Fast Finite Field Hartley Transforms based on Hadamard Decomposition

H.M. de Oliveira
hmo@npd.ufpe.br

R.G.F. Távora
tavora@impa.br

R.J.S. Cintra
rjsc@operamail.com

R.M. Campello de Souza
Ricardo@npd.ufpe.br

CODEC- Communications Research Group
Departamento de Eletrônica e Sistemas
C.P. 7800, 50.711-970 Recife - PE BRAZIL

Abstract

A new transform over finite fields, the Finite Field Hartley Transform (FFHT), was recently introduced and a number of promising applications on the design of efficient multiple access systems and multilevel spread spectrum sequences were proposed. The FFHT exhibits interesting symmetries, which are exploited to derive new Fast Transform Algorithms (FT). These FTs are based on successive decompositions of the FFHT by means of Hadamard-Walsh transforms (HWT). This new approach meets the lower bound on the multiplicative complexity for all the cases investigated so far. The complexity of these new FTs is compared with that of some classical algorithms.

Key-words: Finite Field Transform, Fast Algorithms, Hartley

1 Introduction

Discrete Transforms defined over finite fields are powerful tools in Electrical Engineering, particularly in Digital Signal Processing. The Finite Field Fourier Transform (FFFT) has applications in many fields, including Digital Signal Processing [1] and Error-Control Codes [2]. Another interesting example is the Finite Field Hartley Transform (FFHT), an involutionary (self-inverse) transform introduced by Campello et al. [3, 4, 5]. Recent promising applications of discrete transforms concern the use of the FFHT to design digital multiplex systems, efficient multiple access systems [6] and multilevel spread spectrum sequences [7]. A decisive factor for applications of discrete transforms has been the existence of the so-called fast transforms (FT) for computing it. Since the FFHT is a more symmetrical version of discrete transform, in this paper this symmetry is exploited so as to derive new FTs that require less operations. These FTs, derived for short blocklengths (N$\leq$ 24), are based on successive decompositions in a similar way as the multilayer Hadamard Decomposition proposed by Cintra et al. [8] to compute the Discrete Hartley Transform (DHT) [9]. This new approach, wich is based on decomposition of the FFHT by means of Hadamard-Walsh transforms (HWT), meets the lower bound on the multiplicative complexity of a Discrete Fourier Transform (DFT) [10]. Each HWT implements pre-additions and post-additions. These schemes are easy to implement using Digital Signal Processors (DSP) or low-cost high-speed dedicated Integrated Circuits. The complexity of these new FTs is compared with that of classical algorithms, such as Cooley Tukey radix 2, split radix, Winograd and Rader-Brenner, which were adapted to compute the FFHT [11].

2 The Finite Field Hartley Transform

Finite Field Hartley Transforms are based on a Trigonometry over Galois Fields $GF(q)$, $q = p^r$, $p \equiv 3 \pmod 4$, so that $(p-1)^{1/2}$ is not an element of $GF(q)$. The set $G(q)$ of Gaussian integers over $GF(q)$ plays an important role in this analysis. This set defines a structure $GI(q)$, which is a finite field isomorphic to $GF(q^2)$ [3].

Definition 2.1 *Let ζ be an element of $GI(q)$ with multiplicative order N, where $q = p^r$. The trigonometric functions sin, cos, cas are defined by:*

$$\sin(i) = \frac{\zeta^i - \zeta^{-i}}{2j}, \cos(i) = \frac{\zeta^i + \zeta^{-i}}{2},$$
$$\textit{and } \operatorname{cas}(i) = \sin(i) + \cos(i).$$

Definition 2.2 *Let $v = \{v_0, v_1, ..., v_N\}$ be a vector of $GF(q)$-valued components, $q = p^r$. The Finite Field Hartley Transform (FFHT) is the vector $V = \{V_0, V_1, ..., V_N\}$, with components $V_k \in GI(q^m)$ given by $V_k = \sum_{i=0}^{N-1} v_i cas(ik)$ where ζ is an element of multiplicative order N over $GI(q^m)$.*

The inverse FFHT is given by the following theorem

Theorem 2.1 *The vector $v = \{v_0, v_1, ..., v_N\}$ can be derived from its FFHT according to: $v_i = \frac{1}{N \pmod p} \sum_{k=0}^{N-1} V_k cas(ik)$.*

3 Hadamard Decomposition of the FFHT

The Hadamard decomposition was recentley introduced by Cintra et al. [8] as a tool to compute the Discrete Hartley Transform. This approach allows the minimization of the multiplicative complexity of the DHT for some blocklengths. Since all the properties and symmetries of the DHT are also observed for the FFHT, the application of this algorithm to finite fields should be expected. The minimal multiplicative complexity, μ, of a DFT with blocklength N can be calculated by converting the DFT in a set of cyclic convolutions. A lower bound on μ is presented in [10]. Table 1 shows a few values of $\mu(DFT(N))$ for short blocklengths. Handling

