attacks. Cryptography encryption algorithms play a main role in information security systems. Those algorithms consume a significant amount of computing resources. National Institute of Standards and Technology (NIST) initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive information & in many scenarios, RC6 is the fastest AES finalist. This paper focuses on the analysis of RC6 symmetric encryption algorithm as AES considering certain parameters such as computation time, throughput & power consumption.

Keywords: Security issues, block cipher, encryption attributes, AES, RC6.

I. INTRODUCTION

Security is a protection process against unwanted behavior. Security services provide confidentiality, integrity and availability. Data encryption is the process of scrambling data within a computer or communication system to make it unintelligent in such a way that process can later be reversed by authorized parties to reveal the original data. For this some cryptographic techniques are used. A cryptographic technique uses encryption & decryption methods. Encryption includes conversion of sensitive data "plaintext" into "cipher text" with secret key. The reverse of this is decryption [1].Fig 1 shows basic cryptographic structure.

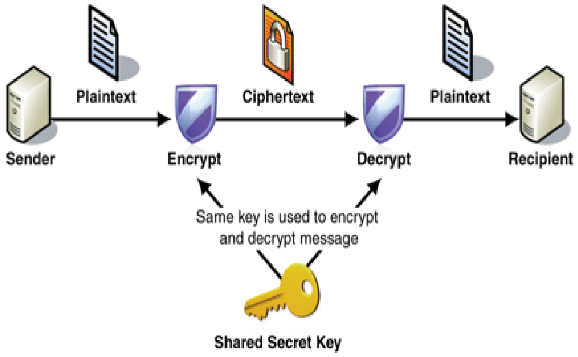


Figure. 1 basic cryptographic structure

For security purpose many cryptographic algorithms developed including AES, DES, 3DES, RC2, Blowfish,RC5 etc. RSA Laboratories submitted RC6 as a candidate for this Advanced Encryption Standard (AES). In 1997, the National Institute of Standards and Technology (NIST) initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive Federal Information. In 1998 was announced the acceptance of fifteen candidate algorithms, and in 1999 five of them were selected. One of them is the RC6 cipher-block. RC6 was built from a heritage of RC5 and was designed to be fast and simple to describe. In many scenarios, RC6 is the fastest AES finalist. RC6 is a symmetric key block cipher, which is a simple, fast, and secure block cipher, was the final candidate algorithm in the AES project of the United States [2]. RC6 remains a good choice for security application because of its simplicity & user friendly approach. AES is superior to RC6 in several important application areas. But there are also places where the two algorithms appear to be equally suitable and there are some application areas where RC6 might offer an interesting alternative to AES.

RC6 block cipher makes essential heavy use of data dependent rotations. Its salient features include the use of four working registers instead of two as in RC5, and the inclusion of integer multiplication as an additional primitive operation. The use of multiplication with four working registers greatly increases the diffusion achieved per round, allowing for greater security, fewer rounds, and increased throughput. It is also capable to handle 128-bits plaintext and ciphertext block sizes and suitable to be implemented simply using hardware or software. RC6 has a variable word size, a variable number of rounds, and a variable-length secret key. RC6 more than meets the requirements for the AES; it is

a. Simple
b. Fast
c. Secure.

This paper focuses on the analysis of RC6 symmetric encryption algorithms as AES considering certain parameters such as encryption decryption throughput, power consumption with other algorithms.

II. RC6 BLOCK CIPHER

Like RC5 and RC6, the enhanced block cipher is a fully parameterized family of encryption algorithms. RC6 has a simple structure and description relative to the other proposed block ciphers. RC6 was one of five finalists for the Advanced Encryption Standard [3]. A version of the enhanced block cipher is more accurately specified as Enhanced-w/r/b. The RC6 algorithm has a modified Feistel structure and presented symbolically as RC6-w/r/b. w means 32 bits as the size of word, r denotes the number of round. If the size of block is 128 bits, then r, the number, is 20. b means 16byte as the number of a key. The key schedule algorithm is used to generate the set of sub keys. The user supplies a key of b bytes, where 0≤ b ≤ 255. From this key, 2r+4 words (w bit each) are derived and stored in the array s[0,…,2r+3]. This array is used in both encryption and decryption [2].

