Intelligent OFDM telecommunication system. Part 3. Anti-eavesdropping and anti-jamming properties of system, based on many-parameter wavelet and Golay transforms

Intelligent OFDM telecommunication system. Part 3. Anti-eavesdropping and anti-jamming properties of system, based on many-parameter wavelet and Golay transforms

V G Labunets[1], D E Komarov[1] , V P Chasovskikh[1], J G Smetanin[2] and E V Ostheimer[3]

[1]Ural State Forest Engineering University, Sibirskiy trakt 37, Ekaterinburg, Russia, 620100
[2]Federal Research Center "Information and Control" of the RAS, Vavilova 44/2, Moscow, Russia, 119333
[3]Capricat LLC, Florida, US

e-mail: vlabunets05@yahoo.com

Abstract. In this paper, we aim to investigate the superiority and practicability of many-parameter wavelet and Golay transforms (MPWT and MPGT) from the physical layer security (PHY-LS) perspective. We propose novel Intelligent OFDM-telecommunication system (Intelligent-OFDM-TCS), based on many-parameter transforms (MPTs). New system uses inverse MPT for modulation at the transmitter and direct MPT for demodulation at the receiver. The purpose of employing the MPTs is to improve the PHY-LS of wireless transmissions against to the wide-band anti-jamming communication. Each MPT depends on finite set of independent Jacobi parameters (angles), which could be changed independently one of another. When parameters are changed, multi-parametric transform is changed too taking form of a set known (and unknown) orthogonal (or unitary) wavelet transforms. We implement the following performances as bit error rate (BER), symbol error rate (SER), peak to average power ratio (PAPR), the Shannon-Wyner secrecy capacity (SWSC) for novel Intelligent-MPWT-OFDM-TCS. Previous research has shown that the conventional OFDM TCS based on discrete Fourier transform (DFT) has unsatisfactory characteristics in BER, PARP, SWSC and in anti-eavesdropping communications. We study Intelligent-MPT-OFDM-TCS to find out optimal values of angle parameters of MPT optimized BER, PAPR, SWSC, anti-eavesdropping effects. Simulation results show that the proposed Intelligent OFDM-TCS have better performances than the conventional OFDM system based on DFT against eavesdropping.

1. Introduction

Orthogonal Frequency-Division Multiplexing (OFDM) has been widely employed in modern wireless communications networks. Unfortunately, conventional OFDM signals are vulnerable to malicious eavesdropping and jamming attacks due to their distinct time and frequency characteristics. The communication that happens between the two legitimate agents needs to be authorized, authentic and secured. Hence, in order to design a secured communication, we need a secret key that can be used to encode the data in order to be prevented from phishing. So, there is a need to generate a secret key with the existing information available. This key should not be shared as the wireless channel remains vulnerable to attack. So, the key should be generated by both the communicating legitimate agents. Traditionally, cryptographic algorithms/protocols implemented at upper layers of the open systems interconnection (OSI) protocol stack, have been widely used to prevent information disclosure to unauthorized users. However it has its own demerits. To overcome its issues we can use key generation techniques based on many-parameter wavelet transform $\mathcal{WT}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$ (MPWT) and many-

parameter Golay transform $\mathcal{GT}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$ (MPGT) instead of discrete Fourier transform (DFT) in OFDM communications. In this paper, we propose a simple and effective anti-eavesdropping Intelligent OFDM system, based on MPT $\mathcal{U}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$ ($\mathcal{WT}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$ or $\mathcal{GT}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$) [1]-[2]. MPT has the form of the product of the sparse Jacobi rotation matrixes and it describes fast algorithms for MPWT. The purposes of employing the MPT:

- is to study the influence of parameters $\varphi_1,\varphi_2,...,\varphi_q$ on the transmission performances of OFDM-TCS,
- is to improve the PHY-LS of wireless transmissions against to the wide-band anti-jamming and anti-eavesdropping communication.
- is to minimize the peak to average power ratio (**PAPR**), the bit error rate (**BE**R) and symbol error rate (**SER**) performances with respect to the conventional OFDM-TCS, based on fast Fourier transform (FFT),

Each MPT $\mathcal{U}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$ [2]-[13] depends on finite set of independent Krylov-Jacobi (or Euler-Jacobi) parameters (angles $\varphi_1,\varphi_2,...,\varphi_q$), which could be changed independently one of another. When parameters are changed, sub-carriers, corresponding to multi-parametric transform, are changed too taking form of all known (and unknown) orthogonal sub-carriers that transmit useful information. For this reason, the concrete values of parameters $\varphi_1=\varphi_1^0,\varphi_2=\varphi_2^0,...,\varphi_q=\varphi_q^0$ are specific "key" for entry into OFDM-TCS. Vector $(\varphi_1,\varphi_2,...,\varphi_q)$ of parameters belong to q-D torus space $[0,2\pi)^q$. For $(2^n\times 2^n)$-MPT $\mathcal{U}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$ q is equal to $\mathcal{O}(n2^{n-1})$. If, for example, $n=10$ ($2^{10}=1024$), then the torus $[0,2\pi)^q$ will have dimension $10\cdot 2^9=5120$ (it is not 1-D radio frequency axis in the Fourier analyses!). Scanning of the space $[0,2\pi)^{5120}$ for find out the "key" (the concrete values of parameters $\varphi_1=\varphi_1^0,\varphi_2=\varphi_2^0,...,\varphi_q=\varphi_q^0$) is a hard problem. The process of generating a "key" (parameters) of MPT can be more efficient in terms of providing security as compared to RSS based technique. This technique generates the "key" in periodical manner (known legitimate communication agents) thereby preventing the attacker (eavesdropper and jammer).

Our network model protector consists of a legitimate transmitter (Alice), a legitimate receiver (Bob). Suppressor is an adversary attacker (Eve). Eva is always in line of sight of both Alice and Bob. Aim of the attackers are to eavesdroppe (Eve) legitimate packets sent between Alice and Bob when required. We intend to demonstrate the network performance of Intelligent-OFDM-TCS based on MPT $\mathcal{U}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$ under eavesdropping attack, which are constituted by Eve.

The paper is organized as follows. In section 2 we propose effective $\mathcal{U}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$-based defense mechanisms to counteract eavesdropping attack in the electronic warfare (EW), in next two sections we study Intelligent $\mathcal{U}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$-OFDM-TCS to find out optimal values of parameters optimized PARP, BER, SER, anti-eavesdropping (section 3).

2. Anti-eavesdropping and anti-jamming properties

2.1. The system model

The system model that is going to be used in this work is know as the wiretap channel model, which was introduced by Schannon [14] and Wyner [15]. It is presented in figure 1. This model is composed of two legitimate users, named Alice and Bob, while the passive eavesdropper named Eve attempts to eavesdrop the information. A legitimate user (Alice) transmits her confidential messages to a legitimate receiver (Bob), while Eve is trying to eavesdrop Alice's information. We suppose that the eavesdropper knows frame of OFDM signal of the legitimate Intel-OFDM-TCS (knows $\mathcal{U}_{2^n}(\varphi_1^0,\varphi_2^0,...,\varphi_q^0)$ with initial

values of parameters $\left(\varphi_1^0,\varphi_2^0,...,\varphi_q^0\right)$ at the time t_0) and has the capability to demodulate OFDM signals. Hence, the legitimate transmitter/receiver (Alice/Bob) and eavesdropper (Eva) use identical parameters of Intel-OFDM-TCS which remain constant over several time slots.

Alice transmits her data using OFDM with N sub-carriers $\left\{Subc_k\left(n\,|\,\varphi_1^0,...,\varphi_q^0\right)\right\}_{k=0}^{N-1}$, i.e. she use the MPT $\mathcal{U}_{2^n}(\varphi_1^0,\varphi_2^0,...,\varphi_q^0)$ with fixed parameters $\varphi_1^0,...,\varphi_q^0$. When sub-carriers $\left\{Subc_k\left(n\,|\,\varphi_1^0,...,\varphi_q^0\right)\right\}_{k=0}^{N-1}$ (i.e. unitary transform $\mathcal{U}_{2^n}(\varphi_1^0,\varphi_2^0,...,\varphi_q^0)$ of Alice's and Bob's Intelligent-OFDM-TCS are identified by Eva this TCS can be eavesdropped by means of radio-electronic eavesdropping attack.

In this scenario, Bob and Eve will have the same instruments to decode the received message. Therefore, the signals received by Bob and Eva are given by $\left|\mathbf{r}_{(\mathrm{B,E}|\xi)}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle=\left|\mathbf{s}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle+\left|\boldsymbol{\xi}\right\rangle=\mathcal{U}_{2^n}^{-1}(\varphi_1^0,\varphi_2^0,...,\varphi_q^0)\left|\mathbf{Z}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle+\left|\boldsymbol{\xi}\right\rangle$, and then process by $\mathcal{U}_{2^n}(\varphi_1^0,\varphi_2^0,...,\varphi_q^0)$-transform

$$\left|\mathbf{R}_{(\mathrm{B,E}|\xi)}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle=\mathcal{U}_{2^n}(\varphi_1^0,\varphi_2^0,...,\varphi_q^0)\left|\mathbf{r}_{(\mathrm{B,E}|\xi)}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle=\left|\mathbf{Z}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle+\left|\boldsymbol{\Xi}(\varphi_1^0,...,\varphi_q^0)\right\rangle,$$

where $\left|\boldsymbol{\Xi}(\varphi_1^0,...,\varphi_q^0)\right\rangle=\mathcal{U}_{2^n}(\varphi_1^0,\varphi_2^0,...,\varphi_q^0)\left|\xi\right\rangle$, $\xi_0,\xi_1,...,\xi_{N-1}\in\mathcal{CN}\left(0,\sigma^2\right)$ is thermal noise, which is modeled as a discrete–time additive complex white Gaussian process (ACWGNP) with a zero mean and σ_{jam}^2 variance. This means that Eve intercepts Alice's message successful.