Table 1: Minimal Multiplicative Complexity achievable for an N-blocklength DFT

N	4	8	12	16
$\mu(DFT(N))$	0	2	4	10

with Finite Field Transforms, the following comments are worthwhile:

1. The minimal multiplicative complexity, $\mu(FFFT(N))$, for a FT over the finite field $GI(p^r)$, is the same as $\mu(DFT(N))$, evaluated over the real field.
2. The relationship between the multiplicative and additive complexity over a finite field strong depends on implementation. For small p, the total complexity (additive plus multiplicative) must be taken into account since their difference is small.

New algorithms for computing the FFHT are introduced in the next section.

3.1 Computing a 4-blocklength FFHT

Let $v \longleftrightarrow V$ be a FFHT transform pair over $GI(7)$. The FFHT, assuming a $cas(.)$ kernel with $\zeta = j$, is computed by:

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 6 & 6 \\ 1 & 6 & 1 & 6 \\ 1 & 6 & 6 & 1 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{bmatrix}.$$

Indeed, no multiplication is needed. Observing further symmetries, columns can be combined through Hadamard blocks in order to reduce the number of additions. Let

$$S_0(1)=(v_3-v_1),\ S_1(1)=(v_3+v_1),$$
$$S_2(1)=(v_0-v_2),\ S_3(1)=(v_0+v_2).$$

It follows that,

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 6 & 0 & 1 & 0 \\ 0 & 6 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} S_0(1) \\ S_1(1) \\ S_2(1) \\ S_3(1) \end{bmatrix}.$$

The number of additions is reduced from 12 to 8 (4 pre-additions and 4 post-additions).

3.2 Computing a 6-blocklength FFHT

Let $v \longleftrightarrow V$ be an FFHT transform pair over $GI(7)$. Considering $\zeta = 3$, the FFHT can be computed by

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 4+j & 3+j & 6 & 3+6j & 4+6j \\ 1 & 3+j & 3+6j & 1 & 3+j & 3+6j \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 3+6j & 3+j & 1 & 3+6j & 3+j \\ 1 & 4+6j & 3+6j & 6 & 3+j & 4+j \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{bmatrix}.$$

Observing the symmetries, a first column combination can be made. Let

$$S_0(1)=(v_4-v_1),\ S_1(1)=(v_4+v_1),\ S_2(1)=(v_5-v_2),$$
$$S_3(1)=(v_5+v_2),\ S_4(1)=(v_0-v_3),\ S_5(1)=(v_0+v_3).$$

Therefore,

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 3+6j & 0 & 4+6j & 0 & 1 & 0 \\ 0 & 3+j & 0 & 3+6j & 0 & 1 \\ 1 & 0 & 6 & 0 & 1 & 0 \\ 0 & 3+6j & 0 & 3+j & 0 & 1 \\ 3+j & 0 & 4+j & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} S_0(1) \\ S_1(1) \\ S_2(1) \\ S_3(1) \\ S_4(1) \\ S_5(1) \end{bmatrix}.$$

Going on with this procedure, a second pre-addition layer is derived:

$$S_0(2)=S_2(1)-S_0(1),\ S_1(2)=S_2(1)+S_0(1),\ S_2(2)=S_3(1)-S_1(1),$$
$$S_3(2)=S_3(1)+S_1(1),\quad S_4(2)=S_4(1),\quad S_5(2)=S_5(1).$$

Finally,

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 4 & 6j & 0 & 0 & 1 & 0 \\ 0 & 0 & 6j & 3 & 0 & 1 \\ 6 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & j & 3 & 0 & 1 \\ 4 & 1j & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} S_0(2) \\ S_1(2) \\ S_2(2) \\ S_3(2) \\ S_4(2) \\ S_5(2) \end{bmatrix}.$$

Since there is only one multiplication (by the same factor) in columns 1 and 4, there will be two multiplications. The total number of additions required to compute a 6-blocklength FFHT is 16 (10 pre-additions and 6 post-additions).