The operations used in RC6 are defined as followings.

▪A+B integer addition modulo 2w

▪A-B integer subtraction modulo 2w

▪A⊕B bitwise exclusive-or of w-bit words

▪A ×B integer multiplication modulo 2w

▪A<<B rotation of the w-bit word A to the left by the amount given by the least significant log w bits of B

▪A>>B rotation of the w-bit word A to the right by the amount given by the least significant log w bits of B

▪(A,B,C,D)=(B,C,D,A) parallel assignment.

RC6 works with 4 w-bit registers A, B, C, D which contain the initial input plaintext as well as the output ciphertext at the end of encryption. The 1st byte of plaintext or ciphertext is placed in the least-significant byte of A, the last byte of plaintext or ciphertext is placed into the most-significant byte of D. Following fig. 2 shows RC6 algorithm

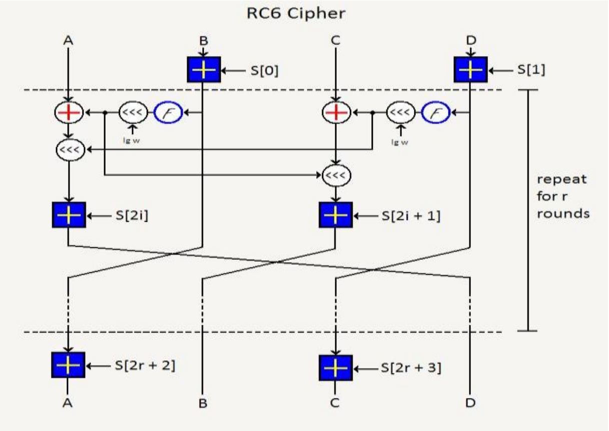
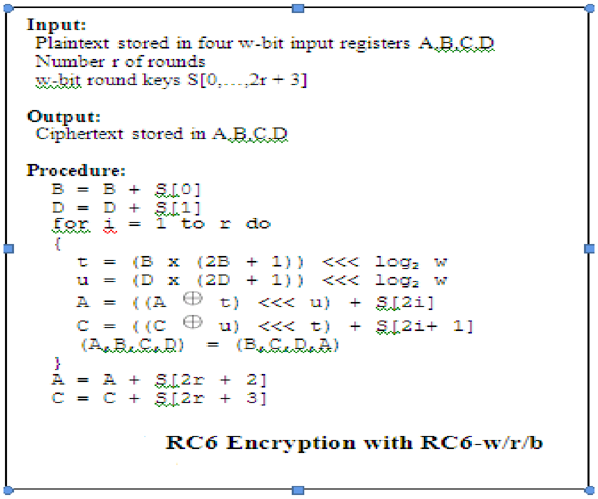


Figure 2 RC6 algorithm

Fig. 3 & 4 shows RC6 encryption and decryption steps.



Input:
Plaintext stored in four w-bit input registers A,B,C,D
Number r of rounds
w-bit round keys S[0,…,2r + 3]

