Cryptographic Performance for Rijndael and RC6 Block Ciphers

Niansheng Liu*, Jianjun Cai, Xiaojuan Zeng, Guanhua Lin,Jiaoru Chen
School of Computer Engineering, Jimei University, Xiamen, China
nsliu@jmu.edu.cn

***Abstract*—This paper deals with the cryptographic performance of Rijndael and RC6 algorithms in real environment. The cryptographic performance of Rijndael and RC6 algorithms is evaluated from the diffusion, confusion, and space-time complexity of them. The diffusion and confusion of them are quantitatively measured by using the avalanche effect and runs test. The time performance metrics are encryption and decryption speeds while space performance metric is memory utilization. The experimental results show that both Rijndael and RC6 have good avalanche properties for the plaintext and key. They are very close to the SAC (Strict Avalanche Criterion). The cipher texts of Rijndael and RC6 have good randomness and unpredictability from the results of runs test. However, the encryption speed of RC6 algorithm is much faster than that of Rijndael algorithm in the same experimental conditions, and is independent of the key length. The encryption and decryption speed of Rijndael are asymmetric although Rijndael algorithm is a symmetric block cipher. Meanwhile, RC6 needs more CPU and memory resources than Rijndael algorithm. So the use of RC6 is beneficial where high encryption speed is required while Rijndael is beneficial where memory resource is key concern.**

Keywords- Rijndael algorithm; RC6 algorithm; avalanche effect; throughput; resource utilization

I. INTRODUCTION

With some wonderful features, such as fast encryption speed, good safety and easy implementation, the block ciphers such as Rijndael and RC6 algorithms have received increasing attention recently[1][2]. Since the communication theory of secrecy systems was published in 1949[3], confusion and diffusion have been two essential properties of the operation of a secure cipher. They can be quantitatively evaluated by using the avalanche effect and the distribution of cipher text substring[4]. H. Feistel firstly introduced the avalanche effect to cryptography[5]. R. Forré proposed the extended definition of the SAC and the corresponding spectral characterization[6]. J. C. H. Castro et al. used the strict avalanche criterion to measure the strengths of some well-known PRNGs[7]. The avalanche effects in cryptography are divided into two types, i.e., plaintext avalanche and key avalanche[8].

The statistical performances of Rijndael and RC6 algorithms have been drawn so much attention since they were proposed[9]. A. J. Elbirt et al. analyzed the core operations of Rijndael and RC6 algorithms, and discussed the results of their FPGA implementations in both non-feedback and feedback modes in terms of throughput and area efficiency[10]. H. K. Verma compared the performance of RC6, Twofish and Rijndael block cipher algorithms for various digital media on the basis of execution time and resource utilization[11]. However, their experimental methods are worth discussing. For example, when the size of key is 24-bytes or 32-bytes, the number of rounds was fixed 10 for Rijndael in their tests. However, the number of rounds shall be 12, 14, respectively, according to the Federal Information Processing Standards Publication 197[12]. Moreover, RC6, Twofish and Rijndael algorithms occupy the nearly identical CPU and memory resources when they operate independently under the same conditions in [11]. This result may go against the people's experience in practice.

The paper deals with the cryptographic performances of Rijndael and RC6 algorithms in real environment. The avalanche effects of Rijndael and RC6 algorithms are quantitatively analyzed by using the statistical method. We also measured and compared the encryption and decryption rates, confusion, CPU utilization and memory utilization for Rijndael and RC6 algorithms in the various experimental conditions.

II. BLOCK CIPHER

A. Rijndael Algorithm

Rijndael algorithm was developed by J. Daemen and V. Rijmen, and became the AES on November 26, 2001[13]. The procedures of AES encryption and decryption are shown in Fig.1.

In Fig.1, these operations such as SubBytes, ShiftRows, MixColumns, AddRoundKey, InvShiftRows, InvSubBytes, InvMixColumns, are described in the FIPS 197 [12]. The final round has a slightly different form and omits the MixColumns operation during encryption.

