Journal of Theoretical and Applied Information Technology
10th March 2015. Vol.73 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TSHIFTCOLUMN: A NEW TRANSFORMATION IN 128-BIT RIJNDAEL KEY EXPANSION TO IMPROVE SECURITY REQUIREMENTS

[1]ZAITON MUDA, [1]SALASIAH SULAIMAN, [1]SHARIFAH MD YASIN, [1]RAMLAN MAHMOD
[1]Faculty of Computer Science and Information Technology, University Putra Malaysia,
43400 UPM Serdang, Selangor, Malaysia
E-mail: [1]zaitonm@upm.edu.my

ABSTRACT

Evolvement in technology has resulted in a large number of new proposals done on Rijndael block cipher. Even though there are many developments done on the enhancement of block cipher algorithm, the industry still requires more as long as security requirements are met. In this paper, we present a new approach called TShiftColumn transformation which is added to the original Rijndael key expansion algorithm to improve security requirements. This new approach follows the green cryptography concept through recycling the existing algorithm by enhancing and improving its security requirements. The TShiftColumn transformation has been tested with two types of tests for security measurement; confusion and diffusion tests. This new transformation has passed the security requirement with better result compared to original Rijndael key expansion algorithm.

Keywords: *green cryptography, TShiftcolumn, Rijndael key expansion, confusion, diffusion*

1. INTRODUCTION

Essential in computer security is to secure the information and communications from unaccredited access. Disclose such information could cause anonymous risk and data loss depends on levels of confidentiality data that has been exposed. There are many types of threats and attacks that have been discovered each year as well as various kinds of methods that was develop to prevent security violation.

Cryptography is one of the techniques in order to secure information that will encrypt the information into unreadable codes. There are three types of cryptography mechanism which are symmetric key, asymmetric key and hashing. These cryptography mechanisms are used in a variety of utilization such as electronic commerce, bank cards, and, computer passwords which aid in securing the connections and transactions. In this paper, we focused on symmetric key mechanisms, which is Rijndael block cipher and only on key expansion transformation. In 2001, the Rijndael block cipher (pronounced "Reign Dahl," "Rain Doll" or "Rhine Dahl") was announced as Advanced Encryption Standard (hereinafter called AES) after it won competition to replace Data Encryption Standard (DES) [1]. Rijndael block cipher was developed by Joan Daemen and Vincent Rijmen, the Belgian cryptographers. It has two parts of transformation; cipher or round transformation and key expansion transformation. Key expansion transformation will generates round keys or subkeys that will be used in cipher transformation for encryption and decryption processes.

After publicize as AES, Rijndael block cipher had received numerous attentions from many researchers whether to cryptanalyze or improve it. Requirement to enhanced or produce novel method in digital world become essential in today's world with advancement of technology for security in computing. Due to this issue, we produce new transformation to be added in the Rijndael key expansion meanwhile preserving its original structure.

The improvements made on existent potential cryptographic structure or algorithm is known as "Green Cryptography" for cleaner engineering. According to [2] the green cryptography concept means recycling cryptographic primitives for building matures (secure) and minimalist (simple) cryptography implementation. The most compelling reason for using the Rijndael is based on a result of being a standard - it receives more crypt analytical attention than any of the other AES finalist candidates. It is fit with the engineering principle of recycling primitives.

There have been some studies done and cryptanalysis attempts on the key expansion that reveals it weakness [3], [4], [5], [6]. Exhaustive key search or generally identified as brute force search, which is the simplest attack against a cryptographic algorithm [7], [8]. This is the fundamental method of trying every probable key in turn until the exact key is recognized. Cryptanalysis is latest technique of learning to break a cipher compared to the brute force attack. There are numerous studies have been carried out on Rijndael block cipher key expansion in order to improve the algorithm in protecting classified data.

2. RELATED WORK

The key expansion algorithm in Rijndael block cipher produces a round cipher key obtained from a master key inputted by user (also known as secret key). It is an iterative element in a block cipher as illustrated in Figure 1. The purpose of a well-built key expansion is to produce block cipher that can be resistant from various kinds of attacks. However, there are weaknesses of Rijndael key expansion that were found in previous work such as, subkey bit leakage, slow diffusion, and high linearity.

