The Design of Wide Interval FH Sequences Based on AES

Hui SHI, Guan-Lin Li, Xin-Rong GUAN, Jing GONG, Yuan-Qing DENG, Bin GAO

College of Communications Engineering, PLA University of Science and Technology, Nanjing, China

*hpky@126.com

*Corresponding author

Keywords: Frequency Diversity, Frequency Hopping (FH), AES, Wide Interval, CTR.

Abstract. For utilization of frequency diversity in frequency hopping (FH) communication to enhance the anti-jamming performance of FH system and improve the transmission reliability under multipath fading channel, FH communication usually hope the launch of the two carrier frequency interval is than a specified value in the adjacent frequency hopping time slot. This paper designs a new FH sequences generator based on AES block cipher, and tests the interval characteristics of the FH sequences produced by the generator. The test results show that the interval of the FH sequences are similar to the ideal values, which can satisfy the requirements of wide interval characteristics of FH codes in the FH communication systems.

Introduction

FH communication has many outstanding advantages such as good concealment, strong abilities of anti-jamming and anti-fading, easy to establish multiple accesses networking and so on, extensively used in the field of wireless communication system especially in the field of military communication. There are three key technologies in FH communication, which are FH sequence generation, frequency synthesis and synchronization technology. Among them, the frequency hopping sequence is used to control the frequency hopping radio frequency variation, and determines on the safety performance of frequency hopping communication system from technology. With high complexity, high security intensity of AES algorithm can improve the FH sequence performance, and improve the security of FH communication system. Balance characteristics, Hamming correlation property, wide interval characteristics and sequence cycle length, generation rate, etc. are used to measure the performance of the FH sequences[1,2]. This paper mainly studies the wide interval characteristics of the new FH sequence generator.

The Wide Frequency Interval Characteristics of FH Sequences

Diversity technology is a typical anti-fading technology, which can greatly improve the multipath fading channel transmission reliability. In order to utilize the frequency diversity of FH communication system to enhance the abilities of anti-interference and anti-MAI(Multiple Access Interference), FH communications system usually hope FH sequences meet the requirements of big enough interval, that is the two carrier frequencies intervals transmitted by the neighboring frequency codes should be wide enough to exceed a given value $D$.

Wide frequency interval is desired, i.e. let $d = |f_{i+1} - f_i|$ be the interval of FH sequences. The value of $d$ is bigger, the FH interval is greater and the ability of anti-tracking of the frequency hopping communication system is stronger. Because $\{f_i\}$ is a Bernoulli random sequence, then the interval of $q$-ray Bernoulli FH sequence probability distribution satisfies [3]:

$$P(d = k) = \begin{cases} \frac{1}{q}, & k = 0 \\ \frac{2(q-d)}{q^2}, & 1 \leq k \leq q-1 \end{cases}$$

(1)
Then the expectation of given interval $E(d)$ can be calculated as:

$$E(d)=\sum_{k=-q}^{q-1} k \cdot \frac{2(q-k)}{q^2} = \frac{2}{q^2} \sum_{k=-q}^{q-1} k \cdot (q-k) = \frac{2}{q^2} \sum_{k=-q}^{q-1} (qk-k^2)$$

$$= \frac{2}{q^2} \left[ \frac{(1+q-1)(q-1)}{2} - (q-1) \cdot q \cdot (2q-1) \right]$$

$$= \frac{1}{q^2} \left[ (q^2-1) -(q-1)(2q-1) \right] = \frac{1}{q} [q^2 - q - \frac{2q^2}{3} + q - \frac{1}{3} ]$$

$$= \frac{q^2 - 1}{3q}$$

$$\Rightarrow q \rightarrow \infty, E(d) \approx \frac{q}{3}$$

In the above formula, $q$ represents the length of the FH sequences. When $q \rightarrow \infty$, $E(d) \approx \frac{q}{3}$, this is FH sequences wide interval characteristics under the ideal state.

**The Structure of new FH Sequences Generator Based on AES Algorithm**

AES algorithm is the most famous private key symmetric block cipher with a 128-bit block size and a key size of 128, 192 or 256 bits [4]. The number of iterations associated with the key is in turn 10, 12 and 14 rounds. Many top level password analysis experts in-depth study shows that the AES algorithm is the best security performance of the block cipher algorithm by far. So far there is no one can find the effective method of crack. In the AES algorithm, both CTR (counter) operation mode and OFB (Output Feedback) operation mode can be applied to generate FH sequences.

![Figure 1. The FH Sequences Generator Based on AES Algorithm CTR Mode.](image)

The main reason for the CTR mode is to make the cycle of FH sequence as long as possible, in order to meet the performance requirements of the FH sequence generator. Because the CTR length is 128 bits, the long cycle is $2^{128} \approx 3.4 \times 10^{38}$. Because of the one-to-one mapping characteristics of AES encryption algorithm, which can guarantee the output FH sequence cycle reaches $2^{128} \approx 3.4 \times 10^{38}$. The cycle period is not only far longer than the traditional method of FH sequence cycles, but also longer than the FH sequence cycle generated by the OFB mode.
The FH sequences generator based on the CTR Mode AES algorithm is illustrated in the Fig. 1. Programming to implement the FH sequence generator based on CTR mode of block cipher AES algorithm. The initial value of IV is from the 0, and then the generator produces 7813 sets of data (128 bits) in each group in turn, so there are 1000000 bits of the first set of random FH sequence, denoted by No.1. Then the initial value of IV plus 1, the generator produces the second group of 1000000bits of random FH sequence again, and so on. Eventually there are 100 set of 1000000 bits of FH sequences, with No. 1 to No. 100 respectively, which can be used to research the wide interval characteristics of FH sequences produced by the proposed FH sequence generator.

