PROCEEDINGS OF SCIENCE

Visual Detection of Stream Cipher Sequences on ZUC Algorithm

Ruoxue Wu[12]
Yunnan University
Kunming, 650091, China
E-mail: rochelle.wu820@gmail.com

Jeffrey ZJ Zheng[3]
Yunnan University
Kunming, 650091, China
E-mail: conjugatelogic@yahoo.com

Xiaoxuan Liang
Yunnan University
Kunming, 650091, China
E-mail: shaw.xuan820@gmail.com

The method of ensuring the network security was usually based on the stream cipher algorithms to encrypt the information. One way of testing the quality of a stream cipher algorithm was used NIST standard for testing. For the shortcoming of those detection methods that measure a segment of key streams, the results were not on systematic approaches. To improve these methods, a systematic measurement and visual scheme on key streams is hereby proposed, which utilizes the testing results in a more accurate manner. By transforming the data into 2D visualization maps, the results are more visible to show the random characteristics of the ZUC

CENet2017
22-23 July 2017
Shanghai, China

[1] Speaker

[2]This work is partially supported by the National Natural Science Foundation of China (61362014).

[3] Corresponding author

© *Copyright owned by the author(s) under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0).*

PoS(CENet2017)081

1. Introduction

With the rapid development of information technology, it plays an important role in modern life and promotes the continuous progress of human civilization. However, as the information technology is more and more convenient for our life. More sensitive information is also demanded to interact with the computer network or public communication facilities [1]. Particularly, the network embedded in our lives, for example, shopping online, e-mail, instant messaging and Internet banking, etc. When these applications become popular, people more and more concern about how to ensure the security of user information. In the Internet communication, ensuring the reliability and robustness of the information has gradually can't be ignored [2]; and it's rather urgent to improve the security of storage, transmission and processing of information. The method of solving this problem is to use the stream cipher encryption. Now, there are many kinds of encryption algorithms in the world [3][4].

ZUC algorithm, developed by China, is a cryptographic algorithm for 4G international communication standard. The input consists of 128 bit original key and vector; and its output is a string of 32 bits of the key stream. The key stream can be used to encrypt or decrypt [5].

Usually, we use the National Institute of Standards and Technology (NIST) detection method to estimate the quality of the sequence encryption algorithm by its random sequence.

2. NIST Standard

2.1Introduction of Detection Methods

NIST testing standards include *16* kinds of test methods, which can be used to test the arbitrary length of 2 binary sequences generated by the hardware or software of pseudo-random number generator. The traditional statistical test method for judging the quality of the sequence generated by an encryption algorithm is to take one of sequences as the detection sequence, and then test the sequence by using NIST detection standard method to. Getting a value of *P*, is P-value. Nest judge P-value. In this paper, we mainly use three kinds of detection methods: Serial test, Cumulative Sums test and Block Frequency test. The main method is Block Frequency test.

2.2Deficiency of Detection Methods

For the traditional detection methods of NIST, it just tests a part of the sequence cipher. The randomness of the sequence cipher is used to estimate to the randomness of the whole sequence cipher and ultimately determine the quality of the sequence encryption algorithm. As it only uses the segment of the sequence cipher, the utilization rate of the whole sequence cipher is not very high, and it is possible that the whole sequence is nonrandom although the detection sequence is random. As a result, there is a large error in the judgment of the algorithm.

3. Improvement of NIST Detection

This paper has improved the detection method because the traditional detection method features a great defect. The new method is used to detect the bulk flows of sequence cipher. Using Cumulative Sums, Block Frequency and Serial to test these ciphers generated by ZUC algorithm and change the parameter values, the results will be represented by the images. By comparing different images to evaluate the characteristics of ZUC algorithm. The method makes up for the low utilization ratio of the sequence cipher to the past detection method and the

PoS(CENet2017)081

disadvantage of results were not intuitive observation. With intuitive understanding and experience, we can easily understand the random characteristics of the ZUC algorithm.

3.1Detection Steps

Different from the conventional method that classifies the sequence only once, the sequence is firstly divided into several subsequences. Although the methods of NIST doesn't explicitly point out the recommended length of the measured data stream. If the length of data stream is a certain value, it will be considered as a relatively-random data stream with some indicators. Next, we'll try to segment these data steam to test them and calculate value of P-values [6] by using NIST.

Assume the initial sequence length be *N*. Firstly, for the grouping sequences, the sequence is divided into several data segments and, set their length be *Length*. If the *Length* is not enough, the data segment will be abandoned. In this sense, a total of $n=\lfloor N/Length \rfloor$ subsequences are obtained. Next, continue to group the subsequences. They will be divided into data segments whose length is *m*. If *m* is not enough, it would be abandoned. Thus we get $\lfloor Length/m \rfloor$ data streams. Now, the initial sequence *N* is divided into $\lfloor N/Length \rfloor * \lfloor Length/m \rfloor$ data streams. The presentations are as follows, suppose *N=100*, *m=3, Length=30*.

