# A lightweight and efficient encryption scheme based on LFSR


## Guangfu Wu*
Department of information engineering
Jiangxi University of Science and Technology, Ganzhou 341000, China
E-mail:wuguangfu@126.com,
*Corresponding author

## Keke Wang
Department of information engineering
Jiangxi University of Science and Technology, Ganzhou 341000, China
E-mail:wangkeke1992@163.com

## Jinjun Zhang
PLA Special Operations University, Guangzhou, 510000, China
Email: autumn915@126.com

## Jiguang He
Centre for Wireless Communications, FI-90014,
University of Oulu, Finland
E-mail:jhe@ee.oulu.fi



**Abstract:** Privacy and trust in wireless networks have attracted plenty of attention in the information age. Various types of high-complexity stream ciphers are exploited for providing security in Global System for Mobile communication (GSM) cell phones. Therefore, this paper proposes a new algorithm, which combines the Vigenère cipher, Linear Feedback Shift Register (LFSR) and one-time pad (OTP), to reduce the computational complexity as well as improve the system security. Beneficial from the combination of their advantages, our proposed algorithm makes attack process more complicated. Particularly, when the Vigenère cipher is expanded to include alphabets, symbols, and numbers, it will become safer and difficult to be broken using frequency or brute force methods, etc. The alphabet entropies of plain and cipher texts are calculated and compared. In addition, the cipher text space is further expanded. The numerical results, obtained through JAVA programming language, illustrate that the proposed cryptosystem is safer than the conventional Vigenère cipher.



**Keywords:** Vigenère cipher; Encryption; Decryption; Linear Feedback Shift Register.

Reference to this paper should be made as follows: Wu,G. ,Wang, K. and He, J.(2016) A Modified Cryptosystem Based on Vigenère Cipher and LFSR, Int. J. Embedded Systems, Vol. xx, No. x/x/x, pp.xx–xx.



**Biographical notes:** Guangfu Wu received the Ph.D. degree in Communication and Information Systems from Xiamen University, Xiamen, China, in 2012. He is currently a Lecturer with the School of Science, JiangXi University of Science and Technology, Ganzhou, China. His current research interests include cryptography and network security, coding theory, and information theory.

Keke Wang is currently working towards the Master degree at School of computer science, JiangXi University of Science and Technology, Ganzhou, China. Her current research interests include cryptography and network security, coding theory, and information theory.

Jinjun Zhang is a lecturer at PLA Special Operations University. His research interests span wireless network security, information theory and millimetre wave MIMO.

Jiguang He is with Centre for Wireless Communications, University of Oulu, Finland, studying toward his Ph.D degree. His research interests span joint source and channel coding, wireless sensor/mesh networks, and wireless network security.

## 1 INTRODUCTION

Claude Shannon first introduced the two terms, diffusion and confusion, to capture the two basic building blocks for any cryptographic systems (Claude, 1949). His idea was to thwart cryptanalysis based on the statistical analysis. The cryptography allows two customers to exchange messages that the others cannot indentify. Companies and operators usually use this technique to keep their data secret during transmission (Kadry, 2010).

Recently, a large number of encryption algorithms have been proposed. Some are extremely cheap but unsafe such as stream cipher while some are safe but expensive like AES. Some are easy on encryption but have heavy computation during user revocation like Identity-Based Encryption (IBE) and Attribute-Based Encryption (ABE) (Li et al., 2015; Li et al., 2014). To sum up, high price should be paid in order to ensure the safety of system. However, different data has different characteristics, thus they need different encryption techniques to protect the important data from attack (Mohit, 2010). In current networks like wireless network, there exists huge amount of information to be exchanged. Most messages request low cost to keep safe, such as normal XML documents, which are widely used for the document storage and exchange over the internet (Zhang et al., 2014). For these messages, a feasible and easy implementation solution is necessary for the common users (Meslhy et al., 2013).