3.3 Computing an 8-blocklength FFHT

Let $v \longleftrightarrow V$ be an FFHT transform pair over $GI(7)$. Let $\zeta = 2+2j$, so the corresponding matrix formulation is,

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \\ V_6 \\ V_7 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 1 & 0 & 6 & 3 & 6 & 0 \\ 1 & 1 & 6 & 6 & 1 & 1 & 6 & 6 \\ 1 & 0 & 6 & 4 & 6 & 0 & 1 & 3 \\ 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 3 & 1 & 0 & 6 & 4 & 6 & 0 \\ 1 & 6 & 6 & 1 & 1 & 6 & 6 & 1 \\ 1 & 0 & 6 & 3 & 6 & 0 & 1 & 4 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{bmatrix}.$$

Defining a 1st order pre-addition layer:

$$\begin{gathered} S_0(1)=(v_5-v_1),\ S_1(1)=(v_5+v_1), \\ S_2(1)=(v_6-v_2),\ S_3(1)=(v_6+v_2), \\ S_4(1)=(v_7-v_3),\ S_5(1)=(v_7+v_3), \\ S_6(1)=(v_0-v_4),\ S_7(1)=(v_0+v_4). \end{gathered}$$

Therefore,

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \\ V_6 \\ V_7 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 3 & 0 & 6 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 6 & 0 & 6 & 0 & 1 \\ 0 & 0 & 1 & 0 & 3 & 0 & 1 & 0 \\ 0 & 6 & 0 & 1 & 0 & 6 & 0 & 1 \\ 4 & 0 & 6 & 0 & 0 & 0 & 1 & 0 \\ 0 & 6 & 0 & 6 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 4 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} S_0(1) \\ S_1(1) \\ S_2(1) \\ S_3(1) \\ S_4(1) \\ S_5(1) \\ S_6(1) \\ S_7(1) \end{bmatrix}.$$

Defining a 2nd pre-addition layer,

$$\begin{gathered} S_0(2)=S_0(1),\ S_1(2)=S_4(1), \\ S_2(2)=S_5(1)-S_1(1),\ S_3(2)=S_5(1)+S_1(1), \\ S_4(2)=S_6(1)-S_2(1),\ S_5(2)=S_6(1)+S_2(1), \\ S_6(2)=S_7(1)-S_3(1),\ S_7(2)=S_7(1)+S_3(1). \end{gathered}$$

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \\ V_6 \\ V_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 4 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} S_0(2) \\ S_1(2) \\ S_2(2) \\ S_3(2) \\ S_4(2) \\ S_5(2) \\ S_6(2) \\ S_7(2) \end{bmatrix}.$$

Since there is only one multiplication (by the same factor) in columns 1 and 2, there are two multiplications. The number of additions is 22 (14 pre-additions and 8 post-additions). It is worthwhile to remark that the additive complexity is less than the one for an 8-DFT calculation by the Winograd algorithm.

3.4 Computing a 12-blocklength FFHT

Let $v \longleftrightarrow V$ be an FFHT transform pair over $GI(p)$. As an example, let $p = 7$ and $\zeta = 3j$. Then $V = Tv$ where,

$$T = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 4+6j & 4+6j & 1 & 3+6j & 4+j & 6 & 3+j & 3+j & 6 & 4+j & 3+6j \\ 1 & 4+6j & 3+6j & 6 & 3+j & 4+j & 1 & 4+6j & 3+6j & 6 & 3+j & 4+j \\ 1 & 1 & 6 & 6 & 1 & 1 & 6 & 6 & 1 & 1 & 6 & 6 \\ 1 & 3+6j & 3+j & 1 & 3+6j & 3+j & 1 & 3+6j & 3+j & 1 & 3+6j & 3+j \\ 1 & 4+j & 4+j & 1 & 3+j & 4+6j & 6 & 3+6j & 3+6j & 6 & 4+6j & 3+j \\ 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 3+j & 4+6j & 6 & 3+6j & 3+6j & 6 & 4+6j & 3+j & 1 & 4+j & 4+j \\ 1 & 3+j & 3+6j & 1 & 3+j & 3+6j & 1 & 3+j & 3+6j & 1 & 3+j & 3+6j \\ 1 & 6 & 6 & 1 & 1 & 6 & 6 & 1 & 1 & 6 & 6 & 1 \\ 1 & 4+j & 3+j & 6 & 3+6j & 4+6j & 1 & 4+j & 3+j & 6 & 3+6j & 4+6j \\ 1 & 3+6j & 4+j & 6 & 3+j & 3+j & 6 & 4+j & 3+6j & 1 & 4+6j & 4+6j \end{bmatrix}.$$

Defining a 1st order pre-addition layer,

$$\begin{gathered} S_0(1)=(v_7-v_1),\ S_1(1)=(v_7+v_1), \\ S_2(1)=(v_8-v_2),\ S_3(1)=(v_8+v_2), \\ S_4(1)=(v_9-v_3),\ S_5(1)=(v_9+v_3), \\ S_6(1)=(v_{10}-v_4),\ S_7(1)=(v_{10}+v_4), \\ S_8(1)=(v_{11}-v_5),\ S_9(1)=(v_{11}+v_5), \\ S_{10}(1)=(v_0-v_6),\ S_{11}(1)=(v_0+v_6). \end{gathered}$$