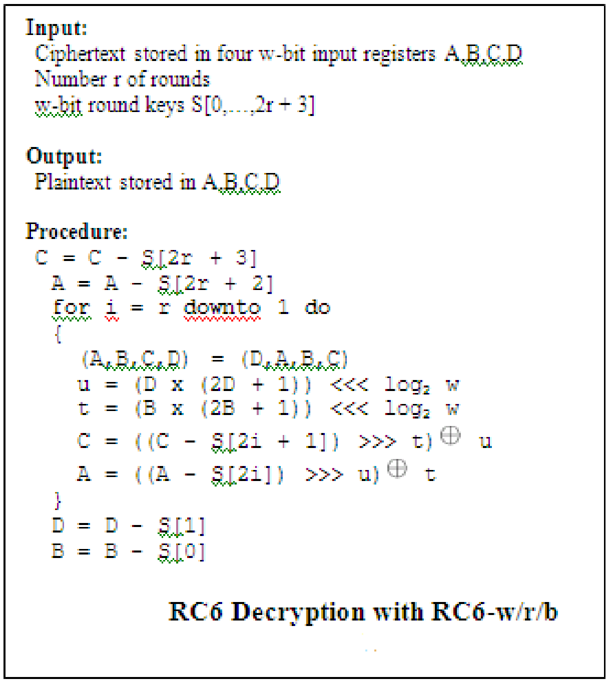
Output:
Ciphertext stored in A,B,C,D

Procedure:

```
$B = B + S[0]$
$D = D + S[1]$
for i = 1 to r do
{
    $t = (B \times (2B + 1)) <<< \log_2 w$
    $u = (D \times (2D + 1)) <<< \log_2 w$
    $A = ((A \oplus t) <<< u) + S[2i]$
    $C = ((C \oplus u) <<< t) + S[2i+ 1]$
    $(A,B,C,D) = (B,C,D,A)$
}
$A = A + S[2r + 2]$
$C = C + S[2r + 3]$
```

RC6 Encryption with RC6-w/r/b

Figure. 3 RC6 encryption procedure



Input:
Ciphertext stored in four w-bit input registers A,B,C,D
Number r of rounds
w-bit round keys S[0,…,2r + 3]

Output:
Plaintext stored in A,B,C,D

Procedure:

```
$C = C - S[2r + 3]$
$A = A - S[2r + 2]$
for i = r downto 1 do
{
    $(A,B,C,D) = (D,A,B,C)$
    $u = (D \times (2D + 1)) <<< \log_2 w$
    $t = (B \times (2B + 1)) <<< \log_2 w$
    $C = ((C - S[2i + 1]) >>> t) \oplus u$
    $A = ((A - S[2i]) >>> u) \oplus t$
}
$D = D - S[1]$
$B = B - S[0]$
```

RC6 Decryption with RC6-w/r/b

Figure. 4 RC6 decryption procedure

III. RC6 ATTRIBUTES

During design of RC6 the aim is to satisfy as many as goals possible to keep cipher simple. Once by keeping cipher simple one can achieved well understood level of security, good performance & versatility of design that makes cipher highly adaptable for future demands. Following are some RC6 design attributes

A. Security through simplicity:

A simple cipher is one that is easily described and readily remembered. RC6 is one of the most accurate assessments of the security of any AES finalists [5]. RC6 is not so complicated as compared to other ciphers. Since it is easy to define simplified and small block size variants of RC6, cryptanalyst can perform far more extensive analysis and experimentation. Also able to make careful decision on how many rounds RC6 should have so that it will give good performance once the security goal has been attained.

B. Performance through simplicity:

Most of today's high-end computing base is deployed in PC's either in the work- place or at home, and these are 32-bit machines. Here RC6 typically offers exemplary performance. We believe that excellent performance of RC6 on 32-bit processors, the close convergence in performance between simple compiled code and hand-optimized assembly, and outstanding performance in Java and in DSP environments, all make RC6 ideally suited to be chosen as the AES.

C. Versatility through simplicity:

RC6 is fully parameterized; the number of encryption rounds, the size of the encryption key (not just the three must support values of 128, 192, and 256 bits), and the block-size can all be easily and readily changed. This kind of edibility used in design feature. For most of the other finalists it is not at all clear how a change to the block size, or the use of an extremely long encryption key, would be accommodated. These could be important considerations. For some applications, a developer may wish to call on a 64-bit block cipher perhaps as a drop-in replacement to DES. With RC6 as the AES, such a variant is readily described. At the other extreme, it is possible that in the near future a 256-bit hash value will be preferred. The most natural way to do this when using an AES candidate as the basis for a hash function would be to change the block-size. Simplicity and versatility go hand-in-hand. Once again, RC6 would be the most suited finalist to become the AES.

IV. COMPARATIVE ANALYSIS AND PERFORMANCE EVALUATION

This paper analyses a method for evaluating performance of selected symmetric encryption of various algorithms. Encryption algorithms consume a significant amount of computing resources. We need a way to make decisions about energy consumption and security to reduce the consumption of battery powered devices. This study evaluates five different encryption algorithms namely; AES, DES, 3DES, RC6 and RC2. The performance measure of encryption schemes will be conducted in terms of energy, changing data types, power consumption, changing packet size and changing key size for the selected cryptographic algorithms [6].