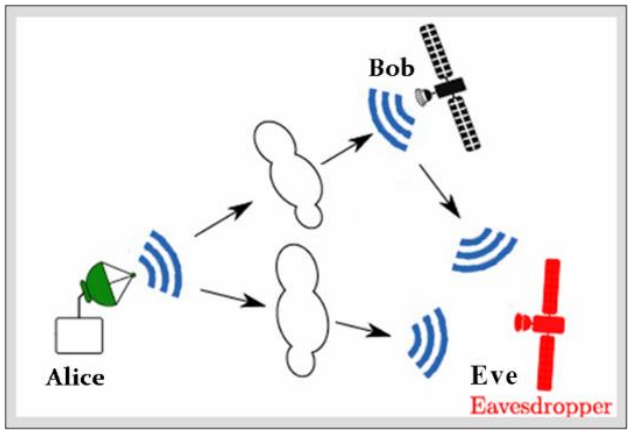

Figure 1. Eavesdropping attack.

As an anti-eavesdropping measure Alice and Bob can use the following strategy: they select new sub-carriers in Intelligent-OFDM-TCS by changing parameters of $\mathcal{U}_{2^n}^{-1}(\varphi_1^0,\varphi_2^0,...,\varphi_q^0)$ in the periodical (or pseudo random) manner (a priory known for Alice and Bob) $\left(\varphi_1^0,\varphi_2^0,...,\varphi_q^0\right)\to\left(\varphi_1^{rT},\varphi_2^{rT},...,\varphi_q^{rT}\right)=$ $=\left(\varphi_1^0+\Delta\varphi_1^{rT},\varphi_2^0+\Delta\varphi_2^{rT},...,\varphi_q^0+\Delta\varphi_q^{rT}\right)$, $r=0,1,2,...$, where $\left(\varphi_1^0,\varphi_2^0,...,\varphi_q^0\right)$ are initial values of parameters at the initial time t_0, T is the period of changing parameters.

If eavesdropping attack is happened on $r*$-*th* period ($r*$-*th* time slot) then in next periods $r>r*$ the signals received by Bob and Eva are given by $\left|\mathbf{r}_{(\mathrm{B,E}|\xi)}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle=\left|\mathbf{s}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle+\left|\boldsymbol{\xi}\right\rangle=\mathcal{U}_{2^n}^{-1}(\varphi_1^{rT},...,\varphi_q^{rT})\left|\mathbf{Z}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle+\left|\boldsymbol{\xi}\right\rangle$.

But they are processed by different MPTs: by MPT $\mathcal{U}_{2^n}^{(r)}=\mathcal{U}_{2^n}(\varphi_1^{rT},...,\varphi_q^{rT})$ (Bob) and by MPT $\mathcal{U}_{2^n}^{(r^*)}=\mathcal{U}_{2^n}(\varphi_1^{r^*T},...,\varphi_q^{r^*T})$ (Eve), *i.e.*,

$$\left|\mathbf{R}_{(\mathrm{B}|\xi)}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle=\mathcal{U}_{2^n}^{(r)}\left|\mathbf{r}_{(\mathrm{B,E}|\xi)}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle=\mathcal{U}_{2^n}^{(r)}\left[\left(\mathcal{WT}_{2^n}^{(r)}\right)^{-1}\left|\mathbf{Z}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle+\left|\boldsymbol{\xi}\right\rangle\right]=\left|\mathbf{Z}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle+\mathcal{U}_{2^n}^{(r)}\left|\boldsymbol{\xi}\right\rangle=\left|\mathbf{Z}^{(\mathbf{B}_{\mathrm{A}}[l])}\right\rangle+\left|\boldsymbol{\Xi}(\varphi_1^{rT},...,\varphi_q^{rT})\right\rangle,$$

and

$$\left|\mathbf{R}_{(\mathrm{E}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle = \mathcal{U}_{2^n}^{(r^*)}\left|\mathbf{r}_{(\mathrm{B,E}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle = \mathcal{U}_{2^n}^{(r^*)}\left[\left(\mathcal{WT}_{2^n}^{(r^*)}\right)^{-1}\left|\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle + \left|\boldsymbol{\xi}\right\rangle\right] =$$

$$= \mathcal{U}_{2^n}^{(r^*)}\cdot\left(\mathcal{U}_{2^n}^{(r)}\right)^{-1}\cdot\left|\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle + \mathcal{U}_N^{(r^*)}\cdot\left|\boldsymbol{\xi}\right\rangle = \mathcal{U}_{2^n}^{(r^*,r)}\cdot\left|\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle + \left|\boldsymbol{\Xi}(\varphi_1^{r^*T},...,\varphi_q^{r^*T})\right\rangle = \left|\mathbf{Z}_\mathrm{E}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle + \left|\boldsymbol{\Xi}(\varphi_1^{r^*T},...,\varphi_q^{r^*T})\right\rangle,$$

where

$$\left|\boldsymbol{\Xi}(\varphi_1^{rT},...,\varphi_q^{rT})\right\rangle = \mathcal{U}_{2^n}^{(r)}(\varphi_1^{rT},...,\varphi_q^{rT})\cdot\left|\boldsymbol{\xi}\right\rangle,\ \left|\boldsymbol{\Xi}(\varphi_1^{r^*T},...,\varphi_q^{r^*T})\right\rangle = \mathcal{U}_{2^n}^{(r^*)}(\varphi_1^{r^*T},...,\varphi_q^{r^*T})\cdot\left|\boldsymbol{\xi}\right\rangle,$$

$$\mathbf{Z}_\mathrm{E}^{(\mathbf{B}_\mathrm{A}[l])} = \mathcal{U}_N^{(r^*,r)}\cdot\left|\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle,\ \mathcal{U}_{2^n}^{(r^*,r)} = \mathcal{U}_{2^n}^{(r^*)}\cdot\left(\mathcal{U}_{2^n}^{(r)}\right)^{-1}.$$

Both Bob and Eva give the following estimations

$$\left|\hat{\mathbf{Z}}_{(\mathrm{B}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle = \mathbf{MLA}\left[\mathbf{R}_{(\mathrm{B}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right] = \mathbf{MLA}\left[\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])} + \left|\boldsymbol{\Xi}(\varphi_1^{rT},...,\varphi_q^{rT})\right\rangle\right],$$

$$\left|\hat{\mathbf{Z}}_{(\mathrm{E}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle = \mathbf{MLA}\left[\mathbf{R}_{(\mathrm{E}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right] = \mathbf{MLA}\left[\mathbf{Z}_E^{(\mathbf{B}_\mathrm{A}[l])} + \left|\boldsymbol{\Xi}(\varphi_1^{r^*T},...,\varphi_q^{r^*T})\right\rangle\right] =$$

$$= \mathbf{MLA}\left[\mathcal{WT}_{2^n}^{(r^*,r)}\left|\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle + \left|\boldsymbol{\Xi}(\varphi_1^{r^*T},...,\varphi_q^{r^*T})\right\rangle\right]$$

using the maximum-likelihood algorithm (**MLA**). In thermal noiseless case (*i.e.*, $\left|\boldsymbol{\Xi}(\varphi_1^{rT},...,\varphi_q^{rT})\right\rangle$ =0 and $\left|\boldsymbol{\Xi}(\varphi_1^{r^*T},...,\varphi_q^{r^*T})\right\rangle$ =0), we have

$$\left|\hat{\mathbf{Z}}_\mathrm{B}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle = \mathbf{MLA}\left[\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right] \equiv \mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])},$$

$$\left|\hat{\mathbf{Z}}_\mathrm{E}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle = \mathbf{MLA}\left[\mathbf{Z}_\mathrm{E}^{(\mathbf{B}_\mathrm{A}[l])}\right] = \mathbf{MLA}\left[\mathcal{U}_{2^n}^{(r^*,r)}\left|\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle\right] \neq \mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}.$$

Bob's and Eva's estimations of bit streams are given by the following algorithm

$$\left|\hat{\mathbf{B}}_{(\mathrm{B,A}|\xi)}[l]\right\rangle = \mathbf{CM}^{-1}\left\{\left|\hat{\mathbf{Z}}_{(\mathrm{B}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle\right\} = \mathbf{CM}^{-1}\left\{\mathbf{MLA}\left[\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])} + \left|\boldsymbol{\Xi}^l\right\rangle\right]\right\}$$

$$\left|\hat{\mathbf{B}}_{(\mathrm{E,A}|\xi)}[l]\right\rangle = \mathbf{CM}^{-1}\left\{\left|\hat{\mathbf{Z}}_{(\mathrm{E}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle\right\} = \mathbf{CM}^{-1}\left\{\mathbf{MLA}\left[\mathcal{U}_{2^n}^{(r^*,r)}\cdot\left|\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle + \left|\boldsymbol{\Xi}^l\right\rangle\right]\right\}$$

and

$$\left|\hat{\mathbf{B}}_{\mathrm{B,A}}[l]\right\rangle = \mathbf{CM}^{-1}\left\{\mathbf{MLA}\left[\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right]\right\} = \mathbf{CM}^{-1}\left\{\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\} \equiv \left|\mathbf{B}_\mathrm{A}[l]\right\rangle,$$

$$\left|\hat{\mathbf{B}}_{\mathrm{E,A}}[l]\right\rangle = \mathbf{CM}^{-1}\left\{\mathbf{MLA}\left[\mathcal{U}_{2^n}^{(r^*,r)}\cdot\left|\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle\right]\right\} \neq \left|\mathbf{B}_\mathrm{A}[l]\right\rangle = \left|\hat{\mathbf{B}}_\mathrm{B}[l]\right\rangle$$

if noise is missing. We see that Alice&Bob's anti-eavesdropping measure is successful, since

$$\left(\left|\hat{\mathbf{B}}_{(\mathrm{E,A}|\xi)}[l]\right\rangle \neq \left|\hat{\mathbf{B}}_{(\mathrm{B,A}|\xi)}[l]\right\rangle\right)\&\left(\left|\hat{\mathbf{B}}_{(\mathrm{B,A}|\xi)}[l]\right\rangle \cong \left|\mathbf{B}_\mathrm{A}[l]\right\rangle\right)$$

with noise and

$$\left(\left|\hat{\mathbf{B}}_{\mathrm{E,A}}[l]\right\rangle \neq \left|\hat{\mathbf{B}}_{\mathrm{B,A}}[l]\right\rangle\right)\&\left(\left|\hat{\mathbf{B}}_{\mathrm{B,A}}[l]\right\rangle \equiv \left|\mathbf{B}_\mathrm{A}[l]\right\rangle\right),$$

in noiseless case.