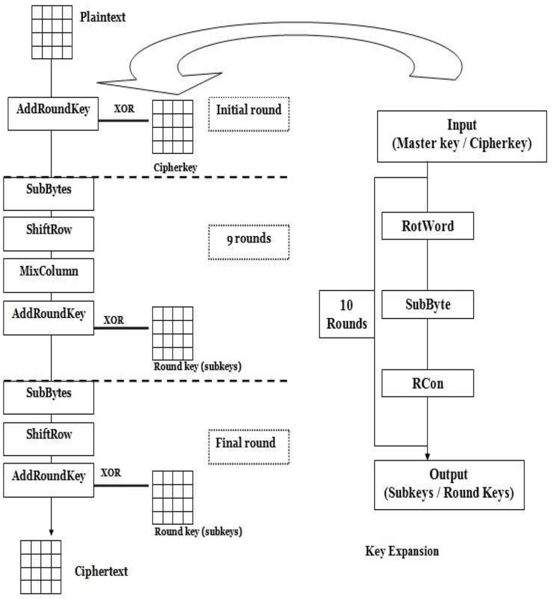

Figure 1: Rijndael Block Cipher Transformation

According to [9], the Rijndael key expansion is more vulnerable toward attacks since there is almost no interaction between different rows. This vulnerability allows an attacker to fix four bytes in the same column independently. There are many modification performed on Rijndael block cipher that are aimed to patch the security flaw.

In 2001, [10] has strengthen the Rijndael key expansion by exploiting a three round of Rijndael cipher function to derived confusion and diffusion properties which follows the principle of a secure cipher. After a year, this proposed key expansion approach by [10] was analyzed by [11]. From his study, the analysis shows that this new design of key expansion could not resist to a related-key attack and is far too expensive for hardware implementations [12].

There is also study that come up with a novel block cipher that adapt from Rijndael block cipher known as new 128-bit block cipher by [13]. In new 128-bit block cipher, there is also new key expansion that include byte inverse for nonlinear component, shift rotation, and XOR operation. However there is no security measurement was conducted on the key expansion algorithm that has been proposed to measure it strength.

In 2011, [14] presented a tweak for the key expansion of Rijndael by adding several rotation operations and extra S-boxes, which does not change the overall structure of the original key expansion. However this new tweak key expansion cannot resist from meet-in-the-middle attacks [15]. After a year, [12], has also improved Rijndael key expansion by eliminating these weak keys.

Most of new proposals done on Rijndael key expansion do not go through any test to measure security for bit diffusion and bit confusion, a concept which was introduced by Shannon [16]. Shannon introduced the ideas of confusion and diffusion, notionally provided by S-boxes and P-boxes (in conjunction with S-boxes) [17]. These terms capture the two basic building blocks for any cryptographic system.

Nevertheless, to enhance the security of Rijndael key expansion, there are two important properties of a secure cipher to be focused on; confusion (mixing bit) and diffusion (each input bit affecting each output bit). Every block cipher involves a transformation of a block of plaintext into a block of ciphertext, where the transformation depends on the key. The mechanism of diffusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key. Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. However, according to [9] Rijndael is somewhat less rigorous in obtaining these properties in key expansion part. An important theoretical underpinning for bit confusion and bit diffusion is the idea of using Frequency and Strict Avalanche Criterion (hereinafter called SAC) tests for both properties respectively. SAC obviates the need for a widely used approximation, allowing more accurate evaluation of the bit diffusion to key expansion. Both of the properties (confusion and diffusion) shall be obtain in this research together with designing new transformation approach in key expansion in order to enhance the security of the cipher. Furthermore, we will compare our tests result with Rijndael key expansion algorithm and ShiftRow approach of key expansion proposed by [18].

3. PROPOSED APPROACH

Rijndael block cipher involves two main parts of transformations which are, cipher transformation and key expansion. Cipher transformation is parameterized using key expansion that consists of four byte words derived using the key expansion routine. The key expansion algorithm takes the cipherkey (input key), and performs a key expansion routine to generate a key scheduling that will be XORing with plaintext and ciphertext in every round. The original Rijndael key expansion algorithm consists of three different byte-orientated transformations which are RotWord, SubByte, and RCon. The key expansion routines create round keys word by word, where word is an array of four bytes. The routines creates 4*(Nr + 1) words that are called w_0, w_1, w_2,.....$w_{4(Nr\ +\ 1)\ -1}$. Illustration process of Rijndael key expansion is shown in Figure 2.