Symmetric key encryption algorithm becomes the first choice due to its simplicity and low cost. Even the implementation of many symmetric key encryption algorithms is usually inefficient, but satisfactory performance can be achieved with Field-Programmable Gate Array (FPGA) and Australian Securities and Investment Commission (ASIC) now (Abdellatif et al., 2014). Furthermore, the robustness of stream ciphers has been proved to be resistant to the attack if they pass the statistical tests (Maytham 2013). The stream ciphers are also employed in many applications such as Secure Socket Layer (SSL) and Wired Equivalent Privacy (WEP) protocols, thus they can be easily used in mobile communication network (Stamp, 2011). WEP is a security protocol that was designed to make a wireless local area network as secure as a wired local area network. However, WEP is a seriously flawed protocol, where the wireless access point shares a single symmetric key with all the users. In this paper, a lightweight and efficient encryption scheme is investigated. The encryption scheme can be used in GSM cell phones. GSM uses a stream cipher to encrypt the data because of the relatively high error rate in the cell phone environment. The encryption scheme can also be used in image encryption on mobile phone (Setyaningsih et al., 2012). The security problems mainly appear on three sections, i.e., encryption process at the sender, decryption process at the receiver and the transmission process (Omolara et al., 2014). There exist many transmission mechanisms used to ensure the security of the transmission over Electronic Product Code (EPC) network (Li et al., 2015). Among all these mechanisms, the cost of data transmission is proportional to the amount of the information. In order to decrease the transmission cost and improve security, two tasks have been done in this paper.

The first task is making the length of the cipher short. The length of the key is controlled to prevent duplication of the cipher text (Li et al., 2014). Therefore, making the cipher short can cut down the cost. The introduction of recursive loop operations on the original password generates a new password with a long length (Mashhadi et al., 2015). The second task is increasing the complexity of the encryption process. We take the existing algorithms' advantages to find a better encryption algorithm. Since attacking the Vigenere cipher is based on the frequency of the letters in the cipher, making the letter uniformly distributed is the main purpose of this paper. To the best of the authors' knowledge, the Linear Feedback Shift Register (LFSR)-based stream ciphers offer a rather simple structure particularly suited for a low hardware complexity implementation of symmetric encryption algorithms (Pasalic, 2009).

Based on the above ideas, a new encryption algorithm has been proposed in this paper to provide security to the information. Moreover, the cipher text space is expanded to 36 symbols including digits, the results of which are compared with the original 26 symbols cipher space. Furthermore, this algorithm can be readily applied to practical software systems (Shakshuki et al., 2005).

This work aims at making the cipher key uniformly distributed in each encryption step. The paper has the following structure: Section 2 describes the existing and related work to the proposed algorithm. Section 3 introduces the proposed new algorithm. Section 4 presents the analysis of the proposed algorithm using numerical results. Extension of cipher text space is presented in Section 5. Conclusions are drawn in Section 6.

## 2 RELATED WORK

Our proposed algorithm is a symmetric and stream cipher combined of the Vigenère cipher, LFSR, and OTP. The Vigenère cipher is one classical low-cost stream cipher; the LFSR method is applied to improve the efficiency of the confusion; and the OTP is the only provably secure encryption algorithm.

Stream Ciphers have been widely used in wireless network, especially for voice encryption (Yang 2009). Their encryption process is easy, fast and of low cost.

Vigenère cipher is a well-known stream cipher, which encrypts message by using a series of different Caesar ciphers based on the letters of a key. It converts the letters a-z in the cipher key and plain text to the numbers 0-25. In other words, the letters of the plain text plus the letters of the cipher key modulo 26 comes to the cipher (Natarajan et al., 2011). The Vigenère cipher has been regarded as safe enough for quite a long time, but it was eventually broken. People found that if the plain text is much longer than the length of cipher key, the frequency of the letter can help to find out the length of the cipher key, and then decrypt the cipher.

Encrypt $P$ using the cipher key $K$,

$$C_i=E_k(P_i)=(P_i+K_i) \mod\{26\} \quad (1)$$

And decrypt $C$ is performed similarly using the key $K$,

$$P_i=D_k(C_i)=(C_i-K_i) \mod\{26\} \quad (2)$$

Where $P = P_0 \dots P_n$ is the plain text, $C = C_0 \dots C_n$ is the cipher text, and $K = K_0 \dots K_m$ is the cipher key.

The frequency of letters can be reduced by adding the number of the characters; the Vigenère cipher can be modified from the original 26 characters to the alpha-qwerty cipher which consists of 92 characters, including digits and some other symbols. These characters are commonly used in the English language and can be input from a computer keyboard. The formula description of the extended version is similar to the original cipher. It uses modulo 92 instead of modulo 26 and cipher text $C_i$ is derived using a sequence different from plain text sequence $P_i$ (Kester ,2013; Kester, 2012).