The AES algorithm performs a Key Expansion routine to generate a key sched-ule. It takes the user-supplied key of 16, 24, or 32 bytes, and returns what is called an ExpandedKey of 16 × 11, 16 × 13, and 16 × 15 bytes respectively. The details can be found in [12].

This work was supported in part by the Natural Science Foundation of Fujian Province, China under Grant 2017J01761, 2012J01279, 2014J01244 and 2015J01264. * Corresponding author: Niansheng Liu

978-1-5386-0533-2/17/$31.00 ©2017 IEEE

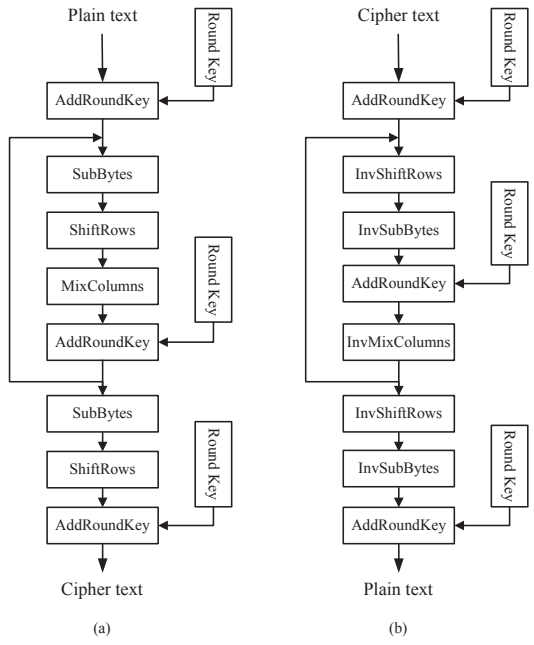

Figure 1. AES algorithm (a) Encryption structure; (b) Decryption structure

Algorithm 1 RC6 encryption algorithm

```
1. Initialize: A=PlainText[1], B=PlainText[2],
               C=PlainText[3], D=PlainText[4],
               R=20, W=32,
               S[0], S[1] …. S[43] (Key Schedule)
2. B = B + S[0]
3. D = D + S[1]
4. for i = 1 → R do
5.   t = (B × (2B + 1))<<<lgW
6.   u = (D × (2D + 1)) <<<lgW
7.   A = ((A ⊕ t)<<<u)+S[2i]
8.   C = ((C ⊕ u)<<<t)+S[2i+1]
9.   (A, B, C, D) = (B, C, D, A)
10. end for
11. A = A + S[2R+2]
12. C = C + S[2R+3]
```

Algorithm 2 RC6 decryption algorithm

```
1. Initialize: A=CipherText[1], B=CipherText[2],
               C=CipherText[3], D=CipherText[4],
               R=20, W=32,
               S[0], S[1] …. S[43] (Key Schedule)
2. C = C - S[2R+3]
3. A = A - S[2R+2]
4. for i = R → 1 do
5.   (A, B, C, D) = (D, A, B, C)
6.   u = (D × (2D + 1)) <<<lgW
7.   t = (B × (2B + 1))<<<lgW
8.   C = ((C - S[2i+1])>>>t) ⊕ u
9.   A = ((A-S[2i])>>>u) ⊕ t
10. end for
11. D = D - S[1]
12. B = B - S[0]
```

Figure 2. Pseudo codes for the RC cipher and inverse cipher

B. RC6 Algorithm

RC6 (Rivest Cipher 6) is a symmetric key block cipher derived from RC5[14]. It was designed by R. Rivest, M. Robshaw, R. Sidney, and Y. L. Yin to meet the requirements of the Advanced Encryption Standard (AES) competition. The pseudo codes of RC6 encryption and decryption are shown in Fig.2. In Fig.2, all arithmetic operations of RC6 are defined and described in [14].

