Front. Electr. Electron. Eng. China (2006) 3: 301–306
DOI 10.1007/s11460-006-0041-0

RESEARCH ARTICLE

LI Zan, CHANG Yi-lin, CAI Jue-ping, WANG Yu-min

Structure of frequency hopping sequences family based on block cipher

Abstract A novel family of frequency-hopping (FH) sequences based on iterated block cipher is proposed for frequencyhopping multiple-access (FHMA) communications. The design offers a class of nonlinear FH codes with high security, large linear span and a uniform spread over the entire frequency bandwidth. Moreover, FH sequences among the family are independent from each other and they perform as well as random patterns in terms of multiple access interference in anti-jamming applications. With the performance of packet error and throughput for FHMA network being derived in theory, many numerical results of the 3DES sequences are presented, comparing with those of shift register sequences and chaotic FH sequences. Efficiently implemented in field programmable gate arrays (FPGA), the generator prototype of the proposed sequence has been realized and incorporated into fast FH radio.

Keywords block cipher, FH sequences, FHMA, VHDL, FPGA

1 Introduction

With the excellent performance in anti-jamming, anti- fading and multiple accesses, FH communication is now widely used in modern military applications. As one of the key techniques in FH communication, the generation of FH sequences determine the transmission performance of FH communication systems to a large extend. Most algebraic designs for frequency hopping codes are based on properties of finite fields such as shift register sequences or reed-solomon (RS) codes [1–4], which are inherently weak in jamming because of their shorter linear span. Some chaotic frequency hoppers [5–8] possess ideal linear complexity, where a shift-register-sequence perturbation should be introduced to circumvent the finite word length effect for their hardware implementation. In this paper, a construction of a novel FH code family is described based on the encrypted mechanism of block cipher. The sequences are shown to have high security, long periods, large linear span, and they produce good performances of multiple-access for FHMA networks.

Translated from *Acta Electronic Sinica,* 2005, 33(4): 620–623 (in Chinese)

LI Zan (✉), CHANG Yi-lin, WANG Yu-min
State Key Laboratory of ISN, Xidian University, Xi'an 710071, China
E-mail: zanli@xidian.edu.cn

CAI Jue-ping
School of Microelectronics, Xidian University,
Xi'an 710071, China

2 FH sequences family based on block cipher

2.1 Generation structure of FH sequences

In the FHMA network, two kinds of important information for synchronization are available for all transceivers. One is the network TOD, the other is the transceiver's identification (ID). It is reasonable to refer to the FH sequences generation process as a kind of cryptography problem. The TOD is known to every one, so it is plaintext. Since the transceiver's ID shared by the sender and the receiver is unique and secret, it becomes the encryption key. The FH code is the cipher text generated by TOD and key. Based on the encrypted mechanism of DES block cipher [7, 8], a novel generator of FH sequences based on the triple encryption scheme 3DES is proposed, as shown in Fig. 1 [9, 10].

In this generator, the 64 bit TOD is divided into 8 bytes P_1, P_2 and $Z_1, Z_2, \cdots, Z_6$, while the key is 144 bits, which is composed of three independent seed keys of 48 bits: key 1, key 2 and key 3. S_{box1} to S_{box3} are three 8×8 substitution boxes (S_{box}). To generate a FH code, the so-called round function, the dashed part in Fig. 1, completes a 16-round iteration according to

$$\begin{cases} P_{2j}^{i+1} = P_{2j-1}^{i} \oplus K^{i} \oplus z_1^{i} \\ P_{2j-1}^{i+1} = S_{boxj}(P_{2j}^{i+1}) \oplus P_{2j}^{i} \oplus z_2^{i} \end{cases}, j = 1,2,3, \quad i = 1,2,\cdots,16 \quad (1)$$