Encryption:

$$E_k(P_1, P_2, \cdots, P_m)=(P_1+K_1, P_2+K_2, \cdots, P_m+K_m) \mod\{92\} \quad (3)$$

Decryption:

$$D_k(C_1, C_2, \cdots, C_m)=(C_1-K_1, C_2-K_2, \cdots, C_m-K_m) \mod\{92\} \quad (4)$$

If the length of the key is as long as the plain text and without repetition, it will be very hard to break like OTP cipher (Babu et al., 2010). This is also utilized in our research. A short cipher is generated first, and then is used to generate a long cipher by logical operations. If the generated cipher key is without repetition, or its length is longer than that of the plain text, the regularity of the cipher will not be found out. Therefore, the plain text will be safe (Wilson et al., 2006). The long cipher has been generated by LFSR. Moreover, LFSR can be easily implemented in hardware and can be readily analyzed mathematically. It provides very good security for transmission (Murali et al., 2008). It is often used to generate the pseudorandom bit sequences in cryptosystem to make the system as much secure as OTP (Golomb, 1967; Razzaq et al., 2012).

There is no absolutely secure encryption method in reality. If the cost of attack is higher than the value of information itself, the attack will be meaningless. Trying all the probably keys, called brute force method, can break any kinds of cipher (Priyam, 2015). The weak point is that it needs the highest cost. Actually, the frequency of the letters in the cipher text can help to break a Vigenère cipher. Thus, distributing the letters uniformly can improve the security of the system. The proposed method will use new successive keys, which depend on the initial key at each encryption step. The decryption is just the inverse process of encryption. Based on these basic theories, many encryption algorithms have been proposed and all of them are very creative, for instance, adding random padding to each byte of stream cipher (Wilson, 2006). However, this method increases the size of the cipher text. Thus we present a new method without changing the size of the cipher text.

## 3 DESCRIPTION OF THE NEW ALGORITHM

Following (Razzaq et al., 2012), we exploit LFSR to produce a key using $K_{i+1}=K_i+K_{i-1}$. Furthermore, we propose a new method that a short key was generated first, which will be used to generate a new cipher according to the length of the plain text. The generated key will be as long as the plain text. The mathematical formula of the new algorithm is given below:

$$K_i=K_{i-n}+K_{i-n+1}+\cdots+K_{i-1}) \mod\{26\}, \quad i \geq n \quad (5)$$

$$K_i=K_i \quad i < n \quad (6)$$

Where $n$ is the length of the cipher key, $K_i$ is the letters of the cipher.

The decryption process has an inverse operation of encryption in order to decipher the cipher text. The following is the detail of the encryption and decryption process.

**Encryption and Decryption Algorithm**

**Encryption**

1. Input the plain text M.
2. Input an original cipher, which would be transmitted from the sender to the receiver (The length of the cipher is determined by the length of the plain text. Longer plain text needs a longer cipher to keep the period, so that the new cipher would not be repeated).
3. Conduct logical operations to cipher according to the length of the plain text .The logical formula is (5) and (6).
   $n$=key.length.
   $K_i$ is the letter of the cipher
4. Generate a new cipher as long as the plain text
5. XOR the binary equivalent of the new cipher to the plain text, and get the cipher text using formula (1).

**Decryption**

1. Input the cipher text $C$.
2. Use transmission cipher to generate the new cipher $K$. The formulation is the same as the encryption process and the new cipher is as long as the cipher text $C$.
3. Apply new cipher $K$ to get plain text $P$ using formula (2).

The Encryption algorithm was implemented using JAVA programming.

**Encryption Algorithm using JAVA programming**

```
1.initialize VigenereTable[][]
2. for   rows=0 to tableRowSize{
3.       for columes=0 to   tableColumeSize {
4.       vignereTable[rows][columes]
5.                          =(rows+columes)%26;
6.        }
7. }
8. get the ASCII number of each letter Ki in key
9. for i=0 to plaintext.length{
10.        If i<key.length
11.          Ki=Ki
12.          else
13.        Ki=Ki-n+Ki-n+1 + ···+Ki-1) mod{26}
14.           key=key+Ki
15. }
16./*Extend the original key to new key using Linear
17.   operation make it as long as the plaintext*/
18.   tableEntry=vignereTable[Pi][Ki]
19.   cChar=(char)(tableEntry+65)
20.   cipherText+=cChar
21.   return   ciphertext
```

## 4 THE ANALYSIS OF PROPOSED DESIGN

In order to evaluate the proposed algorithm, there are two performance metrics to analyse. The first one is the period of the generated cipher. It must be non-periodic and irregular. It has been proved that the formulation designed in this paper can be achieved because the ciphers we get have a fix period. For instance, if the length of the original cipher is 3, the period will be 168. If the length of the original cipher is 4, the period will be 420. If the length of the original cipher is 5, the period will be more than 20000. The period will increase nonlinearly with the length of original cipher. Furthermore, with the Vigenère cipher expanded to include alphabets, symbols and numbers, the period will be much longer. Obviously, the biggest advantage of the new algorithm is that the sender can choose the shortest cipher according to the length of the plain text and meet the aim of security. The second advantage of the new algorithm is hiding the frequency of the letters in the cipher text.