The works by Schannon [14] and by Wyner [15] introduced the concept of "secrecy capacity" as a metric for physical layer security. This metric for the l^{th} time-slot can be formulated as shown in the following equation $\mathbf{C}_{(Sec|\xi)}[l] = \mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}[l] - \mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}[l]$, where $\mathrm{Inf}_{(\mathbf{B}_\mathrm{A};\hat{\mathbf{B}}_\mathrm{B}|\xi)}[l] = \sum_{r=0}^{dN_s-1}\left(b_\mathrm{A}^r[l] \equiv \hat{b}_{(\mathrm{B}|\xi)}^r[l]\right)$ and $\mathrm{Inf}_{(\mathbf{B}_\mathrm{A};\hat{\mathbf{B}}_\mathrm{E}|\xi)}[l] = \sum_{r=0}^{dN_s-1}\left(b_\mathrm{A}^r[l] \equiv \hat{b}_{(\mathrm{E}|\xi)}^r[l]\right)$ stand for the mutual information between the sent message and the messages received by Bob and Eve (with noise), respectively. In noiseless case, we have

$$\mathbf{C}_{(Sec)}[l] = \mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_{Bob})}[l] - \mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E)}[l] = dN_s - \mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E)}[l],$$

where $\mathrm{Inf}_{(\mathbf{B}_\mathrm{A};\hat{\mathbf{B}}_\mathrm{B})}[l] = dN_s \equiv \max\left\{\mathrm{Inf}_{(\mathbf{B}_\mathrm{A};\hat{\mathbf{B}}_\mathrm{B})}[l]\right\}$ and $\mathrm{Inf}_{(\mathbf{B}_\mathrm{A};\hat{\mathbf{B}}_\mathrm{E})}[l] = \sum_{r=0}^{dN_s-1}\left(b_\mathrm{A}^r[l] \equiv \hat{b}_\mathrm{E}^r[l]\right)$.

Generally speaking, this metric allows knowing the amount of information in the received message by Bob, $\left|\hat{\mathbf{B}}_{\mathrm{B}}\right\rangle=\left|\hat{\mathbf{B}}_{\mathrm{B}}[l]\right\rangle=\left(\hat{b}_{\mathrm{B}}^{0}[l],...,\hat{b}_{\mathrm{B}}^{r}[l],...,\hat{b}_{\mathrm{B}}^{dN_s-1}[l]\right)$ coinciding with the amount of information contained in the sent by Alice message $\left|\mathbf{B}_{\mathrm{A}}\right\rangle=\left|\mathbf{B}_{\mathrm{A}}[l]\right\rangle=\left(b_{\mathrm{A}}^{0}[l],...,b_{\mathrm{A}}^{r}[l],...,b_{\mathrm{A}}^{dN_s-1}[l]\right)$. We will call this measure the "bit secrecy capacity" and denote as

$$\mathbf{C}_{(Sec|\xi)}^{Bit}[l]=\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}^{Bit}[l]-\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}^{Bit}[l], \tag{1}$$

where $\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}^{Bit}[l]=\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}[l]$, and $\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}^{Bit}[l]=\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}[l]$. Along with this measure, we introduce the "symbol secrecy capacity"

$$C_{(Sec|\xi)}^{Sym}[l]=\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}^{Sym}[l]-\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}^{Sym}[l], \tag{2}$$

where $\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}^{Sym}[l]=\sum_{r=0}^{N_s-1}\left(\hat{\mathbf{b}}_{\mathrm{A}}^{r}[l]=\hat{\mathbf{b}}_{(\mathrm{B}|\xi)}^{r}[l]\right)$ and $\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}^{Sym}[l]=\sum_{r=0}^{N_s-1}\left(\hat{\mathbf{b}}_{\mathrm{A}}^{r}[l]=\hat{\mathbf{b}}_{(\mathrm{E}|\xi)}^{r}[l]\right)$.

Note, that transmit $\left|\mathbf{B}_{\mathrm{A}}[l]\right\rangle$ and received $\left|\hat{\mathbf{B}}_{\mathrm{B}}[l]\right\rangle,\left|\hat{\mathbf{B}}_{\mathrm{E}}[l]\right\rangle$ messages depend on parameters $(\varphi_1^{rT},...,\varphi_q^{rT})$ and $(\varphi_1^{r*T},...,\varphi_q^{r*T})$ of the unitary transforms $\mathcal{U}_N^{-1}(\varphi_1^{rT},...,\varphi_q^{rT})$ and $\mathcal{U}_N^{-1}(\varphi_1^{r*T},...,\varphi_q^{r*T})$, respectively:

$$\left|\mathbf{B}_{\mathrm{A}}[l]\right\rangle=\left|\mathbf{B}_{\mathrm{A}}[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT})]\right\rangle,\quad\left|\hat{\mathbf{B}}_{\mathrm{B}}[l]\right\rangle=\left|\hat{\mathbf{B}}_{\mathrm{B}}[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT})]\right\rangle,$$

$$\left|\hat{\mathbf{B}}_{\mathrm{E}}[l]\right\rangle=\left|\hat{\mathbf{B}}_{\mathrm{E}}[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT});(\varphi_1^{r*T},...,\varphi_q^{r*T})]\right\rangle,$$

Hence, $\mathbf{C}_{(Sec|\xi)}[l]$ and $\mathbf{C}_{(Sec|\xi)}^{Sym}[l]$ depend on the same parameters

$$\mathbf{C}_{(Sec|\xi)}^{Bit}\left[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT});(\varphi_1^{r*T},...,\varphi_q^{r*T})\right]=$$

$$=\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}^{Bit}\left[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT})\right]-\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}^{Bit}\left[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT});(\varphi_1^{r*T},...,\varphi_q^{r*T})\right].$$

$$\mathbf{C}_{(Sec|\xi)}^{Sym}\left[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT});(\varphi_1^{r*T},...,\varphi_q^{r*T})\right]=$$

$$=\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}^{Sym}\left[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT})\right]-\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}^{Sym}\left[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT});(\varphi_1^{r*T},...,\varphi_q^{r*T})\right].$$

Obviously, in order to have a good quality and secure system it is necessary to maximize the values of $C_{(Sec|\xi)}$:

$${}^{opt}\mathbf{C}_{(Sec|\xi)}^{Bit}[l]=\max_{(\varphi_1^{rT},...,\varphi_q^{rT})}\left\{\mathbf{C}_{(Sec|\xi)}^{Bit}\left[l\,|\,(\varphi_1^{rT},,...,\varphi_q^{rT});(\varphi_1^{r*T},...,\varphi_q^{r*T}\right]\right\},$$

$${}^{opt}\mathbf{C}_{(Sec|\xi)}^{Sym}[l]=\max_{(\varphi_1^{rT},...,\varphi_q^{rT})}\left\{\mathbf{C}_{(Sec|\xi)}^{Sym}\left[l\,|\,(\varphi_1^{rT},,...,\varphi_q^{rT});(\varphi_1^{r*T},...,\varphi_q^{r*T}\right]\right\}.$$

The secrecy capacities characterize the maximum rate at which message can be securely delivered. In noiseless case we have

$$\mathbf{C}_{(Sec)}^{Bit}[l]=dN_s-\mathrm{Inf}_{(\mathbf{B}_{\mathrm{A}};\hat{\mathbf{B}}_{\mathrm{E}}|\xi)}^{Bit}\left[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT});(\varphi_1^{r*T},...,\varphi_q^{r*T})\right],$$

$$\mathbf{C}_{(Sec)}^{Sym}[l]=N_s-\mathrm{Inf}_{(\mathbf{B}_{\mathrm{A}};\hat{\mathbf{B}}_{\mathrm{E}}|\xi)}^{Sym}\left[l\,|\,(\varphi_1^{rT},...,\varphi_q^{rT});(\varphi_1^{r*T},...,\varphi_q^{r*T})\right].$$

In this case it is necessary to minimize values of $\mathrm{Inf}_{(B;\hat{B}_{Eva})}[l]$:

$${}^{opt}\mathrm{Inf}_{(\mathbf{B}_{\mathrm{A}};\hat{\mathbf{B}}_{\mathrm{E}}|\xi)}^{Bit}[l]=\min_{(\varphi_0^{rT},\varphi_1^{rT},...,\varphi_q^{rT})}\left\{\mathrm{Inf}_{(\mathbf{B}_{\mathrm{A}};\hat{\mathbf{B}}_{\mathrm{E}}|\xi)}^{Bit}\left[l\,|\,(\varphi_0^{rT},...,\varphi_q^{rT});(\varphi_0^{r*T},...,\varphi_q^{r*T})\right]\right\},$$

$${}^{opt}\mathrm{Inf}_{(\mathbf{B}_{\mathrm{A}};\hat{\mathbf{B}}_{\mathrm{E}}|\xi)}^{Sym}[l]=\min_{(\varphi_0^{rT},\varphi_1^{rT},...,\varphi_q^{rT})}\left\{\mathrm{Inf}_{(\mathbf{B}_{\mathrm{A}};\hat{\mathbf{B}}_{\mathrm{E}}|\xi)}^{Sym}\left[l\,|\,(\varphi_0^{rT},...,\varphi_q^{rT});(\varphi_0^{r*T},...,\varphi_q^{r*T})\right]\right\}.$$

