Cryptosystems based on RS and BCH codes over finite noncommutative algebras

Cryptosystems based on RS and BCH codes over finite noncommutative algebras

V G Labunets[1] and E Ostheimer[2]

[1]Ural State Forest Engineering University, Sibirsky trakt 37, Ekaterinburg, Russia, 620100
[2]Capricat LLC, Pompano Beach, Florida, US

e-mail: vlabunets05@yahoo.com

Abstract. The purpose of this paper is to introduce new cryptosystems based on linear Reed-Solomon (RC) and Bose-Chaudhuri-Hocquenghem (BCH) codes over finite Cayley-Dickson and finite Clifford algebras with fast code and encode procedures based on fast Fourier-Clifford-Galois transforms

1. Introduction

The idea of public key cryptography (PKC) was introduced by Diffie and Hellman [1] in 1976. Today, most successful PKC-schemes are based on the perceived difficulty of certain problems in particular large finite commutative rings. For example, the difficulty of solving the integer factoring problem (IFP) defined over the ring $\mathbf{Z}_m$ (where m is the product of two large primes) forms the ground of the basic RSA cryptosystem [2-11]. The extended multi-dimension RSA cryptosystem [3], which can efficiently resist low exponent attacks, is also defined over the commutative ring $\mathbf{Z}_m[X]$.

Currently there are many attempts to develop alternative PKC based on different kinds of problems on noncommutative algebraic structures. The most researchers use non-commutative groups as a good alternative platform for constructing public-key cryptosystems: braid groups [12-15], polycyclic groups [12,16], Thompson's groups [16-18].

In this paper, we would like to propose a new method for designing public key cryptosystems based on RS and BCH codes over finite *Cayley-Dickson and finite* Clifford algebras. The key idea of our proposal is that for a given non-commutative algebra, we can define polynomials and take them as the underlying work structure in order to do decoding as NP-hard *for the family of Reed-Solomon codes* over noncommutative algebras.

The rest of the paper is organized as follows: in Section 2, the object of the study (Reed-Solomon and Bose-Chaudhuri-Hocquenghem codes) is described. In Section 3, the proposed method based on noncommutative algebras is explained.

2. The object of the study. Reed-Solomon and Bose-Chaudhuri-Hocquenghem codes

The Bose, Chaudhuri and Hocquenghem (BCH) codes are sub class of cyclic codes. Binary BCH codes were discovered by Hocquenghem in 1959 and independently by Bose and Chaudhuri in 1960.

The Reed-Solomon (RS) Code is an important subset of the non-binary BCH Codes. In 1960, Irving Reed and Gus Solomon published a paper in the *Journal of the Society for Industrial and Applied Mathematics* [19]. This paper described a new class of error-correcting codes that are now called *Reed-Solomon* (R-S) *codes*. These codes have great power and utility, and are today found in many applications in the intelligent communication systems, cognitive radio systems and in various technical communication standards like the *Consultative Committee for Space Data Systems* (CCSDS) Telemetry channel coding standard, the Digital Video Broadcasting (DVB) standards as well as in the *Digital Subscriber Line* (DSL) standard. Historically, RS codes were introduced by Reed and Solomon as valuation codes. In the 1960s and 1970s, RS and BCH codes were primarily studied as cyclic codes. The transform approach was popularized by Blahut in the early 1980s.

In order to understand the encoding and decoding principles of Reed-Solomon (R-S) codes, it is necessary to venture into the area of finite fields known as *Galois Fields* (GF). For any prime number p, there exists a finite field denoted GF(p) that contains p elements. It is possible to extend $\mathbf{GF}(p)$ to a field of p^m elements, called an *extension field* of $\mathbf{GF}(p)$, and denoted by $\mathbf{GF}(q) := \mathbf{GF}(p^m)$, where m is a nonzero positive integer. Note that commutative Galois field $\mathbf{GF}(p^m)$ contains as a subset the elements of $\mathbf{GF}(p)$. Symbols from the extension field $\mathbf{GF}(p^m)$ are used in the construction of classical Reed-Solomon (R-S) codes.

