Intelligent OFDM Telecommunication Systems Based On Many-Parameter Complex Or Quaternion Fourier Transforms

Valeriy G. Labunets[1], Ekaterina Ostheimer[2]

[1]Ural State Forest Engineering University, 37, Sibirskiy Trakt, 620100, Ekaterinburg, Russian Federation
[2]Capricat LLC, Pompano Beach, Florida, USA

vlabunets05@yahoo.com

Abstract. In this paper, we propose novel Intelligent quaternion OFDM-telecommunication systems based on many-parameter complex and quaternion transform (MPFT). The new systems use inverse MPFT (IMPFT) for modulation at the transmitter and direct MPFT (DMPFT) for demodulation at the receiver. The purpose of employing the MPFT 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). Each MPFT depends on finite set of independent parameters (angles). When parameters are changed, many-parametric transform is also changed taking form of different quaternion orthogonal transforms. For this reason, the concrete values of parameters are specific "key" for entry into OFDM-TCS. Vector of parameters belong to multi-dimension torus space. Scanning of this space for find out the "key" (the concrete values of parameters) is hard problem.

Keywords: Many-parameter transforms, complex and quaternion Fourier transform, OFDM, noncommutative modulation and demodulation, telecommunication system, anti-eavesdropping communication.

1. Introduction

In today's world, an important aspect of communication and technology is security. Wars are being fought in the virtual world rather than in the real world. There is a rapid increase in cyber warfare. Ensuring information security is of paramount importance for wireless communications. Due to the broadcast nature of radio propagation, any receiver within the cover range can listen and analyze the transmission without being detected, which makes wireless networks vulnerable to eavesdropping and jamming attacks. 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. Therefore, 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 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 [1]. However, the layered design architecture with transparent physical layer leads to a loss in security functionality [2], especially for wireless communication scenarios where a common physical medium is always shared by legitimate and non-legitimate users. Moreover, the cryptographic protocols can only offer a computational security [3]. As an alternative, exploiting physical layer characteristics for secure transmission has become an emerging hot topic in wireless communications [4–7]. The pioneering work by Wyner in [4] introduced the concept of “secrecy capacity” as a metric for PHY-layer security (PHY-LS). It is pointed out that perfect security is in fact possible without the aid of an encryption keys when the source-eavesdropper channel is a degraded version of the source-destination (main) channel.

As the physical-layer transmission adversaries can blindly estimate parameters of OFDM signals, traditional upper-layer security mechanisms cannot completely address security threats in wireless OFDM systems. Physical layer security, which targets communications security at the physical layer, is emerging as an effective complement to traditional security strategies in securing wireless OFDM transmission. The physical layer security of OFDM systems over wireless channels was investigated from an information-theoretic perspective in [8].

In this paper, we propose a simple and effective anti-eavesdropping and anti-jamming Intelligent OFDM system, based on many-parameter complex or quaternion Fourier transforms (MPFTs). $\mathcal{U}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$. In this paper, we aim to investigate the superiority and practicability of MPFTs from the physical layer security (PHY-LS) perspective. The main advantage of using MPFT in OFDM TCS is that it is a very flexible anti-eavesdropping and anti-jamming Intelligent OFDM TCS. The paper are organized as follows. Section 2 of the paper presents a brief introduction to the conventional OFDM system along with various notations used in the paper and novel Intelligent-OFDM-TCS based on MPFT $\mathcal{U}_{2^n}(\varphi_1,\varphi_2,...,\varphi_q)$ transforms. Section 3 and 4 present many-parameter complex- and quaternion-valued Fourier transforms, respectively. In section 5 we introduce new many-parameter complex- and quaternion-valued all-pass filters.

2. Intelligent complex and quaternion OFDM TCS

The conventional OFDM is a multi-carrier modulation technique that is basic technology having high-speed transmission capability with bandwidth efficiency and robust performance in multipath fading environments. OFDM divides the available spectrum into a number of parallel orthogonal sub-carriers and each sub-carrier is then modulated by a low rate data stream at different carrier frequency. In OFDM system, the modulation and demodulation can be applied easily by means of inverse and direct discrete Fourier transforms (DFT). The conventional OFDM will be denoted by the symbol $\mathcal{F}_N$-**OFDM**. Conventional OFDM-TCS makes use of signal orthogonality of the multiple sub-carriers $e^{j2\pi kn/N}$ (discrete complex exponential harmonics). All sub-carriers $\{\mathbf{subc}_k(n)\}_{k=0}^{N-1} = \{e^{j2\pi kn/N}\}_{k=0}^{N-1}$ form matrix of discrete orthogonal Fourier transform $\mathcal{F}_N = [\mathbf{subc}_k(n)]_{k,n=0}^{N-1} \equiv [e^{j2\pi kn/N}]_{k,n=0}^{N-1}$. At the time, the idea of using the fast algorithm of different orthogonal transforms $\mathcal{U}_N = [\mathbf{subc}_k(n)]_{k,n=0}^{N-1}$ for a software-based implementation of the OFDM's modulator and demodulator, transformed this technique from an attractive [9,10]. OFDM-TCS, based on arbitrary orthogonal (unitary) transform $\mathcal{U}_N$ will be denoted as $\mathcal{U}_N$-**OFDM**. The idea which links $\mathcal{F}_N$-**OFDM** and $\mathcal{U}_N$-**OFDM** is that, in the same manner that the complex exponentials $\{e^{j2\pi kn/N}\}_{k=0}^{N-1}$ are orthogonal to each-other, the members of a family of $\mathcal{U}_N$-sub-carriers $\{\mathbf{subc}_k(n)\}_{k=0}^{N-1}$ (rows of the matrix $\mathcal{U}_N$) will satisfy the same property.

The $\mathcal{U}_N$-**OFDM** reshapes the multi-carrier transmission concept, by using carriers $\{\mathbf{subc}_k(n)\}_{k=0}^{N-1}$ instead of OFDM's complex exponentials $\{e^{j2\pi kn/N}\}_{k=0}^{N-1}$. There are a number of candidates for orthogonal function sets used in the OFDM-TCS: discrete wavelet sub-carriers [11,12], Golay complementary sequences [13-15], Walsh functions [16,17], pseudo random sequences [18,19].

Intelligent-OFDM TCS can be described as a dynamically reconfigurable TCS that can adaptively regulate its internal parameters as a response to changes in the surrounding environment. One of the most important capacities of Intelligent OFDM systems is their capability to optimally adapt their operating parameters based on observations and previous experiences. There are several possible approaches towards realizing such intelligent capabilities. In this work, we aim to investigate the superiority and practicability of MPFTs from the physical layer security perspective.

In this work, we propose a simple and effective anti-eavesdropping and anti-jamming Intelligent OFDM system, based on many-parameter transform. In our Intelligent-OFDM-TCS we use complex or quaternion MPFTs $\mathcal{U}_N(\varphi_1,\varphi_2,...,\varphi_q)$ instead of ordinary DFT $\mathcal{F}_N$. Each MPFT depends on finite set of free parameters $\boldsymbol{\theta} = (\varphi_1,\varphi_2,...,\varphi_q)$, and each of them can take its value form 0 to 2π. When parameters are changed, MPFT is changed too taking form of known (and unknown) complex or quaternion transforms. The vector of parameters $\boldsymbol{\theta} = (\varphi_1,\varphi_2,...,\varphi_q) \in \mathbf{Tor}_q[0,2\pi] = [0,2\pi]^q$ belongs to the *q-D* torus . When the vector $(\varphi_1,\varphi_2,...,\varphi_q)$ runs completely the q-D torus $\mathbf{Tor}_q[0,2\pi]$, the ensemble of the orthogonal quaternion transforms is created. Intelligent OFDM system uses some concrete values of the parameters $\varphi_1 = \varphi_1^0, \varphi_2 = \varphi_2^0,...,\varphi_q = \varphi_q^0$, *i.e.*, it uses a concrete realization of MPFT $\mathcal{QU}_N^0 \equiv \mathcal{QU}_N(\varphi_1^0,\varphi_2^0,...,\varphi_q^0)$. The vector $(\varphi_1^0,\varphi_2^0,...,\varphi_q^0)$ plays the role of some analog key (see Fig. 1), whose knowing is necessary for entering into the TCS with the aim of intercepting the confidential information.

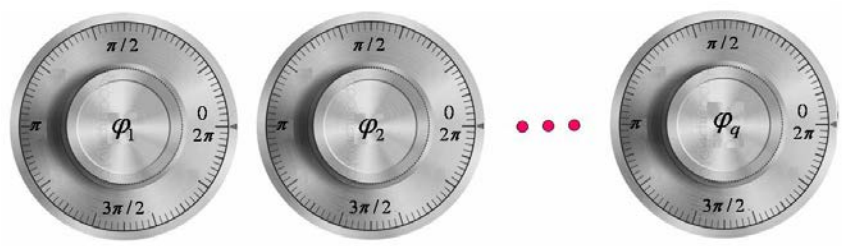

Fig. 1. Key of parameters $(\varphi_1, \varphi_2, ..., \varphi_q)$

Quantity of parameters can achieve the values $p = 10\ 000$. So, searching the vector key by scanning the 10000-dimensional torus $[0, 2\pi]^{10\ 000}$ with the aim of finding the working parameters $(\varphi_1^0, \varphi_2^0, ..., \varphi_q^0)$ is very difficult problem for the enemy cyber-means. But if, nevertheless, this key were found by the enemy in the cyber attack, then the system could change values of the working parameters for rejecting the enemy attack. If the system is one of the TCP type, then in such a case, it will transmit the confidential information on the new sub-carriers (*i.e.*, in the new orthogonal basis). As a result, the system will counteract against the enemy radio-electronic attacks.