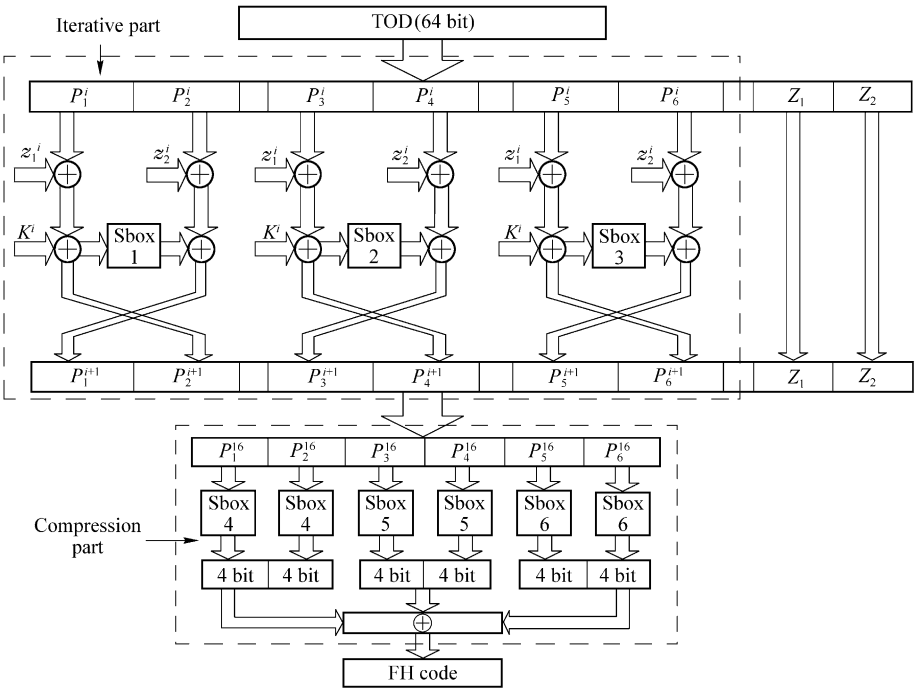

Fig. 1 Generation structure of FH sequences based on block cipher

with i denoting the round number and symbol $\oplus$ representing binary operation of XOR, and each round output $P_j^{i+1}(j=1,2)$ acts as the input of the next round. Note that

$$\boldsymbol{z}_n^i=\begin{cases}Z_n, & i=8,16\\ 0, & \text{others}\end{cases}, i=1,2,\cdots,16,\ n=1,2 \tag{2}$$

k^i is the ith round subkey generated by key schedule under the control of the three seed keys, respectively. After 16 round iterations, the certain n bits $\{p_1,p_2,\cdots,p_n\}$ from the outputs $P_j^{16}(j=1,2)$ are chosen and compressed as:

$$\begin{aligned}C=&\{S_{\text{box}4}(P_2^{16})\oplus S_{\text{box}5}(P_4^{16})\oplus S_{\text{box}6}(P_6^{16})\}\\&+\{S_{\text{box}4}(P_1^{16})\oplus S_{\text{box}5}(P_3^{16})\oplus S_{\text{box}6}(P_5^{16})\}<<4\end{aligned} \tag{3}$$

where << represents left shift operator. After the compressing, certain n bits $\{c_1,c_2,\cdots,c_n\}$ from the outputs C are chosen as the resultant FH code, i.e. $f(\text{TOD})=\sum_{i=1}^{n}c_i2^{n-i}$.

2.2 Performance analysis and simulation results

Following the concepts of diffusion and confusion suggested by Wang and Liu [11], the generated FH sequences based on 3DES block cipher have appealing integrated performances for FHMA communications. Since no analytical results so far are available to conduct performance comparison for pseudorandom number (PN) sequences, we depend more or less upon a statistical approach.

2.2.1 Security

The security of the FH sequences is determined by the encryption mechanism of the block cipher. Being the only nonlinear factor in the scheme, the substitution boxes with cryptographic properties of regularity, differential uniformity, robustness and strict avalanche characteristics make the principles of diffusion and confusion be thoroughly performed through 16 round iterations [11]. Moreover, the design of a good key schedule is also necessary to strengthen the cryptosystem without changing any parameters. Adopting the triple encryption, the encrypted key is lengthened by the three independent seed keys, which makes the scheme secure enough against brute-force attack and immune from linear attack, while the complexity of key searching is 2^{144}. As an opponent can hardly have access to the real plaintext-cipher text pairs, it is difficult to launch the knownplaintext and chosen-plaintext attacks.