An (n,k) linear code $Cod(n,k\,|\,\mathbf{GF}(q))$ is k D subspace of the vector space $\mathbf{GF}^n(q)$ of all n-tuples $\mathbf{c} = (c_0, c_1, ..., c_{n-1})$ over $\mathbf{GF}(q)$, *i.e.*, $Cod(n,k\,|\,\mathbf{GF}(q)) \subset \mathbf{GF}^n(q)$ and $\mathrm{Dim}\{Cod(n,k\,|\,\mathbf{GF}(q))\} = k$. Any k linearly independent codewords $(g_0, g_1, ..., g_{n-1})$ generate $Cod(n,k\,|\,\mathbf{GF}(q))$, in the sense that

$$Cod(n,k\,|\,\mathbf{GF}(q)) = \left\{ \sum_{j=1}^{k} a_j \mathbf{g}_j \,\middle|\, \forall a_j \in \mathbf{GF}(q) \right\}.$$

Thus $Cod(n,k\,|\,\mathbf{GF}(q))$ has q^k distinct codewords.

Reed-Solomon (RS) codes are *nonbinary cyclic* codes with symbols made up of m-bit sequences, where m is any positive integer having a value greater 2. RS(n,k) codes on m-bit symbols exist for all n and k for which $0 < k < n < 2^m + 2$, where k is the number of data symbols being encoded, and n is the total number of code symbols in the encoded block. For the most conventional RS(n,k) code, $(n,k) = (2^m - 1, 2^m - 1 - 2t)$, where t is the symbol-error correcting capability of the code, an $n - k = 2t$ is the number of parity symbols. Reed-Solomon codes achieve the *largest possible* code minimum distance for any linear code with the same encoder input and output block lengths. For Reed- Solomon codes, the code minimum distance is given by [2] $d_{\min} = n - k + 1 = 2t + 1$.

The most natural definition of RS code is in terms of a certain evaluation map from the subspace $\mathbf{GF}^k(q)$ of all n-tuples $\mathbf{m} = (m_0, m_1, ..., m_{k-1})$ (information symbols (massage)) over $\mathbf{GF}(q)$ to the set of codewords $Cod(n,k\,|\,\mathbf{GF(q)}) \subset \mathbf{GF}^n(q)$:

$$\mathbf{m} = (m_0, m_1, ..., m_{k-1}) \mapsto \mathbf{c} = (c_0, c_1, ..., c_{n-1}), \qquad \mathbf{GF}^k(q) \to \mathbf{GF}^n(q) \tag{1}$$

Definition 1. Let $\mathbf{GF}(q)$ be a finite field and $\mathbf{GF}(q)[X]$ denote the $\mathbf{GF}(q)$-space of univariate polynomials where all the coefficients of X are from $\mathbf{GF}(q)$. Pick $D = \{\beta_0, \beta_1, ..., \beta_{n-1}\}$ n different elements of $\mathbf{GF}(q)$ arranged in some arbitrary order and choose n and k such that $k \le n \le q - 1$. The most convenient arrangement is $\beta_0 = \varepsilon^b, \beta_1 = \varepsilon^{b+1}, ..., \beta_i = \varepsilon^{b+i}, ..., \beta_{n-1} = \varepsilon^{b+n-1}$ for a some integer $b + k \le q - 2$, where ε is a primitive element of $\mathbf{GF}(q)$. We define an encoding function for Reed-Solomon code as RS: $\mathbf{GF}^k(q) \to \mathbf{GF}^n(q)$ in the following form. A message $\mathbf{m} = (m_0, m_1, ..., m_{k-1})$ with $m_i \in \mathbf{GF}(q)$ is mapped to a degree $k-1$ polynomial (it is called the information polynomial in the indeterminate X):

$$f_{\mathbf{m}}(X) = m_0 X^0 + m_1 X^1 + ... + m_{k-1} X^{k-1} = \sum_{j=0}^{k-1} m_j X^j. \tag{2}$$

Obviously, $f_{\mathbf{m}}(X)$ is one of the q^k polynomials over $\mathbf{GF}(q)$ of degree less than k. The information polynomial $f_{\mathbf{m}}(X)$ is then mapped into the n-tuple $\left(f_{\mathbf{m}}(\beta_0), f_{\mathbf{m}}(\beta_1),..., f_{\mathbf{m}}(\beta_{n-1})\right)$, i.e.,

$$\mathbf{m} = (m_0, m_1, ..., m_{k-1}) \to f_{\mathbf{m}}(X) \to \left(f_{\mathbf{m}}(\beta_0), f_{\mathbf{m}}(\beta_1),..., f_{\mathbf{m}}(\beta_i),..., f_{\mathbf{m}}(\beta_{n-1})\right),$$