III. Experimental Results and Discussion

The Rijndael and RC6 algorithms are implemented in C# in Microsoft visual studio 2008. The mode of cipher-block chaining (CBC) was used for them. The practical performance was measured on a 2.40GHz Intel(R) Core(TM) i3 CPU with 4GB of RAM running Windows XP professional Version 2002, Service pack 3. When Rijndael and RC6 algorithms are implemented with software under such experiment circumstances, the correctness of their programs is verified by using test vectors in [13] and [14] before performance test. The experimental results of Rijndael and RC6 algorithms are as follows.

A. Diffusion of Rijndael and RC6 Algorithms

The avalanche effect refers to a special and desirable property of cryptographic algorithms. In the case of quality block ciphers, the avalanche effect means that a small change in the key or in the plaintext will cause a drastic change in the cipher text just like an avalanche. The calculating formula of avalanche effect is as follows in general [15].

$$AE = \frac{N_C}{N_T} \times 100\% \tag{1}$$

In Equation (1), AE stands for avalanche effect. If a plaintext or a key is changed slightly during encryption, the cipher text changes significantly. N_C is the number of changed bits in the cipher text while an input is changed slightly. N_T is the total number of bits in the cipher text.

During the test of avalanche effect, we randomly generated 1000 blocks of plain text and 1000 keys as test samples for Rijndael and RC6 algorithms, respectively. The length of each block plain text is 128 bits. The number of 128-bit, 192-bit and 256-bit keys is 400, 300, 300, respectively, among 1000 keys.

For the plaintext avalanche, the number of bits changed in the plain text is 1, 3, 6, 9 and 12, respectively. The position of changed bits in the plain text is randomly selected. The experimental results of plaintext avalanche are shown in TABLE I. These results show that the avalanche effect of plain text for Rijndael and RC6 algorithms approaches to a strict avalanche effect. There is no significant difference in the plaintext avalanche between Rijndael and RC6 algorithms by using Student's t-test at 95% confidence level. Moreover, the plaintext avalanche remains relatively stable. It does not vary with the number of bits changed in the plain text and key. It does not vary with the position of the changed bit too.

Similarly, the experimental results of key avalanche are shown in TABLE II. From TABLE I and II, we can clearly observe that the results of key avalanche for Rijndael and RC6 algorithms is the same as those of plaintext avalanche. The experimental results show that both Rijndael and RC6 algorithms satisfy the SAC property and have good diffusion property.

Combined with the procedure of block cipher algorithms as mentioned earlier, Rijndael algorithm only needs three rounds that any word variation of input, such as plain text or key, can be diffused through each word of cipher text by the operation of SubBytes, ShiftRows, MixColumns and AddRoundKey. However, RC6 algorithm theoretically needs six rounds that any input word variation diffuses into each word of output by the operation of integer addition, subtraction, multiplication, bitwise exclusive-or, and rotation.

TABLE I. PLAINTEXT AVALANCHE FOR RIJNDAEL AND RC6 ALGORITHMS

Number of input bits changed		1	3	6	9	12
Key length 128 bits	Rijndael algorithm (%)	51.70 ± 4.19	48.91 ± 3.52	48.91 ± 3.52	50.39 ± 4.36	48.05 ± 3.61
	RC6 algorithm (%)	49.51 ± 3.47	48.67 ± 4.36	49.51 ± 3.47	50.86 ± 3.28	50.58 ± 4.56
Key length 192 bits	Rijndael algorithm (%)	50.78 ± 3.91	50.00 ± 2.90	51.56 ± 5.47	50.08 ± 3.13	48.16 ± 3.75
	RC6 algorithm (%)	49.45 ± 3.41	51.50 ± 3.51	50.55 ± 4.52	51.10 ± 4.20	48.28 ± 2.60
Key length 256 bits	Rijndael algorithm (%)	49.53 ± 2.95	51.89 ± 2.92	50.91 ± 3.52	48.42 ± 3.46	49.98 ± 4.32
	RC6 algorithm (%)	48.19 ± 3.68	51.80 ± 3.11	49.38 ±3.39	48.91 ± 3.56	49.92 ± 3.26

