Permutation based speech scrambling for next generation mobile communication

Dhanya G [#1], Dr. J. Jayakumari [*2]

[#] Research Scholar, ECE Department, Noorul Islam University, Kanyakumari, Tamilnadu
[1] dhanyagnr@gmail.com
[*] HOD, ECE Department, Noorul Islam University, Kanyakumari, Tamilnadu
[2] hellojayakuari@rediffmail.com

***Abstract*— Scrambling is a really significant method that provides protection in communication systems by using random permutation and pseudorandom binary scrambling method. To enhance the security in communication, OFDM scrambling can provide better protection than an FFT scrambler under same permutation operation. To evaluate the quality of the proposed system, perceptual evaluation of speech quality is used. The objective test SNR and BER are used to estimate the noise performance of the system. STI and CIS were applied to know the performance of the system. From the simulations, it is clear that, the proposed system shows better performance than conventional scrambling technique and it is more robust in the 4th generation of mobile communication.**

Keyword- Speech scrambling, OFDM, Pseudo- random generator, random permutation, speech transmission index, common intelligibility scale

I. INTRODUCTION

As the volatile increase of wireless communication, the voice security is essential in modern communication systems. With the increasing user demands has brought a keen need for message security of transmitting. The rapid improvement of 4G technology offers broader bandwidth, larger data rate, and besides it makes data access at anytime, anywhere basis.

The OFDM is a widely accepted modulation scheme in the fourth generation of mobile communication.

Speech is a simple and natural method for interchanging information between individuals. For protecting the information, encryption and scrambling is used. The encryption provides security on signal level and scrambling provides security on symbol level. The secrecy can be easily be achieved by using scrambling techniques. The scrambler is used to obtain the residual intelligibility as very low as possible and to provide a large key space without altering the bandwidth after scrambling. [1].In this way scrambler improves the security.

In order to avoid eavesdropping the scrambler makes the intelligible signal into an unintelligible signal. The analog scrambling algorithms use permutation of speech segments in time, frequency or time-frequency domain [2].

The encryption algorithms do not provide enough security. During speech communication, the encryption algorithms cannot provide enough security across eavesdroppers.

The frequency domain scrambler split the speech signal into several frequency sub-bands and permutes them. The time domain scrambler breaks the voice signal into short time blocks and these segments are permuted in time. Time domain scrambler breaks the voice signal into short time blocks and these segments are permuted in time. The scramble order and size of the segment may follow a pseudo random scheme [3]. These scramblers do not provide efficient security because the number of permutations is not large enough to offer sufficient protection [4]. Speech scrambler based on Fast Fourier Transform (FFT) retains little residual intelligibility. To reduce the residual intelligibility, this paper proposes a new technique based on QAM mapping and an OFDM method. The Fast Fourier transform based speech scrambler uses two Fourier transform operations, but the OFDM scrambling method needs only two FFT operations. [5]

This report consists of five academic terms. The scrambling operation is explained in 2nd sessions, while in session 3 comprise the proposed scheme. The performance analysis is given in section 4 come after by conclusions in session 5.

II. FREQUENCY DOMAIN SCRAMBLER:

The analog scrambling process can be described using matrix algebra. Let x represent a vector which contain speech samples of length N and F represents the N*N Fast Fourier transform matrix [6].

Let U be FFT of the speech signal x is given by:

$$U=F.\ x$$

The Fourier transform results a new vector u. The N*N permutation matrix P is applied to the speech vector u to produce a vector V.

$$V = P.\ u$$

The inverse transformation $F^{-1}$is applying on v gives a scrambled speech signal y [6].

$$y = F^{-1}.v$$

Table 1 and 2 shows the FFT speech scrambler performance analysis under PESQ and BER. The results do not show a good performance. Because of using four FFTs, the implementation of this scrambler is difficult. Therefore, we offer a safe method to provide better quality of the speech signal.

