An Easy Synchronization Encryption Technique for Short Distance Data Transmission

Faroze Ahmad

Department of Electronics and Communication Engineering
Islamic University of Science and Technology (IUST), Awantipora, Pulwama India

ABSTRACT- The code synchronization between transmitter and receiver is the toughest job in any communication system. In this paper a novel technique for the generation of an unpredictable key, without the need of synchronization, for secure message communication is proposed. In this technique a signal received from a local broadcast transmitter is used to generate the necessary key at the transmitter and the receiver of the secrecy system. The proposed system was implemented in hardware and the results obtained are also presented. The proposed technique also simplifies the synchronization problems for the generation of synchronous keys at the transmitter and the receiver in a multi-user environment.

KEY WORDS: *Secure message communication, encryption, Pseudo-noise sequences and scramblers.*

I. INTRODUCTION

The fast changing needs and the development of new technologies have born new and sensitive communication capabilities in the form of modern communication systems such as: Internet, Electronic Banking, Electronic Mail, Pay Channel Television, Mobile Telephony, Satellite Phone and other forms of electronic communications employed in defense and civil sector. All these communications are vulnerable to threat of interference and eavesdropping. Communication thus needs to be made secure against unauthorized interception known as eavesdropping and against disruption. The standard countermeasure against eavesdropping or passive wiretapping is cryptography (encryption). The importance of encryption in the modern day communication can thus be visualized [1-9]. Several methods have been developed to avoid interception and a few are briefly discussed in detail in section II. Section III discusses the proposed low cost encryption technique with readily available key with no key synchronization requirement. Finally in sections IV and V experimental results and conclusion are respectively presented.

II. BACKGROUND

The popularly used encryption techniques are (1) Substitution Ciphers (2) Transposition Ciphers and (3) Product Ciphers. In substitution ciphers, the bits, characters or blocks of characters are replaced by some substitutes. Transposition Ciphers re-arrange bits or characters in the data. The combination of substitution and transposition ciphers known as product cipher enhances the message security of the system. The idea was first proposed by Shanon in 1949, which showed that meaningful messages could be randomly distributed over the set of all possible cipher text messages, by using 'mixing transformation'. Mixing transformations could be created by applying a transposition followed by an alternating sequence of substitutions and simple linear operations [10]. Modern computer to computer encryption techniques use mathematical algorithms and a key that is provided by the authorized users. Data Encryption Standard (DES), the widely used algorithm for encryption/decryption, was developed by IBM and the federal government in the mid-1970s and adopted by National Institute of Standards and Technology. The DES algorithm enciphers blocks of 64 bits using a 64-bit key. Out of 64 bits, 8 bits are used for error detection and correction within the key itself [11]. Both hardware and software techniques have been used to perform encryption/decryption, depending upon the application. The trade-off between hardware and software is that software is more flexible and easier to change but hardware is faster. Software techniques, based on mathematical algorithms, can be best used in a computer environment. However, for many applications, where the information secrecy is comparatively of lower value, such as cable television, mobile telephony, an expensive encryption is not very interesting [12-17]. In such situations message security techniques, hardware implementable at a low cost are highly preferred. In hardware based encryption techniques, the encryptor generally XORs the binary message signal known as plain text with the secret binary key to generate the cryptogram as shown in Fig.1. At the receiving end the received cryptogram is XORed with the same key and the original binary message signal is recovered. Let C be the plain text, E be the cryptogram and K the key then,

$$C \oplus K = E \qquad (1)$$

then $$E \oplus K = C \qquad (2)$$

Where $\oplus$ represents XOR operation.

An unauthorized receiver without any knowledge of the key will not be able to recover the plaintext information. Hence the secrecy of such a crypto system depends upon the key used at the transmitter and receiver. The key must be unpredictable at any instant of time in order to confuse the interceptor, and therefore must be random in appearance. Since it is difficult to reproduce the replica of the random key at the receiver, therefore pseudo-random usually known as

pseudo-noise (PN)-code (or sequence) is used. This PN-sequence appears to be random in appearance but can be reproduced by some deterministic means [10].