2.2.2 Uniform distributions

In order to enhance the performance of anti jamming and multiple accesses, FH sequences are required to uniformly distribute in the frequency band. In this paper the standard chi-squared (χ^2) test is performed to compare the frequency hopper's output to the desired uniform distribution. FH sequences with equal symbol distribution can increase electrical and electromagnetic invisibility. Assumption H_0: FH sequences uniformly distribute in the frequency band, obeying Pearson theory statistical value χ^2 could be

obtained with

$$\chi^2 = \sum_{t=1}^{k} \frac{[\text{num}(X_t) - NP_t]^2}{NP_t} \quad (4)$$

when N is large enough ($N \geq 50$), the statistical valve obey the χ^2 distribution of freedom $k-r-1$. If $\chi^2 < \chi^2_{(k-r-1);\alpha}$, the assumption H_0 could be accepted at the level of α . There are two types of standards to evaluate the uniform distribution:

1) Equal distribution evaluation: the probability density of FH sequences in a certain frequency band should uniformly distribute, i.e., $P_t = 1/q$. And $\text{num}(X_t)$ is the times of the frequency point $f_{p_t}, t \in (1,2,\cdots,q)$ occurs, and f_{p_t} belongs to frequencies set $\{f_i\}, i = 1,2,\cdots,N$. With the parameters $r = 0, k = q = 2^6$, the creditable range of the assumption H_0 with $\alpha = 0.05$ is $\chi^2_{(k-r-1);\alpha} = \chi^2_{(63);\,0.05} = 82.244\,7$.

2) Continuous property evaluation: the consecutive frequency points in the FH sequences should be uniformly distributed, and $P_t = 1/q^2$. $\text{num}(X_t)$ is times of a certain consecutive set of frequency point in the FH sequences set $\{f_i\}, i = 1, 2\cdots, N$. With parameters $r = 0$ and $k = q^2 = 64^2$, the creditable range of the assumption H_0 with $\alpha = 0.05$ is $\chi^2_{(k-r-1);\alpha} \approx (z_\alpha + \sqrt{2n-1})^2/2 = 4\,244.7$. With different keys and TODs, the simulation results of the sequences ($N = 2^{16}$) are listed in the Table 1.

Table 1 Simulation results of uniform distributions

No.	TOD	KEY	Equal distribution evaluation	Continuous distribution evaluation
			χ^2	
1	000 000	ACBCD2114DAE1577	65.007 8	4 046.0
2	000 000	C6DBF4C91A3CDA2F	71.781 3	3 943.8
3	000 1	169B340989C1D32C	65.789 1	4 000.3
4	14E6F	ACBCD2114DAE1577	75.328 1	4 100.0
5	3BB00	C6DBF4C91A3CDA2F	71.664 1	4 036.3
6	000 001	169B340989C1D32C	60.959 0	3 860.8
7	3A019	ACBCD2114DAE1577	61.498 0	3 985.3
8	432 002	C6DBF4C91A3CDA2F	74.029 3	4 091.3
9	0BA38	169B340989C1D32C	68.582 0	4 145.0

2.2.3 *Independence*

Another chi-squared test is performed to verify the independence between two adjacent outputs. The independence of the FH sequences has been tested with the sequences $F_0 = \{f_0, f_1, \cdots\}$ and their shifted ones $F_i = \{f_{0+i}, f_{1+i}, \cdots\}$ $(i = 1, 2, \cdots, 500)$ over ten runs. Figure. 2 gives χ^2 independent test results of the block cipher based FH sequences compared with M sequences and the logistic mapped chaotic sequences [5,7] using random seeds, which have the degrees of freedom $(q-1)^2 = 255^2$. In Fig. 2, the chaotic sequence generator shows substantial fluctuations, while there is no any abnormal chi-squared point in the proposed sequences and M sequences. Moreover, more than 95 percent of the observations are less than 65 604.561 91 following Eq. (5), which indicates that the 3DES sequences are independent. So they have an obvious advantage if a jamming signal is present because it can reduce detectability or trackability of the FH signal.