The Vigenère cipher was considered unbreakable for nearly 300 years, but finally it was broken successfully by analyzing the frequency of the letters in cipher text. While the plain text is much longer than the key, the key will eventually encrypt the same alphabets previously encrypted by the key. This creates a small pattern of repeating groups of letters. If letters in cipher text are uniform, the attack will be invalid. The experimental results show that the new encryption algorithm almost reaches the goal. The experiment data is shown as follows.

Plain text: Abstract information security is more and more important in a firm's information systems. How to value the information security technologies is an important research issue recently. In this paper, the evaluation model of information security technologies is proposed based on game theory. And the information security technologies include firewall, intrusion detection system and intrusion tolerant which construct the three layers architecture. First, the value of intrusion detection system is presented .Then the relation between firewall, intrusion detection and intrusion tolerant is analysed. It is found that the detection rate and false alarm rate are affected by the performance of the firewall. Research results show that the configuration of the information security technologies determines whether these technologies realized a positive or negative value. Intrusion tolerant is determined by the loss incurred by intrusion, the cost of the redundancy of the system, and performance of firewall and intrusion detection. It is important to a firm by optimal configuration for information security technologies.

Cipher key 1: true

Cipher key 2: label

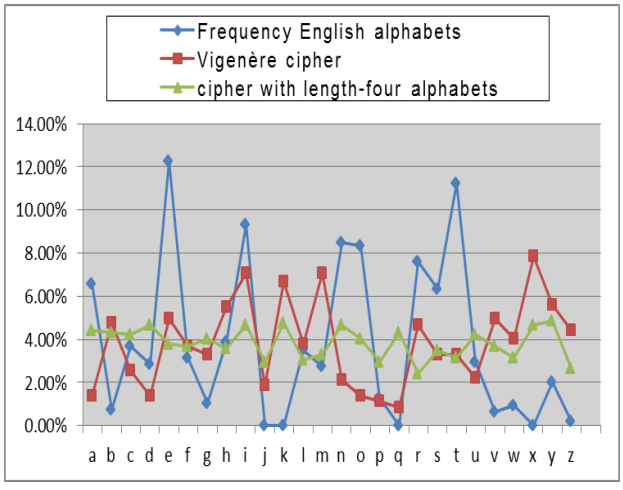
Frequency comparison between the proposed cipher and the traditional vigenère cipher is given in Table 1 and Fig. 1.

Fig.1 shows that the frequencies of the letters are almost uniform (Razzaq et al., 2012). In addition, if the cipher is longer, the letters will be more uniformly distributed. To the same plain text, if the cipher length extended to 5, such as label, the Index of Coincidence (*IC*) for a given alphabet will be smaller (Kartha et al., 2014).

