ISSN 2047-3338

Novel Circuit for the Generation of Gold Sequences for Increased Message Security

Faroze Ahmad[1] and G. Mohiuddin Bhat[2]

[1]E&C Engineering, Islamic University of Science and Technology (IUST), Awantipora, J&K, India
[2]GIAN Cell (J&K), Advisor EDC and Coordinator TUC, University of Kashmir, India

***Abstract*— Secure message communication techniques, based on Spread Spectrum modulation (or message encryption scheme), use a spreading code (or an encryption key) for message security. The commonly used spreading codes or encryption keys are based on m-sequences and Gold codes. Gold sequences are preferred for many applications owing to their data hiding capabilities. The conventional techniques used for the generation of Gold codes use fixed feedback tapings and therefore can prove, sometimes, easy for a hacker to decode or jam the original information signal. A novel circuit for the generation of a Gold code sequences, wherein the feedback tapings change pseudo-randomly, is presented in this paper. The proposed system has been implemented with reduced hardware by using multiplexing process. The experimental results obtained are found to be in step with the theoretical ones.**

***Index Terms*— Gold Codes, M-Sequences, Spread Spectrum and Secure Message Transmission**

I. INTRODUCTION

SPREAD Spectrum (SS) modulation is widely used in military, mobile and other modern communication systems, due to its inherent advantages, such as low probability of intercept and high anti-jamming capability [1]. In a Spread Spectrum modulation the spectrum is deliberately spread over a wider bandwidth to realize improved process gain [2]. There are five types of SS modulation techniques: (a) Frequency Hopping Spread Spectrum (FHSS), (b) Direct Sequence Spread Spectrum (DSSS), (c) Time Hopping Spread Spectrum (THSS), (d) FM Chirp and (e) Hybrid SS. Among all these techniques, the commonly used SS techniques are FHSS and DSSS. FHSS is usually used for implementing military communication and Bluetooth systems because of its better anti-jamming and low probability of intercept capabilities. DSSS finds application in satellite and mobile communication because of its better code division multiple access capability.

SS modulation techniques have been discussed in detail in literature [2], [8]. In all the SS techniques, the spectrum expansion at the transmitter is accomplished by means of a code known as Pseudo-noise (PN) sequence. The same sequence is used at the receiver to de-spread the signal. The probability of intercept and capability of anti-jamming is determined by the length of code sequences used for spectrum expansion. The commonly used PN-sequences are m-sequences, Gold sequences and Kasami sequences [1], [3]. In all these PN-sequences, the feedback tapings are fixed and therefore the sequences generated are limited. In this paper a new technique for the generation of Gold code sequences has been proposed.

Section II of this paper provides a brief description of PN-sequences. In section III the proposed Gold code generator is discussed. Finally in sections IV and V the experimental results and conclusion are respectively presented.

II. BACKGROUND

The term "pseudorandom" or "pseudo-noise" or simply "PN" sequence is used specially to mean a signal which is random in appearance but reproducible by deterministic means. It appears to an unauthorized user, to be a truly random signal. A PN sequence is represented as a sequence of 1s and 0s with certain properties. Among all the sequences, the most commonly used sequences are Maximal sequences (m-sequences) and Gold Code sequences [1].An m-sequence is generated by using a simple linear feedback shift register (LFSRs) with feedback logic of modulo-2 adders (XOR Gates). A simple block diagram of an m-sequence generator is shown in Fig 1.

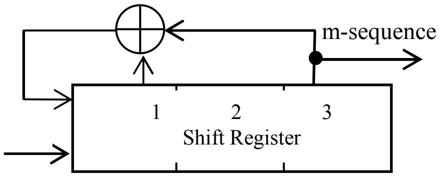

Fig. 1: Conventional m-sequence generator

The length (N) of an m-sequence is given by:

$$N = 2^n - 1 \qquad (1)$$

Where n is the number of stages in the shift register.

Therefore with the no. of stages n=3 as in above circuit, we get the length of m-sequence as N=7.The three basic properties, which are applied to test the randomness appearance, of m-sequences are as under:

a) Balance Property: In each period of the sequence, the number of 1s must differ from the number of 0s at the most by one digit, i.e., No. of 1s=$2^N/2$ and No of 0s= $(2^N/2)$ -1.

b) Run property: A run is defined as sequence of a consecutively single type of bits. Among the runs of 1s and 0s, in each period, one half of the runs are of length 1, one-fourth are of length 2, one-eight are of length 3 and so on [4], [5].

c) Correlation property: If a period of sequence is compared term by term with any cyclic shift to itself, it is best if the number of agreements differ from the number of disagreements by not more than one count [6].Mathematically, the correlation between two sequences p(k) and q(k), with the delay m, is expressed as

$$R(m)= \sum_{k=0}^{N-1} p(k)q(k+m) \qquad (2)$$

If an m-sequence uses an n-bit shift register (with certain fixed feedback tapings) to generate a code of length of (2^n-1) bits, it can be shown that the feedback tapings can be found if 2^nbits of the code word are known. Thus jamming in such situations becomes easy. Therefore choosing a longer code sequence enables good anti-jamming capability. One way to overcome this problem is to use Gold code generators, where larger code sequences are available with better correlation properties [7]. These sequences are generated by combining the preferred pair of m-sequences driven by the same clock as shown in Fig. 2.