MPFT $\mathcal{U}_N(\boldsymbol{\theta})$ has the form of the product of the sparse Jacoby rotation matrixes and which describes a fast algorithm for this transform. The main advantage of using MPFT in OFDM TCS is that it is a very flexible anti-eavesdropping and anti-jamming Intelligent OFDM TCS. To the best of our knowledge, this is the first work that utilizes the MPT theory to facilitate the PHY-LS through parameterization of unitary transforms.

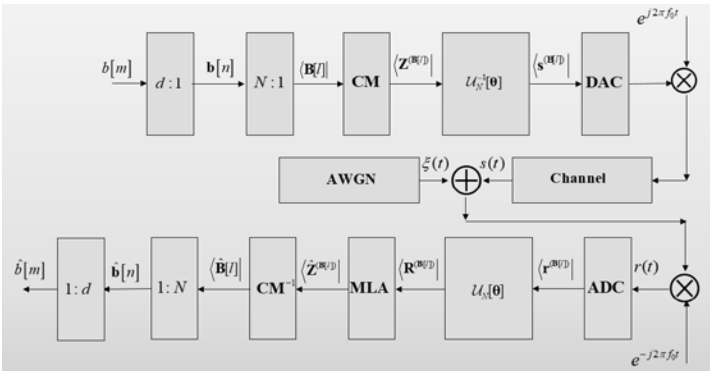

Fig. 2. Block diagram of Intelligent OFDM-TCS

We do study of Intelligent $\mathcal{U}_N(\boldsymbol{\theta})$-OFDM-TCS to find out optimal values of parameters optimized PARP, BER, SER, anti-eavesdropping and anti-jamming effects (see next parts of our work). For simplicity, we consider a single-input single-output OFDM (SISO-OFDM) setup with N sub-carriers (see Fig. 2). Let

$$2^d\text{-}\mathbf{CD} = \begin{cases} \left\{ Z^{(\mathbf{b})} = Z^{(b_0,b_1,\dots,b_{d-1})} \in \mathbf{C} \,\middle|\, \mathbf{b} = (b_0,b_1,\dots,b_{d-1}) \in \{0,1\}^d \right\}, \\ \left\{ Q^{(\mathbf{b})} = Q^{(b_0,b_1,\dots,b_{d-1})} \in \mathbb{H} \,\middle|\, \mathbf{b} = (b_0,b_1,\dots,b_{d-1}) \in \{0,1\}^d \right\} \end{cases}$$

be constellation diagrams on the complex plane $\mathbf{C}$ or on the quaternion algebra $\mathbb{H}$ consisting of 2^d complex $Z^{(\mathbf{b})} = Z^{(b_0,b_1,\dots,b_{d-1})} \in \mathbf{C}$ or quaternion $Q^{(b_0,b_1,\dots,b_{d-1})} \in \mathbb{H}$ points (stars) and numbered by binary d-digital numbers $\langle \mathbf{b} | = (b_0,b_1,\dots,b_{d-1}) \in \{0,1\}^d$. Here $\{0,1\}^d$ is d-D Boolean cube. We interpret row-vector $\langle \mathbf{b} | = (b_0,b_1,\dots,b_{d-1})$ as an address of star $Z^{(\mathbf{b})} = Z^{(b_0,b_1,\dots,b_{d-1})}$ (or $Q^{(b_0,b_1,\dots,b_{d-1})}$) in computer memory. Let us introduce the following designations

$$\mathbf{CM}(b_0,b_1,\dots,b_{d-1}) = \begin{cases} Z^{(b_0,b_1,\dots,b_{d-1})}, \\ Q^{(b_0,b_1,\dots,b_{d-1})}, \end{cases} \quad \langle \mathbf{b} | = \begin{cases} \mathbf{CM}^{-1}\left\{ Z^{(b_0,b_1,\dots,b_{d-1})} \right\} \\ \mathbf{CM}^{-1}\left\{ Q^{(b_0,b_1,\dots,b_{d-1})} \right\} \end{cases} = (b_0,b_1,\dots,b_{d-1}) \in \{0,1\}^d,$$

where $\mathbf{CM}$ and $\mathbf{CM}^{-1}$ are constellation direct and inverse mappings.

The principle of any OFDM system is to split the input 1-bit stream $b[m]$, $m = 0,1,\dots$ into d-bit stream ($\mathbf{B}_2^d$-valued stream): $b[m] = b[nd + r] \to \mathbf{b}[n] = (b_0[n],\dots,b_r[n],\dots,b_{d-1}[n])$, where $\mathbf{b} \in \mathbf{B}_2^d = \{0,1\}^d$, $m = nd + r$, $r = 0,1,\dots,d-1$ and $n = 0,1,2\dots$. Here m is the real discrete time, n is the "time" for d-bit stream $\mathbf{b}(n)$ (i.e., the d-decimation "time" with respect to real discrete time). The $\mathbf{B}_2^d$-valued sequence $\mathbf{b}(n)$ is split into N sub-sequences (sub-streams) $\mathbf{b}[n] = \mathbf{b}[lN + k] \to \langle \mathbf{B}[l] | = (\mathbf{b}^0[l],\dots,\mathbf{b}^k[l],\dots,\mathbf{b}^{N-1}[l])$, where $n = lN + k$, $k = 0,1,\dots,N-1$ and $l = 0,1,2\dots$. The row-vector $\langle \mathbf{B}[l] | = (\mathbf{b}^0[l],\mathbf{b}^1[l],\dots,\mathbf{b}^k[l],\dots,\mathbf{b}^{N-1}[l])$ is called the l^{th} $\{0,1\}^d$-valued time-slot. Here l is the "time" for time-slot $\langle \mathbf{B}[l] |$ (i.e., the N-decimation "time" with respect to d-bit stream "time" n and Nd-decimation "time" with respect to real discrete time m).

The data of the l^{th} time-slot $\langle \mathbf{B}[l] |$ is first being processed by complex or quaternion constellation mappings: $\mathbf{b}^k[l] \to \mathbf{CM}\{\mathbf{b}^k[l]\} = Z_k^{(\mathbf{b}^k[l])}$, or $\mathbf{b}^k[l] \to \mathbf{CM}\{\mathbf{b}^k[l]\} = Q_k^{(\mathbf{b}^k[l])}$, where $k = 0,1,\dots,N-1$, *i.e.*,

$$\left| {}^4\mathbf{Q}^{(\mathbf{B}[l])} \right\rangle = \begin{bmatrix} \mathbf{CM}\{\mathbf{b}^0[l]\} \\ \vdots \\ \mathbf{CM}\{\mathbf{b}^k[l]\} \\ \vdots \\ \mathbf{CM}\{\mathbf{b}^{N-1}[l]\} \end{bmatrix} = \begin{bmatrix} Q_0^{(\mathbf{b}^0[l])} \\ \vdots \\ Q_k^{(\mathbf{b}^k[l])} \\ \vdots \\ Q_{N-1}^{(\mathbf{b}^{N-1}[l])} \end{bmatrix}, \text{ or } \left| Z^{(\mathbf{B}[l])} \right\rangle = \begin{bmatrix} \mathbf{CM}\{\mathbf{b}^0[l]\} \\ \vdots \\ \mathbf{CM}\{\mathbf{b}^k[l]\} \\ \vdots \\ \mathbf{CM}\{\mathbf{b}^{N-1}[l]\} \end{bmatrix} = \begin{bmatrix} Z_0^{(\mathbf{b}^0[l])} \\ \vdots \\ Z_k^{(\mathbf{b}^k[l])} \\ \vdots \\ Z_{N-1}^{(\mathbf{b}^{N-1}[l])} \end{bmatrix}.$$

Complex numbers and quaternions $S^{(\mathbf{B}[l])} := \begin{cases} Z^{(\mathbf{B}[l])} \\ Q^{(\mathbf{B}[l])} \end{cases}$ $(k = 0,1,...,N-1)$ are called data symbols. These symbols are then input into the inverse (complex or quaternion) MPFT $\mathcal{U}_N^{-1}(\boldsymbol{\theta})$ block:

$$\mathcal{U}_N^{-1}(\boldsymbol{\theta}) \circ \begin{bmatrix} S_0^{(\mathbf{b}^0[l])} \\ \vdots \\ S_k^{(\mathbf{b}^k[l])} \\ \vdots \\ S_{N-1}^{(\mathbf{b}^{N-1}[l])} \end{bmatrix} = \begin{bmatrix} s_0^{(\mathbf{B}[l])} \\ \vdots \\ s_v^{(\mathbf{B}[l])} \\ \vdots \\ s_{N-1}^{(\mathbf{B}[l])} \end{bmatrix} = \left| \mathbf{s}^{(\mathbf{B}[l])} \right\rangle.$$