$$\text{prob}\,(\chi^2 > 65\,604.561\,91) = 0.054\,3 \quad (5)$$

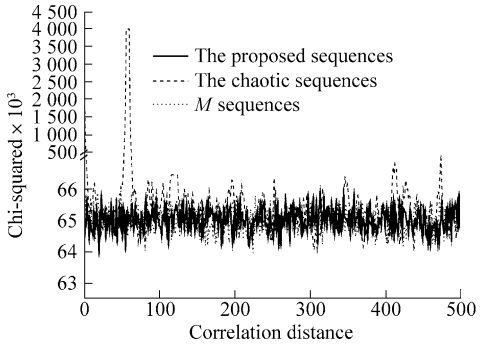

Fig. 2 Independence test of FH sequences

2.2.4 *Linear complexity*

Large linear complexity is an important factor for Bluetooth applications that require high security, which makes their analysis and synthesis difficult by unintended users. The linear span of a sequence is the shortest degree of linear recursion that the sequence satisfies. For M sequences of period $r^L - 1$, its linear span is just the exponent L, which causes the corresponding FH sequence to be easily reconstructed by a jammer from a short observation of the sequence. The linear span of purely random sequences is roughly half of the sequence length [13]. The proposed Bluetooth hopping patterns have nearly optimum large complexity similar to that of the chaotic FH sequences with logistic map function $g(x) = 4x(1-x)$ while being much larger than others. The linear spans, computed by Massey algorithm [12], are given in Table 2.

Table 2 Linear span of FH sequences

	FH code bits	N=200	N=400	N=600	N=800	N=1 000
Proposed	6 bits	100	198	299	397	498
sequences	8 bits	99	200	299	399	497
Chaotic	6 bits	98	197	298	398	498
sequences	8 bits	99	199	299	397	499
M	6 bits	13	13	13	13	13
sequences	8 bits	138	138	138	138	138

Note: N is the sequence length observed

2.2.5 *Frequency gap*

In practical multi-hop Bluetooth applications, a wide arequency gap is desired, i.e. the two carrier frequency gaps transmitted by the neighboring frequency codes should be wide enough to exceed a given value *D*. A Bluetooth hopping sequence with ideal gaps is advantageous for improving the anti-multiple access interference (MAI) abilities of piconets in multi-hop Bluetooth systems. As discussed above, the 3DES-based BT hopping patterns is a Bernoulli sequence for its uniform distribution and good independence. Let $d=|f_{i+1}-f_i|$ be the gap of FH sequences $\{f_i\}$, then the given gap of a *q*-ray Bernoulli FH sequence probability distribution satisfies

$$P(d=k)=\begin{cases}1/q, & k=0\\ 2(q-d)/q^2, & 1\le k\le q-1\end{cases} \tag{6}$$

and the expectation of given gap can be calculated as

$$E(d)=(q^2-1)/3q\approx q/3 \tag{7}$$

Hence the probability of $d\le D$ is given by

$$P(d\le D)=\frac{2D+1}{q}-\frac{D(D+1)}{q^2} \tag{8}$$

It is obvious that a larger number of the available frequency channels will result in smaller probability of $P(d\le D)$. In Bluetooth systems that require a wide gap, if $|f_{i+1}-f_i|\le D$ then another *n* bits from the outputs $P_j^{16}(j=1,2)$ can be chosen as the resultant FH code. In this way, the probability of $P(d\le D)$ can be reduced to an extent less than 7×10^{-5} when $q=2^6, D=2$.

2.2.6 *Multiple-access performance*

In multi-hop Bluetooth networks, the unwanted interfering piconets were assumed to be operated within close proximity to the wanted piconet such that any frequency collision between the two would be viewed as interference, thus requiring a retransmission of the corrupted packet, which is detrimental for synchronous services like voice. The frequency collision statistics is highly dependent on the hopping sequence of the individual piconets. Nevertheless, as far as the authors are aware of, no multiple-access performance analysis of Bluetooth hopping sequences has appeared in open literature yet [1–5]. Here, based on the packet multiple-access model suggested for synchronized Bluetooth network, the performance of packet error and throughput of Bluetooth hopping sequences are derived in theory and validated by simulation results.