The Wide Interval Characteristics of the FH Sequences

The paper tests on the wide interval characteristics of the 100 groups FH sequences above. Due to space limitations, here are just the first 40 sets test results and the test results are shown in Table 1.

Table 1. The Wide Interval Characteristics Test Results of No.1-No.40 FH Sequences.

<table>
<thead>
<tr>
<th>No.</th>
<th>$V_{ave}$</th>
<th>No.</th>
<th>$V_{ave}$</th>
<th>No.</th>
<th>$V_{ave}$</th>
<th>No.</th>
<th>$V_{ave}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>84.99</td>
<td>11</td>
<td>85.34</td>
<td>21</td>
<td>85.95</td>
<td>31</td>
<td>85.35</td>
</tr>
<tr>
<td>2</td>
<td>85.18</td>
<td>12</td>
<td>85.23</td>
<td>22</td>
<td>85.37</td>
<td>32</td>
<td>85.38</td>
</tr>
<tr>
<td>3</td>
<td>84.83</td>
<td>13</td>
<td>85.36</td>
<td>23</td>
<td>85.02</td>
<td>33</td>
<td>84.99</td>
</tr>
<tr>
<td>4</td>
<td>85.44</td>
<td>14</td>
<td>85.28</td>
<td>24</td>
<td>85.46</td>
<td>34</td>
<td>85.17</td>
</tr>
<tr>
<td>5</td>
<td>85.95</td>
<td>15</td>
<td>85.35</td>
<td>25</td>
<td>84.85</td>
<td>35</td>
<td>84.83</td>
</tr>
<tr>
<td>6</td>
<td>85.33</td>
<td>16</td>
<td>85.39</td>
<td>26</td>
<td>85.36</td>
<td>36</td>
<td>85.44</td>
</tr>
<tr>
<td>7</td>
<td>85.02</td>
<td>17</td>
<td>84.99</td>
<td>27</td>
<td>85.27</td>
<td>37</td>
<td>85.95</td>
</tr>
<tr>
<td>8</td>
<td>85.46</td>
<td>18</td>
<td>85.18</td>
<td>28</td>
<td>85.23</td>
<td>38</td>
<td>85.33</td>
</tr>
<tr>
<td>9</td>
<td>84.85</td>
<td>19</td>
<td>84.83</td>
<td>29</td>
<td>85.36</td>
<td>39</td>
<td>85.02</td>
</tr>
<tr>
<td>10</td>
<td>85.50</td>
<td>20</td>
<td>85.44</td>
<td>30</td>
<td>85.27</td>
<td>40</td>
<td>85.46</td>
</tr>
</tbody>
</table>

From Table 1, the following conclusions can be obtained:

① Each group interval of FH sequences is about fluctuations near 85. The interval average of 100 groups FH sequences is 85.2689, the standard deviation is only 0.27562981.

② Under the ideal condition, the ideal value of $V_{ave}$ is 256/3, that is 85.33. So the actual interval value is very close to the ideal value. The obtained FH sequences produced by the new FH sequence generator are accord with the theory. It is shown that the proposed FH sequence generator based on AES algorithm is enough to meet the requirements of FH communication on wide interval characteristics.

Test on the FH Sequence Generation Rate

The paper also has test the FH sequence generation rate produced by the generator based on AES algorithm as shown in figure 1. The test computer configuration is Core i3-3110m CPU, the CPU frequency is 2.4 GHz and the memory is 4.0 G. With the computer generated 100 groups of 1 million-bit binary FH sequences share 2 minutes and 23 seconds, the average generation of 1 groups of 1 million-bit binary the FH sequence takes 1.43 seconds. A 1 million-bit binary frequency hopping sequence is equivalent to 125000 FH codes, that is to say number 87412 FH sequences can be produced every second, enough to meet the application requirement of high speed FH. Due to adopt the CTR mode of AES algorithm as shown in Fig.1, the FH sequence cycle is $2^{128} \approx 3.4 \times 10^{38}$, far longer than the current FH sequence generator cycle, safety performance is better.

Summary

The paper puts forward a new structure of the FH sequences generator based on CTR mode of the AES algorithm. Programming tests the main technical performance of FH sequences generated by this method. The research results show that FH sequences generated by the method are high safety
performance, good technical performance and production speed is much faster than existing methods, which can meet the high speed and high security strength the application requirement of frequency hopping.

Acknowledgment

This work was financially supported by the National Natural Science Foundation of China (No. 61501512) and Natural Science Foundation of Jiangsu Province(No. BK20150718).

Summary

If you follow the “checklist” your paper will conform to the requirements of the publisher and facilitate a problem-free publication process.

References