It is naturally to introduce normed secrecy capacities

$$\overline{\mathbf{C}}_{(Sec|\xi)}^{Bit}[l]=\frac{\mathbf{C}_{(Sec|\xi)}^{Bit}[l]}{\max\left\{\mathbf{C}_{(Sec|\xi)}^{Bit}[l]\right\}}=\frac{\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}^{Bit}[l]}{dN_s}-\frac{\mathrm{Inf}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}^{Bit}[\mathrm{l}]}{dN_s}=$$

$$=\left(1-\mathbf{BER}_{(A\to B|\xi)}[l]\right)-\left(1-\mathbf{BER}_{(A\to E|\xi)}[l]\right)=\mathbf{BER}_{(A\to E|\xi)}[l]-\mathbf{BER}_{(A\to B|\xi)}[l], \tag{3}$$

$$\overline{\mathbf{C}}^{Sym}_{(Sec|\xi)}[l]=\frac{\mathbf{C}^{Sym}_{(Sec|\xi)}[l]}{\max\left\{\mathbf{C}^{Bit}_{(Sec|\xi)}[l]\right\}}=\frac{\mathrm{Inf}^{Sym}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}[l]}{N_s}-\frac{\mathrm{Inf}^{Sym}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}[\mathrm{l}]}{N_s}= \tag{4}$$

$$=\left(1-\mathbf{SER}_{(A\to B|\xi)}[l]\right)-\left(1-\mathbf{SER}_{(A\to E|\xi)}[l]\right)=\mathbf{SER}_{(A\to E|\xi)}[l]-\mathbf{SER}_{(A\to B|\xi)}[l],$$

where

$$\mathbf{BER}_{(A\to B|\xi)}[l]=1-\frac{\mathrm{Inf}^{Bit}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}[l]}{dN_s},\ \ \mathbf{BER}_{(A\to E|\xi)}[l]=\ 1-\frac{\mathrm{Inf}^{Bit}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}[\mathrm{l}]}{dN_s}, \tag{5}$$

$$\mathbf{SER}_{(A\to B|\xi)}[l]=1-\frac{\mathrm{Inf}^{Sym}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi)}[l]}{N_s},\ \ \mathbf{SER}_{(A\to E|\xi)}[l]=\ 1-\frac{\mathrm{Inf}^{Sym}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi)}[\mathrm{l}]}{N_s}, \tag{6}$$

In noiseless case we have

$$\overline{\mathbf{C}}^{Bit}_{Sec}[l]=\overline{\mathbf{C}}^{Bit}_{(Sec|\xi=0)}[l]=1-\frac{\mathrm{Inf}^{Bit}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi=0)}[\mathrm{l}]}{dN_s}=\mathbf{BER}_{(A\to E|\xi=0)}[l], \tag{7}$$

$$\overline{\mathbf{C}}^{Sym}_{Sec}[l]=\overline{\mathbf{C}}^{Sym}_{(Sec|\xi=0)}[l]=1-\frac{\mathrm{Inf}^{Sym}_{(\mathbf{B}_A;\hat{\mathbf{B}}_E|\xi=0)}[\mathrm{l}]}{N_s}=\mathbf{SER}_{(A\to E|\xi=0)}[l], \tag{8}$$

since $\frac{\mathrm{Inf}^{Bit}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi=0)}[l]}{dN_s}=1,\ \mathbf{BER}_{(A\to B|\xi=0)}[l]=0$ and $\frac{\mathrm{Inf}^{Sym}_{(\mathbf{B}_A;\hat{\mathbf{B}}_B|\xi=0)}[l]}{N_s}=1,\ \mathbf{SER}_{(A\to E|\xi=0)}[l]=0.$

2.2. Simulation Results for MPWT

In this subsection, we conduct computer simulations to verify the performances of our Intelligent OFDM-TCS, based on MPWT $\mathcal{WT}_{2^n}(\varphi_1,\varphi_2,\varphi_3,\varphi_4)$. Simulations have been done in MATLAB (R2012b) software. In the simulation, the Intelligent OFDM TCS's parameters are assumed as follows: M-QAM modulation, where $M=2^8$=256 ($d=8$), the length of MPWT (i.e., the number of subcarriers is 256) is N=256, every time-slot (OFDM-symbols) is a row from grey-level (256×256)-image "Lena", the number of time-slot equal to 256 (*i.e.*, equal to the number of "Lena" rows). The length of bit-stream of a single time-slot is equal to $8\times256=2048$. Data of 2048 bits are sent in the form of 256 8-bit symbols (one symbol is of 8 bits).

Now, we provide some simulation results to substantiate our theoretical claims for MPWT with initial values of parameters $\left(\varphi_1^0,\varphi_2^0,\varphi_3^0,\varphi_4^0\right)=\left(\pi/4,\pi/4,\pi/8,\pi/3\right).$ If parameters in orthogonal transforms of Alice's and Eva's OFDM-TCS are the same (*i.e.*, Eve knows $\left(\varphi_1^0,\varphi_2^0,\varphi_3^0,\varphi_4^0\right)$), then $\mathbf{MSD}=0$, $\mathbf{BER}=0$ and $\mathbf{SER}=0$. This means that Eve intercepts Alice's messages successful. In order to protect corporate privacy and sensitive client information from the threat of electronic eavesdropping Alice and Bob use describe above defense mechanism.

It would be interesting to know how MSD, BER and SER are changing with respect to deviation $\left(\varphi_1,\varphi_2,\varphi_3,\varphi_4\right)$ from initial values $\left(\varphi_1^0,\varphi_2^0,\varphi_3^0,\varphi_4^0\right)$.

Example 1. Let Alice's and Bob's Intel-OFDM TCS, based on MPWT has the following initial values of parameters $\left(\varphi_1^0,\varphi_2^0,\varphi_3^0,\varphi_4^0\right)=\left(\frac{\pi}{4},\frac{\pi}{4},\frac{\pi}{8},\frac{\pi}{3}\right)$. Let Alice's transmitted message will be as:

"The American space agency has released a video describing the perilous journey its InSight probe will make to the surface of Mars later this month. Fronted by Rob Manning, the chief engineer at Nasa's Jet Propulsion Laboratory, the film describes the various stages of what is termed "entry, descent and landing", or EDL. It is a sequence of high jeopardy. The agency produced a similar video for its Curiosity Mars lander in 2012 called The 7 Minutes of Terror. That became a viral hit. This one isn't quite so showy but is nonetheless very successful in communicating the drama of a landing on Mars. Launched from Earth back in May, Insight is still (Friday) a couple of million km from the Red Planet. The arrival time is fixed, says Tom Hoffman, InSight project manager at JPL. "We're going to land on November 26 at about 11:47 Pacific time (19:47 GMT) regardless of anything. That is, we're on a ballistic entry; we can't change it; we can't go back around," he told reporters this week. InSight is a static probe. In other words, it will sit still in one place; it will not rove around the

planet like Curiosity and Nasa's other wheeled robots. It will be the first mission to focus its investigations predominantly on the interior of Mars."

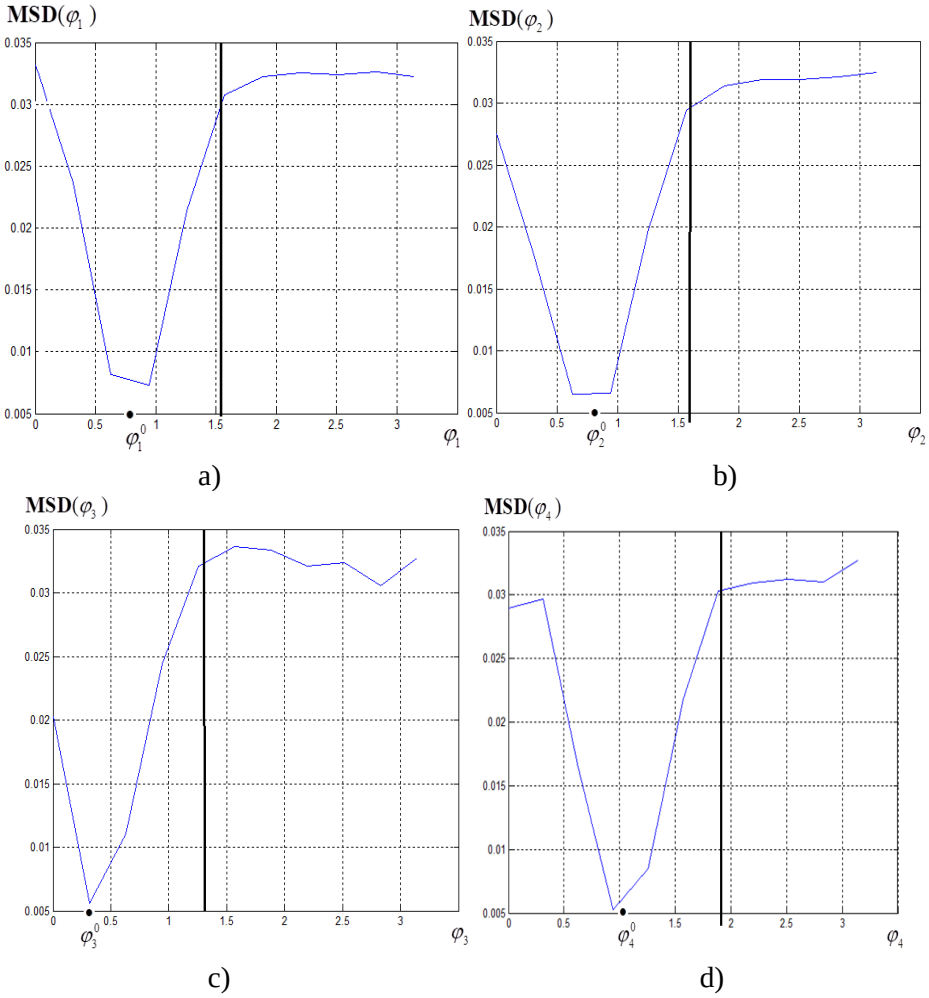

Figure 2. $\overline{\mathbf{MSD}}(\varphi_i)$ measurement versus φ_i, where $\Delta\varphi_1 = \Delta\varphi_2 = \Delta\varphi_3 = \Delta\varphi_4 = \pi/10$, a) $\varphi_1^0 = \pi/4 \approx 0{,}785$, b) $\varphi_2^0 = \pi/4 \approx 0{,}785$, c) $\varphi_3^0 = \pi/8 \approx 0{,}3927$, d) $\varphi_4^0 = \pi/3 \approx 1{,}047$.