whose components $f_{\mathbf{m}}(\beta_i)$ are equal to the evaluations of the polynomials $f_{\mathbf{m}}(X)$ at each field element $\beta_i \in \mathbf{GF}(p)$:

$$f_{\mathbf{m}}(\beta_i) = m_0 \beta_i^0 + m_1 \beta_i^1 + ... + m_{k-1} \beta_i^{k-1} = \sum_{j=0}^{k-1} m_j \beta_i^j, \quad 0 \le i \le n-1, \tag{3}$$

or

$$f_{\mathbf{m}}(\beta_i) = f_{\mathbf{m}}(\varepsilon^{b+i}) = m_0 \varepsilon^{(b+i)0} + m_1 \varepsilon^{(b+i)1} + ... + m_{k-1} \varepsilon^{(b+i)(k-1)} = \sum_{j=0}^{k-1} m_j \varepsilon^{(b+i)j}, \quad 0 \le i \le q-2, \tag{4}$$

for a common special case $\beta_0 = \varepsilon^b, \beta_1 = \varepsilon^{b+1}, ..., \beta_i = \varepsilon^{b+i}, ..., \beta_{n-1} = \varepsilon^{b+n-2}$ and $n = q-1$. The code generators may thus as polynomials

$$\begin{aligned}
\mathbf{g}_0 &= \left(1,\ \varepsilon^{(b+0)\cdot 1},\ \varepsilon^{(b+0)\cdot 2},\ ...,\ \varepsilon^{(b+0)\cdot(n-1)}\right),\\
\mathbf{g}_1 &= \left(1,\ \varepsilon^{(b+1)\cdot 1},\ \varepsilon^{(b+1)\cdot 2},\ ...,\ \varepsilon^{(b+1)\cdot(n-1)}\right),\\
\mathbf{g}_2 &= \left(1,\ \varepsilon^{(b+2)\cdot 1},\ \varepsilon^{(b+2)\cdot 2},\ ...,\ \varepsilon^{(b+2)\cdot(n-1)}\right),\\
&... \qquad .....,\\
\mathbf{g}_{k-1} &= \left(1, \varepsilon^{(b+k-1)\cdot 1}, \varepsilon^{(b+k-1)\cdot 2}, ..., \varepsilon^{(b+k-1)\cdot(n-1)}\right).
\end{aligned}$$

Hence, generator matrix for RS codes is the *Van Der Monde* matrix with $n \times k$ size

$$\begin{bmatrix}
1 & 1 & ... & 1\\
\varepsilon^{1\cdot(b+0)} & \varepsilon^{1\cdot(b+1)} & ... & \varepsilon^{1\cdot(b+k-1)}\\
... & ... & ... & ...\\
\varepsilon^{(n-1)\cdot(b+0)} & \varepsilon^{(n-1)\cdot(b+1)} & ... & \varepsilon^{(n-1)\cdot(b+k-1)}
\end{bmatrix}$$

and encoding a message block $\mathbf{m} = (m_0, m_1, ..., m_{k-1})$ via the evaluation map in (4) is equivalent to computing the Fourier-Galois Transform of the n-tuple $(0,...,0,m_{b+0},m_{b+1},...,m_{b+k-1},0,...,0)$:

$$\begin{bmatrix} c_0\\ c_1\\ c_2\\ ...\\ ...\\ c_i\\ ...\\ ...\\ c_{n-2}\\ c_{n-1} \end{bmatrix} = \left[\begin{array}{cccc:cccc:ccc}
1 & 1 & ... & 1 & 1 & ... & 1 & 1 & ... & 1\\
1 & \varepsilon^{1\cdot 1} & ... & \varepsilon^{1\cdot(b+0)} & \varepsilon^{1\cdot(b+1)} & ... & \varepsilon^{1\cdot(b+k-1)} & \varepsilon^{1\cdot(b+k)} & ... & \varepsilon^{1\cdot(n-1)}\\
1 & \varepsilon^{2\cdot 1} & ... & \varepsilon^{2\cdot(b+0)} & \varepsilon^{2\cdot(b+1)} & ... & \varepsilon^{2\cdot(b+k-1)} & \varepsilon^{2\cdot(b+k)} & ... & \varepsilon^{2\cdot(n-1)}\\
... & ... & ... & ... & ... & ... & ... & ... & ... & ...\\
... & ... & ... & ... & .... & ... & ... & ... & ... & ....\\
1 & \varepsilon^{i\cdot 1} & ... & \varepsilon^{i\cdot(b+0)} & \varepsilon^{i\cdot(b+1)} & ... & \varepsilon^{i\cdot(b+k-1)} & \varepsilon^{i\cdot(b+k)} & ... & \varepsilon^{i\cdot(n-1)}\\
... & ... & ... & ... & ... & ... & .... & ... & ... & ...\\
... & ... & ... & ... & ... & ... & .... & ... & ... & ...\\
1 & \varepsilon^{(n-2)\cdot 1} & ... & \varepsilon^{(n-2)\cdot(b+0)} & \varepsilon^{(n-2)\cdot(b+1)} & ... & \varepsilon^{(n-2)\cdot(b+k-1)} & \varepsilon^{(n-2)\cdot(b+k)} & ... & \varepsilon^{(n-2)\cdot(n-1)}\\
1 & \varepsilon^{(n-1)\cdot 1} & ... & \varepsilon^{(n-1)\cdot(b+0)} & \varepsilon^{(n-1)\cdot(b+1)} & ... & \varepsilon^{(n-1)\cdot(b+k-1)} & \varepsilon^{(n-1)\cdot(b+k)} & ... & \varepsilon^{(n-1)\cdot(n-1)}
\end{array}\right] \begin{bmatrix} 0\\ ...\\ 0\\ m_{b+0}\\ m_{b+1}\\ \cdots\\ m_{b+k-1}\\ 0\\ \cdots\\ 0 \end{bmatrix}$$

A codewords has a zero symbols in the coordinate corresponding to β_i if and only if $f_{\mathbf{m}}(\beta_i) = 0$; *i.e.,* if and only if β_i is a root of equation $f_{\mathbf{m}}(X) = 0$. By the fundamental theorem of algebra if $\deg\{f_{\mathbf{m}}(X)\} \le k-1$ then equation $f_{\mathbf{m}}(X) = 0$ can have at most $k-1$ roots in $\mathbf{GF}(q)$.

3. Methods

In this section, we describe a construction technique of BCH and RS codes over finite noncommutative algebras in order to prove that maximum-likelihood decoding is NP-hard *for the family of Reed-Solomon codes* over noncommutative algebras. There are noncommutative extensions of GF(p) in the form of Clifford or Cayley-Dickson algebras of p^m elements

$$Cl_m(p) = ClifAlg_m\left\{i_1, i_2, ..., i_s \,|\, \mathbf{GF}(p)\right\},\ CD_m(p) = CayDicAlg_m\left\{i_1, i_2, ..., i_s \,|\, \mathbf{GF}(p)\right\}.$$

Let us denote $Alg_m(p) = Cl_m(p),\ CD_m(p)$, where $m = q^s$ for any prime number q and a nonzero positive integer s. Symbols from the Clifford or Cayley-Dickson algebras $Alg_m(p)$ (instead of symbols from the field $\mathbf{GF}(p^m)$) we are going to use in the construction of generalized Reed-Solomon codes. Let X be a formal noncommutative variable with respect to elements $a \in Alg_{2^m}(p)$, *i.e.*, $aX \neq Xa$. We introduce two noncommutative products with one key $\left[\downarrow \kappa\right]$

$$a^{[\downarrow\kappa]}X^i := \overbrace{\underbrace{X\cdots X}_{\kappa}\cdot\underbrace{X\cdots X}_{i-\kappa}}^{\downarrow\kappa}{}_{i} = \underbrace{X\cdots X}_{\kappa}\cdot a\cdot\underbrace{X\cdots X}_{i-\kappa} = X^{\kappa}\cdot a\cdot X^{i-\kappa},\ \ \kappa = 0,1,...,i$$

Obviously, $a^{[\downarrow 0]}X^i = a\cdot X^i,\quad a^{[\downarrow i]}X^i = X^i\cdot a$ are the left and right multiplications, respectively. We now define a special set of polynomials

$$Alg^{[\downarrow\boldsymbol{\kappa}]}\left[X\right] := \left\{ f^{[\downarrow\boldsymbol{\kappa}]}(X) = \sum_{i=0}^{n-1} a_i^{[\downarrow\kappa_i]}X^i = \sum_{i=0}^{n-1} X^{\kappa_i}a_i X^{i-\kappa_i} \,\middle|\, \left(a_i \in Alg\right)\&\left(a_i X^i \neq X^i a_i\right) \right\}$$

with a bunch of keys $\left[\downarrow\boldsymbol{\kappa}\right] = \left[\downarrow\left(\kappa_0, \kappa_1, ..., \kappa_{n-1}\right)\right] \in \mathbf{Z}_1 \times \mathbf{Z}_2 \times ... \times \mathbf{Z}_{n-1}$. For example,