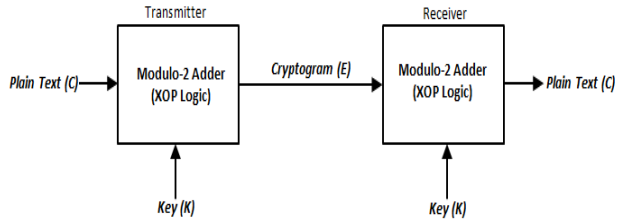


Fig. 1: Conventional message security system

The commonly used PN-sequences are m-sequences, Gold sequences and Kasami sequences. These sequences, with their properties, have been discussed in [18]. Many circuits for the generation of complex PN-sequences have been reported in the literature, but seem to be expensive and require more hardware [19-20]. Besides the level of encryption, PN-code synchronization between the transmitter and the corresponding receiver is indispensable. This code synchronization is the most difficult process in any secure communication system.

An alternative method to enable cost effective encryption of audio and video signals is to use scramblers. Scrambling is a coding technique which basically randomizes the data streams. The low cost, high speed and easy to use are the main features of scramblers [16]. A scrambler circuit consists of a shift register with some feedback loops and XOR gates as shown in Fig. 2. The previously transmitted message bits are stored in a shift register, and are further used for key generation. The input data stream is modulo-2 added with the key generated and transmitted as encrypted data, known as cryptogram, to the intended receiver. To recover the data at the receiving end, the scrambled data stream is multiplied (modulo-2 added) by the same key used at the transmitter as shown in Fig. 3. To illustrate the system, let C be the input data, usually known as plain text, applied to the scrambler and let E denotes cryptogram. Further, if a_i represents the i^{th} tap gain and D represents the delay operator, then mathematically [10] E is given by

$$E = C \oplus K$$

$$E = C \oplus \left[a_1 D^1 E \oplus a_2 D^2 E \oplus ..... \oplus a_N D^N E \right]$$

$$E = C \oplus \left[a_1 D^1 \oplus a_2 D^2 \oplus ..... \oplus a_N D^N \right] E$$

If the Boolean function $a_1D^1 \oplus a_2D^2 \oplus a_3D^3 \oplus ..... \oplus a_ND^N$ is denoted by f, then

$$E = C \oplus [\, f \,] E$$

$$E = C \oplus K$$

Where K = fE, is the key used to generate cryptogam E.

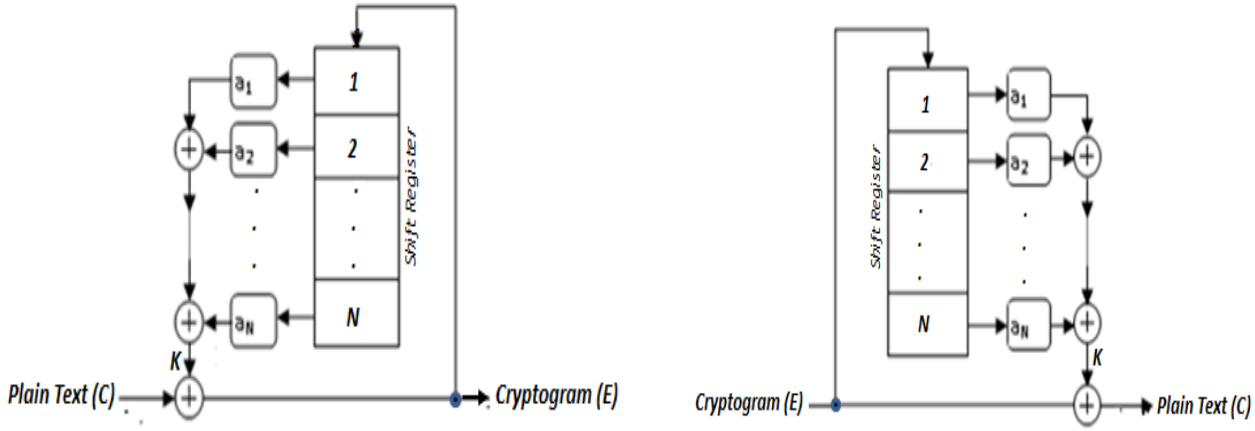


Fig. 2: Conventional Scrambler and Descrambler

Since the logic used in the descrambler is same as that of in the scrambler, by the process of modulo-2 addition we have

$$C = E \oplus \left[a_1 D^1 \oplus a_2 D^2 \oplus ..... \oplus a_N D^N \right] E$$