The sequences of coefficients $s_0^{(\mathbf{B}[l])},...,s_v^{(\mathbf{B}[l])},...,s_{N-1}^{(\mathbf{B}[l])}$ can be conveniently visualized as discrete composite complex-valued or quaternion-valued signals to be transmitted. They are sums of modulated complex-valued or quaternion-valued $\mathbf{subc}_k(v\,|\,\boldsymbol{\theta})$ sub-carriers: $s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}) = \sum_{k=0}^{N-1} S_k^{(\mathbf{b}^k[l])} \cdot \mathbf{subc}_k(v\,|\,\boldsymbol{\theta})$, *i.e.*, $s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}) = \sum_{k=0}^{N-1} Z_k^{(\mathbf{b}^k[l])} \cdot \mathbf{subc}_k(v\,|\,\boldsymbol{\theta})$, for complex TKS and

$$s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}) = \sum_{k=0}^{N-1} Q_k^{(\mathbf{b}^k[l])} \circ \mathbf{subc}_k(v\,|\,\boldsymbol{\theta}) \text{ or } s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}) = \sum_{k=0}^{N-1} \mathbf{subc}_k(v\,|\,\boldsymbol{\theta}) \circ Q_k^{(\mathbf{b}^k[l])}$$

for quaternion TKS (it is noncommutative modulation) , where N is the number of sub-carriers. All sub-carriers transmit dN data bits. Let the symbol $key = 0$ means multiplication of the data vector $\left\langle \mathbf{Q}^{(\mathbf{B}[l])} \right| = \left(Q_0^{(\mathbf{B}[l])},...,Q_v^{(\mathbf{B}[l])},...,Q_{N-1}^{(\mathbf{B}[l])} \right)$ on the matrix element $\mathbf{subc}_k(v\,|\,\boldsymbol{\theta})$ of $\mathcal{U}_N^{-1}(\boldsymbol{\theta}) = \left[\mathbf{subc}_k(v\,|\,\boldsymbol{\theta})\right]_{k,v=0}^{N-1}$ from the left (L) and the symbol $key = 1$ means the multiplication from the right (R). Then the N-D binary vector $\mathbf{key} = (key_0, key_1,...,key_{N-1})$ is the digital vector key (see Fig. 3) showing onto the way, by which the multiplication of the MPFT matrix $\mathcal{U}_N^{-1}(\boldsymbol{\theta})$ on the data vector $\left| \mathbf{Q}^{(\mathbf{B}[l])} \right\rangle$ has to be implemented:

$$\left| \mathbf{s}^{(\mathbf{B}[l])} \right\rangle = \mathcal{U}_N^{-1}(\boldsymbol{\theta};\mathbf{key}) \circ \left| \mathbf{Q}^{(\mathbf{B}[l])} \right\rangle \;\Rightarrow\; \begin{cases} \mathbf{subc}_k(v\,|\,\boldsymbol{\theta}) \circ Q_k^{(\mathbf{b}^k[l])}, & key_k = 0, \\ Q_k^{(\mathbf{b}^k[l])} \circ \mathbf{subc}_k(v\,|\,\boldsymbol{\theta}), & key_k = 1, \end{cases}.$$

where $\left\{\mathbf{subc}_k(v\,|\,\boldsymbol{\theta})\right\}_{k,n=1}^{N}$ are the set of matrix elements of quaternion transform, *i.e.*, $\mathcal{U}_N^{-1}(\boldsymbol{\theta};\mathbf{key}) = \left[\mathbf{subc}_k^{key_k}\left(n\,|\,\theta_1,\theta_2,...,\theta_p\right)\right]_{k,n=0}^{N-1}$. So, the number of such keys is equal to 2^N. They form the Boolean cube $\mathbf{B}_2^N$. Knowing this digital key is necessary to enter into the Intelligent OFDM TCS.

Digital data $\left\langle \mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right|$ is interpolated by digital-to-analog converter $\left\langle \mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right| \xrightarrow{\text{DAC}} s^{(\mathbf{B}[l])}(t\,|\,\boldsymbol{\theta})$, $\left(t \in [0,T]\right)$ in generating the analog signal $s^{(\mathbf{B}[l])}(t\,|\,\boldsymbol{\theta})$. It is then AM-modulated $\left[1+m\cdot s^{(\mathbf{B}[l])}(t\,|\,\boldsymbol{\theta})\right]\cdot e^{j2\pi f_0 t}$ to the carrier frequency f_0 and radiated to a wireless medium, the so-called radio channel (RF), before it is picked up at the receiver side. Here m is the AM-modulation index.

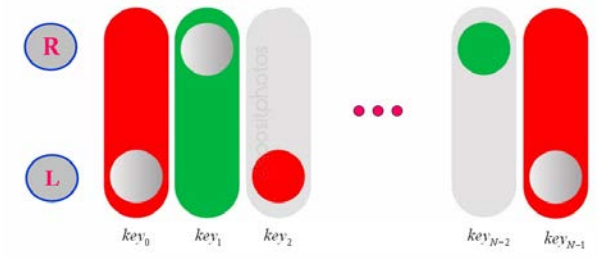

Fig. 3. N -D binary vector-key $\mathbf{key}=(key_0, key_1,..., key_{N-1})$

At the receiver side, after AM-demodulation and discretization by analog-to-digital converter (ADC) from received signal $r(t\,|\,\boldsymbol{\theta})$ we obtain the received symbols $\left\langle \mathbf{r}^{(\mathbf{B}[l])}(\boldsymbol{\theta})\right|$. They are the transmitted symbols $\left\langle \mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta})\right|$ plus additive Gaussian noise samples: $\left\langle \mathbf{r}^{(\mathbf{B}[l])}(\boldsymbol{\theta})\right| = \left(r_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}),...,r_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}_q),...,r_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta})\right)=$

$$=\left\langle \mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta})\right|+\left\langle \xi\right| = \left(s_0^{(\mathbf{B}[l])}(\boldsymbol{\theta})+\xi_0(l),...,s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta})+\xi_v(l),...,s_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta})+\xi_{N-1}(l)\right).$$

At the receiver side the process is reversed to obtain the data. The signal $\left\langle \mathbf{r}^{(\mathbf{B}[l])}\right| = \left(r_0^{(\mathbf{B}[l])},...,r_v^{(\mathbf{B}[l])},...,r_{N-1}^{(\mathbf{B}[l])}\right)$ is demodulated by direct MPFT. The output of DMPFT is represented as follow:

$$\left\langle \mathbf{R}^{(\mathbf{b}^k[l])}(\boldsymbol{\theta})\right| = \left\langle \mathbf{r}^{(\mathbf{B}[l])}(\boldsymbol{\theta})\right|\cdot \mathcal{U}_N(\boldsymbol{\theta}) = \begin{cases} \left\langle \mathbf{Z}^{(\mathbf{B}[l])}\right| + \left\langle \Xi(l\,|\,\boldsymbol{\theta})\right|, \\ \left\langle \mathbf{Q}^{(\mathbf{B}[l])}\right| + \left\langle \Xi(l\,|\,\boldsymbol{\theta})\right|. \end{cases}$$

After that the maximum-likelihood algorithm (**MLA**) gives the optimal estimation of the signal $\left\langle \mathbf{Z}^{(\mathbf{B}[l])}\right|$ or $\left|\mathbf{Q}^{(\mathbf{B}[l])}\right\rangle$:

$$\begin{cases} \mathbf{MLA}\left[\left\langle \mathbf{Z}^{(\mathbf{B}[l])}\right| + \left\langle \Xi(l\,|\,\boldsymbol{\theta})\right|\right] = \\ \mathbf{MLA}\left[\left\langle \mathbf{Q}^{(\mathbf{B}[l])}\right| + \left\langle \Xi(l\,|\,\boldsymbol{\theta})\right|\right] = \end{cases}$$

$$=\begin{cases} \left(\mathbf{MLA}\left[\hat{Z}_0^{(\mathbf{b}^0[l])}+\Xi_0(l\,|\,\boldsymbol{\theta})\right],...,\mathbf{MLA}\left[\hat{Z}_{N-1}^{(\mathbf{b}^{N-1}[l])}+\Xi_{N-1}(l\,|\,\boldsymbol{\theta})\right]\right) = \\ \left(\mathbf{MLA}\left[\hat{Q}_0^{(\mathbf{b}^0[l])}+\Xi_0(l\,|\,\boldsymbol{\theta})\right],...,\mathbf{MLA}\left[\hat{Q}_{N-1}^{(\mathbf{b}^{N-1}[l])}+\Xi_{N-1}(l\,|\,\boldsymbol{\theta})\right]\right) = \end{cases}$$