The proposed approach for key expansion algorithm has four byte-orientated transformations which are RotWord, SubByte, Rcon and TShiftColumn. The TShiftColumn transformation was applied in order to contribute a diffusion property which was lacked in the original key expansion. The diffusion concept is necessary to obscure the cipherkey (input key) during key expansion routine. Diffusion property achieves through mixing and reordering (such as shifting and rotations) of data. The TShiftColumn transformation approach has three steps as shown in Figure 3. It begins with left shifting the bit value then XOR with the value in same column. Second, the result from XOR is shifted to the right. Lastly, column will be shifted over different offsets.

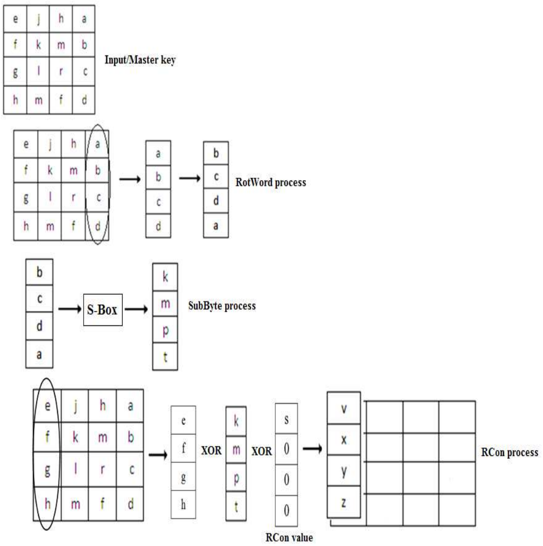

Figure 2: Rijndael Key Expansion Transformations

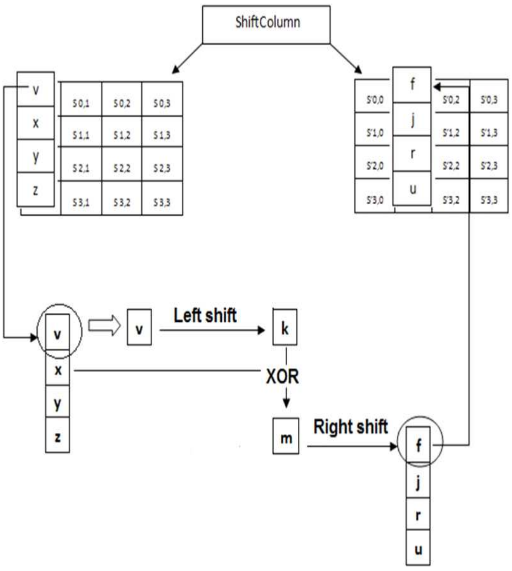

Figure 3: TShiftColumn Transformation Process

This transformation was applied in each ten rounds in key expansion algorithm. The following explanations will describe more detail about the key expansion algorithm of the proposed approach. The expansion of the cipherkey into key expansion proceeds according to process in Figure 3. The expanded key is a linear array of 4-byte words (see Table 1).

Table 1: Definition of Notations

Notations	Definitions
k	Key: Group of 32 bits that is treated either as a single entity (column) or as an array of bytes.
Nk	Number of key word. Nk = 128-bits key/32-bit word = 4.
Nr	Number of rounds. Nr = 10.

```
KeyExpansion(byte key[4*Nk], word k[Nr+1,Nc], Nc, Nk, Nr)
begin
    i = 0
    while (i < Nk)
        k[i] = word [key[4*i+3], key[4*i+2], key[4*i+1], key[4*i] ]
        i = i + 1
    end while
    i = Nk
    while (I < Nc * (Nr + 1))
        word temp = k[i - 1]
        if (i mod Nk == 0)
            temp = (SubByte(RotWord(temp)) xor
            RCon[i / Nk])
        end if
            k[i] = k[i - Nk] xor temp
        if (i mod Nk == 3)
        // Apply the new approach "ShiftColumn" transformation
            word temp1 [4][4]
            for (c = 3; c >= 0; c-1)
                temp1[c][r] = k[Nk + c]
            ShiftColumn (temp1);
        end if
        i = i + 1
    end while
end
```