This can also be put as under

$$C = E(1 \oplus f)$$

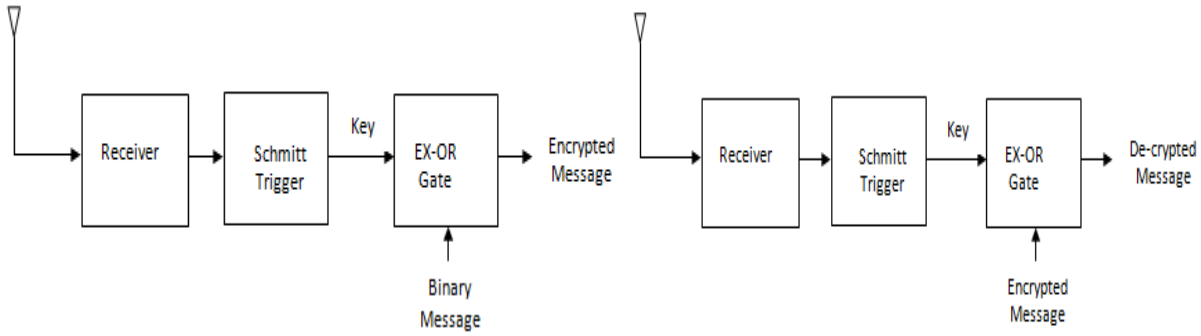
This shows that the plain text can be recovered faithfully by the descrambler.

Though the security offered by scramblers is not as high as provided by some advanced encryption techniques (like DES), however, the available security is found to be adequately suitable for many applications. Besides encryption, scramblers are commonly used to avoid D.C. wander or residual D.C. by avoiding long strings of 0's & 1's. This enables easy clock synchronization as it is often essential to have sufficient transitions in the transmitted data for clock extraction. The main problem with scrambling systems is that if a single error occurs in the scrambled data, it propagates into a burst of errors after descrambling. This requires highly complex circuitry for error detection and correction.

Keeping the foregoing discussion in view, the author presents an interesting low-cost encryption/decryption technique, with no code synchronization requirement.

III. PROPOSED CIRCUIT

The proposed circuit is shown in Fig. 3. The two receivers used at the transmitting side and the receiving end are precisely tuned. Therefore the demodulated analog signals available at the outputs of both the receivers are almost exactly same in shape and amplitude. The received signal from a particular transmitting station is demodulated and adequately amplified by the receivers and applied to a wave shaping circuits (Schmitt trigger). The output of the Schmitt trigger is a binary train of pulses which are used as the *secret key* by the authorized users. At the transmitter, the binary message (known as plain text) is applied to the other input of the Ex-OR gate. The output of the Ex-OR gate is the encrypted message which is then transmitted to the intended receiver. At the receiver the encrypted message is applied to the one of the inputs of the Ex-OR gate, the other input of which is fed with the key generated by the Schmitt trigger which is the replica of the key generated at the transmitting end of the authorized user. Hence by the principle of EX-OR operation as given in equations (1) and (2), the signal recovered at the output of the EX-OR gate is the original transmitted binary message.

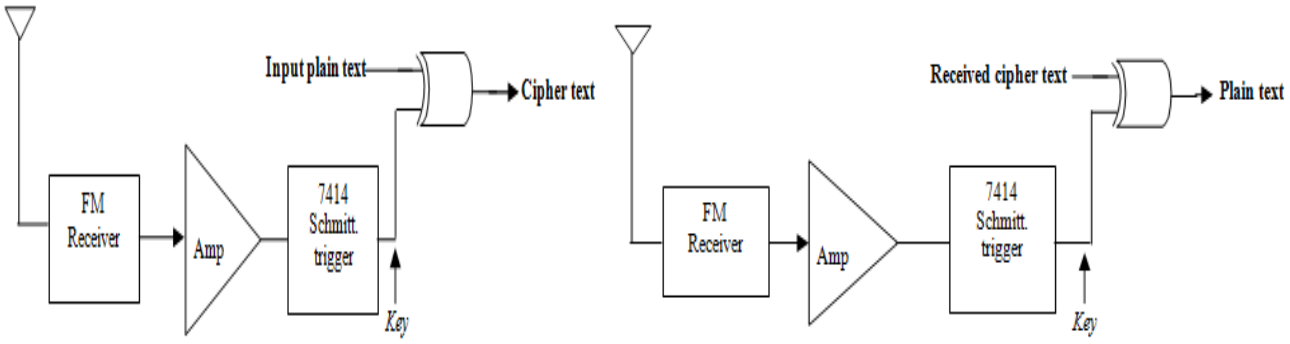


(a) (b)