$$=\begin{cases} \left(\min\limits_{Z\in 2^d\text{-}\mathbf{CD}} \rho\left\{\hat{Z}_0^{(\mathbf{b}^0[l])}+\Xi_0(l\,|\,\boldsymbol{\theta}),Z\right\},...,\min\limits_{Z\in 2^d\text{-}\mathbf{CD}} \rho\left\{\hat{Z}_{N-1}^{(\mathbf{b}^{N-1}[l])}+\Xi_{N-1}(l\,|\,\boldsymbol{\theta}),Z\right\}\right) = \\ \left(\min\limits_{Q\in 2^d\text{-}\mathbf{CD}} \rho\left\{\hat{Q}_0^{(\mathbf{b}^0[l])}+\Xi_0(l\,|\,\boldsymbol{\theta}),Q\right\},...,\min\limits_{Q\in 2^d\text{-}\mathbf{CD}} \rho\left\{\hat{Q}_{N-1}^{(\mathbf{b}^{N-1}[l])}+\Xi_{N-1}(l\,|\,\boldsymbol{\theta}),Q\right\}\right) = \end{cases}$$

$$=\begin{cases}\left\langle \hat{\mathbf{Z}}_{opt}^{(\mathbf{B}[l])}\right| = \left(\hat{Z}_0^{(\mathbf{b}^0[l])},...,\hat{Z}_k^{(\mathbf{b}^k[l])},...,\hat{Z}_{N-1}^{(\mathbf{b}^{N-1}[l])}\right). \\ \left\langle \hat{\mathbf{Q}}_{opt}^{(\mathbf{B}[l])}\right| = \left(\hat{Q}_0^{(\mathbf{b}^0[l])},...,\hat{Q}_k^{(\mathbf{b}^k[l])},...,\hat{Q}_{N-1}^{(\mathbf{b}^{N-1}[l])}\right),\end{cases}$$

where ρ is the Euclidean distance on $\mathbf{C}$ or $\mathbb{H}$ and the symbol "$\wedge$" over means estimated value. Finally, estimation of bit stream is given as

$$\left\langle \hat{\mathbf{B}}[l\,|\,\boldsymbol{\theta}]\right| = \left(\hat{\mathbf{b}}^0[l\,|\,\boldsymbol{\theta}],...,\hat{\mathbf{b}}^{N-1}[l\,|\,\boldsymbol{\theta}]\right) =$$

$$= \mathbf{QCM}^{-1}\left\{\left\langle \hat{\mathbf{Z}}_{opt}^{(\mathbf{B}[l])}(\boldsymbol{\theta})\right|\right\} = \left(\mathbf{QCM}^{-1}\left\{\hat{Z}_0^{(\mathbf{b}^0[l])}(\boldsymbol{\theta})\right\},..,\mathbf{QCM}^{-1}\left\{\hat{Z}_{N-1}^{(\mathbf{b}^{N-1}[l])}(\boldsymbol{\theta})\right\}\right),$$

for complex TKS and

$$\left\langle \hat{\mathbf{B}}[l\,|\,\boldsymbol{\theta}]\right| = \left(\hat{\mathbf{b}}^0[l\,|\,\boldsymbol{\theta}],...,\hat{\mathbf{b}}^{N-1}[l\,|\,\boldsymbol{\theta}]\right) =$$

$$\mathbf{QCM}^{-1}\left\{\left\langle \hat{\mathbf{Q}}_{opt}^{(\mathbf{B}[l])}(\boldsymbol{\theta})\right|\right\} = \left(\mathbf{QCM}^{-1}\left\{\hat{Q}_0^{(\mathbf{b}^0[l])}(\boldsymbol{\theta})\right\},..,\mathbf{QCM}^{-1}\left\{\hat{Q}_{N-1}^{(\mathbf{b}^{N-1}[l])}(\boldsymbol{\theta})\right\}\right),$$

for quaternion NKS, where $\hat{\mathbf{b}}^k[l\,|\,\boldsymbol{\theta})] \to \hat{\mathbf{b}}[lN+k\,|\,\boldsymbol{\theta})] \to \hat{b}\left[(lN+k)d+r\,|\,\boldsymbol{\theta}\right] = \hat{b}\left[m\,|\,\boldsymbol{\theta}\right]$ is an estimation of initial bit stream. Here, $m=\left[(lN+k)d+r\right]=lNd+kd+r$ and $l=0,1,2,...$, $k=0,1,...,N-1$, $r=0,1,...,d-1$. The **BER** and **SER** for l^{th} time slot are defined as

$$\mathbf{BER}_{\mathcal{U}}[l\,|\,\boldsymbol{\theta}] = \frac{1}{Nd}\sum_{m=0}^{Nd-1}\left(b\left[m\middle|\boldsymbol{\theta}\right]\oplus\hat{b}\left[m\middle|\boldsymbol{\theta}\right]\right),\ \ \mathbf{SER}_{\mathcal{U}}[l\,|\,\boldsymbol{\theta}] = \frac{1}{N}\sum_{k=0}^{N-1}\left(\hat{\mathbf{b}}^k\left[l\middle|\boldsymbol{\theta}\right]\neq\hat{\mathbf{b}}^k\left[l\middle|\boldsymbol{\theta}\right]\right).$$

As we see in digital Intelligent-OFDM TCS, many-parameter sub-carriers are used to carry the digital data $\left\{S_k^{(\mathbf{b}^k[l])}\right\}_{k=0}^{N-1}$. By this reason, all coefficients $s_0^{(\mathbf{B}[l])}(\boldsymbol{\theta};\mathbf{key}),...,s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta};\mathbf{key}),...,s_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta};\mathbf{key})$ depend on parameters $\boldsymbol{\theta}=(\varphi_1,...,\varphi_q)$ and vector $\mathbf{key}=(key_0,key_1,...,key_{N-1})$. This dependence can be used for multiple purposes such as, anti-eavesdropping and anti-jamming in order to increase the system secrecy. It is interesting to minimize the peak to average power ratio $\mathbf{PARP}_{\mathcal{U}}[l\,|\,\boldsymbol{\theta}]$, the bit error rate $\mathbf{BER}_{\mathcal{U}}[l\,|\,\boldsymbol{\theta}]$, symbol error rate $\mathbf{SER}_{\mathcal{U}}[l\,|\,\boldsymbol{\theta}]$, inter-symbol interference $\mathbf{ISI}_{\mathcal{U}}[l\,|\,\boldsymbol{\theta}]$ by chaining of parameters $\boldsymbol{\theta}$.

3. Fast many-parameter complex Fourier transforms

Fast Fourier transform is the following iteration procedure (see Fig. 4):

$$\mathcal{F} = \frac{1}{\sqrt{2^n}}\prod_{r=1}^{n}\left(\left[I_{2^{r-1}}\otimes\left(I_{2^{n-r}}\oplus\Delta_{2^{n-r}}\left(\varepsilon^{\cdot 2^{r-1}}\right)\right)\right]\cdot\left[I_{2^{r-1}}\otimes\mathbf{F}_2\otimes I_{2^{n-r}}\right]\right), \qquad (1)$$

where $\mathbf{F}_2=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$, $\Delta_{2^{n-r}}\left(\varepsilon^{2^{r-1}}\right)=\mathbf{Diag}_{2^{n-r}}\left(1,\varepsilon^{2^{r-1}\cdot 1},\varepsilon^{2^{r-1}\cdot 2},...,\varepsilon^{2^{r-1}\cdot(2^{n-r}-1)}\right)$. Its iteration steps are indexed by integer $r\in\{1,2,...,n\}$. For each iteration r we introduce digital representation for $p\in\{0,1,...,2^{n-1}-1\}$: $p=p(k_r,s_r)=2^{r-1}k_r+s_r$. where $k_r\in\{0,1,...,2^{r-1}-1\}$, $s_r\in\{0,1,...,2^{n-r}-1\}$. Let and $q(k_r,s_r)=p(k_r,s_r)+2^{n-1}$. Obviously, $q\in\{2^{n-1},,...,2^n-1\}$.

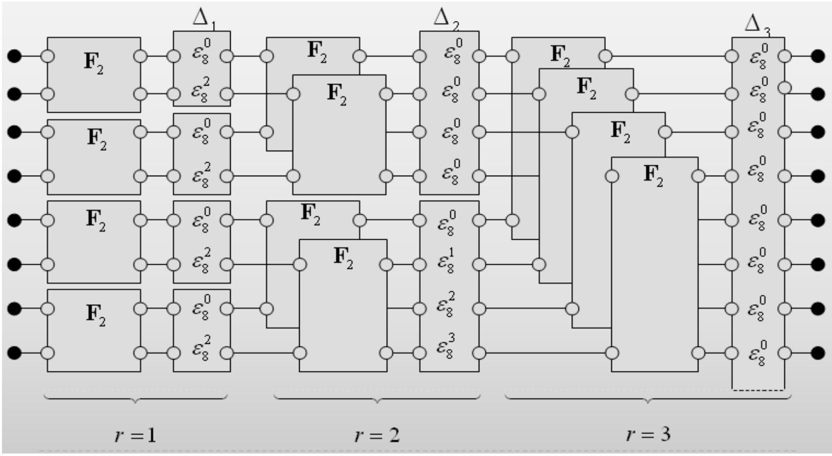

Fig. 4. Fast Fourier transforms for $N=8$.