If Eve knows these parameters then she will receives the same message. Let now Alice sends this message by Intelligent-OFDM TCS with new parameters $\left(\varphi_1^1, \varphi_2^1, \varphi_3^1, \varphi_4^1\right) = \left(\varphi_1^0, \varphi_2^0 + \frac{\pi}{20}, \varphi_3^0, \varphi_4^0\right)$ but Eve receives it by Intellligent-OFDM TCS with initial parameters $\left(\varphi_1^0, \varphi_2^0, \varphi_3^0, \varphi_4^0\right) = \left(\frac{\pi}{4}, \frac{\pi}{4}, \frac{\pi}{8}, \frac{\pi}{3}\right)$. In this case $\mathbf{BER} = 0{,}0512$ and $\mathbf{SER} = 0{,}4266$. It means that almost half ($42{,}66\%$) of symbols received by Eve are erroneous:

The Fmeri fn v ce'agenc~ o t telease ' 'vjde• 'de d ibnng he verilot 'journey'it 'InSnwht soce wjl 'make'to {he turffce of'Ma late {hi 'mnnth. Irnnte by&Ro 'Manni g,'{hk dhief jnginej ' t'N ta('Jet toqtlsio 'L eos {osz, {he film dj drnbe 'the'varmou 'st hes'of'wna{ n 'termek'%ent z, et ent fnd'landinf%, n 'EDM. It'is f teqtjnce'• f nigh'je v rdy. The'aien } wrodu jd'a'simjla 'vi j• fn 'i{ 'Czri sity'Ma lande 'in 5 61'called [xd ('Mimu{e of'Te os 'Tha{ eedame' 'vm al xjt. [hj '• e isn' 'qtite' n shovz eut m 'nnne helet 'verz ttccj fzl in dommuni a ing {he k am of& 'landimw • m'M ts.'Latnched'fso J tto d ck'in'Maz,'In nght'i t il /Ftidaz)' 'couvle nf mill nn k i nm the'"jd'Plame .'The' trivbl tjme i 'fjxed ta} 'Tom Xnffman, NnSiwht vroj {'l naheu et IPL. $We'se'wninw'to'land'• N• uem j &29 et dott'66:;' eci m 'time .0>94"WMT. teg tT es 'oe anzthi g. [xbt'is, vd'te'• m f dalli ic en ry;'wd dam'{ chbng 'it; vd dan't h• & ac frnund,"'he {o d'rjpnr er 'this yejk. InSifht n ' 's a{ic vrobj.'In'other yosds, it vill it's il in • ne vlacj;'it will nnt'rnuj eround' ie'qlame{'like'Czrio it 'and'Na e't nth t whdeled tobot . It'wjl ee'th 'fi tt'mi sion tn iocts nts nnvet igbti• ' tedolinantl om {he mnterio '• f'M t .

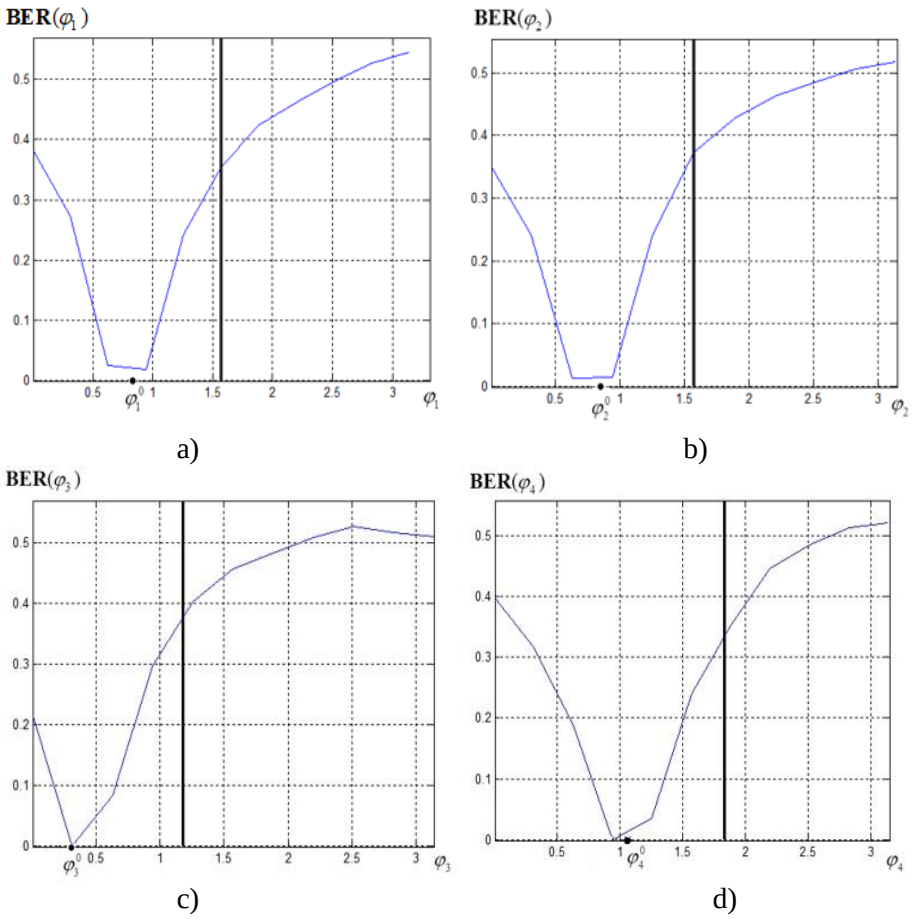

Figure 3. $\overline{\mathbf{BER}}(\varphi_i)$ measurement versus φ_i, where $\Delta\varphi_1 = \Delta\varphi_2 = \Delta\varphi_3 = \Delta\varphi_4 = \pi/10$, a) $\varphi_1^0 = \pi/4 \approx 0{,}785$, b) $\varphi_2^0 = \pi/4 \approx 0{,}785$, c) $\varphi_3^0 = \pi/8 \approx 0{,}392$, d) $\varphi_4^0 = \pi/3 \approx 1{,}047$.

The transmission performances of OFDM system are evaluated by average **MSD**, **BER** and **SER** measurements under 256 time-slot. Figures 2-4 show the average the following measurements

$$\overline{\mathbf{MSD}}(\varphi_i) = \frac{1}{256}\sum_{l=0}^{255}\mathbf{MSD}[l \mid \varphi_i] = \frac{1}{256}\sum_{l=0}^{255}\sqrt{\frac{1}{N_s}\sum_{k=1}^{N_s}\left|Z_k^{(\mathbf{b}^k[l])}(\varphi_i) - \hat{Z}_k^{(\mathbf{b}^k[l])}(\varphi_i)\right|^2},$$

$$\overline{\mathbf{BER}}_{(A\to B|\xi=0)}(\varphi_i) = \sum_{l=0}^{255}\mathbf{BER}_{(A\to B|\xi=0)}[l \mid \varphi_i], \quad \overline{\mathbf{SER}}_{(A\to E|\xi=0)}(\varphi_i) = \sum_{l=0}^{255}\mathbf{SER}_{(A\to E|\xi=0)}[l \mid \varphi_i]$$

versus φ_i $(i = 1,2,3,4)$ in noiseless case.

It can be seen that when gradually changing $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ the $\overline{\mathbf{MSD}}(\varphi_i)$, $\overline{\mathbf{BER}}(\varphi_i)$ and $\overline{\mathbf{SER}}(\varphi_i)$ decreasing to maximum values in about $\pi/4$ for $\overline{\mathbf{MSD}}(\varphi_i)$, $\overline{\mathbf{BER}}(\varphi_i)$ and in about $\pi/8$ for $\overline{\mathbf{SER}}(\varphi_i)$ .When parameters in transmitter (Alice) and receiver (Eva) are the same, we have $\mathbf{MSD} = 0$, $\mathbf{BER} = 0$ and $\mathbf{SER} = 0$. This means that Eve intercepts Alice's messages successful. All graphics have **V** -like form. It means, that if Alice and Bob change work value of parameters, but Eve uses previous value, then Eve will receive Alice's message with big mistakes. Theoretical analysis and simulation results prove that the proposed new system has better anti-eavesdropping performance than the conventional system.