Therefore, $V = T^{(1)}S(1)$, where

$$T^{(1)} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 3+j & 0 & 3+j & 0 & 6 & 0 & 4+j & 0 & 3+6j & 0 & 1 & 0 \\ 0 & 4+6j & 0 & 3+6j & 0 & 6 & 0 & 3+j & 0 & 4+j & 0 & 1 \\ 6 & 0 & 1 & 0 & 1 & 0 & 6 & 0 & 6 & 0 & 1 & 0 \\ 0 & 3+6j & 0 & 3+j & 0 & 1 & 0 & 3+6j & 0 & 3+j & 0 & 1 \\ 3+6j & 0 & 3+6j & 0 & 6 & 0 & 4+6j & 0 & 3+j & 0 & 1 & 0 \\ 0 & 6 & 0 & 1 & 0 & 6 & 0 & 1 & 0 & 6 & 0 & 1 \\ 4+6j & 0 & 3+j & 0 & 1 & 0 & 4+j & 0 & 4+j & 0 & 1 & 0 \\ 0 & 3+j & 0 & 3+6j & 0 & 1 & 0 & 3+j & 0 & 3+6j & 0 & 1 \\ 1 & 0 & 1 & 0 & 6 & 0 & 6 & 0 & 1 & 0 & 1 & 0 \\ 0 & 4+j & 0 & 3+j & 0 & 6 & 0 & 3+6j & 0 & 4+6j & 0 & 1 \\ 4+j & 0 & 3+6j & 0 & 1 & 0 & 4+6j & 0 & 4+6j & 0 & 1 & 0 \end{bmatrix}.$$

A second order pre-addition layer can be defined according to,

$$\begin{gathered} S_0(2)=S_6(1)-S_0(1),\ S_6(2)=S_9(1)-S_3(1), \\ S_1(2)=S_6(1)+S_0(1),\ S_7(2)=S_9(1)+S_3(1), \\ S_2(2)=S_7(1)-S_1(1),\ S_8(2)=S_{10}(1)-S_4(1), \\ S_3(2)=S_7(1)+S_1(1),\ S_9(2)=S_{10}(1)+S_4(1), \\ S_4(2)=S_8(1)-S_2(1),\ S_{10}(2)=S_{11}(1)-S_5(1), \\ S_5(2)=S_8(1)+S_2(1),\ S_{11}(2)=S_{11}(1)+S_5(1). \end{gathered}$$

Therefore, $V = T^{(2)}S(2)$, where

$$T^{(2)} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 4 & j & 0 & 0 & 6j & 3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 3+j & 0 & 0 & 0 & 4+j & 0 & 0 & 0 & 1 & 0 \\ 0 & 6 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3+6j & 0 & 0 & 0 & 3+j & 0 & 0 & 0 & 1 \\ 4 & 6j & 0 & 0 & j & 3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 1 & 0 \\ j & 4 & 0 & 0 & 4 & j & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3+j & 0 & 0 & 0 & 3+6j & 0 & 0 & 0 & 1 \\ 6 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 3+6j & 0 & 0 & 0 & 4+6j & 0 & 0 & 0 & 1 & 0 \\ j & 4 & 0 & 0 & 4 & 6j & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Going further, a 3rd order pre-addition layer is defined:

$$\begin{gathered} S_0(3)=S_4(2)-S_1(2),\ S_6(3)=S_7(2)-S_3(2), \\ S_1(3)=S_4(2)+S_1(2),\ S_7(3)=S_7(2)+S_3(2), \\ S_2(3)=S_5(2)-S_0(2),\ S_8(3)=S_8(2), \\ S_3(3)=S_5(2)+S_0(2),\ S_9(3)=S_9(2), \\ S_4(3)=S_6(2)-S_2(2),\ S_{10}(3)=S_{10}(2), \\ S_5(3)=S_6(2)+S_2(2),\ S_{11}(3)=S_{11}(2). \end{gathered}$$

Thus $V = T^{(3)}S(3)$, where

$$T^{(3)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 6j & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & j & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & j & 3 & 0 & 0 & 0 & 1 \\ j & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 4 & 0 & j & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 6j & 3 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 6j & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 4 & 6j & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Since there is just one multiplication by the same factor in columns 2, 3, 5 and 8, the total number of multiplications is 4. The number of additions required to compute the FFHT is 44 (32 pre-additions and 12 post-additions). The multiplicative complexity reaches the minimum theoretical complexity and again the additive complexity is the same as the one obtained for the DHT [8].