**Table 1** Frequency analysis of the proposed cipher and the traditional Vigenère cipher

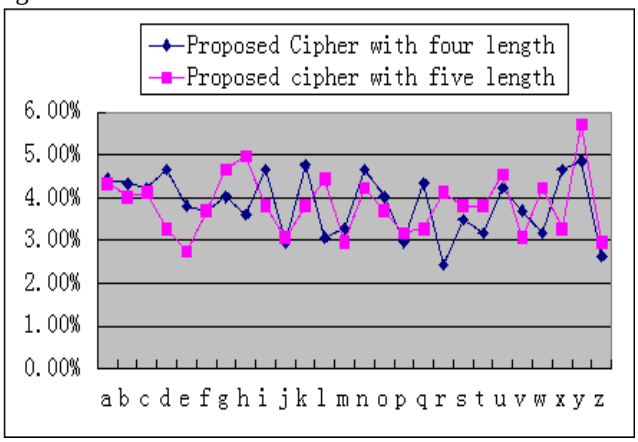
| English alphabet | Frequency English alphabets | Vigenère cipher | cipher with length-four alphabets | Cipher with length-five alphabets |
|---|---|---|---|---|
| a | 6.56% | 1.37% | 4.44% | 4.34% |
| b | 0.74% | 4.76% | 4.34% | 4.02% |
| c | 3.70% | 2.54% | 4.23% | 4.13% |
| d | 2.86% | 1.37% | 4.66% | 3.28% |
| e | 12.28% | 4.97% | 3.81% | 2.75% |
| f | 3.17% | 3.70% | 3.70% | 3.70% |
| g | 1.05% | 3.28% | 4.02% | 4.66% |
| h | 3.91% | 5.50% | 3.60% | 4.97% |
| i | 9.32% | 7.09% | 4.66% | 3.81% |
| j | 0.00% | 1.90% | 2.96% | 3.07% |
| k | 0.00% | 6.67% | 4.76% | 3.81% |
| l | 3.49% | 3.81% | 3.07% | 4.44% |
| m | 2.75% | 7.09% | 3.28% | 2.96% |
| n | 8.47% | 2.11% | 4.66% | 4.23% |
| o | 8.36% | 1.37% | 4.02% | 3.70% |
| p | 1.27% | 1.16% | 2.96% | 3.17% |
| q | 0.00% | 0.84% | 4.34% | 3.28% |
| r | 7.62% | 4.66% | 2.43% | 4.13% |
| s | 6.35% | 3.28% | 3.49% | 3.81% |
| t | 11.22% | 3.28% | 3.17% | 3.81% |
| u | 2.96% | 2.22% | 4.23% | 4.55% |
| v | 0.63% | 4.97% | 3.70% | 3.07% |
| w | 0.95% | 4.02% | 3.17% | 4.23% |
| x | 0.00% | 7.83% | 4.66% | 3.28% |
| y | 2.01% | 5.61% | 4.87% | 5.72% |
| z | 0.21% | 4.44% | 2.64% | 2.96% |

**Fig. 1.** Frequency comparison between the proposed cipher and the traditional Vigenère cipher




Regarding frequency analysis of the cipher text, the new algorithm is more difficult than traditional classical cipher. The English alphabet frequency, Vigenère cipher frequency and proposed cipher frequency are stated in the Table 1. Fig. 2 gives the frequency comparison of the proposed cipher with length four and five letters. From the Fig. 2, we easily know that there exists small difference between length four and five.

**Fig. 2.** Frequency Comparison between ciphers with different lengths




Obviously, small cipher produces large or unknown periods. Thus, it is difficult to break the proposed cipher compared to traditional Vigenère cipher. The expression of *IC* is in the form of

$$IC=\frac{\sum_{i=a}^{i=z} f_i(f_i-1)}{N(N-1)} \quad (7)$$

Where $N$ is the length of the text and $f_i$ is the number of each letter. When the *IC* is smaller, the frequency will be more uniform. However, the effect will be very small when the cipher length is long enough, which means the period of generated cipher is longer than that of the plain text.

*IC* is computed according to (7). The *IC* of an arbitrary string of English text is 0.065, but for a random string alphabet, the *IC* is 0.038. Thus, if the *IC* is closer to 0.038, the more likely that we have a random polyalphabetic cipher. The aim of our encryption method is to make the frequencies of plain text become more uniform distributed or nearly the same for each letter, that is to say, the *IC* is close to 0.038.

Chi-square test is the degree of deviation for a statistical sample between actual observation value and the inference theory value. The Chi-square value is calculated by

$$\chi^2=\sum_{i=1}^{k}\frac{(A_i-E_i)^2}{E_i} \quad (8)$$

When Chi-square value is smaller, the deviation is smaller. If the actual observation value is completely equal to the theory value, then the Chi-square value will be 0.

Variance is a dispersion degree measure of discrete random variable or a set of data. Variance in probability theory is employed to measure the degree of deviation between random variables and the mathematical expectation (i.e. mean)

$$D(X)=\sum_{i=1}^{n} p_i(X_i-\mu)^2 \quad (9)$$

$$\mu=E(X) \quad (10)$$

According to the formulation (9), the greater the variance, the greater the data distribution dispersed.

Entropy is a measure of uncertainty, $p_i$ is used to express the uncertainty probability of the emergence of information *i*. The whole information uncertainty (with $n$ letters) can be expressed by formulation (11).

$$S=-K\sum_{i=1}^{n} p_i \log_2(p_i) \quad (11)$$

Where $K$ is a constant, here, $K$ =1.When the occurrence probability of each letter is equal, $p_i$ =1/$n$. $S$ gets the maximum value 4.700, that is, the entropy reaches the biggest value 4.700. The more equality of the information, the greater the entropy will be.