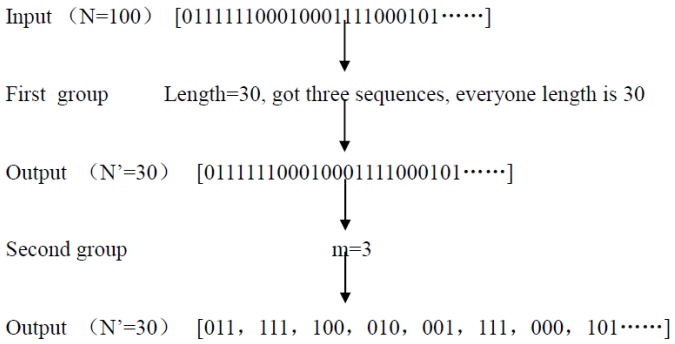


Figure 1: Grouping Method of Data

According to the data streams, we choose any of Serial test, Cumulative Sums test and Block Frequency test to calculate each stream. Then we will get $\lfloor N/length \rfloor * \lfloor length/m \rfloor$ P-value [7].

If the key stream is enough, we would get massive P-value through segmentation. The huge amount of data are unable of using the traditional analysis methods to carry out analysis. So for statistic number of P-values, the same values are grouped together. As the key stream is enough, we will get a variety of P-values. Actually, the situation is more complex, so we need more statistics. Statistics the number of P-values in *0 ~ 0.1, 0.1 ~ 0.2, 0.2 ~ 0.3, ... , 0.9 ~ 1.0* data streams. Then calculate the percentage of each group, recorded as *p1, p2, p3, ... , p10,* when P-value in *0 ~ 0.1, 0.1 ~ 0.2, 0.2 ~ 0.3, ... , 0.9 ~ 1.0.*

After getting the statistics, we need to use the method of system segmentation. Using Formula (1) to calculate the value of the coordinate [8].

$$x=\sum_{i=1}^{10} p_i^2, \quad y=\sum_{i=1}^{10} \sqrt{p_i}, \tag{3.1}$$

Then, the values are represented on 2D images, finally, we get images.

3.2Experiment Environment and Sample

In this paper, the test environment is Samsung notebook computer with Quad-Core Processor, DDR3 4GB memory, windows7 64 bit ultimate operating system. The test software is

PoS(CENet2017)081

MATLAB R2014a. The test samples were 8 bit binary cipher stream generated by the ZUC algorithm. The sample size was 100 thousand, 200 thousand, 500 thousand and 1 million, named ZUC-10w.txt, ZUC-20w.txt, ZUC-50w.txt and ZUC-100w.txt.

3.3Detection Result

In the visual model, the parameters of sample size, length, m and detection methods can be changed. Changing these parameters can lead to different changes in the image. The sample sizes are divided into 100 thousand, 200 thousand, 500 thousand and 1 million. The range of length and m is 1~*N*. The detection methods include Cumulative Sums, Block Frequency and Serial. By using the control variable method, change the single variable while keeping other variables unchanged. The results are expressed in image. The groups are shown as follows.

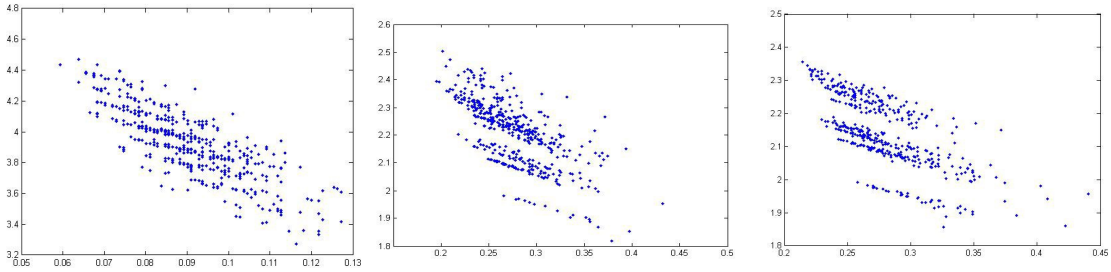
3.3.1Change of the Detection Methods withOther Variables Unchanged

As shown in Table 1

Method	m	Length	Sample	Graphic r
Serial	3	9	zuc-20w.txt	Fig.3.2(a)
Cumulative Sums				Fig.3.2(b)
Block Frequency				Fig.3.2(c)

Table 1: Different Detection Methods

Test results are shown as follows:



(a) Serial (b) Cumulative Sums (c) Block Frequency

Figure 2: Different Detection Methods

3.3.2Detection of Key Streams with Different Lengths

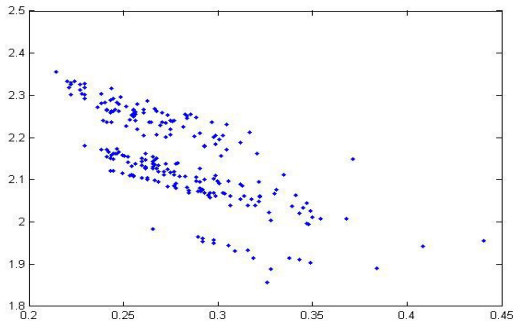
The results are shown in Table 2

Method	m	Length	Sample	Graphic
Block Frequency	3	9	zuc-10w.txt	Fig.3.3(a)
			zuc-20w.txt	Fig.3.3(b)
			zuc-50w.txt	Fig.3.3(c)
			zuc-100w.txt	Fig.3.3(d)

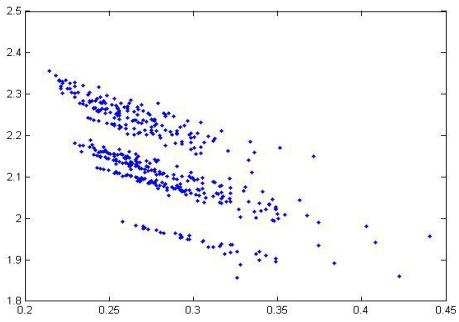
Table 2: Different Sample Size

Test results are shown as follows:

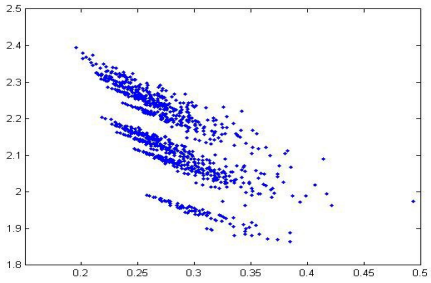
PoS(CENet2017)081



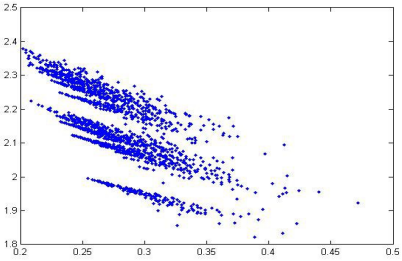
(a)size=100,000



(b) size=200,000



(c) size=500,000



(d) size=1,000,000

Figure 3: Different Sample Size

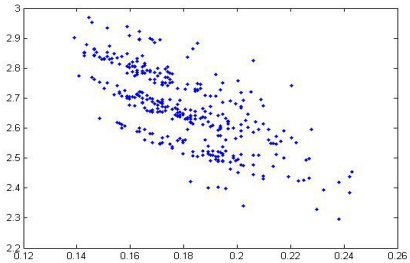
3.3.3Different Parameter m

The results areshown in Table 3

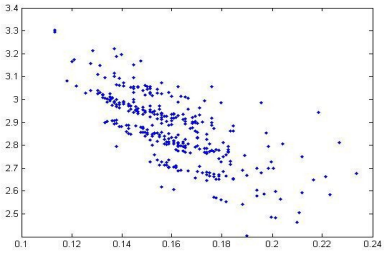
Method	m	length	Sample	Graphic
BlockFrequency	1	12	zuc-20w.txt	Fig.3.4(a)
	4			Fig.3.4(b)
	6			Fig.3.4(c)
	12			Fig.3.4(d)

Table 3: Different Parameter m

Test results are shown as follows:

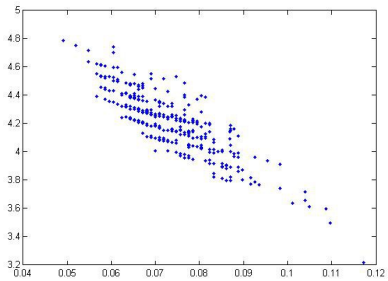


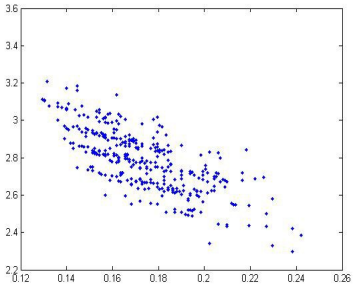
(a) m=1



(b) m=4

PoS(CENet2017)081





(c) m=6 (d) m=12

Figure 4: Different Parameter m

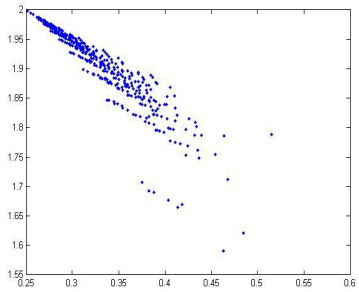
3.3.4Different Parameter Length

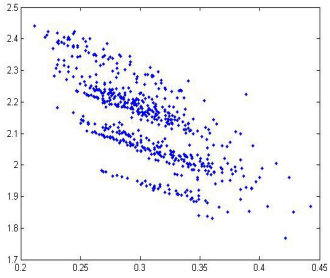
The results are shown in Table 4

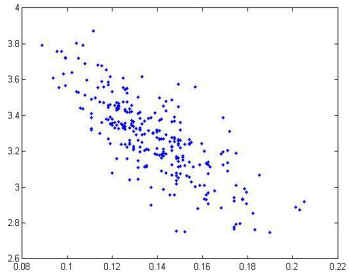
Method	m	Length	Sample	Graphic
BlockFrequency	3	3	zuc-20w.txt	Fig.3.5(a)
		6		Fig.3.5(b)
		15		Fig.3.5(c)
		36		Fig.3.5(d)
		48		Fig.3.5(e)
		99		Fig.3.5(f)

Table 4: Different Parameter Length

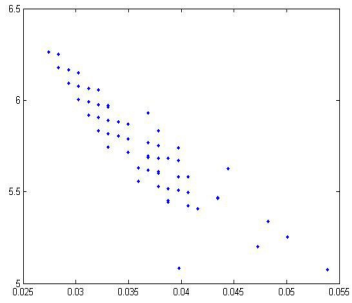
Test results are shown as follows:

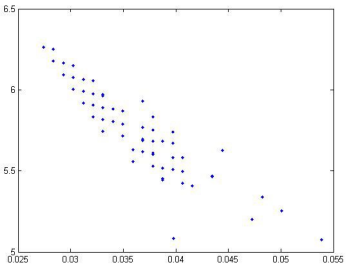


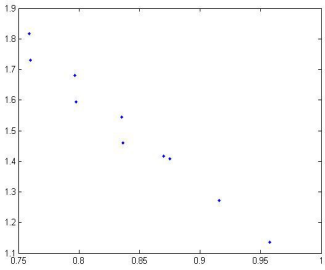




(a) Length=3 (b) Length=6 (c) Length=15







(d) Length=36 (e) Length=48 (f) Length=99

Figure 5: Different Parameter Length

3.4Analysis

1. Different detection methods to detect the same sequences, the image is similar.

2. When the sample size becomes larger, the spot on the image is also increased, the trend and characteristic of the whole image become clearer and more intuitive.

PoS(CENet2017)081

3. When only *m* is changed, if the value is larger, the points were more scattered on the image.

4. When only the *Length is changed*, if the value is more suitable, characteristics of the image will be more obvious. When the *Length* become bigger, points on the image are more dispersed.

5. The traditional method of judging the quality of the algorithm depends on whether the P-value is greater than *0.1*. If larger than *0.1*, it is proved that the pseudo-random sequence generated by the algorithm has good randomness and the algorithm is better. In this paper, judge the merits of the algorithm based on values of points on the image. From the image, it can be seen that all the points are randomly distributed; so the pseudo-random sequence generated by the ZUC algorithm has good randomness, in other words, ZUC algorithm performs better.

4. Conclusion

In this paper, by using the improved NIST standard to test the ZUC algorithm, the performance of the ZUC algorithm and intuitive response to the results can be demonstrated and the results show that the pseudo-random sequence have good randomness. Although some achievements have been made in this respect. It is still unable to further verify the cause of the special circumstances and other situation.

References

[1] ZHANG H H, HAN W B, et al. *Summarize of Cyberspace Security*[J]. Science in China, 2016.1.22

[2] DING C S, XIAO G Z. *Stream cryptography and Its Applications*[M]. Beijing: National Defence Industry Press, 1994.

[3] DU H H. *Analysis of ZUC algorithm and Research on the method of Cube cryptographic analysis*[D]. Shandong Normal University, 2013.

[4] FENG X T. *3GPP LTE International encryption standard ZUC algorithm*[J]. Information and communication security, 2011

[5] LI G, TAO L, GAO X W. *Research and implementation of Zu Chongzhi algorithm based on FPGA*[J]. Journal of Beijing Electronics Science and Technology Institute, 2012,20 (4):13-18

[6] LIU Z W. *Research on random testing of cryptographic algorithms*[D]. Xi'an Electronic Technology University, 2011

[7] NIST Special Publication 800-22. *A statistical test suite for random and pseudo- random number generators for cryptographic applications*[S]. 2008.

[8] Zheng J Z J, Zheng C H H and Kunii T L. *A Framework of Variant Logic Construction for Cellular Automata[EB/OL]*. (2011)http://www.intechopen.com/books/cellular-automata-innova-tive-modelling-for-science-and-engineering/a-framework-of-variant-logic-construction-for-cellular-automata.

PoS(CENet2017)081