Fig. 3: Proposed technique (a) Key used at authorised transmitter (b) Key used at authorised receiver

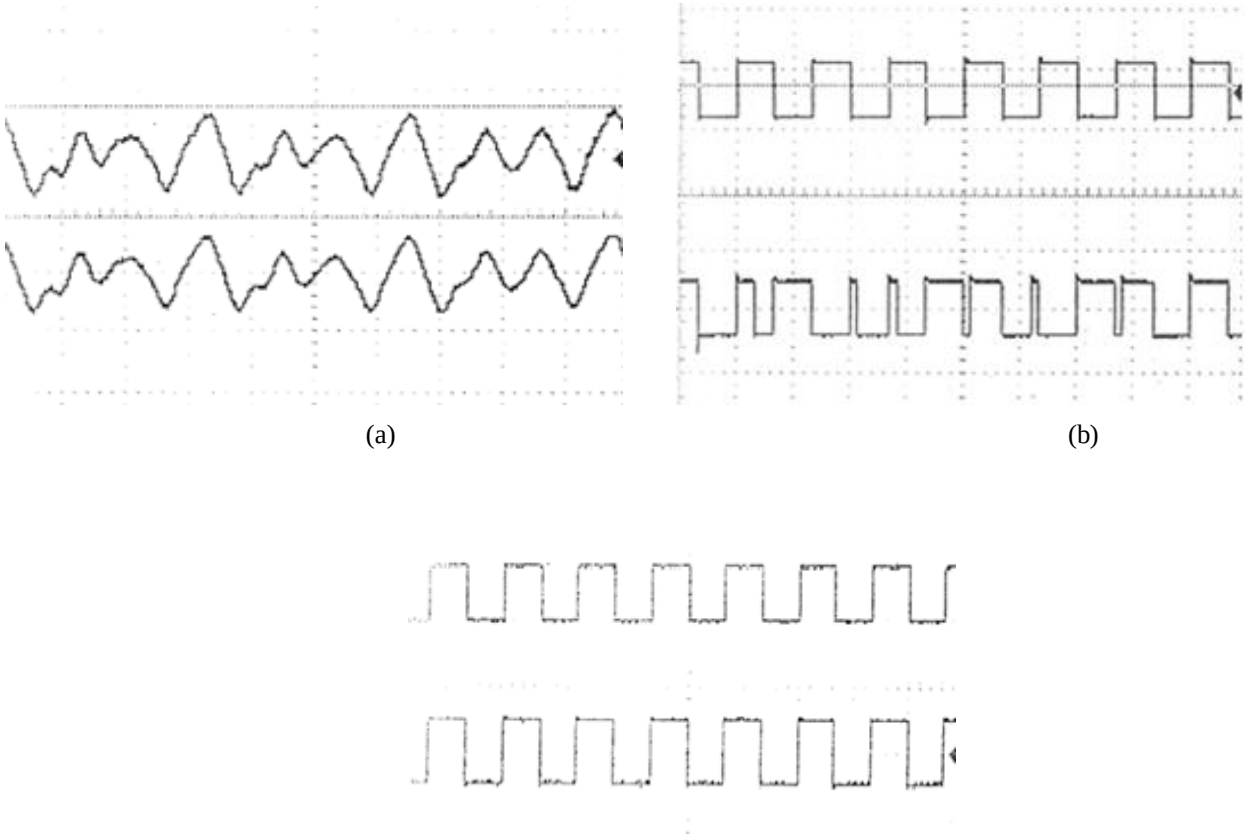
IV. EXPERIMENTAL RESULTS

For experimental investigation, a readily available, local frequency modulated (FM) signal was used. IC 7486 and IC 7414 were respectively used as EX-OR gate and Schmitt trigger. The received FM reference signal was demodulated at the transmitter as well as at the receiver with properly designed FM demodulators. Assuming sufficient amplifying gain in the FM receivers, it can be shown that each FM receiver generates similar demodulated signals, as shown in Fig. 5 (a), which might be the speech or music signals broadcast by an FM radio transmitter. This reference signal was next converted into a pulse train signal using Schmitt Trigger as shown in Fig. 5(b). The binary message, which is a square wave signal, was applied from a function generator. The signal recovered at the receiver is shown in Fig. 5(c).