**Table 2** Cryptanalysis of cipher text

| Cryptanalysis | Vigenere cipher | Cipher length is 4 | Cipher length is 5 |
|---|---|---|---|
| *IC* | 0.0482 | 0.03872 | 0.03869 |
| Chi-square statistic | 252.4444 | 31.7222 | 30.8889 |
| Variance | 57.8685 | 58.0367 | 58.3381 |
| Standard deviation | 7.6071 | 7.6182 | 7.6379 |
| Alphabet entropy | 4.4946 | 4.6710 | 4.6734 |

The alphabet entropy of new encryption algorithm approximates to the maximum entropy. From the definition of entropy, Table 2 demonstrates that the new encryption method is stronger. The *IC* of new algorithm is much smaller than that of the original Vigenère cipher, and there is a larger deviation in the new encryption method compared to that in Vigenère cipher. In a normal English text of alphabet *a-z*, the standard deviation is normally 3.80868 and the variance is 14.50603 (Kester et al., 2013). Both of them have been improved obviously in the new proposed algorithm. Moreover, when the length of the cipher is increased from 4 to 5, the deviation has minor improvement.

## 5 EXTENSION OF CIPHER TEXT SPACE

As it is mentioned above, if the cipher text space is expanded to 36 symbols (include 26 alphabets and 10 digits), the key period will be longer and it will greatly increase the security of the cipher. Furthermore, if both the cipher text space and cipher key space are expanded to 36 symbols, the cipher will be safer, which is demonstrated by the experimental data.

The frequency of the alphabets has changed in Table 3 (the same cipher key encrypts the same plain text).

Many data has been calculated to make a comparison of different encryption spaces, shown in Table 4. It can be figured out from the entropy of the cipher text that the method greatly increases the security of the cipher. If the cipher text space consists of only 26 symbols with length five cipher key, the entropy of the cipher text is 4.6734. However, when only the cipher text space has been expanded to 36 symbols, the entropy of the cipher text is 5.0824. While the cipher key space is also expanded to 36 symbols, the entropy of the cipher text is 5.1289, which is larger than the other two values. It indicates that the cipher text become safer. The distribution of the symbols in the cipher text will be more evenly. When the cipher text space has been expanded to 36 symbols, the maximum entropy of the cipher text is 5.1699. Meanwhile the entropy of the cipher text with the proposed encryption method is 5.1289; it is close to the maximum value.

**Table 3** Frequency analysis of different encryption spaces

| Encryption space | Encryption space is 26 with length five cipher | Cipher text space is 36 and cipher key space are 26 | Both cipher text space and cipher key space are 36 |
|---|---|---|---|
| a | 4.34% | 2.65% | 1.59% |
| b | 4.02% | 3.28% | 2.33% |
| c | 4.13% | 2.33% | 3.07% |
| d | 3.28% | 1.69% | 3.92% |
| e | 2.75% | 1.91% | 2.44% |
| f | 3.70% | 2.12% | 1.91% |
| g | 4.66% | 2.12% | 2.97% |
| h | 4.97% | 2.44% | 3.5% |
| i | 3.81% | 1.91% | 2.97% |
| j | 3.07% | 2.33% | 2.44% |
| k | 3.81% | 1.38% | 3.07% |
| l | 4.44% | 2.01% | 4.24% |
| m | 2.96% | 1.27% | 3.39% |
| n | 4.23% | 2.97% | 1.8% |
| o | 3.70% | 2.44% | 3.81% |
| p | 3.17% | 2.22% | 2.97% |
| q | 3.28% | 1.91% | 3.39% |
| r | 4.13% | 3.07% | 2.33% |
| s | 3.81% | 3.07% | 2.86% |
| t | 3.81% | 3.71% | 2.86% |
| u | 4.55% | 4.56% | 2.54% |
| v | 3.07% | 2.97% | 2.44% |
| w | 4.23% | 4.03% | 2.86% |
| x | 3.28% | 3.28% | 3.39% |
| y | 5.72% | 5.72% | 2.97% |
| z | 2.96% | 2.97% | 1.8% |
| 0 | 0 | 4.13% | 2.86% |
| 1 | 0 | 3.39% | 3.18% |
| 2 | 0 | 3.71% | 3.18% |
| 3 | 0 | 2.86% | 1.06% |
| 4 | 0 | 2.12% | 2.54% |
| 5 | 0 | 2.54% | 2.86% |
| 6 | 0 | 3.92% | 2.12% |
| 7 | 0 | 3.6% | 2.75% |
| 8 | 0 | 2.54% | 3.07% |
| 9 | 0 | 0.85% | 2.54% |