For fixed integer $r\in\{1,2,...,n\}$ and $p_r,q_r\in\{0,1,...,2^{n-r}-1\}$ let

$$\Delta_{2^{n-r+1}}^{(p_r,q_r)}=\Delta_{2^{n-r+1}}^{(p_r,q_r)}\left(\varepsilon_{p_r}^{a(p_r)}\mid\varepsilon_{q_r}^{b(q_r)}\right)=\mathbf{Diag}_{2^{n-r+1}}\left\{\overbrace{\underbrace{1,...,\varepsilon_{p_r}^{a(p_r)}}_{p_r},1,...,1}^{2^{n-r}}\middle|\overbrace{\underbrace{1,...,\varepsilon_{q_r}^{b(q_r)}}_{p_r},1,...,1}^{2^{n-r}}\right\},$$

where $a=a(p_r),b=b(q_r)$ are integers depending on positions p_r and $q_r=p_r+2^{n-r}$, respectively. Here $\varepsilon=\exp(2\pi j/2^n)$. For $\left(I_{2^{n-r}}\oplus\Delta_{2^{n-r}}\left(\varepsilon^{\cdot 2^{r-1}}\right)\right)$ from (1) we have

$$I_{2^{n-r}}\oplus\Delta_{2^{n-r}}\left(\varepsilon_{p_r}^{p_r\cdot 2^{r-1}}\right)=\mathbf{Diag}_{2^{n-r}}(1,1,,...,1)\oplus\mathbf{Diag}_{2^{n-r}}\left(1,\varepsilon^{1\cdot 2^{r-1}},\varepsilon^{2\cdot 2^{r-1}},...,\varepsilon^{(2^{n-r}-1)\cdot 2^{r-1}}\right)=$$

$$=\prod_{p_r=0}^{2^{n-r}-1}\Delta_{2^{n-r+1}}^{(p_r,p_r+2^{n-r})}\left(1_{p_r}^{p_r}\mid\varepsilon_{p_r+2^{n-r}}^{p_r\cdot 2^{r-1}}\right).$$

Now we are going to use in fast Fourier transform the following radix-$(2^{r-1},2^{n-r})$ representation of $p,q\in\{0,1,...,2^{n-1}-1\}$: $p=p(k_r,s_r)=2^{r-1}k_r+s_r$, $q(k_r,s_r)=p(k_r,s_r)+$ $+2^{n-r}$, where $k_r\in\{0,1,...,2^{r-1}-1\}$, $s_r\in\{0,1,...,2^{n-r}-1\}$ and $r\in\{1,2,...,n\}$. We can write diagonal matrices of FFT (for all $r\in\{1,2,...,n\}$) as

$$I_{2^{r-1}}\otimes\left(I_{2^{n-r}}\oplus\Delta_{2^{n-r}}\left(\varepsilon_{p_r}^{p_r\cdot 2^{r-1}}\right)\right)=\prod_{k_r=0}^{2^{r-1}-1}\prod_{s_r=0}^{2^{n-r}-1}\Delta_{2^n}^{(p(k_r,s_r),q(k_r,s_r))}(1_{p(k_r,s_r)}^{s_r}\mid\varepsilon_{q(k_r,s_r)}^{s_r\cdot 2^{n-r}}).\qquad(2)$$

Then fast DFT (1) takes the following form

$$\mathcal{F}=\prod_{r=1}^{n}\left(\left[\prod_{k_r=0}^{2^{r-1}-1}\prod_{s_r=0}^{2^{n-r}-1}\Delta_{2^n}^{(p(k_r,s_r),q(k_r,s_r))}\left(1_{p(k_r,s_r)}^{s_r}\middle|\varepsilon_{q(k_r,s_r)}^{s_r\cdot 2^{n-r}}\right)\right]\cdot\left[\prod_{k_r=0}^{2^{r-1}-1}\prod_{s_r=0}^{2^{n-r}-1}\mathbf{J}_{2^n}^{p(k_r,s_r),q(k_r,s_r)}(\pi/4)\right]\right)=$$

$$=\prod_{r=1}^{n}\left(\prod_{s_r=0}^{2^{n-r}-1}\prod_{k_r=0}^{2^{r-1}-1}\left[\Delta_{2^n}^{(p(k_r,s_r),q(k_r,s_r))}\left(1^{s_r}_{p(k_r,s_r)}\middle|\varepsilon^{s_r\cdot 2^{n-r}}_{q(k_r,s_r)}\right)\cdot \mathbf{J}_{2^n}^{p(k_r,s_r),q(k_r,s_r)}(\pi/4)\right]\right), \qquad (3)$$

where

$$\mathbf{J}_N^{(p,q)}(\varphi_{pq})=\begin{array}{c c}
 & \begin{array}{ccccccc} & & p & & q & & \end{array}\\
\begin{array}{c} \\ \\ p \\ \\ q \\ \\ \\ \end{array} &
\left(\begin{array}{ccc|c|c|cc}
1 & \cdots & 0 & \cdots & 0 & \cdots & 0\\
\vdots & \ddots & \vdots & & \vdots & & \vdots\\
0 & \cdots & c_{p,q} & \cdots & s_{p,q} & \cdots & 0\\
\vdots & & \vdots & 1 & \vdots & & \vdots\\
0 & \cdots & s_{p,q} & \cdots & -c_{p,q} & \cdots & 0\\
\vdots & & \vdots & & \vdots & \ddots & \vdots\\
0 & \cdots & 0 & \cdots & 0 & \cdots & 1
\end{array}\right)
\end{array},$$

is the Jacobi rotation, $c_{p,q}=\cos(\varphi_{p,q}),\ s_{p,q}=\sin(\varphi_{p,q})$.

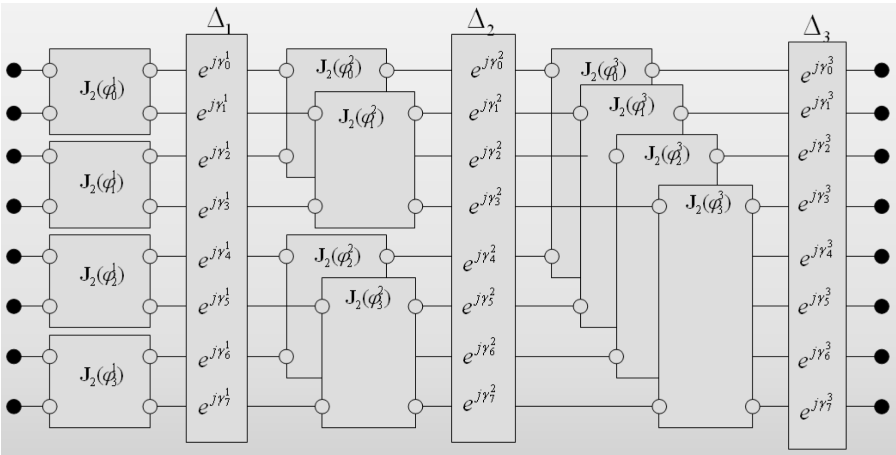

Fig. 5. Fast complex-valued many-parameter Fourier transforms for $N=8$, where we have $n\cdot 2^{n-1}=12$ φ-parameters $\boldsymbol{\varphi}^1=\left(\varphi_0^1,\varphi_1^1,\varphi_2^1,\varphi_3^1\right)$, $\boldsymbol{\varphi}^2=\left(\varphi_0^2,\varphi_1^2,\varphi_2^2,\varphi_3^2\right)$, $\boldsymbol{\varphi}^3=\left(\varphi_0^3,\varphi_1^3,\varphi_2^3,\varphi_3^3\right)$, and $n\cdot 2^n=24$ γ-parameters $\boldsymbol{\gamma}^1=\left(\gamma_0^1,\gamma_1^1,...,\gamma_7^1\right)$, $\boldsymbol{\gamma}^2=\left(\gamma_0^2,\gamma_1^2,...,\gamma_7^2\right)$, $\boldsymbol{\gamma}^3=\left(\gamma_0^3,\gamma_1^3,...,\gamma_7^3\right)$.