TABLE.I. FFT speech scramblers based on PESQ

Type of Scrambler	PESQ (Rayleigh)	PESQ (Rician)
FFT scrambler	2.07	1.98

TABLE.II. Evaluating random permutation with PRBS scrambling using different parameters

Type of scrambler	Eb/N0	BER
FFT scrambler with (Ricin) channel	12	0.6129
FFT scrambler with (Rayleigh) channel	12	0.548

A. *Permutation:*

The scrambling process does not increase the bandwidth of the system. Permutation is restricted to M! FFT coefficients lying within the speech band 300-3000Hz. The possible number of permutations is M! [7]. An efficient permutation method generates M! Permutations from a random number seed lying between 0 and 1. We can use this random number as a key in the scrambling process. Random numbers are generated utilizing a pseudo random binary generator. This will reorder the speech segments and make the words unintelligible.

On the receiver side, the same key and the pseudo random binary generator are used to retrieve the original speech.

The speech scrambler based on Fast Fourier Transform retains a considerable security in the data transmission and the system is more complex by the use of four FFTs.

III. ANALYSIS OF THE PROPOSED SYSTEM:

To get rid of the drawbacks of the existing system, proposed a new technique OFDM-based speech scrambler. The block diagram of the projected scheme is indicated in figure (1).

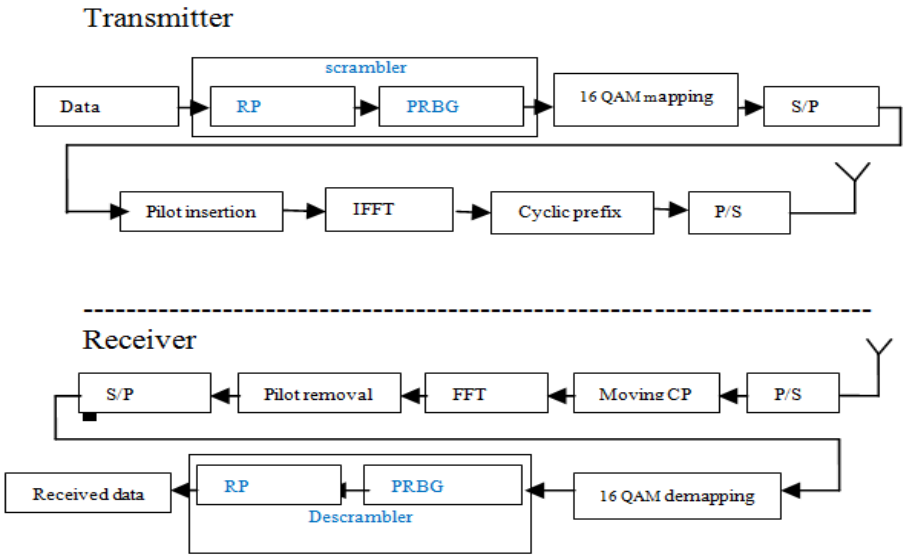

Fig. 1: Proposed OFDM based speech scrambler block diagram [8]

The proposed system is based on the combination of two permutations, random permutation and pseudo random binary scrambling. The random permutation reorders the speech segments in time, which is performed by a seed. It produces a scrambled data, which is unintelligible to others. The pseudo random binary scrambling is done by using a pseudorandom binary generator along with a key. The PRBS performs an XOR operation with the

outputs of PRBG and the random permutation. The output of the PRBS is a scrambled output, which has not any similarity with the original signal, it makes an unintelligible signal. This data is transmitted through the channel. It is crypt analytically secured algorithm and it produces low residual intelligibility.[8]

At the receiver side, descrambling is performed by using the same seed and key in the transmitter side.

For analyzing the system the following parameters are applied.

TABLE III. Parameters of proposed OFDM based speech scrambler [8]

Parameter	Value
FFT size(IFFT)	64
Bandwidth of transmission channel	300-3400Hz
Bandwidth of the input speech channel	0-3000Hz
Number of subcarriers	52
Sampling frequency	8kHz
Subcarrier spacing	312.5 kHz
Data symbol duration Td	3.2microsec
Cyclic prefix duration Tcp	0.8 micro Sec
Total symbol duration Ts(Td + Tcp)	4 micro Sec
Mapping and demapping schemes	16 QAM

Let X is the input data be an array of t elements, k denotes the position of an array. X_k be the value of the k^{th} position element of permuted data array. R denotes the random data and P_k is the position of the random data. The position change of the random data is expressed as q_k. It will obtained by the expression

$$q_k = \begin{cases} P_{k+1} & \text{if } 1 \le k \le t\text{-}1 \\ P_1 & \text{if } k=t \end{cases}$$

The scrambled random data after applying q_k is expressed as RR_k. f is the position function.

$$RR_k = f^{-1} q_k$$

The scrambled output after first permutation can be denoted as X'(k)

$$X'(k) = Xq_k \quad \text{----------} \qquad (1)$$

This is the output of the first scrambler.