Here analysis is based on power consumption in case of encryption and decryption time for different file sizes. For this researcher encrypts a different file size ranges from 321 K byte to 7.139Mega Byte139MegaBytes for text data, from 33 Kbytes to 8262 Kbytes for audio data, and from 4006 Kbytes to 5073 Kbytes for video files[10].

A. Encryption of different packet size:

Encryption throughput: Encryption time is used to calculate the throughput of an encryption scheme [7]. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is decreased. Experimental results for this compassion point are shown Figure 5 at encryption stage. [15].

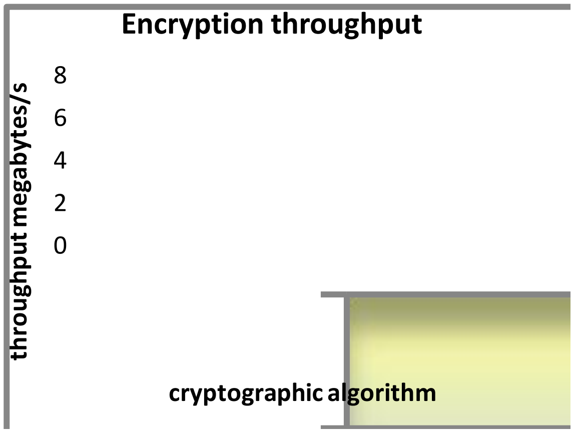


Figure. 5 Throughput of each encryption algorithm (Megabyte/Sec)

Power consumption: In Fig.6, we show the performance of cryptographic algorithms in terms of Power consumption for encryption process with a different data block size (Micro joule/byte)

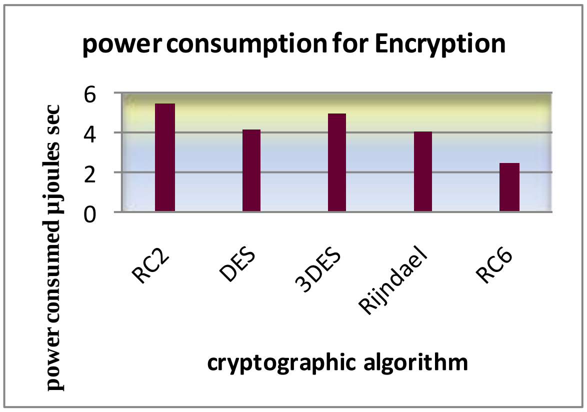


Figure.6 Power consumption for encrypt different Text document Files (Micro Joule/Byte)

Power consumption (% of power consumed): In Fig. 7, we show the performance of cryptographic algorithms in terms of Power consumption by calculating difference in battery consumed for encryption process with a different data block size.

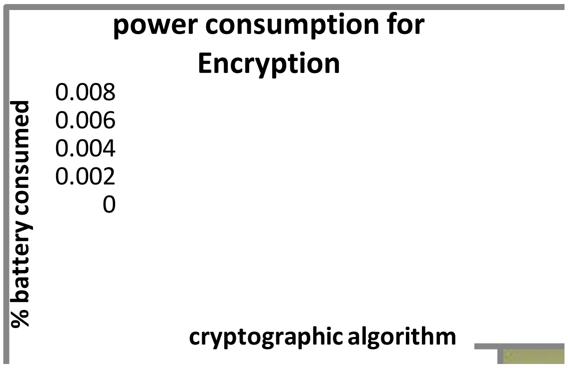


Figure. 7 Power consumption for encrypt different Text document Files

The results show the superiority of RC6 algorithm over other algorithms in terms of the power consumption, processing time, and throughput (when we encrypt the same data). Another point can be noticed here that RC6 requires less power, and less time than all algorithms. A third point can be noticed here that AES has an advantage over other 3DES, DES and RC2 in terms of power consumption, time consumption, and throughput. A fourth point can be noticed here that 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics. Finally, it is found that RC2 has low performance and low throughput when compared with other five algorithms in spite of the small key size used.