Our generalization of (3) is based on Jacobi matrices $\mathbf{J}_{2^n}^{(p,q)}(\varphi^r_{(p,q)})$ instead of $\mathbf{J}_N^{(p,q)}(\pi/4)$ and on arbitrary phasors: $\Delta_{2^n}^{(p(k_r,s_r),q(k_r,s_r))}\left(1^{s_r}_{p(k_r,s_r)}\middle|\varepsilon^{s_r\cdot 2^{n-r}}_{q(k_r,s_r)}\right)\to\Delta_{2^n}^{(p(k_r,s_r),q(k_r,s_r))}\left(e^{j\gamma^r_{p(k_r,s_r)}}\mid e^{j\gamma^r_{q(k_r,s_r)}}\right)$:

$$\mathcal{F}\left(\boldsymbol{\varphi}^1,\boldsymbol{\varphi}^2,...,\boldsymbol{\varphi}^n;\boldsymbol{\gamma}^1,\boldsymbol{\gamma}^2,...,\boldsymbol{\gamma}^n\right)=$$

$$=\prod_{r=1}^{n}\left(\prod_{s_r=0}^{2^{n-r}-1}\prod_{k_r=0}^{2^{r-1}-1}\left[\Delta_{2^n}^{(p(k_r,s_r),q(k_r,s_r))}\left(e^{j\gamma^r_{p(k_r,s_r)}}\mid e^{j\gamma^r_{q(k_r,s_r)}}\right)\cdot\mathbf{J}_{2^n}^{(p(k_r,s_r),q(k_r,s_r))}\left(\varphi^r_{(p(k_r,s_r),q(k_r,s_r))}\right)\right]\right), \qquad (4)$$

It is $3n\cdot 2^{n-1}$- parameter complex-valued Fourier-like transform (see Fig. 5) with $n\cdot 2^{n-1}$ φ-parameters

$$\boldsymbol{\varphi}^1=\left(\varphi_0^1,\varphi_1^1,...,\varphi_{2^{n-1}-1}^1\right),\ \ \boldsymbol{\varphi}^2=\left(\varphi_0^2,\varphi_1^2,...,\varphi_{2^{n-1}-1}^2\right),\ \ldots,\ \boldsymbol{\varphi}^n=\left(\varphi_0^n,\varphi_1^n,...,\varphi_{2^{n-1}-1}^n\right),$$

and $n\cdot 2^n=24$ γ-parameters

$$\boldsymbol{\gamma}^1=\left(\gamma_0^1,\gamma_1^1,...,\gamma_{2^n-1}^1\right),\ \ \boldsymbol{\gamma}^2=\left(\gamma_0^2,\gamma_1^2,...,\gamma_{2^n-1}^2\right),\ \ldots,\ \boldsymbol{\gamma}^n=\left(\gamma_0^n,\gamma_1^n,...,\gamma_{2^n-1}^n\right).$$

4. Fast many-parameter quaternion Fourier transforms

The space of quaternions denoted by $\mathbb{H}$ were first invented by W.R. Hamilton in 1843 as an extension of the complex numbers into four dimensions [20]. General information on quaternions may be obtained from [21].

Definition 1. Numbers of the form ${}^4\mathbf{q}\ =\ a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$, where $a,b,c,d\in\mathbf{R}$ are called quaternions, where 1) $\mathbf{1}$ is the real unit; 2) $\mathbf{i},\mathbf{j},\mathbf{k}$ are three imaginary units.

The addition and subtraction of two quaternions ${}^4\mathbf{q}_1=a_1+x_1\mathbf{i}+y_1\mathbf{j}+z_1\mathbf{k}$ and ${}^4\mathbf{q}_2=a_2+x_2\mathbf{i}+y_2\mathbf{j}+z_2\mathbf{k}$ are given by

$${}^4\mathbf{q}_1\pm{}^4\mathbf{q}_2\ =(a_1\pm a_2)+(b_1\pm b_2)\mathbf{i}+(b_1\pm b_2)\mathbf{j}+(b_1\pm b_2)k.$$

The product of quaternions for the standard format Hamilton defined according as:

$${}^4\mathbf{q}_1\circ{}^4\mathbf{q}_2=\ (a_1+b_1\mathbf{i}+c_1\mathbf{j}+d_1\mathbf{k})\circ(a_2+b_2\mathbf{i}+c_2\mathbf{j}+d_2\mathbf{k})=\left(a_1a_2-b_1b_2-c_1c_2-d_1d_2\right)+$$
$$+\left(a_1b_2+b_1a_2+c_1d_2-d_1c_2\right)\mathbf{i}+\left(a_1c_2+c_1a_2+d_1b_2-b_1d_2\right)\mathbf{j}+\left(a_1d_2+d_1a_2+b_1c_2-c_1b_2\right)\mathbf{k},$$

where $\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-1;$ $\mathbf{i}\circ\mathbf{j}=-\mathbf{i}\circ\mathbf{j}=\mathbf{k},$ $\mathbf{i}\circ\mathbf{k}=-\mathbf{k}\circ\mathbf{i}=\mathbf{j},$ $\mathbf{j}\circ\mathbf{k}=-\mathbf{k}\circ\mathbf{j}=\mathbf{i}$. The set of quaternions with operations of multiplication and addition forms 4-D algebra $\mathbb{H}=\mathbb{H}\left(\mathbf{R}\,|\,1,\mathbf{i},\mathbf{j},\mathbf{k}\right):=\mathbf{R}+\mathbf{Ri}+\mathbf{Rj}+\mathbf{Rk}$ over the real field $\mathbf{R}$.

Number component a and direction component ${}^3\mathbf{r}=b\mathbf{i}+c\mathbf{j}+d\mathbf{k}\in\mathbf{R}^3$ were called the *scalar* and 3-D *vector* parts of quaternion, respectively. A non–zero element ${}^3\mathbf{r}=bi+cj+dk$ is called pure vector quaternion. Since $\mathbf{i}\circ\mathbf{j}=\mathbf{k}$, then a quaternion ${}^4\mathbf{q}\ =\ a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}=(a1+b\mathbf{i})+(c\mathbf{j}+d\mathbf{i}\circ\mathbf{j})=(a+b\mathbf{i})+\ \ +(c+d\mathbf{i})\circ\mathbf{j}=\mathbf{z}+\mathbf{w}\circ\mathbf{j}$ is the sum of two complex numbers $\mathbf{z}=a+b\mathbf{i},$ $\mathbf{w}=c+d\mathbf{i}$ with a new imaginary unit $\mathbf{j}$.

Definition 2. Let ${}^4\mathbf{q}\ =\ a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}\in\mathbb{H}(\mathbf{R})$ be a quaternion. Then ${}^4\overline{\mathbf{q}}\ =$ $=\ \overline{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}}=a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}$ is the conjugate of ${}^4\mathbf{q}$, and $N({}^4\mathbf{q})=$ $=\ \|{}^4\mathbf{q}\|=\sqrt{a^2+b^2+c^2+d^2}=\sqrt{{}^4\overline{\mathbf{q}}\circ{}^4\mathbf{q}}=\sqrt{{}^4\mathbf{q}\circ{}^4\overline{\mathbf{q}}}$ is the norm of ${}^4\mathbf{q}$.

Definition 3. Quaternions $\left\{{}^3\mathbf{r}\,\middle|\,N({}^3\mathbf{r})=1\right\}$ of unit norm are called unit pure vector quaternions and denotes as $\left\{{}^3\boldsymbol{\mu}\,\middle|\,N({}^3\boldsymbol{\mu})=1\right\}$. They form a 2-D sphere $\mathbb{S}^2\subset\mathbf{R}^3$ and parameterized by the Euler angles ${}^3\boldsymbol{\mu}(\beta,\theta)=\mathbf{i}\cos\beta+\mathbf{j}\sin\beta\cos\theta+\mathbf{k}\sin\beta\sin\theta\in\mathbf{S}^2.$

For each quaternion ${}^3\boldsymbol{\mu}(\beta,\theta)$ we have ${}^3\boldsymbol{\mu}^2(\beta,\theta)={}^3\boldsymbol{\mu}^2(\beta,\theta)\circ{}^3\boldsymbol{\mu}^2(\beta,\theta)=-1.$ This unit-vector product identity represents the generalization of the complex-variable identity $i^2=-1$. This means that, if in the ordinary theory of complex numbers there are only two different square roots of negative unity ($+i$ and $-i$) and they differ only in their signs, then in the quaternion theory there are infinite numbers of different square roots of negative unity. The exponential function $e^{{}^3\boldsymbol{\mu}(\beta,\theta)\cdot\gamma}=\cos\gamma+{}^3\boldsymbol{\mu}(\beta,\theta)\sin\gamma$ is called quaternion-valued phasor.