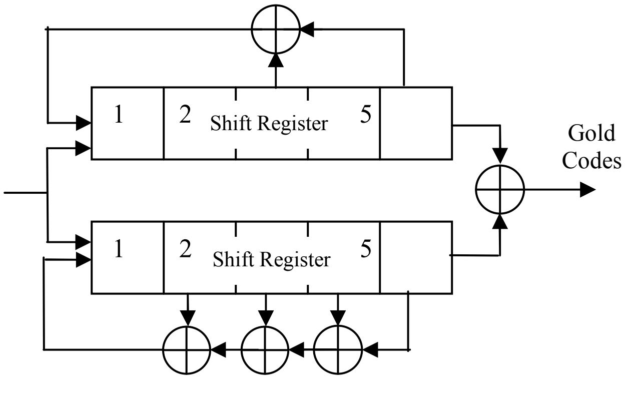

Fig. 2: Conventional Gold code Generator

Both the m-sequences use the same clock and are of equal length, the Gold code sequences generated are of the same length (N = 2^n-1). By giving one of the codes a delay with respect to other code, different sequences can be generated. The number of sequences that can be obtained is S_N= 2^{n-1}, where n is the size (length) of shift register [2]. Thus larger number of sequences can be generated using the same shift registers. With a proper choice of m-sequence pairs, a good cross-correlation can be maintained between all created Gold Codes [2]. In conventional Gold code sequences the feedback logic of LFSRs is fixed, and therefore the resultant sequences can be decoded by an eavesdropper or a jammer [3]. In this paper the authors present a more secure Gold code generator wherein the feedback tapings of the m-sequence generators are kept on changing in a pseudo-random manner, which enables the generation of more complex Gold codes and thus having better message hiding and anti-jamming capabilities. Simplicity of the circuits makes the technique attractive for low cost CDMA applications.

III. PROPOSED GOLD CODE GENERATOR

Fig. 3 shows the proposed circuit where two m-sequence generators M_1 and M_2 are combined. Both the sequences, generated by M_1 and M_2, work in the same manner.

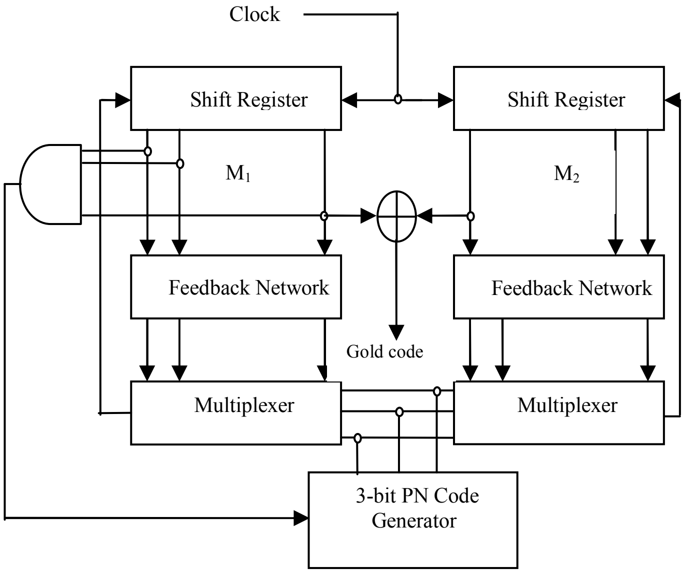

Fig. 3: Proposed Gold Code Generator

Choosing from the table [2], the valid sets of feedback tapings for sequences M_1 and M_2 are:

{[M_{1a}=10,9,8,7,6,5,4,3],[M_{1b}=10,8,5,1], [M_{1c}=10,9,8,6,5,1],

[M_{1d}=10,8,4,3], [M_{1e}=10,8,7,6,2,1], [M_{1f}=10,5,2,1]}and

{[M_{2a}=10,9,7,6,4,1], [M_{2b}=10,7,6,4,2,1], [M_{2c}=10,5,3,2],

[M_{2d}=10,9,6,5,4,3], [M_{2e}=10,9,4,2], [M_{2f}=10,9,7,6,4,3,2,1]}.