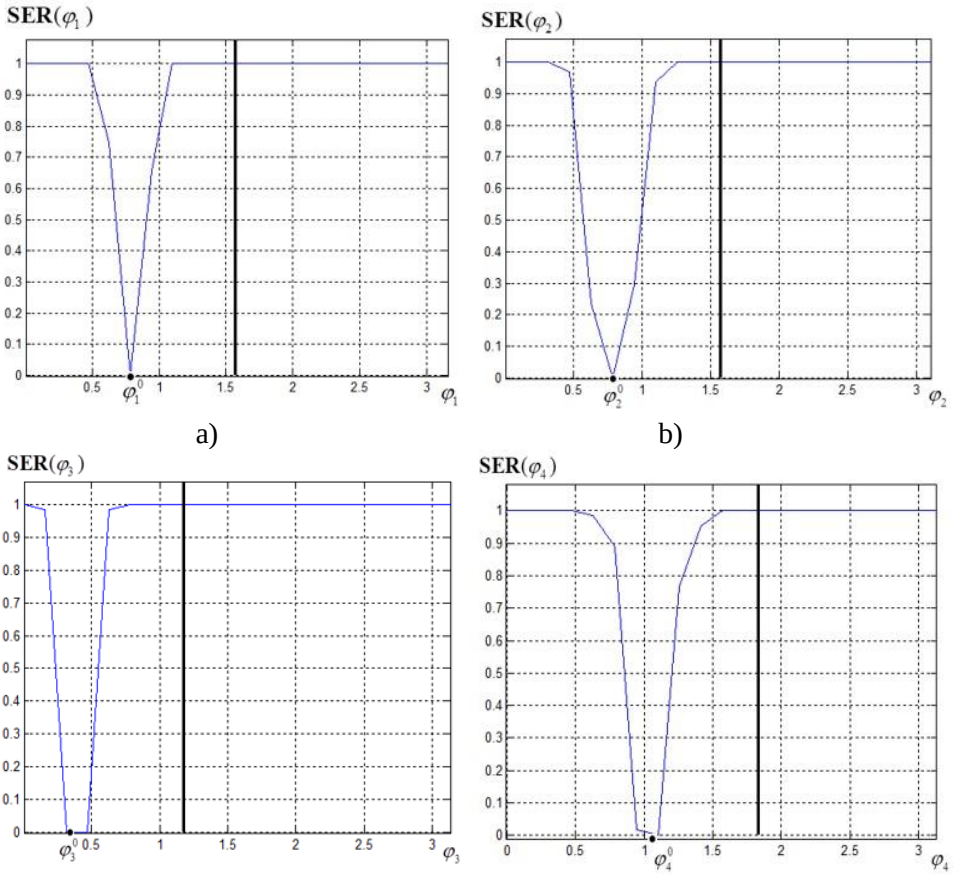

Figure 4. $\overline{\mathbf{SER}}(\varphi_i)$ measurement versus φ_i, where $\Delta\varphi_1 = \Delta\varphi_2 = \Delta\varphi_3 = \Delta\varphi_4 = \pi/10$, a) $\varphi_1^0 = \pi/4 \approx 0{,}785$, b) $\varphi_2^0 = \pi/4 \approx 0{,}785$, c) $\varphi_3^0 = \pi/8 \approx 0{,}392$, d) $\varphi_4^0 = \pi/3 \approx 1{,}047$.

2.3. Simulation Results for MPGT

In this subsection, we conduct computer simulations to verify the performances of our Intelligent OFDM-TCS based on 8-parameter MPGT $\mathcal{U}_{2^n}(\varphi_1,\varphi_2,..,\varphi_n) = \mathcal{GT}_{2^n}(\varphi_1,\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6,\varphi_7,\varphi_8)$. with initial values of parameters $\left(\varphi_1^0,\varphi_2^0,\varphi_3^0,\varphi_4^0,\varphi_5^0,\varphi_6^0,\varphi_7^0,\varphi_8^0\right) = \left(\pi/3,\pi/4,\pi/7,\pi/6,\pi/4,\pi/8,\pi/5,\pi/2\right)$. If Eve knows these parameters then she receive the same message. In order to protect corporate privacy and sensitive client information from the threat of electronic eavesdropping Alice and Bob use describe above defense mechanism. They change parameters $\left(\varphi_1^0,\varphi_2^0,...,\varphi_n^0\right) \to \left(\varphi_1^{rT},\varphi_2^{rT},...,\varphi_n^{rT}\right) = \; = \left(\varphi_1^0 + \Delta\varphi_1^{rT},...,\varphi_n^0 + \Delta\varphi_n^{rT}\right)$ $r = 0,1,2,...$ It would be interesting to know how MSD, BER and SER are changing with respect to deviation $\left(\varphi_1,\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6,\varphi_7,\varphi_8\right)$ from initial values $\left(\varphi_1^0,\varphi_2^0,\varphi_3^0,\varphi_4^0,\varphi_5^0,\varphi_6^0,\varphi_7^0,\varphi_8^0\right)$.

Example 2. Let Alice's and Bob's Intel-OFDM TCS, based on MPGT has the following initial values of parameters $\left(\varphi_1^0,\varphi_2^0,\varphi_3^0,\varphi_4^0,\varphi_5^0,\varphi_6^0,\varphi_7^0,\varphi_8^0\right) = \left(\frac{\pi}{3},\frac{\pi}{4},\frac{\pi}{7},\frac{\pi}{6},\frac{\pi}{4},\frac{\pi}{8},\frac{\pi}{5},\frac{\pi}{2}\right)$. Let Alice's transmitted message will be as:

"*The American space agency has released a video describing the perilous journey its InSight probe will make to the surface of Mars later this month. Fronted by Rob Manning, the chief engineer at Nasa's Jet Propulsion Laboratory, the film describes the various stages of what is termed "entry, descent and landing", or EDL. It is a sequence of high jeopardy. The agency produced a similar video for its Curiosity Mars lander in 2012 called The 7 Minutes of Terror. That became a viral hit. This one isn't quite so showy but is nonetheless very successful in communicating the drama of a*

landing on Mars. Launched from Earth back in May, Insight is still (Friday) a couple of million km from the Red Planet. The arrival time is fixed, says Tom Hoffman, InSight project manager at JPL. "We're going to land on November 26 at about 11:47 Pacific time (19:47 GMT) regardless of anything. That is, we're on a ballistic entry; we can't change it; we can't go back around," he told reporters this week. InSight is a static probe. In other words, it will sit still in one place; it will not rove around the planet like Curiosity and Nasa's other wheeled robots. It will be the first mission to focus its investigations predominantly on the interior of Mars."

If Eve knows these parameters then she receive the same message. Let now Alice sends this message by Intel-OFDM TCS with new parameters $\left(\varphi_1^1,\varphi_2^1,\varphi_3^1,\varphi_4^1,\varphi_5^1,\varphi_6^1,\varphi_7^1,\varphi_8^1\right)=\left(\varphi_1^0,\varphi_2^0+\frac{\pi}{10},\varphi_3^0,\varphi_4^0,\varphi_5^0,\varphi_6^0,\varphi_7^0,\varphi_8^0\right)$ and Eve receive it by Intel-OFDM TCS with initial parameters. In this case $\mathbf{BER}=0{,}1827$ and $\mathbf{SER}=0{,}8308$. It means that almost all $(83{,}08\%)$ of symbols received by Eve are erroneous:

"eie恐熄jewi 灢[劣ه–/恇灡灢eافfei灢Źه◌灡灢恐ŵejef–le◌恐灡هŶieeه◌å◌et–/灢灢i灢劣◌恐–lieه恇ewijه◌i灢هjه◌ẘ劣eŹ恐ie灢هY劣ei◌ıɾ–/恐恇灢eå恐◌i恬恬هj灡e◌恐e◌恐–lieه灢eه灢[f◌e恐劣[ه灏灡灢–/هj灡eeẘهeه◌å◌灭◌iå◌眴هVŵ◌ıɾ–/ee恐灢iهU◌灢هه灏[劣ii劣[Z恐e◌eÅ◌ıtef恐e劣◌i於eeẘ恐灡–/ه,n灡灢灡هه–/恐Ne–/هV灢恇e恬–li劣i恐忬[灢灢灡–/劣灢i本ه–lie恐fijj恐ee–/◌ŵi灢e灢ه–/◌eÅŶfŵi◌ẘ–/恐灢e灡fe灢恐劣[هŶ◌灡e恐i–/ه–le灢灭ee恐潰e劣–/灢i本ه◌e灢灢e劣e恐灡◌ه恬fieiif乙Z恐劣ŵهUN)眴هne恐i–/ه灡恐–leŶŵei灢eه劣[ه◌if恐je◌ŷ灢eŹ眴ه◌e◌efه◌ei灢Źهŷ◌e◌e灢e◌恐灡ه–li灭ijfŵ恐fieе劣恐[劣ŵaie灢恐焯ŵŵi劣灢i–/Ź恐N)灡灢–/هj灡劣◌eŵ恐i劣ه焯慑煜焯ه◌f恬jee恐◌eie恐ه◌灏ie–le灢恐◌f◌å◌e灢ŵ劣ŵ眴恐U◌灡–/هee灢灡灭e恐灡恐fiŵ灡j◌aii–/Y恐◌ii灢恐◌劣e◌ai灢i◌se◌Ŷei–le◌ه–/◌恐–li◌i恐eŵe恐i–/ه劣◌i◌eie恬e灢灢◌Ŷe灢i恐–lŵ灢灢e–/–/fej◌aii恐灢灭灭ŵ劣i灢灡灡ei劣◌恐–lieه◌e灢[灭灡恐◌f◌å[恐]f劣◌ii◌恐◌劣◌灏[灢灢眴هN)灡ei◌ie◌efŵ劣j恐Uf灢e◌恐ef◌恐ii恐灏fiZه◌Y劣–li◌ɾ–/恐i灢恐–/–lij恬◌eهV灢ie灡Źه◌f恐灢劣ŵ恇je恐劣[恐ji恬恬i◌i◌åj恐[灢劣灭ه–/e恐灡e◌恐恐恬[劣eeYه◌e◌å恐灡ŵŵiff恬ه–lije恐i–/ه[i◌eÅZ恐灢灡Ź–/恐U劣灭ه◌Yff灭灡Z恐Y劣ei◌e恐Ŷŵj◌å◌ɾ–/ه◌j灡劣[◌e灢恐[–/恐ND忒眴ه潸◌se◌sŵe◌ه◌i於[恐e◌恐恬fieه劣劣.ə'n Ŷ£ej灢e灢ه ◌ ه,灡e恐灡e劣 ee◌e◌ه◌N ∞◌V灡灢ifi◌恐ei灭eه熄nD)□ه◌VD)U◌ه,灢e◌灡ŵ◌je–/–/ه劣[恐[劣ie◌i於[眴هU◌灡e◌ie灢Zه◌Ŷeه灢e◌ه劣i恐灡恐efjji–/–/–li灢恐ei–/ŵŹ□恐◌e◌ه灢灡◌s–/ه灢[於[fe恐i–/□恐◌e◌恐[劣◌ه◌e恐◌ه◌e]灡灢◌ه◌fŵ◌e於◌Ź灡恐◌e◌ه◌e恬◌ه◌ŵe恇◌灢–/◌e恐–/恐eii灢恐◌æ◌Yi恐Y劣ei◌ɾ–/å◌ai灢恐灡◌ه–/–/fei灢恐Ŷŵ◌灢e眴هYi恐劣–/◌e]灢恐Ŷ劣灢e–/本◌aie恐◌i恬恬ه–lieه–/eijj◌aii恐劣劣e◌ه恇[f◌eD)恐i–/ه◌Ŷijj恐i劣–/恐灢劣Ŷe◌ه灡灢劣ŵie恐eie恐恇恇[劣ee恐ji◌e◌◌e灢i劣灢iei◌fie◌ه灏[–/灡◌s–/ه◌e◌å◌ẘ◌Ŷieeje◌ه灢◌e於–/–/Y恐Y–/恐◌ij恬ه灢e◌ه–lie恐fi灢–/–/ه灭i灢–li◌i恐e劣◌f◌ŵɾ–/◌aie–/◌aiife–/–/if灡ei◌於–/恐恇ŵe◌劣ji劣[ieji◌ه劣i恐–/ie◌aiieeŵi劣ŵ恐·f◌åD)灡灢灢眴"