**Fig. 3.** Frequency comparison of different encryption spaces

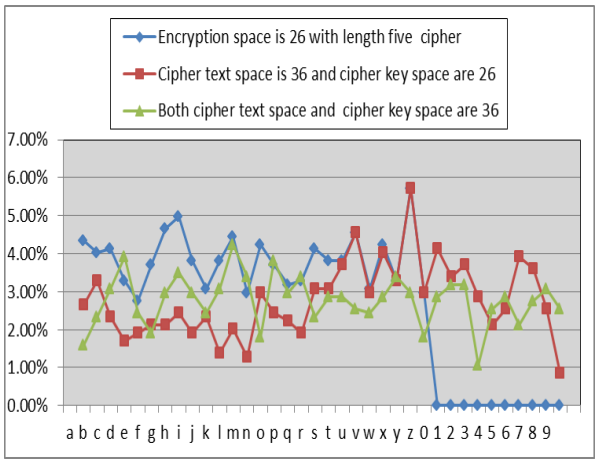



**Table 4 Comparison of different encryption space**

| Cryptana-lysis | Cipher text space is 26 with length five cipher | Cipher text space is 36 and cipher key space is 26 | Both Cipher text space and cipher key space is 36 |
|---|---|---|---|
| *IC* | 0.03869 | 0.0302 | 0.02828 |
| Chi-square statistic | 30.8889 | 118.1538 | 52.4615 |
| Variance | 58.3381 | 98.1955 | 102.7329 |
| Standard deviation | 7.6379 | 9.9094 | 10.1357 |
| Alphabet entropy | 4.6734 | 5.0824 | 5.1289 |

## 6 CONCLUSION

The proposed encryption method has smaller *IC* which indicates a stronger approach of the new algorithm. We employ the original cipher to create a new cipher, whose period is longer than that of the plain text. Therefore, the security has been improved as long as the length of the cipher is enough. It is meaningless to increase the length of the cipher anymore. The proposed encryption method is a modified combination of the Vigenère cipher, LFSR and OTP. The purpose for this method is to improve the security of the information communication while keep the stream cipher's low cost property. OTP is safe but it is difficult to implement, thus the new algorithm in this paper is trying to resolve it. The experimental results show that the algorithm has been significantly improved compared to the conventional. The proposed solution has been found to be secure for frequency analysis attack since the key period is larger than that of the plain text. Meanwhile, in our proposed algorithm, calculating the shortest length of the cipher could cut down the transmission cost. Increasing length of the cipher results in safer transmissions. Furthermore, the cipher text space has been expanded. In this case, the symbol distribution of the cipher text will become more evenly and subsequently the security will be improved significantly. Furthermore, the proposed encryption system can be applied to email and communication systems as well.

## ACKNOWLEDGEMENT

This work was supported in part by the National Natural Science Foundation of China (Nos. 11461031, 61462034, and 61562037), by Natural Science Foundation of Jiangxi, China (No. 20151BAB217016).

## REFERENCES

Abdellatif, K., Roselyne, C.A., Mehrez, H.,(2014),"Low cost Solutions for secure remote reconfiguration of FPGAs"

International Journal of Embedded Systems, Jan, Vol. 6, Issue 2-3, pp. 257-265.

Babu, K.R., Kumar, S.U. and Babu, A.V.( 2010) "A Survey on Cryptography and Steganography Methods for Information Security" International Journal of Computer Applications Vol.12, No.2,pp.49-53.

Claude, E.(1949) "Communication Theory of Secrecy Systems", Bell System Technical Journal, Vol.28-4, pp.656-715.

Golomb, S. W. (1967) "Shift Register Sequences." San Francisco, CA: Holden-Day.

Stamp, M.(2011). "Information Security: principles and practices". John Wiley & Sons, Inc., Hoboken, New Jersey. pp.50-52.

Kartha, R.S. and Paul, V. (2014) "Survey: Recent Modifications in Vigenere Cipher" IOSR Journal of Computer Engineering(IOSR-JCE) ,Vol. 16, No. 2, pp. 49-53.

Kester, Q.A.(2015.3) "A hybrid cryptosystem based on Vigenère cipher and columnar transposition cipher", International Journal of Advanced Technology & Engineering Research (IJATER).Vol.3, No.1, pp.141-147.

Kester, Q.A.(2012) "A cryptosystem based on Vigenère cipher with varying key", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol.1, No.10, pp.108-113.