B. Decryption of different packet size:

Decryption throughput: Experimental results for this compassion point are shown Fig.8

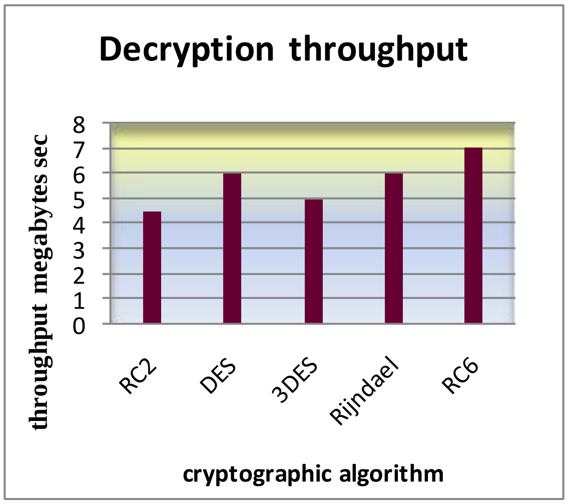


Figure. 8 Throughput of each decryption algorithm (Megabyte/Sec)

Power consumption (Micro joule/byte): Experimental results for this compassion point are shown Fig.9

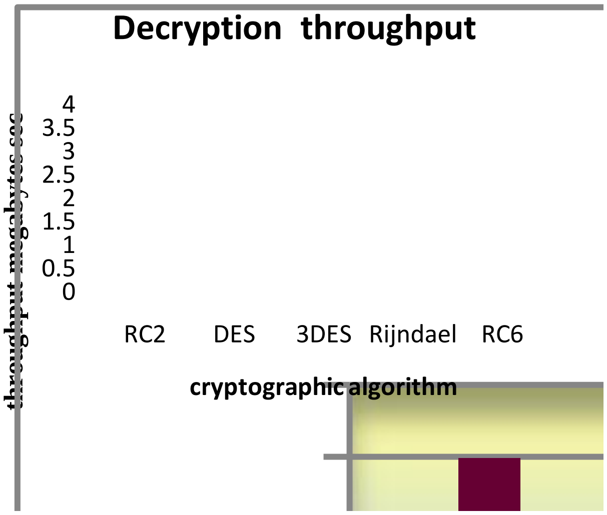


Figure. 9 Power consumption for Decrypt different Text document Files (Micro Joule/Byte)

It is found that in decryption stage RC6 is better than the other algorithms in throughput and power consumption. The second point which should be noticed here is that RC2 requires less time than all algorithms except RC6. Finally, Triple DES (3DES) still requires more time than DES.

C. The Effect of Changing Key Size on Power Consumption:

The performance comparison point concerns with changing different key sizes for different algorithm. For processing different key size data directly affects on power consumption. Following fig.9 shows two types of data packets 4006 kb and 4415 kb used for AES, RC2, RC6, DES & 3DES algorithms. From analysis it shows that RC6 and AES require similar processing time. Thus it shows RC6 is the fastest AES candidate from all other. Also DES works less efficient than all other algorithms.