The implementation of feedback logic for m-sequences M_1 and M_2 is respectively shown in Fig. 4 and Fig. 5.

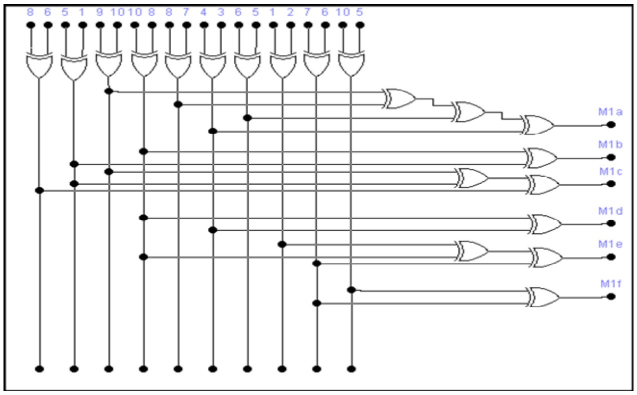

Fig. 4: Feedback Network for M_1

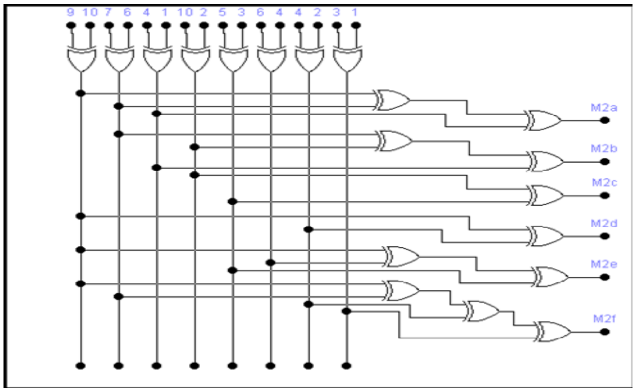

Fig. 5: Feedback Network for M_2

At a particular instant of time, a particular set of feedback tapings M_{1a}, $M_{1b,\ldots}M_{1f}$ of m-sequence generator M_1 are respectively used with feedback tapings M_{2a}, $M_{2b,\ldots,}$ M_{2f} of m-sequence generator M_2. Both the sequences M_1 and M_2 are driven by the same clock and therefore act synchronously. A 10-bit shift register has been used in both the m-sequence generators which can generate different sets of code sequences depending upon the valid sets of feedback tapings. The multiplexers select any one of the feedback tapings from each of the m-sequences at a particular instant of time, depending upon the code available at their data select lines. A 3-bit PN-code generator is used to generate the pseudorandom code for the data select lines of the multiplexers.

This further enhances the complexity of the code sequences and hence confuses the jammer to know about the transition from one sequence to another. Since a 3-stage PN–generator has been used, the number of codes available at its output (also at the select lines of the multiplexer) is seven, i.e. 001, 010, 011, 100, 101, 110, 111. Now suppose at any instant of time, the code word is 001, the multiplexers will select the feedback tapings [M_{1a}=10,8,7,6,5,4,3] and [M_{2a}=10,9,7,6,4,1] and a specific code is generated at a particular stage of the shift register. Once the length of this code is completed, the 3-bit PN generator, used to drive multiplexers, receives a high-to-low pulse from the output of an AND gate when all the stages of the shift register make a transition from *"all one state"* (111) to some other state. This high-to-low pulse will change the code at the output of the 3-bit PN code generator and therefore directing multiplexers to select another set of feedback tapings. The change in feedback tapings generates a new code at the output of the shift registers. In this way all the feedback tapings can be used to generate different codes. The codes generated by M_1 and M_2 are applied to the two inputs of XOR gate, which generates the required Gold codes.

IV. EXPERIMENTAL RESULTS

The proposed system has been implemented in hardware using IC74151 as multiplexer, IC 7486 as X-OR gates for implementing feedback networks, IC74LS76 (J-K flip flop) in combination with IC7400 (NAND gate) as shift registers and divide-by-N counters. The divide-by-count, N, decides the length of a particular PN-sequence at the output of the LFSR, corresponding to a particular selected set of feedback tapings. The time domain waveform for Gold sequence generated by the circuit is shown in Fig. 6. The input clock signal required by the circuits was taken from function generator. The circuit was tested with a frequency of 1Hz and 100KHz for static and dynamic test respectively. The experimental results obtained go in step with calculated theoretical ones.