This scrambled output is fed to the pseudorandom binary generator and applying a pseudo random binary scrambling. In this scrambler XOR operation is executed with a random key (K). The output of the second permutation is X"(k). It is obtained by XOR the output of the first permutation and the output of PRBG. R'_k is the random binary data generated by PRBG.

$$X''(k) = \text{round}(R'_k) \ \text{XOR} \ X'_k$$

Round function rounds to the closest whole number.

X"(k) is given as the input of the QAM mapping. The QAM mapped output is then converted to parallel form. After inserting pilots, data are given to the IFFT operation. The cyclic prefix is added to the output of IFFT and the data is converted back to serial form for transmission. Rayleigh and Rician channels are utilized for transferring the information.

At the recipient side, inverse operations are executed.

$$X'(k) = X''(k) \ \text{XNOR round}(R'_k)$$

$$P_k = \begin{cases} q_{k-1} & \text{if } 2 \le k \le t\text{-}1 \\ q_t & \text{if } k=1 \end{cases}$$

$$X_k = f^{-1}(Pk)$$

Here two types of permutations are used to seed and key. Thus, it is more crypt analytically secured scrambling based on OFDM system.

IV. PERFORMANCE MEASUREMENT:

The quality and intelligibility of speech were evaluated by a perceptual evaluation of speech quality (PESQ), speech transmission index (STI) and common intelligibility scale (CIS). The noise performance is measured by signal to interference plus noise ratio (SINR) and Bit error rate (BER).

A. *Perceptual Evaluation of Speech Quality (PESQ)*

PESQ is used to compare an original speech signal with the received speech signal. The received speech signal is recognized as "degraded signal" and the original speech signal is known "reference signal" [9]. The Perceptual evaluation of speech quality (PESQ), it computes the quality of a speech signal by a 5-point scale. The 5 corresponds to the excellent speech quality, 4 for sound, 3 for fair, 2 for poor and corresponds to bad or unsatisfactory speech quality, is shown in table 4 [9]

TABLE.IV. Comparison of OFDM speech scramblers based on PESQ [8]

Type of OFDM	PESQ (Rayleigh)	PESQ (Ricin)
OFDM with RP	2.17	2.019
OFDM with RP & PRBS	2.28	2.089

B. *Speech Intelligibility Measurement*

Two parameters are applied for measuring speech intelligibility

Speech Transmission Index (STI)
Common Intelligibility Scale (CIS)

The range of the speech transmission index lies between 0 and 1. The 0 indicates bad and the 1 indicates excellent. The weighted sum of Modulation transfer function (MTF) is used to measure speech transmission index (STI). Modulation transfer index (MTI) is deduced from a modulation transfer function (MTF). Here STI is calculated for a band of frequencies. SNR ranges are limited from +15db to -15db [10]. Speech transmission index computes all the factors in the speech transmission path, affects intelligibility.

TABLE 5: Relation between STI and speech intelligibility [9]

STI	.00-.30	.30-.45	.45-.60	.60-.75	.75-1.00
Speech intelligibility	Bad	Poor	Fair	Good	Excellent

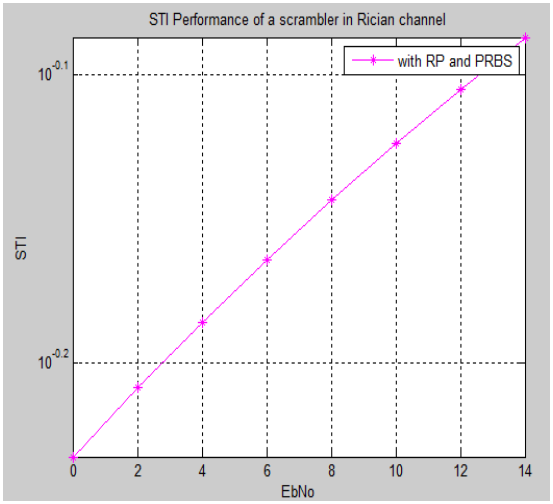

Fig. 2(a)