3.5 Computing a 16-blocklength FFHT

Let $v \longleftrightarrow V$ a FFHT pair over $GI(p)$. Assuming $p = 7$ and $\zeta = 2 + 4j$, the corresponding transform is $V = Tv$, where

$$T = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 2j & 4 & 2j & 1 & 6j & 0 & j & 6 & 5j & 3 & 2j & 6 & j & 0 & 6j \\
1 & 4 & 1 & 0 & 6 & 3 & 6 & 0 & 1 & 4 & 1 & 0 & 6 & 3 & 6 & 0 \\
1 & 2j & 0 & 5j & 6 & 6j & 4 & 6j & 6 & 5j & 0 & 2j & 1 & j & 3 & j \\
1 & 1 & 6 & 6 & 1 & 1 & 6 & 6 & 1 & 1 & 6 & 6 & 1 & 1 & 6 & 6 \\
1 & 6j & 3 & 6j & 1 & 5j & 0 & 2j & 6 & j & 4 & j & 6 & 2j & 0 & 5j \\
1 & 0 & 6 & 4 & 6 & 0 & 1 & 3 & 1 & 0 & 6 & 4 & 6 & 0 & 1 & 3 \\
1 & 6j & 0 & 6j & 6 & 2j & 3 & 2j & 6 & 6j & 0 & j & 1 & 5j & 4 & 5j \\
1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\
1 & 5j & 4 & 5j & 1 & j & 0 & 6j & 6 & 2j & 3 & 2j & 6 & 6j & 0 & j \\
1 & 3 & 1 & 0 & 6 & 4 & 6 & 0 & 1 & 3 & 1 & 0 & 6 & 4 & 6 & 0 \\
1 & 5j & 0 & 2j & 6 & j & 4 & j & 6 & 2j & 0 & 5j & 1 & 6j & 3 & 6j \\
1 & 6 & 6 & 1 & 1 & 6 & 6 & 1 & 1 & 6 & 6 & 1 & 1 & 6 & 6 & 1 \\
1 & j & 3 & j & 1 & 2j & 0 & 5j & 6 & 6j & 4 & 6j & 6 & 5j & 0 & 2j \\
1 & 0 & 6 & 3 & 6 & 0 & 1 & 4 & 1 & 0 & 6 & 3 & 6 & 0 & 1 & 4 \\
1 & 6j & 0 & j & 6 & 5j & 3 & 5j & 6 & j & 0 & 6j & 1 & 2j & 4 & 2j
\end{bmatrix}.$$

Defining now a first order pre-addition layer,

$$\begin{array}{c}
S_0(1)=(v_9-v_1), S_1(1)=(v_9+v_1), \\
S_2(1)=(v_{10}+v_2), S_3(1)=(v_{10}+v_2), \\
S_4(1)=(v_{11}-v_3), S_5(1)=(v_{11}+v_3), \\
S_6(1)=(v_{12}-v_4), S_7(1)=(v_{12}+v_4), \\
S_8(1)=(v_{13}-v_5), S_9(1)=(v_{13}+v_5), \\
S_{10}(1)=(v_{14}-v_6), S_{11}(1)=(v_{14}+v_6), \\
S_{12}(1)=(v_{15}-v_7), S_{13}(1)=(v_{15}+v_7), \\
S_{14}(1)=(v_0-v_8), S_{15}(1)=(v_0+v_8).
\end{array} \quad (1)$$

Therefore, $V = T^{(1)}S(1)$, where

$$T^{(1)} = \begin{bmatrix}
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
5j & 0 & 3 & 0 & 5j & 0 & 6 & 0 & j & 0 & 0 & 0 & 6j & 0 & 1 & 0 \\
0 & 4 & 0 & 1 & 0 & 0 & 0 & 6 & 0 & 3 & 0 & 6 & 0 & 0 & 0 & 1 \\
5j & 0 & 0 & 0 & 2j & 0 & 1 & 0 & j & 0 & 3 & 0 & j & 0 & 1 & 0 \\
0 & 1 & 0 & 6 & 0 & 6 & 0 & 1 & 0 & 1 & 0 & 6 & 0 & 6 & 0 & 1 \\
j & 0 & 4 & 0 & j & 0 & 6 & 0 & 2j & 0 & 0 & 0 & 5j & 0 & 1 & 0 \\
0 & 0 & 0 & 6 & 0 & 4 & 0 & 6 & 0 & 0 & 0 & 1 & 0 & 3 & 0 & 1 \\
6j & 0 & 0 & 0 & j & 0 & 1 & 0 & 5j & 0 & 4 & 0 & 5j & 0 & 1 & 0 \\
0 & 6 & 0 & 1 & 0 & 6 & 0 & 1 & 0 & 6 & 0 & 1 & 0 & 6 & 0 & 1 \\
2j & 0 & 3 & 0 & 2j & 0 & 6 & 0 & 6j & 0 & 0 & 0 & j & 0 & 1 & 0 \\
0 & 3 & 0 & 1 & 0 & 0 & 0 & 6 & 0 & 4 & 0 & 6 & 0 & 0 & 0 & 1 \\
2j & 0 & 0 & 0 & 5j & 0 & 1 & 0 & 6j & 0 & 3 & 0 & 6j & 0 & 1 & 0 \\
0 & 6 & 0 & 6 & 0 & 1 & 0 & 1 & 0 & 6 & 0 & 6 & 0 & 1 & 0 & 1 \\
6j & 0 & 4 & 0 & 6j & 0 & 6 & 0 & 5j & 0 & 0 & 0 & 2j & 0 & 1 & 0 \\
0 & 0 & 0 & 6 & 0 & 3 & 0 & 6 & 0 & 0 & 0 & 1 & 0 & 4 & 0 & 1 \\
j & 0 & 0 & 0 & 6j & 0 & 1 & 0 & 2j & 0 & 4 & 0 & 2j & 0 & 1 & 0
\end{bmatrix}.$$