1) $\kappa_0 \in \{0\} = \mathbf{Z}_1$, it is trivial case: $a^{[\downarrow 0]}\left(X^0\right) \equiv a$;
2) $\kappa_1 \in \{0,1\} = \mathbf{Z}_2$, in this case we have two variants:
   $a^{[\downarrow 0]}\left(X^1\right) = aX^1,\ a^{[\downarrow 1]}\left(X^1\right) = X^1 a$;
3) $\kappa_2 \in \{0,1,2\} = \mathbf{Z}_3$, in this case we have three variants:
   $a^{[\downarrow 0]}\left(X^2\right) = aX^2,\ a^{[\downarrow 1]}\left(X^2\right) = X^1 aX^1,\ a^{[\downarrow 2]}\left(X^2\right) = X^2 a$;
4) $\kappa_3 \in \{0,1,2,3\} = \mathbf{Z}_4$, for this case we obtain four variants
   $a^{[\uparrow 0]}\left(X^3\right) = aX^3,\ a^{[\downarrow 1]}\left(X^3\right) = X^1 aX^2,\ a^{[\downarrow 2]}\left(X^3\right) = X^2 aX^1,\ a^{[\downarrow 3]}\left(X^3\right) = X^3 a.$

There are $n! = 1\cdot 2\cdot 3\cdots n$ similar bunch of keys $\left[\downarrow\boldsymbol{\kappa}\right] = \left[\downarrow\left(\kappa_0, \kappa_1, ..., \kappa_{n-1}\right)\right]$.

Example 1. For $\left[\downarrow\boldsymbol{\kappa}\right] = \left[\downarrow(0,0,...,0)\right]$ and $\left[\downarrow\boldsymbol{\kappa}\right] = \left(\downarrow(0,1,2,...,n-1)\right)$ we obtain right- and left-side polynomials

$$f^{\left[\downarrow(0,0,...,0)\right]}(X) = f^{l}(X) = \sum_{i=0}^{n-1} a_i^{[\downarrow 0]}\left(X^i\right) = \sum_{i=0}^{n-1} a_i \cdot X^i,$$

$$f^{\left[\downarrow(0,1,2,...,n-1)\right]}(X) = {}^{r}f(X) = \sum_{i=0}^{n-1} a_i^{[\downarrow i]}\left(X^i\right) = \sum_{i=0}^{n-1} X^i \cdot a_i.$$

Let $Alg^{[\downarrow\boldsymbol{\kappa}]}\left[X\right]$ by the ring of univariate polynomials over $Alg_{2^m}(p)$ with a bunch of keys $\left[\downarrow\boldsymbol{\kappa}\right] = \left[\downarrow\left(\kappa_0, \kappa_1, ..., \kappa_{n-1}\right)\right]$.

Reed-Solomon codes with the bunch of keys $\left[\downarrow\boldsymbol{\kappa}\right] = \left[\downarrow\left(\kappa_0, \kappa_1, ..., \kappa_{n-1}\right)\right]$ are obtained by evaluating certain subspaces of $Alg^{[\downarrow\boldsymbol{\kappa}]}\left[X\right]$ in set of points $D = \left\{x_0, x_1, ..., x_{n-1}\right\}$ which are subsets of

$Alg_{2^m}(p)$. Specifically, a Reed-Solomon codes $Code\left\{D,k \mid f^{[\sigma]}(X), Alg_{2^m}(p)\right\}$ of length n and dimension k over $Alg_{2^m}(p)$ are defined as follows:

$$Code^{(l)}\left\{D,k \mid f^{[\downarrow\boldsymbol{\kappa}]}(X), Alg_{2^m}(p)\right\} :=$$

$$=\left\{\left(f^{[\downarrow\boldsymbol{\kappa}]}(x_0), f^{[\downarrow\boldsymbol{\kappa}]}(x_1),..., f^{[\downarrow\boldsymbol{\kappa}]}(x_{n-1})\right) \mid \left(f^{[\downarrow\boldsymbol{\kappa}]}(X) \in Alg_{2^m}^{[\downarrow\boldsymbol{\kappa}]}(p)[X]\right) \& \left(\deg\left\{f^{[\downarrow\boldsymbol{\kappa}]}(X)\right\} < k-1\right)\right\}.$$

Thus a Reed-Solomon code is completely specified in terms of its evaluation set $D=\{x_1, x_2,..., x_n\}$ and its dimension k.