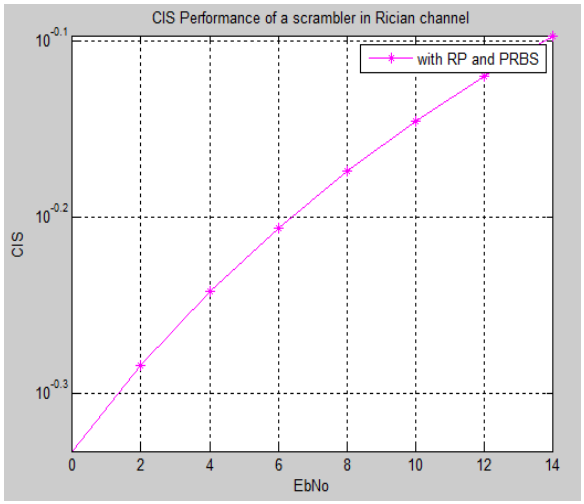

Fig. 2(b)

Fig.2. a) STI performance of OFDM based speech scrambler under Rician channel b) CIS performance of OFDM based speech scrambler under Rician channel.

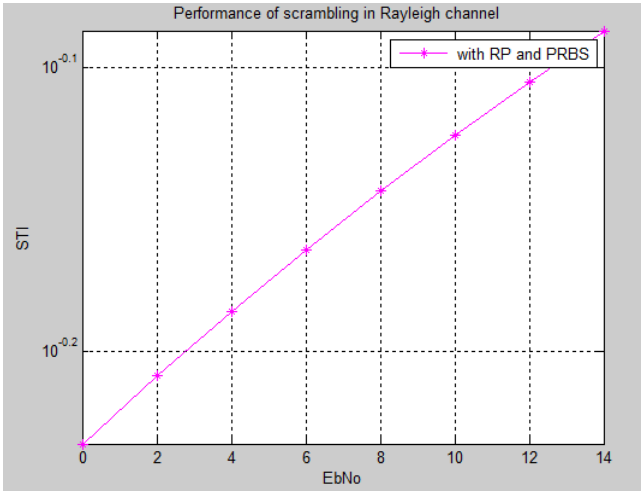

Fig. 3(a)

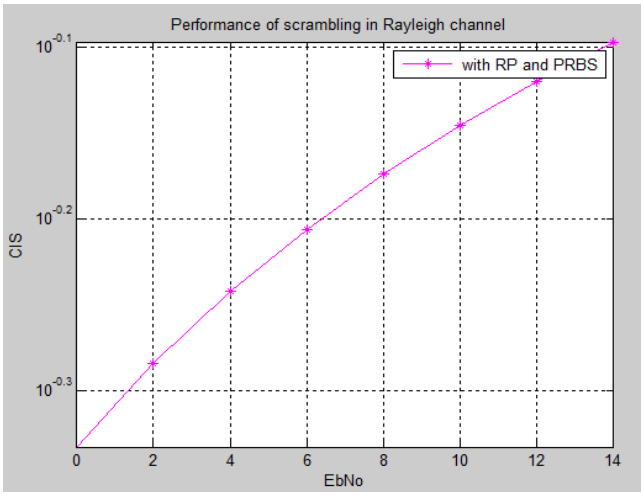

Fig. 3(b)

Fig.3. a) STI performance of OFDM based speech scrambler under Rayleigh channel b) CIS performance of OFDM based speech scrambler under Rayleigh channel.

The simulation results show that, the quality of the speech and the intelligibility of the speech are excellent, also the noise performance is low in this scrambler. Thus, the proposed scrambler RP with PRBS is the best scrambling technique in future communication.

TABLE 6: Evaluating random permutation with PRBS scrambling using different parameters

Type of OFDM	Eb/N0	BER	SINR	STI	CIS
OFDM with RP & PRBS (rician)	12	0.3129	0.1515	.7853	.7583
OFDM with RP&PRBS (Rayleigh)	12	0.4064	0.1351	0.7853	0.7999

The simulation results show that, in table 6, the quality of the speech and the intelligibility of the speech are excellent, also the noise performance is low in this scrambler. Thus, the proposed scrambler RP with PRBS is the best scrambling technique in future communication.