Figure 4: Key Expansion Algorithm of Proposed Approach

This approach using 128-bit key length, so the value of Nk is 4 which is number of 32-bit words comprising the 128-bit cipherkey. All other words are defined recursively in terms of words with smaller indices. In Figure 4, SubByte is a function that returns a 4-byte word in which each byte is the result of applying the Rijndael S-box to the byte at the corresponding position in the input word. The RotWord returns a word in which the bytes are a cyclic permutation of those in its input. This transformation consists of a cyclic shift of the bytes in a word (RotWord), followed by the application of a table lookup to all four bytes of the word (SubByte). The new approach, TShiftColumn transformation is then applied for each word which is not done in the original Rijndael approach. This produced the result of subkey (output) which is the final output for the new approach key expansion as illustrated in Figure 5.

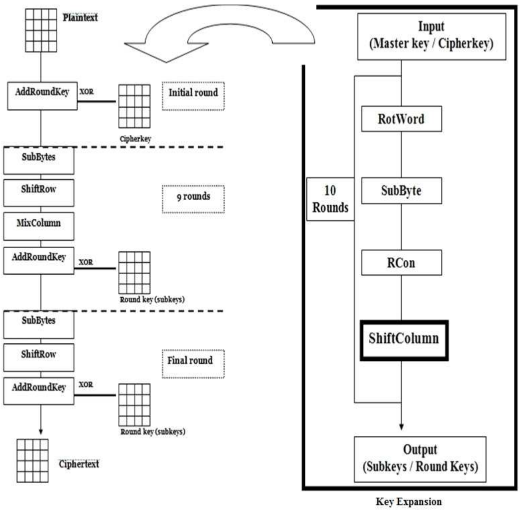

Figure 5: Enhancement of Rijndael Key Expansion Structure with TShiftColumn Approach

4. TEST

Security measurement is a performance (benchmark) evaluation that is needed to evaluate our proposed algorithm. The need for random numbers arises in many cryptographic applications [19]. In general the cipher designer strives to obtain bit confusion (or substitution) and bit diffusion (each input bit affecting each output bit). Much effort is spent in obtaining these properties in cipher algorithms. Indeed, the Rijndael block cipher algorithm attains these properties very elegantly. The Rijndael key expansion, however, is somewhat less rigorous in obtaining these properties (bit confusion and diffusion).

In this paper, total of 30 subkeys was generated from three key expansion algorithms which are original Rijndael key expansion, the ShiftRow approach [18], and the TShiftColumn approach. The input (master key) for each key expansion algorithms was obtained from user input (non-random). As a yardstick to measure the confusion and diffusion properties of the key expansion proposal, two basic statistical tests (frequency and SAC test) are used. These tests are described in detailed as the following.

3.1 Frequency Test

The focus of the test is on the proportion of zeroes and ones for the entire sequence. The purpose of this test is to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. The test assesses the closeness of the fraction of ones to ½, that is, the number of ones and zeroes in a sequence should be about the same. The latest NIST package has 15 tests and all subsequent tests depend on the passing of this test (frequency test) and there is no evidence to indicate that the tested sequence is non-random.

If the computed p-value (probability value) is < 0.01, the sequence is concluded to be non-random with 99% confidence. Otherwise, the sequence is random with 99% confidence. Large positive values of sequence length of bit string are the indicative of too many ones, and large negative values of sequence length of bit string are the indicative of too many zeros. However, it should be noted that passing the frequency test does not mean the stream (bit) is not patterned. Hence the frequency test is not sufficient on its own as a test for randomness of a key stream [20].

3.2 Strict Avalanche Criterion Test (SAC)

Another important test used in this research is the Strict Avalanche Criterion (SAC) test, also known as One-Sample Kolmogorov-Smirnov test (1-Sample K-S test) in the SPSS software. The purpose of the SAC test is to test that half of the output bits change with a 1-bit change in input (cipher key). The resulting test statistic is the Kolmogorov-Smirnov statistic denoted by D based on test output results. The following explanations are the detail of this test.