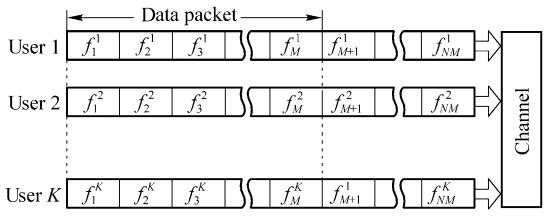

Fig. 3 The system model of FHMA network

As is often the case, in a multiple access environment, it is required that the mutual interference between transmitters should be kept at as low a level as possible. This mutual interference occurs when two or more sources transmit the same frequency slot at the same time. The system model of multi-access is shown in Fig. 4, where the working clock of the network is synchronized and transmission of each packet should occupy *M* hopping slots. It is considered that any frequency collision among the $K(K\ge2)$ users should result in the failing transmission of the packet to which the collided frequency slot belongs. Let $f_m^k(k=1,2,\cdots,K;m=1,2,\cdots,M)$ denotes the *m*th FH code of user *k* in one data packet, and then the successful transmission probability of one packet is expressed as:

$$P_r(M,K,q)=(1-q^{-1})^{M(K-1)} \tag{9}$$

Then the probability of packet error $P_e(M,K,q)$ is obtained by

$$P_e(M,K,q)=1-P_r(M,K,q) \tag{10}$$

Equations (13) and (14) are the normalized throughput of a Bluetooth network under the condition of finite piconets and of $K>>1$, respectively.

$$\eta(K,M,q,G)=\sum_{i=1}^{K} i(1-q^{-1})^{M(i-1)}\frac{G^{i-1}e^{-G}}{i!} \tag{11}$$

$$\eta(M,q,G)\overset{K>>1}{=}e^{-G[1-(1-q^{-1})^M]}\approx e^{-G\frac{M}{q}} \tag{12}$$

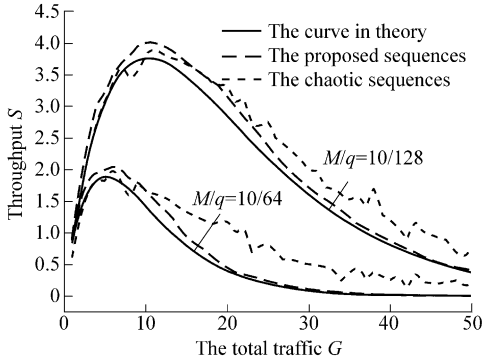

Fig. 4 The performance of $S\sim(M,q,G)$

According to the analysis above, it can be stated that the ratio of the packet length *M* to the frequency codes number *q* is the most important parameter to determine the throughput *S* and the normalized throughput η in multi-hop Bluetooth networks. Choosing the different parameters for simulations, the various FH sequences results of $S\sim(M,q,G)$ and $\eta\sim(M,q,G)$ when $K>>1$ compared with the theoretical ones are depicted in Figs. 5 and 6, respectively, in which the proposed sequences are nearly consistent with the theoretical ones. So we conclude that FH sequences produce almost as good performance as

random hopping patterns when used in multi-hop systems.