C. *Noise Performance*

The SINR and BER performance of OFDM based PRBS scrambler is compared with the OFDM based random permutation scrambler under fading channels (Rayleigh and Rician) shown in table 7. The Signal to Interference plus Noise Ratio is defined as the ratio between Signal power (Ps) and Interference power (PICI) plus noise power (N0) [8].

$$SINR = PS / PICI + N0 \text{ ----------} \quad (7)$$

The speech.wav was given as the input signal. For Rayleigh and Rician channel models, flat fading paths are employed and the K factor of 1 is used for rician channel [8]. BER is calculated using the parameter Eb/N0. The random permutation with PRBS scrambling shows better performance and it has a low bit error rate when compared with the others [8]

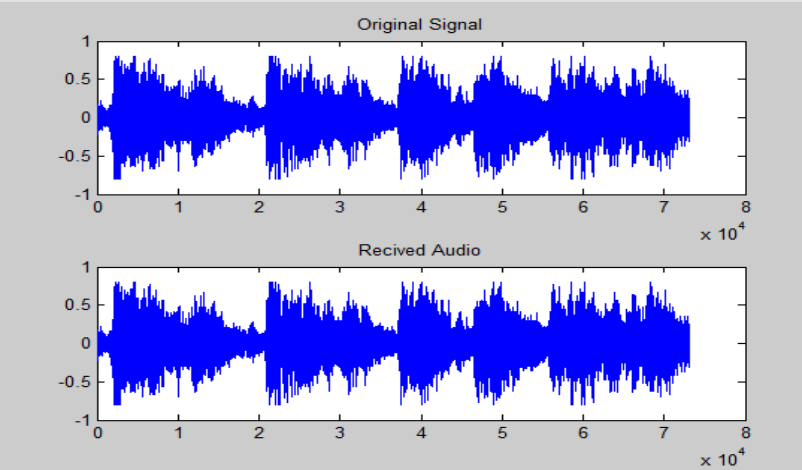

Fig.4. Original and reconstructed speech waveform [8]

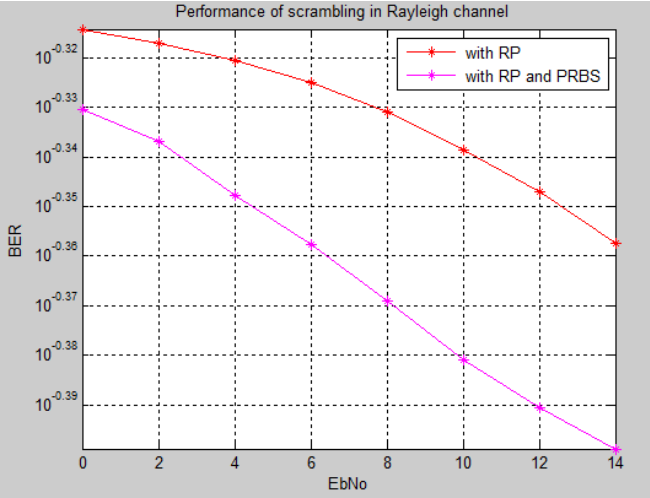

Fig. 5(a)

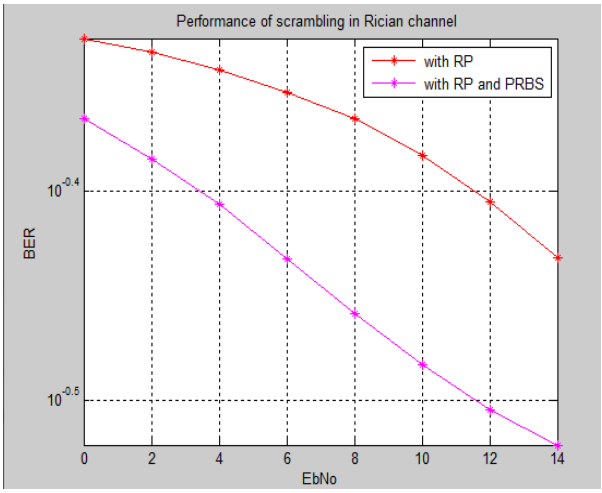

Fig. 5(b)

Fig.5. BER performance of OFDM based speech scrambler (a) Rayleigh and (b) Rician channel.