We are going to use the expression (4) for obtaining many-parameter quaternion Fourier-like transform. It based on the left and right side quaternion-valued phasors:

$$\mathcal{QF}\left(\boldsymbol{\omega}\,|\,\left\{\mathbf{key}^r\right\}_{r=1}^n\right)=$$

$$=\prod_{r=1}^{n}\left(\prod_{s_r=0}^{2^{n-r}-1}\prod_{k_r=0}^{2^{r-1}-1}\left[\Delta_{2^n}^{(p(k_r,s_r),q(k_r,s_r))}\left({}_{key^r_{p(k_r,s_r)}}e^{{}^3\boldsymbol{\mu}^r_{p(k_r,s_r)}(\boldsymbol{\beta}^r,\boldsymbol{\theta}^r)\cdot\gamma^r_{p(k_r,s_r)}}\,|_{key^r_{q(k_r,s_r)}}\,e^{{}^3\boldsymbol{\mu}^r_{q(k_r,s_r)}\cdot(\boldsymbol{\beta}^r,\boldsymbol{\theta}^r)\gamma^r_{q(k_r,s_r)}}\right)\cdot\right.\right. \quad (5)$$

$$\left.\left.\cdot\mathbf{J}_{2^n}^{p(k_r,s_r),q(k_r,s_r)}\left(\varphi^r_{(p(k_r,s_r),q(k_r,s_r))}\right)\right)\right],$$

where $\boldsymbol{\omega}=\left(\boldsymbol{\varphi}^1,\boldsymbol{\varphi}^2,...,\boldsymbol{\varphi}^n;\boldsymbol{\gamma}^1,\boldsymbol{\gamma}^2,...,\boldsymbol{\gamma}^n;\boldsymbol{\beta}^1,\boldsymbol{\beta}^2,...,\boldsymbol{\beta}^n;\boldsymbol{\theta}^1,\boldsymbol{\theta}^2,...\boldsymbol{\theta}^n\right)$, $key^r_{p(k_r,s_r)}$ and $key^r_{q(k_r,s_r)}$ are binary keys at ${}_{key^r_{p(k_r,s_r)}}e^{{}^3\boldsymbol{\mu}^r_{p(k_r,s_r)}(\boldsymbol{\beta}^r,\boldsymbol{\theta}^r)\cdot\gamma^r_{p(k_r,s_r)}}$ and ${}_{key^r_{q(k_r,s_r)}}e^{{}^3\boldsymbol{\mu}^r_{q(k_r,s_r)}\cdot(\boldsymbol{\beta}^r,\boldsymbol{\theta}^r)\gamma^r_{q(k_r,s_r)}}$. They indicate about the left side or the right side multiplications, respectively. Here ${}^3\boldsymbol{\mu}^r_p(\boldsymbol{\beta}^r_p,\boldsymbol{\theta}^r_p)=\left({}^3\boldsymbol{\mu}^r_0(\beta^r_0,\theta^r_0),{}^3\boldsymbol{\mu}^r_1(\beta^r_1,\theta^r_1),...,{}^3\boldsymbol{\mu}^r_{2^n-1}(\beta^r_{2^n-1},\theta^r_{2^n-1})\right)$ are quaterion-valued imaginary units parameterized by angles $(\boldsymbol{\beta}^r_p,\boldsymbol{\theta}^r_p)$. New transform $\mathcal{QF}\left(\boldsymbol{\omega}\,|\,\left\{\mathbf{key}^r\right\}_{r=1}^n\right)$ is $7n\cdot 2^{n-1}$ - parameter quaternion-valued Fourier-like transforms with $n\cdot 2^{n-1}$ φ - parameters, $n\cdot 2^n$ γ -, β - and θ -parameters and with the branch of binary crypto-keys $\left\{\mathbf{key}^r\right\}_{r=1}^n$.

5. Many-parameter complex and quaternion all-pass filters

In this section we introduce special classes of many-parametric all-pass discrete cyclic filters. The output/input relation of the discrete cyclic filter is described by the discrete cyclic convolution:

$$y(n)=\mathbf{Filt}_{\mathcal{F}}\{x(n)\}=\sum_{m=0}^{N-1}h(n\underset{N}{\ominus}m)x(m)=(h*x)(n)=\left(\mathcal{F}^{\dagger}\cdot\mathbf{Diag}\left\{\left|H(k)\right|e^{i\varphi(k)}\right\}\cdot\mathcal{F}\right)\cdot x(n),$$

where $x(n), y(n)$ are input and output signals, respectively, $h(n)$ is the impulse response, $H(k)=\left|H(k)\right|e^{i\varphi(k)}=\mathcal{F}\{h(n)\}$ is the frequency response, $\underset{N}{\ominus}$ is difference modulo N and $*$ is the symbol of cyclic convolution, $\mathbf{Filt}_{\mathcal{F}}=\left[h(n\underset{N}{\ominus}m)\right]_{n,m=0}^{N-1}$ is the cyclic $(N\times N)$ – matrix with the kernel $h(n)$. We will concentrate our analysis on all-pass filters whose frequency response can be expressed in the form $H(k)=\left|H(k)\right|e^{i\varphi(k)}$, where frequency response magnitude is constant for all frequencies, for example, $\left|H(k)\right|\equiv 1,\ k=0,1,2,...,N-1.$ So, for all-pass filter $\mathbf{Filt}_{\mathcal{F}}$ has the following complex-valued impulse $\left|h(n)\right\rangle = \mathcal{F}\cdot\left|e^{i\varphi(k)}\right\rangle$ and frequency responses $\left|H(k)\right\rangle = \left|e^{i\varphi(k)}\right\rangle$. Hence, $y(n) = \mathbf{Filt}_{\mathcal{F}}\{x(n)\} = \left(\mathcal{F}^{\dagger}\cdot\mathbf{Diag}\left\{e^{i\varphi(k)}\right\}\cdot\mathcal{F}\right)\{x(n)\}$. We are going to consider this filter as a parametric filter

$$\mathbf{Filt}_{\mathcal{F}}^{(\boldsymbol{\varphi})} = \mathbf{Filt}_{\mathcal{F}}^{(\varphi_0,\varphi_1,\ldots,\varphi_{N-1})} = \mathcal{F}^{\dagger}\cdot\mathbf{Diag}\left\{e^{i\varphi(k)}\right\}\cdot\mathcal{F} = \mathcal{F}^{\dagger}\cdot\mathbf{Diag}\left\{e^{i\varphi_0}, e^{i\varphi_1},\ldots,e^{i\varphi_{N-1}}\right\}\cdot\mathcal{F} \quad (6)$$

with N free parameters $\boldsymbol{\varphi} = (\varphi_0,\varphi_1,\ldots,\varphi_{N-1})$. Obviously, all-pass filter $\mathbf{Filt}_{\mathcal{F}}^{(\boldsymbol{\varphi})}$ (as linear transform) is many-parameter unitary cyclic $(N\times N)-$matrix.

Our the first natural generalization of (6) is based on an arbitrary unitary transform $\mathcal{U}$ instead of Fourier transform $\mathcal{F}$:

$$\mathbf{Filt}_{\mathcal{U}}^{(\boldsymbol{\varphi})} = \mathbf{Filt}_{\mathcal{U}}^{(\varphi_0,\varphi_1,\ldots,\varphi_{N-1})} = \mathcal{U}^{\dagger}\cdot\mathbf{Diag}\left\{e^{i\varphi(k)}\right\}\cdot\mathcal{U} = \mathcal{U}^{\dagger}\cdot\mathbf{Diag}\left\{e^{i\varphi_0}, e^{i\varphi_1},\ldots,e^{i\varphi_{N-1}}\right\}\cdot\mathcal{U}. \quad (7)$$

The second generalized is based on quaternion-valued exponents (phasors) $\left\{{}_{{}^{C}key_p} e^{{}^{3}\boldsymbol{\mu}(\gamma_p^C,\theta_p^C)\alpha_p^C}\right\}$ $(p = 0,1,\ldots,N-1)$ and two quaternion Fourier transforms:

$$\mathbf{QFilt}_{\mathcal{QF}}\left(\boldsymbol{\alpha}^C,\boldsymbol{\gamma}^C,\boldsymbol{\theta}^C;{}^{L}\boldsymbol{\omega},{}^{R}\boldsymbol{\omega}\,|\,\mathbf{key}^C,\left\{{}^{L}\mathbf{key}^r\right\}_{r=1}^{n},\left\{{}^{R}\mathbf{key}^r\right\}_{r=1}^{n}\right) =$$
$$= \mathcal{QF}^{\dagger}\left({}^{L}\boldsymbol{\omega}\left|\left\{{}^{L}\mathbf{key}^r\right\}_{r=1}^{n}\right.\right)\cdot\mathbf{Diag}\left\{{}_{{}^{C}key_0} e^{{}^{3}\boldsymbol{\mu}(\gamma_0^C,\theta_0^C)\cdot\alpha_0^C},\ldots,{}_{{}^{C}key_{N-1}} e^{{}^{3}\boldsymbol{\mu}(\gamma_{N-1}^C,\theta_{N-1}^C)\cdot\alpha_{N-1}^C}\right\}\cdot\mathcal{QF}\left({}^{R}\boldsymbol{\omega}\left|\left\{{}^{R}\mathbf{key}^r\right\}_{r=1}^{n}\right.\right). \quad (8)$$

where ${}^{C}\mathbf{key} = \left({}^{C}key_0,{}^{C}key_1,\ldots,{}^{C}key_{N-1}\right)$, $\boldsymbol{\alpha}^C = \left(\alpha_0^C,\alpha_1^C,\ldots,\alpha_{N-1}^C\right)$, $\boldsymbol{\gamma}^C = \left(\gamma_0^C,\gamma_1^C,\ldots,\gamma_{N-1}^C\right)$, $\boldsymbol{\theta}^C = \left(\theta_0^C,\theta_1^C,\ldots,\theta_{N-1}^C\right)$. Here ${}^{L}\boldsymbol{\omega},\left\{{}^{L}\mathbf{key}^r\right\}_{r=1}^{n}$ and ${}^{R}\boldsymbol{\omega},\left\{{}^{R}\mathbf{key}^r\right\}_{r=1}^{n}$ are parameters of left and right quaternion Fourier transforms $\mathcal{QF}^{\dagger}\left({}^{L}\boldsymbol{\omega}\left|\left\{{}^{L}\mathbf{key}^r\right\}_{r=1}^{n}\right.\right)$, $\mathcal{QF}\left({}^{R}\boldsymbol{\omega}\left|\left\{{}^{R}\mathbf{key}^r\right\}_{r=1}^{n}\right.\right)$, respectively.