TABLE II. KEY AVALANCHE FOR RIJNDAEL AND RC6 ALGORITHMS

Number of input bits changed		1	3	6	9	12
Key length 128 bits	Rijndael algorithm (%)	50.00 ± 3.08	50.65 ± 4.34	50.65 ± 4.34	49.77 ± 4.66	51.41 ± 4.78
	RC6 algorithm (%)	49.61 ± 3.81	50.24 ± 3.43	49.61 ± 3.81	50.34 ± 3.84	50.23 ± 2.50
Key length 192 bits	Rijndael algorithm (%)	49.22 ± 5.47	50.00 ± 3.91	50.00 ± 5.47	50.00± 3.91	50.08 ± 4.11
	RC6 algorithm (%)	49.53 ± 4.05	52.19 ± 3.14	48.09 ± 3.42	49.45 ± 4.02	48.28 ± 4.46
Key length 256 bits	Rijndael algorithm (%)	49.92 ± 5.23	49.84 ± 3.41	50.01 ± 4.52	51.67 ± 4.46	49.18 ± 4.52
	RC6 algorithm (%)	51.22 ± 6.05	51.07 ± 3.47	50.86 ±4.39	49.61 ± 4.51	49.67 ± 4.34

B. Confusion of Rijndael and RC6 Algorithms

We quantitatively investigate the confusion of Rijndael and RC6 algorithms by using runs test. The runs test can be used to decide if a data set is from a random process [16]. The results of runs test for Rijndael and RC6 Algorithms are shown in TABLE III.

TABLE III. RESULTS OF RUNS TEST FOR RIJNDAEL AND RC6 CIPHER TEXT

Runs length	Run	Percentage of the Rijndael cipher text runs (%)	Percentage of the RC6 cipher text runs (%)
1	0	50.00 ± 3.91	50.00 ± 3.84
	1	50.00 ± 3.91	50.00 ± 3.84
2	00	26.97 ± 3.45	25.96 ± 3.52
	01	24.25 ± 1.42	25.03 ± 2.08
	10	24.31 ± 1.40	24.67 ± 1.96
	11	24.48 ± 5.00	24.34 ± 5.23
3	000	12.11 ± 5.43	12.22 ± 5.21
	001	12.80 ± 1.69	12.73 ± 1.89
	010	13.19 ± 3.52	12.99 ± 3.87
	011	12.03 ± 2.30	12.23 ± 3.32
	100	12.60 ± 1.76	12.50 ± 1.82
	101	12.36 ± 3.03	12.43 ± 3.84
	110	11.89 ± 2.22	12.19 ± 4.89
	111	13.02 ± 5.69	12.71 ± 2.69

From TABLE III, we can clearly observe that different binary substrings show the quasi-uniform distribution in the whole cipher text. The passing rate of runs test is 100% at the 5% significance level when the length of runs is 1, 2 and 3, respectively. This shows that the cipher text of Rijndael has good randomness and unpredictability. Although there is no significant difference in the results of runs test between Rijndael and RC6, the mean value distribution of RC6 is better than that of Rijndael.

C. Speeds of Data Encryption and Decryption

The speeds of data encryption and decryption are regarded as a vital performance measure of cryptographic algorithms. The calculating formulae of data encryption and decryption are as follows, respectively.

$$V_e = \frac{N_p}{T_e} \tag{2}$$

$$V_d = \frac{N_c}{T_d} \tag{3}$$

Where V_e and V_d stand for the encryption and decryption speed, respectively. T_e is the encryption time. N_p represents the bit number of plaintext to be encrypted. T_d is the decryption time. N_c denotes the bit number of cipher text to be decrypted.