Kumar, M., Reena, M., Rakesh, K.P. and Poonam S.(2010). "Comparing Classical Encryption with Modern Techniques", S-JPSET, Vol.1, No.1:pp.49-54.

Li, J., Li, J.W., Chen, X.F., Jia, C.F., and Lou W.J. (2015). Identity based Encryption with Outsourced Revocation in Cloud Computing. IEEE Transactions on Computers. Vol.64,No.2, pp.425-437.

Li, J., Huang, X.Y., Li, J.W., Chen, X.F., Xiang, Y. (2014). Securely Outsourcing Attribute based Encryption with Check Ability. IEEE Transactions on Parallel and Distributed Systems, Vol.25,No.8, pp. 2201-2210.

Li, J., Chen, X.F., Li, M.Q., Li, J.W., Lee, P., Lou, W.J.(2014). "Secure Deduplication with Efficient and Reliable Convergent Key Management". IEEE Transactions on Parallel and Distributed Systems, 25(6), pp. 1615-1625.

Li, Z.W., Li, Q., Xu, Z.B., Jiang, H., Li, K.C.(2015),"A secured Transmission model for EPC network" International Journal of Embedded Systems, Vol. 7,Issue 3-4, pp. 324- 333.

Mashhadi, S. and Dehkordi, M.H. (2015) "Two Verifiable multi Secret sharing schemes based on nonhomogeneous linear Recursion and LFSR public-key cryptosystem" Information Sciences Vol. 294, pp.31–40.

Maytham, M.H., Kenji, Y. and Ali, M.S.(2013). "RC4-2S :RC4 Stream Cipher with Two State Tables", Information Technology Convergence Security, pp.13-20.

Meslhy, E., Abdelakader, H.and El-Etriby, S. (2013) "Data Security Model for Cloud Computing" Journal of Communication and Computer Vol. 10, pp. 1047-1062.

Murali, P. and Senthilkumar, G. (2008) "Modified Version of Playfair Cipher using Linear Feedback Shift Register" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12,pp.26-29.

Natarajan, S., Ganesan, M., Ganesan, K.(2011) "A Novel Approach for Data Security Enhancement Using Multi Level Encryption Scheme" Sairam Natarajan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2,No.1, pp. 469-473.

Omolara, O.E., Oludare, A.I. and Abdulahi, S.E. (2014), "Developing a Modified Hybrid Caesar Cipher and Vigenère Cipher for Secure Data Communication" Compute Engineering and Intelligent Systems ,Vol.5, No.5. pp.34-46.

Pasalic, E.(2009) "On Guess and Determine Cryptanalysis of LFSR-Based Stream Ciphers", IEEE Transactions on Information Theory, Vol. 55, No. 7, pp.3398-3406.

Priyam, A.(2015) "Extended Vigenère using double Transposition Cipher with One Time Pad Cipher" Intl J Engg Sci Adv Research June; Vol 1,No.2,pp.62-65.

Razzaq, A. and Mahmood, Y. ( 2012) "Strong Key Machanism Generated by LFSR based Vigenère Cipher," The 13th International Arab Conference on Information Technology ACIT'. Vol. 10, No.13, pp.544-548.

Seifedine, K. and Mohahad, S.(2010). "An Improvement of RC4 Cipher Using Vigenere Cipher", International Journal of Computational Intelligence and Information Security Vol.1 No.3. pp. 83-92.

Setyaningsih, E.,Iswahyudi, C., Widyastuti, N., (2012), "Image Encryption on Mobile Phone using Super Encryption Algorithm",TELKOMIKA,Vol.10,No.4, pp.815-824.

Shakshuki, E., Luo, Z.H. and Gong, J. (2005)."A Security System Implementation Using Software Agents", International Journal of High Performance Computing and Networking -Vol. 3, Issue 5-6, pp. 366-377.

Wilson, P.I. and Garcia, M.(2006) "A Modified Version of the Vigenère Algorithm" IJCSNS International Journal of Computer Science and Network Security, Vol.6 No.3, pp.140-143.

Yang, X., Chen, H.H., Du, X.J. and Mohsen, G.(2009). "Stream-Based Cipher Feedback Mode in Wireless Error Channel", IEEE Transaction on Wireless Communications, Vol.8, No. 2, pp.622-626.

Zhang, J.Q.,Varadharjan, V. Mu, Y.(2005)."Secure Distribution and Access of XML Documents" International Journal of High Performance Computing and Networking, Vol.3, Issue 5-6, pp. 356-365.