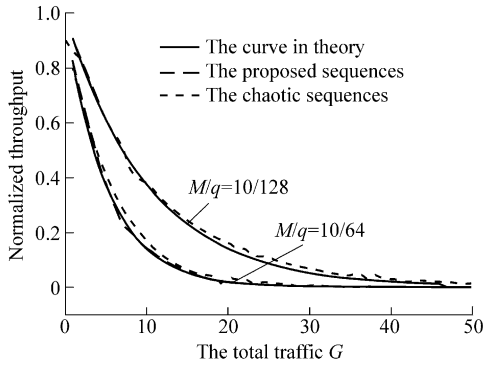

Fig. 5 The performance of $\eta \sim (M,q,G)$

3 FPGA realization

The design and analysis of block-cipher-based frequency hopping systems have laid the foundation for the block cipher FH codes for practical applications. Despite that most FH pattern generations involve complicated nonlinearity; the proposed cryptosystem is efficient and suitable for digital use due to its regularity and modularity. According to the finite state machine (FSM) method [14, 15], the very large scale integrated circuit(VLSI) architecture of the algorithm is efficiently implemented using VHDL language, which offers great flexibility to design high-speed and high-density digital hardware. In VHDL development, the system contains four top level functional modules, i.e., RECEIVE, COUNTER_64, PROCESS and OUTPUT, and the state machine decides the time to transform from one state to another and generates enable signals for each modules. Figures. 6 and 7 are the hardware structure and state machine of the FH sequences generator respectively. So the FH sequence generator operates with state interactions of all levels.

The generator prototype is synthesized in ALTERA FPGA of FLEX10K20, with its working parameters shown in Table 3. To save hardware resource, 50 % of the embedded array blocks (EAB) in the chip is utilized to perform the memory fetch operations of S_{box}, and the hardware implementation cost 71 % of the total equivalent gates including the I/O interface with low consumption current of 10 mA for supply voltage of 5 V. The realized chip can support work frequency up to 24 MHz with stability and fast operation, as listed in Table 4. The generator also has a friendly I/O interface, which is flexible to initialize the system TOD or change the user's key in real time. In summary, the block-cipher-based FH codes generator is cost-effective and well-performing in practical FHMA applications.

Table 3 Parameters

System clock	1.5 MHz
Max hopping rate	23 850 hops/s
TOD	64 bits
User key	144 bits
Frequency slots	2^n(n =1, 2,⋯, 6)

Table 4 Operation time

System clock/MHz	Operation time/μs
1.5	35.18
3	17.50
6	8.65
12	4.38
24	2.15

4 Conclusions

We have presented a new family of FH sequences based on block ciphers. The proposed sequences are useful for asynchronous FHMA systems under the threat of intelligent jamming, because they possess high security, optimum linear complexity, uniform distribution, good independence, large family size and nearly ideal performance of multiple access. So it has an encouraging prospect in FHMA systems for military and commercial applications.