TABLE VII. Comparison of different types of OFDM speech scramblers based on a BER under Rayleigh and Rician channels [8]

Type of OFDM	Eb/N0	Rayleigh	Rician
Without scrambling	10	0.4818	0.4105
OFDM with RP	10	0.4727	0.3250
OFDM with RP & PRBS	10	0.4663	0.2714

The comparison table 7 shows that the suggested method (RP with PRBS scrambling) gives better performance than the two other methods.

V. CONCLUSION:

The scrambling technique applied to OFDM explained here provides a speech security than using an FFT scrambler. From the experimental solutions, the OFDM with RP and PRBS is the best scrambler for the proposed applications. The results show that PESQ is 4.3 for OFDM with RP and PRBS under rician channel and 4.3 for Rayleigh channel. The offered method does not need any bandwidth expansion. The quality of the recovered signal is good and also it is a crypt analytically secured algorithm. It is an encouraging technique for high quality data transmission in 4G communication and also it is an excellent technique for establishing a high security in next generation mobile communication system.

REFERENCES:

[1] SENK, V, DELIC, V.D.;MILOSEVIC, V.S "A NEW SPEECH SCRAMBLING CONCEPT BASED ON HADAMARD MATRICES" SIGNAL PROCESSING LETTERS, IEEE (VOLUME:4 , ISSUE: 6), DOI:10.1109/97.586036, PAGES: 161 – 163, JUNE 1997.

[2] de Andrade, J.F, de Campos, M.L.R. ; Apolinario, J.A. "Speech privacy for modern mobile communication systems" IEEE International Conference on ICASSP 2008- DOI: 10.1109/ICASSP.2008.4517975 pages: 1777 - 1780 March 31 2008-April 4 2008

[3] Francisco Assis de O. Nascimento(1) and Ricardo G. Toscano(2) "Frequency Speech Scrambler Based on the Hartley Transform and the Insertion of Random Frequency Components" The International Journal of FORENSIC COMPUTER SCIENCE ,DOI:10.5769/ J201201001 or http://dx.doi.org/10.5769/J201201001, pages: 8-15, 2012

[4] Eng. Sattar B. Sadkhan, N. H. Kaghed "Design and Evaluation of Transform – Based Speech Scramblers using different Wavelet Transformations" Fifth International Symposium. (CSNDSP), Communication Systems, Networks And Digital Signal Processing. Volume: fith – 2006,

[5] D. C. Tseng, J. H. Chiu "An OFDM Speech Scrambler without Residual Intelligibility"TENCON 2007-2007IEEE Region10conferenceDOI:10.1109/TENCON.2007.4428903, Publication Year:2007, Pages:1-4

[6] sridharan, s., dawson, e. ; goldburg, b. "fast fourier transform based speech encryption system" communications, speech and vision, ieee proceedings (volume:138 , issue: 3) ,doi:10.1049/ip-i-2.1991.0029, pages:215 – 223, june 1991

[7] Borujeni, S.E "Speech encryption based on fast Fourier transform permutation" Electronics, Circuits and Systems, 2000. ICECS 2000. The 7th IEEE International Conference on (Volume:1), 10.1109/ICECS.2000.911539, pages: 290 - 293 vol.1,2000

[8] Dhanya G, Dr. J Jayakumari, "Optimal speech scrambling technique for OFDM based system", International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 9, Number 24 (2014) pp. 28871-28878

[9] Tiago H. Falk1 andWai-Yip Chan2, "Performance Study of Objective Speech QualityMeasurement for ModernWireless-VoIP Communications", EURASIP Journal on Audio, Speech, and Music Processing,Volume 2009, Article ID 104382, 11 pages.

[10] Jianfen Ma, Yi Hu and Philipos C. Loizou, "Objective measures for predicting speech intelligibility in noisy conditions based on new band-importance functions", Acoustical Society of America, May 2009