The experimental results of V_e and V_d are shown in TABLE IV. In TABLE IV, the encryption or decryption speed of RC6 algorithm is so much faster than that of Rijndael algorithm, and remains stable with the increase of key length. Meanwhile, the encryption and decryption speed of Rijndael algorithm shows a slight upward trend with the increase of data size to be encrypted or decrypted while the speed of RC6 algorithm presents a down trend. Finally, the practical speed of encryption is not the same as that of decryption although Rijndael algorithm is a symmetric encryption. However, RC6 algorithm has the same speed whether encrypting or decrypting.

TABLE IV. SPEED OF ENCRYPTION AND DECRYPTION FOR RIJNDAEL AND RC6 ALGORITHMS

Data size (Kb)			64	128	192	256	320
Key length 128 bits	Encryption (Mb/s)	Rijndael algorithm	78.70 ± 20.47	66.90 ± 7.37	70.10 ± 8.31	74.60 ± 17.13	88.20 ± 18.24
		RC6 algorithm	30517 ± 0	30517 ± 0	26153 ± 0	26039 ± 1398	25794 ± 2030
	Decryption (Mb/s)	Rijndael algorithm	23.20± 4.26	30.30 ± 2.95	32.50 ± 1.65	33.70 ± 1.64	32.60 ± 1.65
		RC6 algorithm	30517 ± 0	30517 ± 0	27899 ± 2254	26039 ± 1398	26815 ± 1194
Key length 192 bits	Encryption (Mb/s)	Rijndael algorithm	78.10 ± 6.94	94.10 ± 11.50	99.30 ± 26.24	99.80 ± 13.68	105.80 ± 16.78
		RC6 algorithm	30517 ± 0	30517 ± 0	26153 ± 0	26039 ± 1398	26815 ± 1194
	Decryption (Mb/s)	Rijndael algorithm	31.90 ± 2.47	36.10 ± 3.18	39.90 ± 1.97	40.10 ± 1.66	41.30 ± 1.16
		RC6 algorithm	30517 ± 0	30517 ± 0	27899 ± 2254	26580 ± 1142	27509 ± 731
Key length 256 bits	Encryption (Mb/s)	Rijndael algorithm	97.80 ± 15.93	110.70 ± 28.67	114.00 ± 18.34	108.10 ± 15.38	119.70 ± 13.65
		RC6 algorithm	30517 ± 0	30517 ± 0	26153 ± 0	26851 ± 856	26584 ± 1219
	Decryption (Mb/s)	Rijndael algorithm	37.80 ± 3.88	45.10 ± 1.97	46.70 ± 1.16	46.40 ± 1.43	46.20 ± 1.69
		RC6 algorithm	30517 ± 0	30517 ± 0	27462 ±2108	27122 ± 0	27278 ± 975

TABLE V. RESOURCE UTILIZATION FOR RIJNDAEL AND RC6 ALGORITHMS

Resource utilization	CPU (%)	Memory (Kb)
Rijndael algorithm	0.20 ± 0.05	287 ± 60
RC6 algorithm	0.77 ± 0.21	2448 ± 925

D. Resource Utilization

Seven different types of digital media such as text, picture, audio, video, and so on, are encrypted or decrypted by Rijndael and RC6 algorithms. The utilization of CPU and memory for each algorithm was measured. For the accuracy point of view, we execute every file 10 times and take the average of them.

TABLE V shows the utilization of CPU and memory for Rijndael and RC6 algorithms. The average CPU utilization of RC6 algorithm is more than 3 times than that of Rijndael algorithm. The average memory utilization of RC6 algorithm is more than 8 times than that of Rijndael algorithm.