Defining a 2nd order pre-addition layer,

$$\begin{array}{c}
S_0(2)=S_4(1)-S_0(1), S_1(2)=S_4(1)+S_0(1), \\
S_2(2)=S_9(1)-S_1(1), S_3(2)=S_9(1)+S_1(1), \\
S_4(2)=S_2(1), S_5(2)=S_{10}(1), \\
S_6(2)=S_{11}(1)-S_3(1), S_7(2)=S_{11}(1)+S_3(1), \\
S_8(2)=S_{12}(1)-S_8(1), S_9(2)=S_{12}(1)+S_8(1), \\
S_{10}(2)=S_{13}(1)-S_5(1), S_{11}(2)=S_{13}(1)+S_5(1), \\
S_{12}(2)=S_{14}(1)-S_6(1), S_{13}(2)=S_{14}(1)+S_6(1), \\
S_{14}(2)=S_{15}(1)-S_7(1), S_{15}(2)=S_{15}(1)+S_7(1).
\end{array} \quad (2)$$

Then, $V = T^{(2)}S(2)$, where

$$T^{(2)} = \begin{bmatrix}
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 5j & 0 & 0 & 3 & 0 & 0 & 0 & 6j & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 3 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
2j & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & j & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 1 \\
0 & j & 0 & 0 & 4 & 0 & 0 & 0 & 5j & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 1 & 0 \\
j & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 5j & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 6 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 1 \\
0 & 2j & 0 & 0 & 3 & 0 & 0 & 0 & j & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 4 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
5j & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 6j & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 6 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 6j & 0 & 0 & 4 & 0 & 0 & 0 & 2j & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 1 & 0 \\
6j & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 2j & 0 & 0 & 0 & 1 & 0 & 0
\end{bmatrix}.$$

The columns do not cope. However, multiplying both the 5 and 6 columns by $2 \in GF(7)$, they can be combined with columns 13 and 14, respectively. Defining then a 2nd order pre-addition layer (with two multiplications in columns 10 and 11),

$$\begin{array}{c}
S_0(3)=S_0(2), S_1(3)=S_1(2), \\
S_2(3)=S_8(2), S_3(3)=S_9(2), \\
S_4(3)=S_2(2), S_5(3)=S_{10}(2), \\
S_6(3)=S_{11}(2)-S_3(2), S_7(3)=S_{11}(2)+S_3(2), \\
S_8(3)=S_{12}(2)-4S_4(2), S_9(3)=S_{12}(2)+2S_4(2), \\
S_{10}(3)=S_{13}(2)-4S_5(2), S_{11}(3)=S_{13}(2)+2S_5(2), \\
S_{12}(3)=S_{14}(2)-S_6(2), S_{13}(3)=S_{14}(2)+S_6(2), \\
S_{14}(3)=S_{15}(2)-S_7(2), S_{15}(3)=S_{15}(2)+S_7(2).
\end{array}$$

Finally, $V = T^{(3)}S(3)$, where

$$T^{(3)} = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 5j & 6j & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
2j & 0 & 0 & j & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & j & 5j & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
j & 0 & 0 & 5j & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 2j & j & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
5j & 0 & 0 & 6j & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 6j & 2j & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
6j & 0 & 0 & 2j & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0
\end{bmatrix}.$$