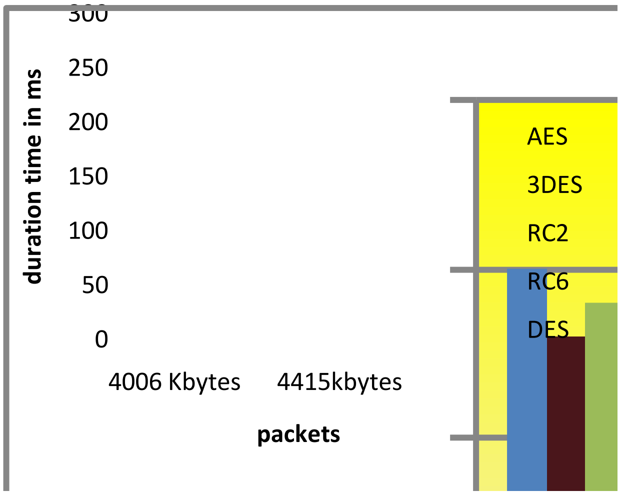


Figure. 9 effect of changing key size on power consumption

V. CONCLUSION

This paper describes about analysis of RC6 block cipher for encryption efficiency analysis and security evaluation. Effect of secret key length and different data block size on encryption quality is evaluated and compared using several test values. Results obtained show that the RC6 block cipher achieved the most better encryption quality for the choices of word size w = 32, number of rounds = 20, and secret key length b = 16. Based on such results, the optimal version of RC6-w/r/b block cipher algorithm that gives maximum encryption quality is estimated to be RC6-32/20/16. From an engineer's perspective, the use of RC6 block cipher algorithm as a candidate for data encryption is very promising for real-time communications in military, industrial, as well as commercial applications.

Encryption algorithm play an important role in communication security where encryption time, Memory usages output byte and battery power are the major issue of concern. The selected encryption AES, DES, 3DES, RC2 and RC6 algorithms are used for performance evaluation. Based on the different files used it was concluded that RC6 algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm. RC6 is an elegant, fast, and well analyzed cipher, and would normally be considered the obvious best candidate to be used to protect sensitive Information & in many scenarios, RC6 is the fastest AES finalist. This analysis will be used for future work of data encryption of RC6 and in improvement of encryption time and less memory usage.

VI. REFERENCES

[1] W.Stallings, "Cryptography and Network Security 4thEd," Prentice Hall , 2005,PP. 58-309 .

[2] W.R. Sam Emmanuel, *Member, IAENG* 'Impact of Multiencryption in Data Security' International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December, 2009

[3] Y. R.L. Rivest, M.J.B. Robshaw, R.Sidney, and Y.L. Yin, "Some Comments on the First Round AES Evaluation of RC6,"availableat http://csrc.nist.gov/encryption/aes/round1/pubcmnts.htm.

[4] L.R. Knudsen and W. Meier. Correlations in RC6.

[5] S. Contini, R.L. Rivest, M.J.B. Robshaw, and Y.L. Yin. The security of RC6. Available from www.rsasecurity.com/rsalabs/aes/.

[6] A.A. Tamimi, "Performance Analysis of Data Encryption Algorithms.RetrievedOctober1,2008From http://www.cs.wustl.edu/~jain/cse56706/ftp/encryption_perf/index.html http://www.codeproject.com/KB/security/hexenc.aspx

[7] "A Performance Comparison of Data Encryption Algorithms, " IEEE[Information and Communication Technologies, 2005]. ICICT 2005.First International Conference, 2006-02-27, PP. 84- 89.

[8] A. Nadeem, "A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, pp. 84-89, 2006.

[9] Results of comparing tens of encryption algorithms using different settings- Crypto++ benchmark- .Retrieved October1,2008, from:http://www.eskimo.com/~weidai/benchmarks.html

[10] "A New Balanced Encryption Algorithm with Elevated Security Base on Key Update", R. Ganesan and A. Arul Lawrence Selvakumar, European Journal of Scientific Research, ISSN 1450-216X Vol.60 No.2 (2011), pp. 177-194

[11] M. Shand and J. Vuillemin. Fast implementations of RSA cryptography. In *11th IEEE Symposium on COMPUTER ARITHMETIC*, 1993.

[12] J. Daeman, and V. Rijmen, AES Proposal:Rijndael, http://www.esat.kuleuven.ac.be/rijmen/rijndael/rijndaeldocV2.zip, 1999.

[13] Daemen, J. and Rijmen, V. "Rijndael: The Advanced Encryption Standard."Dr.Dobb's Journal, March 2001,PP. 137-139.

[14] K. Naik, D. S.L. Wei, "Software Implementation Strategies for Power-Conscious Systems, " Mobile Networks and Applications, 6, 291-305, 2001.

[15] R.L. Rivest, M.J.B. Robshaw, R.Sidney, and Y.L. Yin, "Some Comments on the First Round AES Evaluation of RC6," available at

[16] http:// csrc.nist.gov/encryption/aes/round1/pubcmnts.

Ht m.