In Kolmogov-Smirnov, the D value is the largest absolute difference between the cumulative observed proportion and the cumulative proportion expected on the basis of the hypothesized distribution [21]. The computed D is compared to a table of critical values of D in the 1-Sample K-S test for a given sample size [22]. For samples > 35, the critical value at the 0.01 level is approximately 1.36/SQRT(n), where n equal to the sample size. If the computed D-value less than 1.628, the researcher fails to reject the null hypothesis that the distribution of the criterion variable is not different from the hypothesized distribution with 99% confidence for the critical value 0.01.

5. RESULT ANALYSIS

This section will further discuss on the result analysis for both tests. Figure 6 shows plotted graph for frequency test and Figure 7 shows plotted graph for SAC test. In Figure 6, all subkeys from TShiftColumn approach passed the frequency test and 8 from 10 subkeys got higher p-value than original Rijndael key expansion and ShiftRow approach. This is due to TShiftColumn transformation contributes to the security key expansion algorithm by forming a linear mixing layer which increases the bit confusion output.

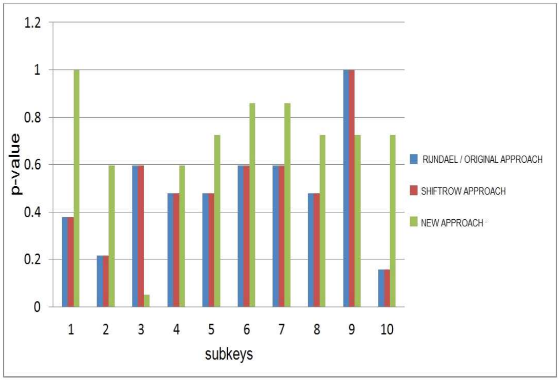

Figure 6: Result of Frequency Test

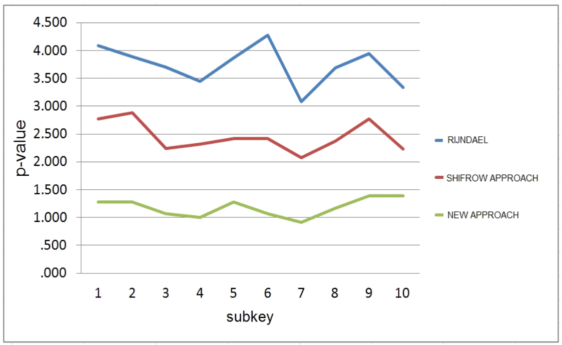

Figure 7: Result of SAC Test

Figure 7 shows that the D-values of 10 subkeys in the TShiftColumn approach are less than 1.628 while subkeys of the other two approaches did not passed this test which D-values are more than

1.628. This is because the TShiftColumn transformations ensure that all of the bytes in subkeys affect each other, which generates high diffusion over multiple rounds in order to increase the bit diffusion output that contributes to the security of key expansion algorithm.

6. CONCLUSION

In this paper, a new key transformation has been introduced, called TShiftColumn approach which is added to the original Rijndael key expansion. Objective of this study is to strengthen Rijndael key expansion security due to many attempts to break it. We preserve Rijndael original structure to follow the concept of green cryptography since Rijndael is a standard encryption and also it is suitable as primitives' structure to be improved. After analyzing using two statistical tests (frequency and SAC test), the result shows that the new approach succeed in passing all tests and gives better results especially in diffusion property. It concludes that TShiftColumn approach contribute to the enhancement security in Rijndael key expansion.

REFRENCES:

[1] P. Penchalaiah and D. Seshadri, "Effective Comparison and Evaluation of DES and Rijndael Algorithm (AES)", *International Journal on Computer Science and Engineering*, Vol. 2, 2010, pp. 1641-1645.

[2] J. Troutman and V. Rijmen, "Green Cryptography: Cleaner Engineering Through Recycling", *IEEE Security & Privacy*, 2009, pp. 71-73.

[3] G. Carter, E. Dawson, and L. Nielsen, "Key Schedule Classification of the AES Candidates" *Proceedings of 3rd AES Conference*, National Institute of Standards and Technology (NIST, New York, USA), April 13-14, 2000, pp. 1-15.