We assume that if a codeword $\mathbf{s} \in Code\left\{D,k \mid f^{[\downarrow\boldsymbol{\kappa}]}(X), Alg_{2^m}(p)\right\}$ of is transmitted and the vector $\mathbf{y} \in Alg_{2^m}^{n}(p)$ is received, the maximum-likelihood decoding task consists of computing a codeword $\mathbf{v} \in Code\left\{D,k \mid f^{[\downarrow\boldsymbol{\kappa}]}(X), Alg_{2^m}(p)\right\}$ that minimizes $d(\mathbf{s},\mathbf{v})$, where $d(\cdot,\cdot)$ denotes the Hamming distance. The corresponding decision problem can be formally stated as follows. We let c_i be the codeword symbols, where i runs from 0 to $n-1$, *i.e.*,

$$(c_0, c_1,..., c_{n-1}) = \left(f^{[\downarrow\boldsymbol{\kappa}]}(x_0), f^{[\downarrow\boldsymbol{\kappa}]}(x_1),..., f^{[\downarrow\boldsymbol{\kappa}]}(x_{n-1})\right) \tag{5}$$

and let m_i be the information symbols, where i runs from 0 to $k-1$. An RS coding procedures can then be defined by relating c_j to m_i according to

$$c_j = f^{[\downarrow\boldsymbol{\kappa}]}(x_j) = \sum_{i=0}^{k-1} m_i^{[\downarrow\kappa_i]} x_j^i = \sum_{i=0}^{k-1} x_j^{\kappa_i} \cdot m_i\, x_j^{i-\kappa_i} \tag{6}$$

or in matrix form

$$\begin{bmatrix} c_0 \\ c_1 \\ ... \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} x_0^0 & x_0^1 & ... & x_0^{k-1} \\ x_1^0 & x_1^1 & ... & x_1^{k-1} \\ ... & ... & ... & ... \\ x_{n-1}^0 & x_{n-1}^1 & & x_{n-1}^{k-1} \end{bmatrix} \begin{bmatrix} m_0^{[\downarrow(\kappa_0,\kappa_1,...,\kappa_{k-1})]} \\ m_1^{[\downarrow(\kappa_0,\kappa_1,...,\kappa_{k-1})]} \\ ... \\ m_{k-1}^{[\downarrow(\kappa_0,\kappa_1,...,\kappa_{k-1})]} \end{bmatrix} =$$

$$\begin{bmatrix} x_0^0(\circ) & x_0^{\kappa_1}\cdot(\circ)\cdot x_0^{1-\kappa_1} & ... & x_0^{\kappa_{k-1}}\cdot(\circ)\cdot x_0^{k-\kappa_{k-1}} \\ x_1^0(\circ) & x_1^{\kappa_1}\cdot(\circ)\cdot x_1^{1-\kappa_1} & ... & x_1^{\kappa_{k-1}}\cdot(\circ)\cdot x_1^{k-\kappa_{k-1}} \\ ... & ... & ... & ... \\ x_{n-1}^0(\circ) & x_{n-1}^{\kappa_1}\cdot(\circ)\cdot x_{n-1}^{1-\kappa_1} & ... & x_{n-1}^{\kappa_{k-1}}\cdot(\circ)\cdot x_{n-1}^{k-\kappa_{k-1}} \end{bmatrix} \begin{bmatrix} m_0 \\ m_1 \\ ... \\ m_{k-1} \end{bmatrix}. \tag{7}$$

where the symbol $(\circ)$ in $x_i^{\kappa_j}\cdot(\circ)\cdot x_i^{1-\kappa_j}$ means the place for m_j. These generator matrices have forms of discrete Vandermonde-Clifford-Galois transform (if $Alg_{2^m}(p) = Cl_{2^m}(p)$) or Vandermonde -Caley-Dickson-Galois (if $Alg_{2^m}(p) = CD_{2^m}(p)$) transform with a bunch of keys $\left[\downarrow\boldsymbol{\kappa}\right] = \left[\downarrow(\kappa_0,\kappa_1,...,\kappa_{n-1})\right]$. If we define $\varepsilon \in Alg_{2^m}(p)$ to be a primitive element of power n (i.e., the powers of ε^j, where j runs from 1 to $n-1$, are all different from each other), then RS codes for $x_j = \varepsilon^{j-1}$ $(j=1,2,...,n)$ can then be defined as