Quaternion cyclic transform $\mathbf{QFilt}_{\mathcal{QF}}\left(\boldsymbol{\alpha}^C,\boldsymbol{\gamma}^C,\boldsymbol{\theta}^C;{}^{L}\boldsymbol{\omega},{}^{R}\boldsymbol{\omega}\,|\,\mathbf{key}^C,\left\{{}^{L}\mathbf{key}^r\right\}_{r=1}^{n},\left\{{}^{R}\mathbf{key}^r\right\}_{r=1}^{n}\right)$ has $7n\cdot 2^{n-1}$ left parameters ${}^{L}\boldsymbol{\omega}$, $7n\cdot 2^{n-1}$ right parameters ${}^{R}\boldsymbol{\omega}$ and $3\cdot 2^{n}$ center parameters $\boldsymbol{\alpha}^C,\boldsymbol{\gamma}^C,\boldsymbol{\theta}^C$. Total number of parameters is $(14n+6)\cdot 2^{n-1}$. Moreover, $\mathbf{QFilt}_{\mathcal{QF}}$ has three branches of binary crypto-keys $\mathbf{key}^C,\left\{{}^{L}\mathbf{key}^r\right\}_{r=1}^{n},\left\{{}^{R}\mathbf{key}^r\right\}_{r=1}^{n}$.

6. Conclusions

In this paper, we proposed a novel Intelligent OFDM-telecommunication systems based on a new unified approach to the many-parametric representation of complex and quaternion Fourier transforms. The new systems use inverse MPFT for modulation at the transmitter and direct MPFT for demodulation at the receiver. Each MPT depends on finite set of independent parameters (angles), which could be changed in dependently of one another. For each fixed values of parameter we get the unique orthogonal transform. 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 MPFT in OFDM TCS is that it is a very flexible system allowing to construct Intelligent OFDM TCS for electronic warfare (EW). EW is a type of armed struggle using electronic means against enemy to “change the quality of information”. EW includes (consists) of suppressor and protector. 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 protects such assets and those of friendly forces. In order to protect corporate privacy and sensitive client information against the threat of electronic eavesdropping and jamming protector uses intelligent OFDM-TCS, based on MPFTs. The system model that is going to be used in this work is know as the wiretap channel model, which was introduced in 1975 by Wyner [4]. This model is composed of two legitimate users, named Alice and Bob.

A legitimate user (Alice) transmits her confidential messages to a legitimate receiver (Bob), while Eve will be trying to eavesdrop Alice’s information. An active jammer, named Jamie, attempts to jam up this information. Alice transmits her data using OFDM with N complex- or quaternion-valued sub-carriers $\left\{\mathbf{qsubc}_k(n\,|\,\varphi_1^0,...,\varphi_q^0)\right\}_{k=0}^{N-1}$, i.e. she use the unitary transform $\mathcal{QF}_N^0=\mathcal{QF}_N(\boldsymbol{\theta}^0)$ with fixed parameters $\boldsymbol{\theta}^0=(\varphi_1^0,...,\varphi_q^0)$. When sub-carriers $\left\{\mathbf{qsubc}_k(n\,|\,\varphi_1^0,...,\varphi_q^0)\right\}_{k=0}^{N-1}$ (i.e. unitary transform $\mathcal{QF}_N(\boldsymbol{\theta}^0)$) of Alice’s and Bob’s Intelligent-OFDM-TCS are identified by Eve (or Jammi) this TCS can be eavesdropped (or jammed) by means of Radio-Electronic Eavesdropping Attack (REEA). 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 of $\mathcal{QF}_N(\boldsymbol{\theta})$ in the periodical (or in pseudo random) manner: $\mathcal{QF}_N(\boldsymbol{\theta}^0)\to\mathcal{QF}_N(\boldsymbol{\theta}^1)\to...\to\mathcal{QF}_N(\boldsymbol{\theta}^r)\to...\quad r=0,1,2,...$, where $\boldsymbol{\theta}^r=\boldsymbol{\theta}^0+r\cdot\Delta\boldsymbol{\theta}$ and $\boldsymbol{\theta}^0$ are initial values of parameters at the initial time t_0.

7. Acknowledgements

The reported study was funded by RFBR, project number 19-29-09022-мк and by the Ural State Forest Engineering’s Center of Excellence in «Quantum and Classical Information Technologies for Remote Sensing Systems.

References

1. Liang X., Zhang K., Shen X., Lin X. Security and privacy in mobile social networks: challenges and solutions, IEEE Wireless Commun., 2014, 21(1), pp. 33–41.
2. Jorswieck E., Tomasin S., Sezgin A. Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing, Proc. IEEE, 2015, 103(10), pp. 1702–1724.
3. Zhang N., Lu N., Cheng N., Mark J. W., Shen X. S. Cooperative spectrum access towards secure information transfer for CRNS, IEEE J. Sel. Areas Commun., 2013, 31(11), pp. 2453–2464.

4. Wyner A. D. The wiretap channel, Bell Sys. Tech. J., 1975, 54(8), pp. 1355–1387.
5. Renna F., Laurenti N., Poor H. V. Physical-layer secrecy for OFDM transmissions over fading channels, IEEE Trans. Inf. Forens. Security, 2012, 7(4), pp. 1354-1367.
6. Chorti A., Poor H. V. Faster than Nyquist interference assisted secret communication for OFDM systems, Proceedings of the IEEE Asilomar Conf. Signals, Systems and Comput., 2011, pp. 183-187.
7. Wang X. Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks, IEEE Trans. Inf. Forens. Security, 2011, 6(3), pp. 693-702.
8. Wang H. M., Yin Q., Xia X. G . Distributed beamforming for physical-layer security of two-way relay networks, IEEE Trans. Signal Process., 2012, 60(7), pp. 3532-3545.
9. Manhas P., Soni M.K. Comparison of OFDM System in Terms of BER using Different Transform and Channel Coding, International Journal of Engineering and Manufacturing, 2016, vol. 1, pp. 28-34.
10. Patchala S., Sailaja M. Analysis of Filter Bank Multi-Carrier system for 5G communications, International Journal of Wireless and Microwave Technologies, 2019, vol.9, no.4, pp. 39-50.
11. Gupta M. K., Tiwari S. Performance evaluation of conventional and wavelet based OFDM System, International Journal on Electronics and Communication, 2013, vol. 67, no.4, pp 348– 354,.
12. Kaur H., Kumar M., Sharma A. K, Singh H.P. Performance Analysis of Different Wavelet Families over Fading Environments for Mobile WiMax System, International Journal of Future Generation Communication and Networking, 2015, vol. 8, pp 87-98.
13. Halford K., Halford S., Webster M., Andren C. Complementary code keying for rake-based indoor wireless communication, Proceedings of IEEE International Symposium on Circuits and Systems, 1999, pp. 427– 430.
14. Golay M. J. E. Complementary series IEEE Trans. Inform. Theory, 1961, 7, pp. 82–87.
15. Davis J. A., Jedwab J. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes, IEEE Trans. Inform. Theory, 1999, 45, pp. 2397–2417.
16. Michailow N., Mendes L., Matthe M., Festag I., Fettweis A., Robust G. WHT-GFDM for the next generation of wireless networks, IEEE Communications Letters, 2015, 19, pp. 106–109.
17. Xiao J., Yu J., Li X., Tang Q., Chen H., Li F., Cao Z., Chen L. Hadamard transform combined with companding transform technique for PAPR reduction in an optical direct-detection OFDM system, IEEE J. Opt. Commun. Netw., 2012, 4(10), pp. 709–714.
18. Wilkinson T. A., Jones A. E. Minimization of the peak to mean envelope power ratio of multicarrier transmission schemes by block coding, Proceedings of the IEEE 45th Vehicular Technology Conf. , 1995, pp. 825-829.
19. Wilkinson T. A., Jones A. E. Combined coding for error control and in creased robustness to system nonlinearities in OFDM, Proceedings of the IEEE 46th Vehicular Technology Conf., 1996, pp. 904-908.
20. Hamilton W. R . Elements of Quaternions, New York: Chelsea Pub. Com., 1969, p. 242
21. Ward J. P. Quaternions and Cayley Numbers: Algebra and Applications, Dordrecht, Netherlands: Kluwer Academic Publishers, 1997, p. 218.