[4] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting, "Improved Cryptanalysis of Rijndael", *Proceedings of 7th Fast Software Encryption Workshop*, New York (USA), April 10-12, 2001, pp. 213-230.

[5] C.J. Hee, M. Kim, J.Y. Lee, and S.W. Kang, "Improved Impossible Differential Cryptanalysis of Rijndael and Crypton", *Proceedings of 4th International Conference Seoul* , Korea, December 6–7, 2001, pp. 39-49.

[6] A. Biryukov and D. Khovratovich, "Related-Key Cryptanalysis of the Full AES-192 and AES-256", *Proceedings of 15th International Conference on the Theory and Application of Cryptology and Information Security*, Japan, December 6-10, 2009, pp. 1-18.

[7] J.J. Quisquater and F.X. Standaert, "Exhaustive Key Search of the DES: Updates and Refinements", *Proceedings of Special-purpose Hardware for Attacking Cryptographic Systems Workshop*, ECRYPT (Paris, France), February 24 -25, 2005, pp. 1-7.

[8] A.A. Milad, Z. Muda, Z.A. Muhamad Noh, and M.A. Algaet, "Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack)", *Journal of Computer Science*, Vol. 8, No. 2, 2012, pp. 1191-1197.

[9] J. Huangi and X. Lai, "Revisiting Key Schedule's Diffusion in Relation with Round Function's Diffusion", *International Journal of Designs, Codes and Cryptography*, Vol 9, 2013, pp. 1-19.

[10] L. May, M. Henricksen, W. Millan, G. Carter, and E. Dawson, "Strengthening the Key Schedule of the AES", *Proceedings of 7th Australasian Conference*, Melbourne (Australia), July 3–5, 2002, pp. 226-240.

[11] H. Wu, "Related-cipher Attacks", *Proceedings of 4th International Conference of ICICS*, Singapore, December 9–12, 2002, pp. 447-455.

[12] J. Choy, A. Zhang, K. Khoo, M. Henricksen, and A. Poschmann, "AES Variants Secure Against Related-key Differential and Boomerang Attacks", *Proceedings of 5th IFIP WG 11.2 International Workshop*, Crete (Greece), June 1-3, 2011, pp. 191-207.

[13] M.A. Fakariyah, "A new 128-bit block cipher", *Ph.D Thesis*, Universiti Putra Malaysia, Selangor, Malaysia, 2009.

[14] I. Nikolic, "Tweaking AES", *Proceedings of 17th International Workshop: Selected Areas in Cryptography*, Ontario (Canada), August 12-13, 2010, pp. 198-210.

[15] J. Huang and X. Lai, " Transposition of AES Key Schedule", *IACR Cryptology ePrint Archive*, 2012, pp. 1-13.

[16] C. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, Vol 28, 1949, pp. 656-715.

[17] D. Rezaeipour and M.R. Said, "The Vulnerability Analysis and the Security Evaluation of Block Ciphers", *International*

Mathematical Forum, Vol 5, No. 42, 2010, pp. 2071 – 2075.

[18] Z. Muda, R. Mahmod, and M.R. Sulong, "Key Transformation Approach for Rijndael Security", *Information Technology Journal*, Vol 9, 2010, pp. 290-297.

[19] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A Statistical Test Suite For Random and Pseudorandom Number Generators for Cryptographic Applications", *NIST Special Publication 800-22*, Revised 2010.

[20] H. Gustafson, E. Dawson, L. Nielsen, and W.A. Caelli, "Computer Package for Measuring the Strength of Encryption Algorithms", *Computers and Security*, Vol. 13, 1994, pp. 687-697.

[21] S. Sulaiman, Z. Muda, and J. Juremi. "The New Approach of Rijndael Key Schedule", *Proceeding of Cyber Security, Cyber Warfare and Digital Forensic (CyberSec),* Kuala Lumpur (Malaysia), June 26-28, 2012, pp. 23-27.

[22] F.J. Massey, "The Kolmogorov-Smirnov Test for Goodness of Fit", *American Statistical Association*, Vol 46, 1951, pp. 68 – 78.