(a) **(b)**

Fig. 4 Implementation of proposed circuit (a) Key used at authorised transmitter (b) Key used at authorised receiver



(a) (b)

(c)

Fig. 5 Waveforms generated by two FM receivers operated separately. *(Upper: Demodulated at transmitter) (Lower: Demodulated at corresponding receiver)* (b) Encryption at the transmitter *(Upper: Plain Text signal) (Lower: Encrypted signal)* (c) De-cryption at the receiver (Upper: Plain text data transmitted at the sender) (Lower: De-crypted data at the receiver)

V. CONCLUSION

A simple technique for encryption of data is presented. The proposed technique simplifies the synchronization problems for the generation of keys at the transmitter and the receiver in a multi-user environment. The technique could be used for short distance secure message communication at low data speeds, since the phase errors are introduced by the channel for long distances communication or at high data rates. The proposed technique is practically implemented in hardware. The experimental results have been found to be satisfactory and are presented in this paper.

REFERENCES

[1] D. J. Torrieri, "Principles of secure communication systems", Artech House, Inc., 1985.

[2] R. Benjamin, "Security consideration in communication systems and networks", IEEE Proc., Vol. 137, Pt. I, No. 2, pp. 61-72, April 1990.

[3] J. A. Adam et al, "The privacy problem", IEEE Spectrum, Vol. 32, No. 12, Dec. 1995.

[4] B. Shneier, "Applied cryptography,"John Wiley & Sons Inc., New York, 1996.

[5] K. Rossen,"Network security : Just say 'know' at layer 7", Data Commun. Intl., pp. 103-106, Mar. 1991.

[6] Charles C. Wood, "Future application of cryptology", Proc. symp. security & privacy, pp. 70-74, April 1981.

[7] A. Kh. Al-Jabri et al, "Secure progressive transmission of compressed images", IEEE Trans. Cons. Elect., Vol. 42, No. 3, pp. 504-512, Aug. 1996.

[8] A. C. Bandyopadyaya et al, "Is your personal communication really personal?", Proc. 36th Annual Tech. Conven. of IETE, pp. 89-102, Hyderabad, India, Oct. 1-2, 1993.

[9] J. L. Massey, "Contemporary cryptology, an introduction", New York Press, 1992.

[10] G. Mohiuddin Bhat, "Design and development of novel electronic circuits for efficient & secure message communication", Ph.D. thesis, Department of Electronic Engineering, Aligrah Muslim University, Aligrah, India, 1997.

[11] Stanford H. et al, "Telecommunications for Managers", Third Edition, pp. 272-274, Prentice Hall, 1995.

[12] C. Sindhu et al, "Real-time speech cipher system", Proc. 36th Annual Tech. Conven. IETE, pp. 149-156, Hyderabad, India, Oct., 1-2, 1993.

[13] A. Marwaha et al, "A new encryption scheme using product transformations" , Proc. 20th National Sys. Con., NSC-96, pp. 361-367, Trivandrum, India, Dec. 19-21, 1996.

[14] C. H. Bennet et al, "Generalized privacy amplification", IEEE Trans. Inf. Theory, Vol. IT-41, No. 6, pp. 1915, Nov. 1995.

[15] Bhat, Mohiuddin & Wasim Ahmad : "Reliable and secure data transmission", Electronics Engineering, Vol. 68, No. 832, pp. 32-34, April 1996, London, U. K.

[16] Wasim Ahmad & Mohiuddin Bhat, "Scrambler for data", Electronics World, pp. 227-228, Mar. 1997.

[17] H. J. Bekar, F. C. Piper, "Digital speech scrambling", New Electronics, 15(18) 21, pp. 94, Sept. 1982.

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

[19] G. M. Bhat and Faroze Ahmad, "New LFSR circuits for generating complex code sequences", Electronics World, London, pp.40-43, 2007.

[20] Faroze Ahmad and G.M. Bhat, "Novel circuit for the generation of Gold sequences for increased message security" International journal of computer science and telecommunications, Vol. 3, Issue 5, May 2012.