There is only one multiplication in columns 1, 2, 3, 4, 5 and 6, besides two pre-multiplications, so the total complexity is 8. The number of additions is 50 (40 pre-additions and 16 post-additions). In this case, the number of multiplications is less than 10, the minimum expected multiplication complexity [10]. It can be concluded that there are two trivial multiplications. It is not simple to identify which are the trivial multiplications from the observation of matrices over $GI(7)$. Carrying on the same analysis over another finite field, the same combination of columns was observed, i.e. the approach does not depend on the finite field but on the length. Let $v \longleftrightarrow V$ be an FFHT pair over $GI(p)$. Considering now $p = 31, \zeta = 7 + 13j$, the transform matrix T will be,

$$T = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 20 & 0 & 11 & 30 & 6 & 23 & 6 & 30 & 11 & 0 & 20 & 1 & 25 & 8 & 25 \\
1 & 0 & 30 & 23 & 30 & 0 & 1 & 8 & 1 & 0 & 30 & 23 & 30 & 0 & 1 & 8 \\
1 & 11 & 23 & 11 & 1 & 25 & 0 & 6 & 30 & 20 & 8 & 20 & 30 & 6 & 0 & 25 \\
1 & 30 & 30 & 1 & 1 & 30 & 30 & 1 & 1 & 30 & 30 & 1 & 1 & 30 & 30 & 1 \\
1 & 6 & 0 & 25 & 30 & 11 & 8 & 11 & 30 & 25 & 0 & 6 & 1 & 20 & 23 & 20 \\
1 & 23 & 1 & 0 & 30 & 8 & 30 & 0 & 1 & 23 & 1 & 0 & 30 & 8 & 30 & 0 \\
1 & 6 & 8 & 6 & 1 & 11 & 0 & 20 & 30 & 25 & 23 & 25 & 30 & 20 & 0 & 11 \\
1 & 30 & 1 & 30 & 1 & 30 & 1 & 30 & 1 & 30 & 1 & 30 & 1 & 30 & 1 & 30 \\
1 & 11 & 0 & 20 & 30 & 25 & 23 & 25 & 30 & 20 & 0 & 11 & 1 & 6 & 8 & 6 \\
1 & 0 & 20 & 8 & 30 & 0 & 1 & 23 & 1 & 0 & 30 & 8 & 30 & 0 & 1 & 23 \\
1 & 20 & 23 & 20 & 1 & 6 & 0 & 25 & 30 & 11 & 8 & 11 & 30 & 25 & 0 & 6 \\
1 & 1 & 30 & 30 & 1 & 1 & 30 & 30 & 1 & 1 & 30 & 30 & 1 & 1 & 30 & 30 \\
1 & 25 & 0 & 6 & 30 & 20 & 8 & 20 & 30 & 6 & 0 & 25 & 1 & 11 & 23 & 11 \\
1 & 8 & 1 & 0 & 30 & 23 & 30 & 0 & 1 & 8 & 1 & 0 & 30 & 23 & 30 & 0 \\
1 & 25 & 8 & 25 & 1 & 20 & 0 & 11 & 30 & 6 & 23 & 6 & 30 & 11 & 0 & 20
\end{bmatrix}.$$

Considering the first order pre-addition layer (eqn.1) and the second order pre-addition layer (eqn.2), $V = T^{(2)}S(2)$, where

$$T^{(2)} = \begin{bmatrix}
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
20 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 25 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 1 & 0 \\
0 & 20 & 0 & 0 & 8 & 0 & 0 & 0 & 25 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 30 & 0 & 0 & 0 & 30 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
6 & 0 & 0 & 0 & 0 & 23 & 0 & 0 & 0 & 20 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 8 & 0 & 0 & 0 & 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 25 & 0 & 0 & 23 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 30 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 30 & 0 & 0 & 0 & 1 \\
11 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 23 & 0 & 0 & 0 & 1 & 0 \\
0 & 11 & 0 & 0 & 8 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 30 & 0 & 0 & 0 & 30 & 0 & 0 & 0 & 1 \\
25 & 0 & 0 & 0 & 0 & 23 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 23 & 0 & 0 & 0 & 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 6 & 0 & 0 & 23 & 0 & 0 & 0 & 20 & 0 & 0 & 0 & 1 & 0 & 0 & 0
\end{bmatrix}.$$

Again, some columns do not cope. But, multiplying both columns 5 and 6 by $4 \in GF(31)$, they can be combined with columns 14 and 13, respectively. The same occurs with columns 10 and 9, which will combine with columns 1 and 2, respectively. A third layer of pre-additions, including four pre-multiplications in columns 1, 2, 5 and 6, is given by

$$\begin{gathered}
S_0(3)=S_7(2)-S_3(2),\ S_1(3)=S_7(2)+S_7(2), \\
S_2(3)=S_8(2)-7S_1(2),\ S_3(3)=S_7(2)+8S_1(2), \\
S_4(3)=S_9(2)-7S_0(2),\ S_5(3)=S_9(2)+7S_0(2), \\
S_6(3)=S_2(2),\ S_7(3)=S_{10}(2), \\
S_8(3)=S_{12}(2)-4S_4(2),\ S_9(3)=S_{12}(2)+4S_4(2), \\
S_{10}(3)=S_{13}(2)-4S_5(2),\ S_{11}(3)=S_{13}(2)+4S_5(2), \\
S_{12}(3)=S_{14}(2)-S_6(2),\ S_{13}(3)=S_{14}(2)+S_6(2), \\
S_{14}(3)=S_{15}(2)-S_{11}(2),\ S_{15}(3)=S_{15}(2)+S_{11}(2).
\end{gathered}$$