IV. CONCLUSION

The cryptographic performance of RC6 and Rijndael has been analyzed with a set of input files. The experimental results conclude that both Rijndael and RC6 have good plaintext avalanche and key avalanche properties. They are very close to the SAC. The encryption or decryption speed of RC6 algorithm is much faster than that of Rijndael algorithm in the same experimental conditions, and does not vary with the size of key. Result also concludes that the encryption and decryption speed of Rijndael are asymmetric although Rijndael algorithm is a symmetric block cipher. However, RC6 algorithm has the same speed whether encrypting or decrypting. With the increase of data to be encrypted or decrypted, the encryption or decryption speed of RC6 shows a slight down trend while Rijndael presents the opposite trend. There is significant difference between RC6 and Rijndael in the resource utilization. From the user point of view, RC6 block cipher algorithm is faster and simpler than Rijndael block cipher algorithms. However, RC6 needs more CPU and memory resources than Rijndael. RC6 is mostly suitable for these occasions where high encryption speed is required while Rijndael is beneficial to the other occasions where memory resource is key concern.

REFERENCES

[1] J. S. Park, K. S. Bae, C. Y. Choi, D. H. Choi, and J. C. Ha, "A fault-resistant implementation of AES using differential bytes between input and output," Journal of Supercomputing, vol. 67, no. 3, pp. 615-634, Mar. 2014.

[2] S. S. Liu, Z. Gong and L. B. Wang, " Cryptanalysis of Reduced-Round DASH," Journal of Computer Science and Technology, vol.28, no.1, pp. 159-164, Jan. 2013.

[3] C. E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, Oct.1949.

[4] I. Muniraj, C. Guo, R. Malallah, et al, " Choice of optical system is critical for the security of double random phase encryption systems," Optical Engineering, vol. 56, no. 6, pp. 1-14(063103), Jun. 2017.

[5] H. Feistel, "Cryptography and Computer Privacy," Scientific American, vol. 228, no. 5, pp. 15-23, May 1973.

[6] R. Forré, "The strict avalanche criterion: spectral properties of boolean functions and an extended definition," Proceeding CRYPTO '88 Proceedings on Advances in cryptology, Lecture Notes in Computer Science, Springer-Verlag, Berlin, vol. 403, pp. 450-468, 1990.

[7] J. C. H. Castro, J. M. Sierra, A. Seznec, A. Izquierdo, A. Ribagorda, "The strict avalanche criterion randomness test," Mathematics and Computers in Simulation, vol. 68, no.1, pp. 1-7, Feb. 2005.

[8] L. Q. Min, and G. R. Chen, "A novel stream encryption scheme with avalanche effect," The European Physical Journal B, vol.86, no. 459, pp. 1-13, Nov. 2013.

[9] A. Dandalis, V. K. Prasanna, J. D. P. Rolim, "A comparative study of performance of AES final candidates using FPGAs," Lecture Notes in Computer Science, vol.1965, pp. 125-140, 2000.

[10] A. J. Elbert, E. Yip, B. Chetwynd, and C. Paar: "An FPGA implementation and performance evaluation of the AES block cipher candidate algorithm finalists", IEEE Transactions on Very Large Scale Integration Systems, vol. 9, no. 4, pp. 545-557, Aug. 2001.

[11] H. K. Verma, and R. K. Singh, "Performance analysis of RC6, Twofish and Rijndael block cipher algorithms," International Journal of Computer Applications, vol. 42, no.16, pp. 1-7, Mar. 2012.

[12] National Institute of Standards and Technology: Advanced encryption standard, FIPS 197, US Department of Commerce, Washington D.C., Nov. 2001.

[13] J. Daemen and V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard," New York: Springer-Verlag, 2002, pp.1-178.

[14] R. Rivest, M. Robshaw, R. Sidney and Y. Yin, "The RC6TM Block Cipher," v.1.1, Aug. 1998. http://people.csail.mit.edu/rivest/pubs/RRSY98.pdf

[15] A. K. Mandal, and A. Tiwari, "Analysis of Avalanche Effect in Plaintext of DES using Binary Codes, " International Journal of Emerging Trends & Technology in Computer Science, vol.1, no.3, pp. 166-171, Sep. 2012.

[16] J. V. Bradley, "Distribution-Free Statistical Tests," New Jersey: Prentice-Hall, 1968, pp. 279-311.