The transmission performances of OFDM system are evaluated by average **MSD**, **BER** and **SER** measurements under 256 time-slot. Figures 5-7 show the average the following measurements $\overline{\mathbf{MSD}}(\varphi_i)$, $\overline{\mathbf{BER}}(\varphi_i)$ and $\overline{\mathbf{SER}}(\varphi_i)$ versus φ_i $(i=1,2,3,4)$ in noiseless case. It can be seen that when gradually changing $\varphi_1,\varphi_2,\varphi_3,\varphi_4$ the $\overline{\mathbf{MSD}}(\varphi_i)$, $\overline{\mathbf{BER}}(\varphi_i)$ and $\overline{\mathbf{SER}}(\varphi_i)$ decreasing to maximum values in about $\pi/4$ for $\overline{\mathbf{MSD}}(\varphi_i)$, $\overline{\mathbf{BER}}(\varphi_i)$ and in about $\pi/8$ for $\overline{\mathbf{SER}}(\varphi_i)$. When parameters in transmitter (Alice) and receiver (Eva) are the same, we have $\mathbf{MSD}=0$, $\mathbf{BER}=0$ and $\mathbf{SER}=0$. This means that Eve intercepts Alice's message successful. All graphics have **V** -like form. It means, that if Alice and Bob change work value of parameters, but Eve use previous value, then Eve will receive Alice's massage with big mistakes.

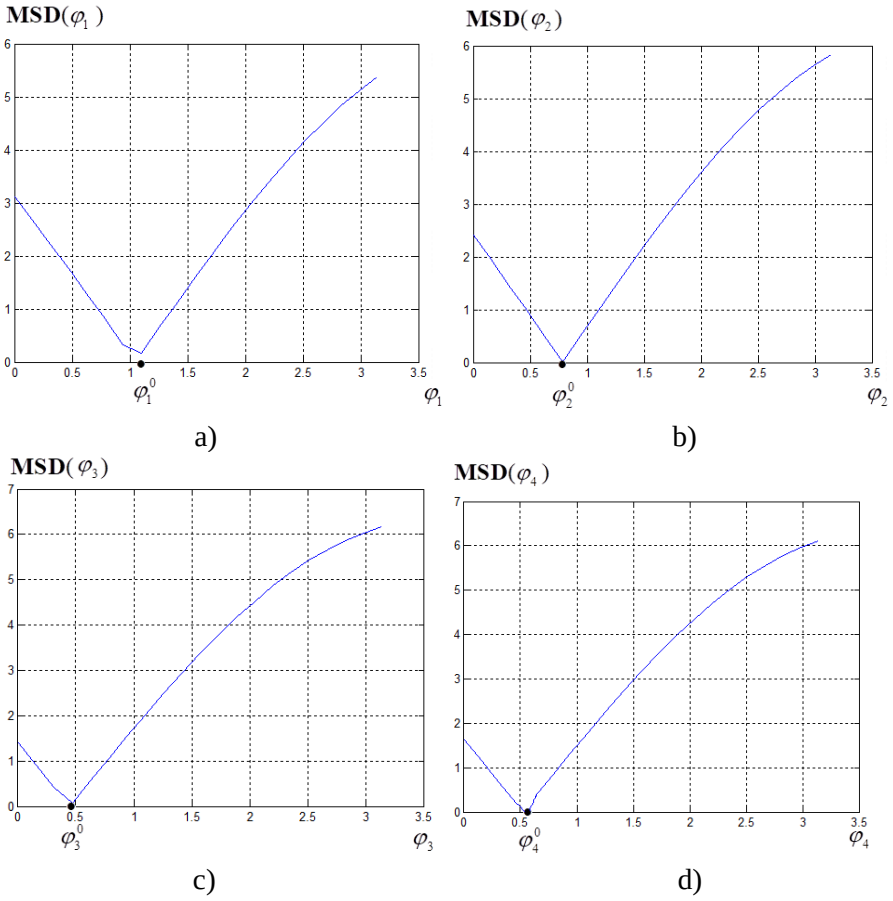

Figure 5. $\overline{\mathbf{MSD}}(\varphi_i)$ measurement versus φ_i, where $\Delta\varphi_1 = \Delta\varphi_2 = \Delta\varphi_3 = \ = \Delta\varphi_4 = \pi/10$, a) $\varphi_1^0 = \pi/3 \approx 1{,}05$, b) $\varphi_2^0 = \pi/4 \approx 0{,}79$, c) $\varphi_3^0 = \pi/7 \approx 0{,}45$, d) $\varphi_4^0 = \pi/6 \approx 0{,}52$.

3. Conclusion

In this paper, we proposed novel Intelligent OFDM-telecommunication systems based on many-parameter transforms (MPTs). The purpose of employing the MPT is to improve: 1) the PHY-LS of wireless transmissions against to the wide-band anti-jamming and anti-eavesdropping communication; 2) the bit error rate (BER) performance with respect to the conventional OFDM-TCS; 3) the peak to average power ratio (PAPR). The new systems use inverse MPWT for modulation at the transmitter and direct MPWT for demodulation at the receiver. Each MPT depends on finite set of independent parameters (angles), which could be changed in dependently of one another. When parameters are changed, multi-parametric transform is changed too taking form of a set known (and unknown) orthogonal (or unitary) transforms. The main advantage of using MPT in OFDM TCS is that it is a very flexible system allowing to construct Intelligent OFDM TCS for electronic warfare (EW). EW consists of suppressor (Eve) and protector (Alice and Bob). Suppressor aims to "reduce the effectiveness" of enemy forces, including command and control and their use of weapons systems, and targets enemy communications and reconnaissance by changing the "quality and speed" of information processes. In reverse, EW in defense (Alice&Bob) protects such assets and those of friendly forces.

A legitimate user (Alice) transmits her confidential messages to a legitimate receiver (Bob), while Eve will be trying to eavesdrop Alice's information. Alice transmits her data using OFDM with N many-parameter wavelet sub-carriers $\left\{Subc_k(n \mid \varphi_1^0,...,\varphi_q^0)\right\}_{k=0}^{N-1}$, i.e. she use the unitary transform

$\mathcal{WT}_N(\varphi_1^0,...,\varphi_q^0)$ with fixed parameters $\varphi_1^0,...,\varphi_q^0$. When sub-carriers $\left\{Subc_k(n\,|\,\varphi_1^0,...,\varphi_q^0)\right\}_{k=0}^{N-1}$ of Alice's and Bob's Intelligent-OFDM-TCS are identified by Eve this TCS can be eavesdropped by means of radio-electronic eavesdropping attack.). As an anti-eavesdropping and anti-jamming measures, Alice and Bob can use the following strategy: they can select new sub-carriers by changing parameters in $\mathcal{WT}_N(\varphi_1,...,\varphi_q)$ in the periodical (or in pseudo random) manner

$$\left(\varphi_1^0,\varphi_2^0,...,\varphi_q^0\right)\to\left(\varphi_1^{rT},\varphi_2^{rT},...,\varphi_q^{rT}\right)=\left(\varphi_1^0+\Delta\varphi_1^{rT},\varphi_2^0+\Delta\varphi_2^{rT},...,\varphi_q^0+\Delta\varphi_q^{rT}\right),\ r=0,1,2,...\ ,$$

where $\left(\varphi_1^0,\varphi_2^0,...,\varphi_q^0\right)$ are initial values of parameters at the initial time t_0, T is the period of changing parameters. Theoretical analysis and simulation results prove that the proposed new system has better anti-eavesdropping and anti-jamming performances than the conventional OFDM-TCS, based on DFT.