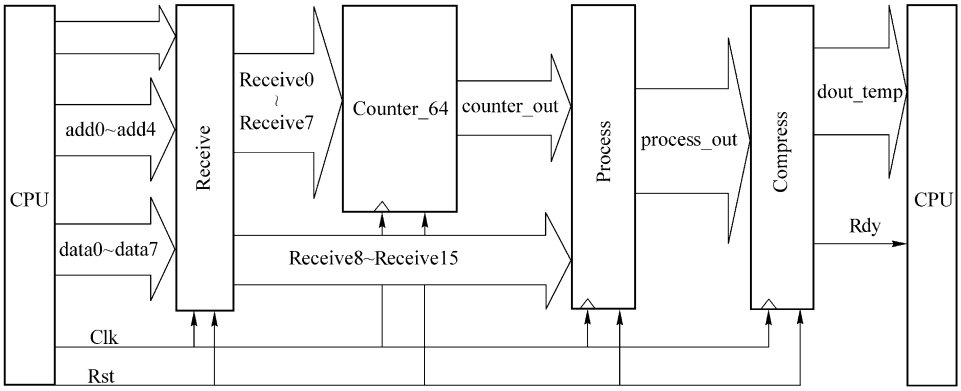

Fig. 6 Hardware structure of FH sequences

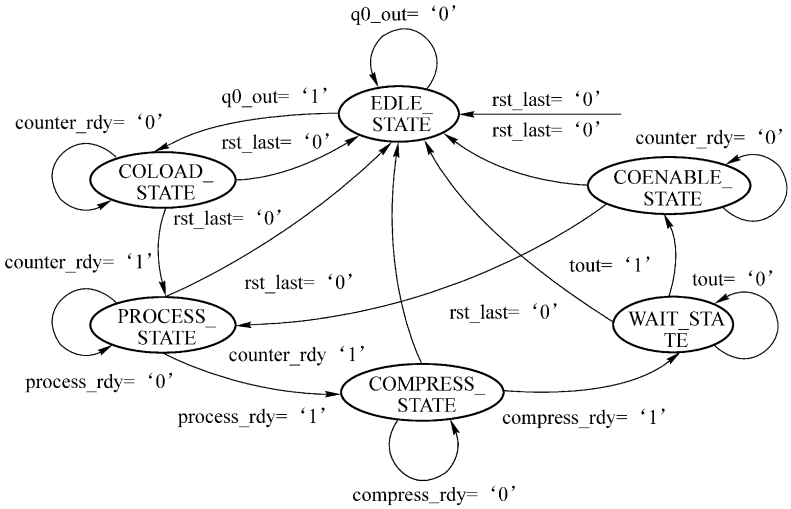

Fig. 7 State machine of FH sequences generator

Using FLEX10K20 series FPGA, We have completed an FH code generator with a small silicon area, low power consumption and fast operation, which has been adopted in 1 032 hops/s FHMA transceivers.

Acknowledgements This study was supported by the National Natural Science Foundation of China (No. 60402040), Natural Science Foundation of Shaanxi Province (No. 2005F29), the 10th Fok Ying Tong Education Foundation for Young Teacher (No. 101065), China.

References

1. Mei Wen-hua, Yang Yi-xian, Families of FH sequences based on pseudorandom sequences over GF(p), ICCT2002, 2002, 1(5): 536–538
2. F. M., D A., Hit probability between frequency hopping sequences generated by Reed-Solomon and Hermitian codes, Electronics Letters, 1996, 32(11): 962–963
3. Wang Hai-yang, Zhang Shen-ru, Mei Wen-hua et al., Reproducing algorithm of Lempel-Greenberger sequence and improved model in hopping frequency, Journal on Communications, 2003, 24(1): 98–103 (in Chinese)
4. Seong-Bok Park, K. Wang-Eog Lee, Young-Kyun Choi, Some good frequency hopping sequences with arbitrary number of slots, IEEE Military Communications Conference MILCOM, 2001(2): 1325–1329
5. Ling Cong, Wu xiao-fu, Design and realization of an FPGA-based generator for chaotic frequency hoping sequences, IEEE Trans. Circuits and Syst.I, 2001, 48(5): 521–532
6. Wang hong-xia, Yu Jue-bang, A new cipher quasi-chaotic frequency hopping sequence for FH/CDMA communications, IEEE International Conference on Communications, Circuits and Systems and West Sino Expositions, 2002: 497–501
7. Ling Cong, Sun Song-geng, Frequency-hopping sequences by chaotic maps for FH/CDMA communications, Acta Electronica Sinica, 1999, 27(1): 67–69 (in Chinese)
8. Deng Hong-min, He Song-bai, Yu Jue-bang, A frequency-hopping system based on a specific chaotic map, Journal of Systems Engineering and Electronics, 2002, 24(10): 45–46
9. Li Zan, Chang Yi-lin, Jin Li-jun, A novel family of frequency hopping sequences for multi-hop bluetooth networks, IEEE Trans. Consumer Electronics, 2003, 49(4):1084–1089
10. Li Zan, Chang Yi-lin, Jin Li-jun, et al., Analysis of FHMA performance on block cipher based frequency hopping sequences, IEEE Communications letters, 2004, 8(7):434–436
11. Wang Yum-in, Liu Jian-wei, Security of Communication Network —Theory and Technology, Xi’an: Xidian University Press, 1999: 126–152 (in Chinese)
12. James L., Massey, Shift-register synthesis and BCH decoding, IEEE Trans. Information theory, 1969, IT-15(1): 122–127
13. Rueppel R. A, Analysis and design of stream ciphers, New York: Springer- Verlag, 1986
14. Kuusilinna K. et al., Finite State Machine Encoding for VHDL Synthesis, IEE Proceedings: Computers and Digital Techniques, 2001, 148(1): 23–30
15. Bolchini C., Montandon, R. et al., Design of VHDL-based totally self-checking finite-state machine and data-path descriptions, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2000, 8(1): 98–103
16. Morrow R. K., Packet throughput in slotted Aloha DS/SSMA radio systems with random signature sequences. IEEE Trans. on Communation, 1992, 40(7): 1223–1230