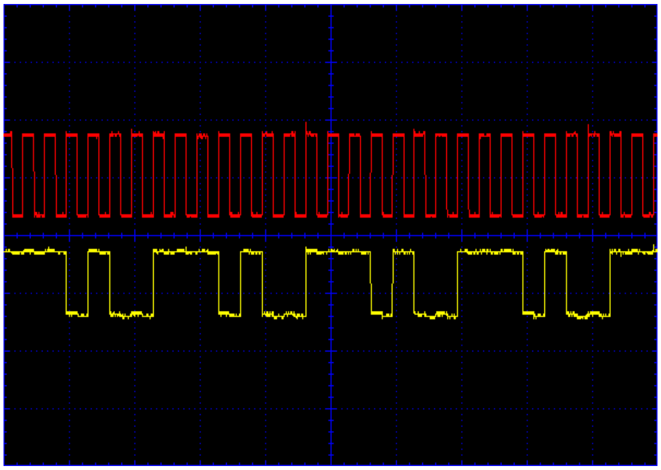

Fig. 6: Upper: Waveforms Generated by the Proposed Circuit
Lower: Gold sequence

V. CONCLUSION

Spread Spectrum modulation techniques and data encryption schemes require longer and complex code sequences with good correlation properties in order to avoid jamming, experience low probability intercept and offer better message hiding capabilities. Conventionally, m-sequences and Gold code sequences are commonly used for generating these codes. In conventional m-sequence/Gold code generators, the feedback tapings are fixed which results into the generation of reduced length sequences. A modified scheme for Gold Code Sequence generation, employing an LFSR with randomly changing feedback connections, has been implemented with reduced hardware. The proposed Gold code sequence generator has been experimentally tested using hardware modules. The results of experimental investigation are satisfactory.

REFERENCES

[1] Fangfang Chen, JingyuHua, Cheng Zhao and Shouli Zhou, "Fast generation of Bent Sequence family"InformationTechnologyJourna", 9(7) pp1397-1402, 2010.

[2] R.C. Dixon, "Spread-spectrum systems with commercial applications", John Wiley & Sons Inc., 1994.

[3] S. Kalita and P. P. Sahu, "A new modified sequence generator for direct sequence spread spectrum (DSSS)", National Conference on Electronics, Communication and Signal Processing, NCECS, Siliguri Institute of Technology, Siliguri, 19th September 2011.

[4] Haykin, S 'Communication Systems'. 4th Edition, New York: John Wiley and Sons, 2001.

[5] AlkaSawlikar and Manisha Sharma, "Analysis of different Pseudo Noise sequences", International Journal of Computer Technology and Electronics Engineering (IJCTEE), Volume1, Isseue 2, OCT 2011.

[6] M.I. Youssef ,A.E.Emam and M. AbdElghanyet ,"Direct sequence SS technique with residue number system", Int. journal of Electrical and Electronics Engineering 3:4, 2009.

[7] V. Anil Kumar, A. Mitra, S. R. Prasanna, "Performance Analysis of Different PN Sequences for Speech Encryption", International Journal of Information and Communication Engg, 2008.

[8] KamiloFeher, "Wireless Digital Communications: *Modulation & Spread Spectrum Applications",* Prentice-Hall of India Private Limited, New Delhi-110001, 2003.

Dr. Faroze Ahmad received M.Sc. (Electronics) in 2000 and Ph.D. (Electronics) in 2007 from University of Kashmir, Srinagar India. He is presently serving as Assistant Professor in E&C Engineering at Islamic University of Science and technology (IUST) Awantipora, J&K India. The major areas of research of Dr. Farozeinclude Message Encryption and Spread Spectrum Communication System.

Prof. G. Mohiuddin Bhat was born in Kashmir on 1st Feb., 1964. Prof. Bhat obtained his M.Sc. (Electronics) from the University of Kashmir, Srinagar (India) in 1987, M.Tech. (Electronics) from Aligarh Muslim University (AMU), Aligarh (India) in 1993 and Ph.D. Electronics Engg. from AMU, Aligarh, (India) in 1997. The major field of research of Dr. Bhat is Signal Processing Techniques and Secure Message Communication.

He has served as Assistant Professor, Associate professor and now as Professor & Director, University Science Instrumentation Centre (USIC), University of Kashmir. He has published many research papers on his area of interest. He has worked in the area of Mobile Radio Communication, Spread Spectrum Communication and Neural Networks and has guided many research degrees leading to the award of M.Phil and Ph.D. His present research interest include Secure Message Communication, Neural networks and Signal Processing techniques for communication.

Prof. Bhat is a member of many scientific bodies and professional societies. Prof Bhat has received two Indian Patents for two innovative technologies which are under process of commercialization. Prof. Bhat is the Chairman of GIAN Cell-J&K, Advisor EDC and Co-ordinator TUC, at University of Kashmir which are the professional bodies for indigenous technology innovation and technolo-preneurship development in the State of Jammu& Kashmir (India).