Therefore, $V = T^{(3)}S(3)$, where

$$T^{(3)} = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 20 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 20 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 25 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 23 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 25 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 23 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}.$$

The required number of multiplications is 10 (4 pre-multiplications, 2 multiplications in column 4, 2 multiplications in column 5, 1 multiplication in column 7 and 1 multiplication in column 8). The number of additions is 60 (44 pre-additions, 16 post-additions). A complexity comparison of N-blocklengths FFHT fast algorithms (N=8 and N=16) is given in Tables 2 and 3

Table 2: Complexity of the 8-FFHT

Fast algorithms	$M(8)$	$A(8)$	$(M+A)(8)$
Cooley-Tukey-4	12	48	60
Split-Radix	8	42	50
Cooley-Tukey-2	4	26	30
Rader-Brenner	2	24	26
Hadamard Decomposition	2	22	24

Table 3: Complexity of the 16-FFHT

Fast algorithms	$M(16)$	$A(16)$	$(M+A)(16)$
Cooley-Tukey-2	20	74	94
Cooley-Tukey-4	14	70	84
Split-Radix	12	64	76
Rader-Brenner	10	64	74
Hadamard Decomposition	10	60	70

In the above examples, the Hadamard decomposition algorithm presents a lower complexity to compute an FFHT compared to existing FFFT/DFT algorithms. Multiplicative complexity saving regarding classical Cooley-Tukey is 50% (N=16, N=8). The total complexity saving regarding the same algorithm is roughly 25% (N=16), 20% (N=8).

4 Conclusions

A Fast Finite Field Hartley Transform based on Walsh-Hadamard decomposition was developed and applied for some short block lengths, meeting the lower bound on the multiplicative complexity. The total complexity (additive and multiplicative) of the algorithm was compared to that of some classical algorithms and the lower values were obtained for the FT. These FTs are atractive and easy to implement using low-cost high-speed dedicated Integrated Circuits.

References

[1] I.S. Reed, T.K. Truong, The use of Finite Field to Compute Convolutions, IEEE Trans. Info. Theory, IT-21, pp.208-213, Mar., 1975.

[2] R.E. Blahut, Transform Techniques for Error-Control Codes, IBM J. Res. Dev., vol.23, pp.299-315, May, 1979.

[3] R.M. Campello de Souza, H.M. de Oliveira, A. N. Kauffman, A. J. A. Paschoal, Trigonometry in Finite Fields and a New Hartley Transform, Proc. of the IEEE Int. Symp. on Info. Theory, ISIT, Cambridge, MA, Aug. , 1998.

[4] R.M. Campello de Souza, H.M. de Oliveira, A. N. Kauffman, The Hartley Transform in a Finite Field In: IEEE/SBT International Telecommunication Symposium, ITS, pp. 245-250, São Paulo, Brazil, 1998.

[5] R.M. Campello de Souza, H.M. de Oliveira, A. N. Kauffman. The Complex Finite Field Hartley Transform, 5th Int. Symp. on Commun. Theory and Applications, ISCTA, Ambleside, UK, Jul., 1999.

[6] H.M. de Oliveira, R.M. Campello de Souza, and A.N. Kauffman, Efficient Multiplex for Band-limited Channels: Galois Division Multiple Access, Proc. of the Workshop on Coding and Cryptography, WCC 99, pp.235-241, Paris, Jan., 1999.

[7] H.M. de Oliveira, R.M. Campello de Souza, Orthogonal Multilevel Spreading Sequence Design, 5th Int. Symp. on Commun. Theory and Applications, ISCTA, Ambleside, UK, Jul., 1999.

[8] R.J.S. Cintra, H.M. de Oliveira, R.M. Campello de Souza, Multilayer Hadamard Decomposition of Discrete Hartley Transform, Simp. Bras. de Telecom., SBrT, Sept. 2000.

[9] R.N Bracewell. The Discrete Hartley Transform, J. Opt. Soc. Amer., vol.73, pp.1832-1835, 1983.

[10] M.T Heideman, Multiplicative Complexity, Convolution, and the DFT, Springer-Verlag, 1988.

[11] R.M. Campello de Souza, R.G.F. Távora, D. Silva, H.M. de Oliveira. On Fast Finite Field Hartley Transform Algorithms, International Conference on System Engeneering Communication and Information Technology, Punta-Arenas, Apr., 2001.