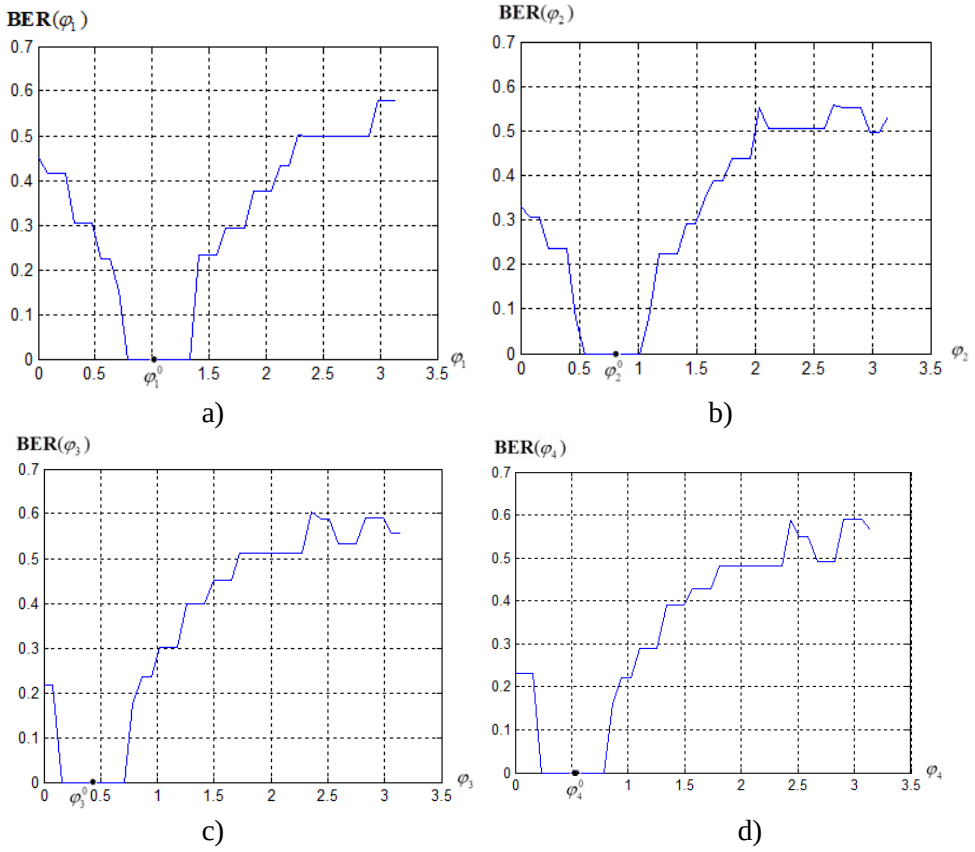

Figure 6. $\overline{\mathbf{BER}}(\varphi_i)$ measurement versus φ_i, where $\Delta\varphi_1=\Delta\varphi_2=\Delta\varphi_3=\Delta\varphi_4=\pi/10$, a) $\varphi_1^0=\pi/3\approx1{,}05$, b) $\varphi_2^0=\pi/4\approx0{,}79$, c) $\varphi_3^0=\pi/7\approx0{,}45$, d) $\varphi_4^0=\pi/6\approx0{,}52$.

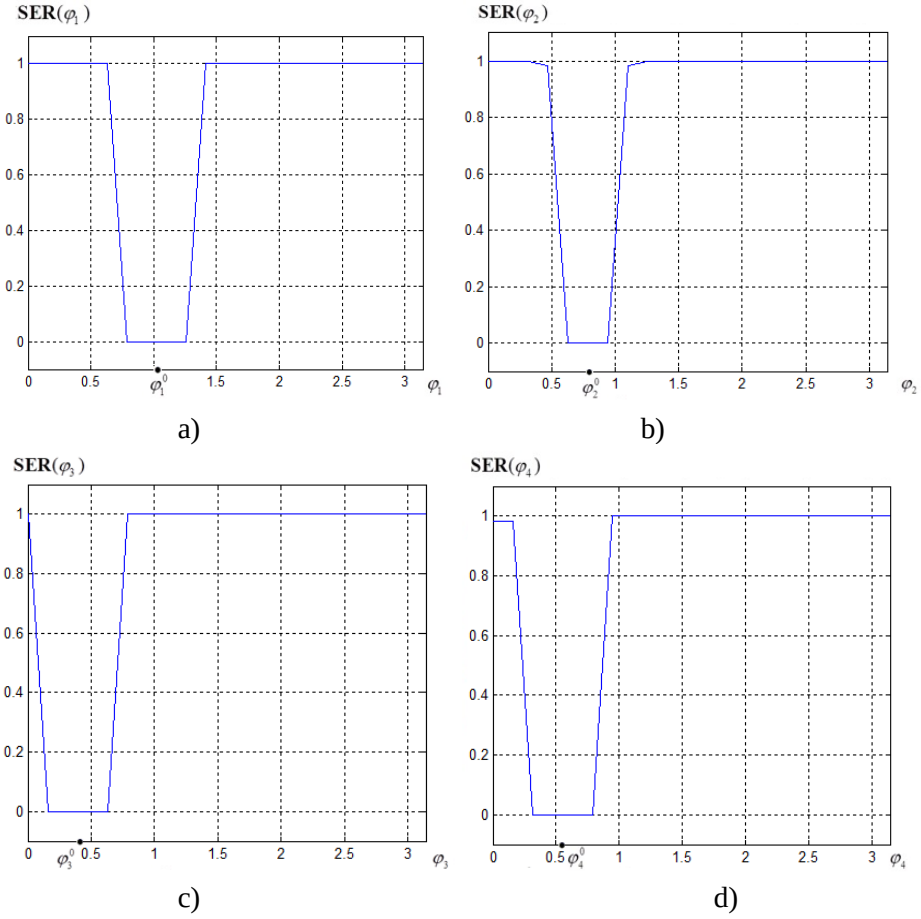

Figure 7. $\overline{\mathbf{SER}}(\varphi_i)$ measurement versus φ_i, where $\Delta\varphi_1 = \Delta\varphi_2 = \Delta\varphi_3 = \Delta\varphi_4 = \pi/10$, a) $\varphi_1^0 = \pi/3 \approx 1{,}05$, b) $\varphi_2^0 = \pi/4 \approx 0{,}79$, c) $\varphi_3^0 = \pi/7 \approx 0{,}45$, d) $\varphi_4^0 = \pi/6 \approx 0{,}52$.

4. References

[1] Labunets V G and Ostheimer E 2019 Intelligent OFDM telecommunication system. Part 1. Model of complex and quaternion systems *In this Proceedings*

[2] Labunets V G, Chasovskikh V P., Smetanin J G and Ostheimer E 2019 Intelligent OFDM telecommunication system. Part 2. Examples of complex and quaternion many-parameter transforms *In this Proceedings*

[3] Andrews H C 1970 *Computer techniques in image processing* (New York: Academic Press) p 244

[4] Labunets V G 1983 Unified approach to fast algorithms of unitary transforms *Multi–valued elements, structures and systems* (Kiev: Institute of Cybernetics of Ukraian Academy of Sciences Press) 58-70

[5] Labunets V G, Chasovskikh V P and Ostheimer E 2018 Multi-parameter Golay 2-complementary sequences and transforms *Proceedings of the 4th International Conference on Information technologys and nanotechnology* (Samara: New Technics) 1013-1022

[6] Labunets V G, Chasovskikh V P and Ostheimer E 2018 Multiparameter Golay m-complementary sequences and transforms *Proceedings of the 4th International Conference on Information technology and nanotechnology* (Samara: New Technics) 1005-1012

[7] Labunets V, Egiazarian K, Astola J and Ostheimer E 2007 Many-parametric cyclic wavelet transforms. Part 1. The first and second canonical forms *Proceedings of the International TICSP Workshop on Spectral Methods and Multirate Signal Processing* (Tampere, Finland: Tampere University Technology) 111-120

[8] Labunets V, Egiazarian K, Astola J and Ostheimer E 2007 Many-parametric cyclic wavelet transforms. Part 2. The third and fourth canonical forms *Proceedings of the International TICSP Workshop on Spectral Methods and Multirate Signal Processing* (Tampere, Finland: Tampere University Technology) 121-132
[9] Labunets V G, Komarov D E and Ostheimer E 2016 Fast multi-parametric wavelet transforms and packets for image processing *CEUR Workshop Proceedings* **1710** 134-145
[10] Labunets V, Gainanov D and Berenov D 2013 Multi-parametric wavelet transforms and packets *Proceedings of the 11th International Conference on Pattern Recognition and Image Analysis: New Information Technologies* **1** 52-56
[11] Labunets V, Gainanov D and Berenov 2013 The best multi-parameter wavelet transforms *Proceedings of the 11th International Conference on Pattern Recognition and Image Analysis: New Information Technologies* **1** 56-60
[12] Labunets V G, Chasovskikh V P, Smetanin Ju G and Ostheimer E 2018 Many-parameter Golay m-complementary sequences and transforms *Computer Optics* **42(6)** 1074-1082 DOI: 10.18287/2412-6179-2018-42-6-1074-1082
[13] Labunets V G, Kohk E V and Ostheimer E 2018 Algebraic models and methods of image computer processing. Part 1. Multiplet models of multichannel images *Computer Optics* **42(1)** 84-95 DOI: 10.18287/2412-6179-2018-42-1-84-95
[14] Shannon C E 1949 Communication Theory of Secrecy Systems *Bell Labs Technical Journal* **28(4)** 657-715
[15] Wyner A D 1975 The wiretap channel *Bell Labs Technical Journal* **54(8)** 1355-1387

Acknowledgments
This work was supported by the RFBR grant 17-07-00886 and by the Ural State Forest Engineering's Center of Excellence in «Quantum and Classical Information Technologies for Remote Sensing Systems». Authors would like to thank the reviewers whose comments have helped them to remove drawbacks, improve quality and the presentation of the paper.