$$c_j = f^{[\downarrow\boldsymbol{\kappa}]}(x_j)\Big|_{x_j=\varepsilon^{j-1}} = f^{[\downarrow(\kappa_0,\kappa_1,...,\kappa_{k-1})]}(\varepsilon^{j-1}) = \sum_{i=1}^{k-1} \varepsilon^{\kappa_i(j-1)} \cdot m_i \cdot \varepsilon^{(i-\kappa_i)(j-1)}, \tag{8}$$

This has the form of discrete Fourier-Clifford-Galois or Fourier-Caley-Dickson-Galois transforms with a bunch of keys $\left[\downarrow\boldsymbol{\kappa}\right] = \left[\downarrow(\kappa_0,\kappa_1,...,\kappa_{n-1})\right]$ (DFCGTs or DFCDGTs) over $Alg_{2^m}(p)$, where the

k "frequency" components (from d until $d+k-1$) are given by the information symbols $u_0, u_1, ..., u_{k-1}$, and the other $n-k$ frequency components are fixed to zero [5].

Example 2. For $\left[\downarrow \boldsymbol{\kappa}\right]=\left[\downarrow(0,0,...,0)\right]$ and $\left[\downarrow \boldsymbol{\kappa}\right]=\left[\downarrow(0,1,2,3,...,n-1)\right]$ we have right- and left-side transforms

$$c_j = f^{(r)}(x_j)=\sum_{i=1}^{k-1}\varepsilon_j^{i(j-1)}\cdot m_i,\ \ c_j = f^{(l)}(x_j)=\sum_{i=1}^{k-1} m_i\cdot\varepsilon_j^{i(j-1)}. \tag{9}$$

These transforms can be viewed as polynomial evaluations (5). Since evaluating a polynomial at multiple points can be implemented as a DFT, DFTs can be used to reduce the encode computational complexity, if a bunch of keys is known. When $n=2^l$, the Cooley-Tukey algorithm can be carried out.

4. Quaternization of classical codes and Fourier-Galois transforms

In this section we going to consider a Reed-Solomon codes $Code\left\{D,k \mid f^{\left[\downarrow\boldsymbol{\kappa}\right]}(X), Alg_{2^m}(p)\right\}$ over quaternion algebras.

4.1. Quaternions

The quaternions, denoted by $\mathsf{H}(\mathbf{R})$, were first invented by W. R. Hamilton in 1843 as an extension of the complex numbers into four dimensions [20].

Definition 2. *The Hamilton Quaternion Algebra over the set of the real numbers* $\mathbf{R}$, *denoted by* $\mathsf{H}(\mathbf{R})$, *is the associative unital algebra given by the following representation:*

1) $\mathsf{H}(\mathbf{R}):=\left\{\alpha = a+bi+cj+dk \middle| a,b,c,d\in\mathbf{R}\right\}=\left\{\alpha = (a+bi)+(c+di)\,j \middle| a+bi, c+di\in\mathbf{C}\right\}$;

2) 1 is the multiplicative unit;

3) $i^2=j^2=k^2=-1$;

4) $ij=-ij=k,\ ik=-ki=j,\ jk=-kj=i$.

If $\alpha = a+bi+cj+dk\in\mathsf{H}(\mathbf{R})$ then its scalar part is $Sc(\alpha)=\alpha_0=a\in\mathbf{R}$ and its vector part is $Vec\{\alpha\}=\vec{\alpha}=bi+cj+dk\in\mathbf{R}^3$. Hence, $\alpha = a+bi+cj+dk=a+\vec{\alpha}$. We can write the product of two quaternions in terms of these three representations in the following ways:

$$\begin{aligned}
1)\ \alpha_1\alpha_2 &= (a_1+b_1i+c_1j+d_1k)(a_2+b_2i+c_2j+d_2k)=\\
&=(a_1a_2-b_1b_2-c_1c_2-d_1d_2)+(a_1b_2+b_1a_2+c_1d_2-d_1c_2)i+\\
&+(a_1b_2+b_1a_2-d_1b_2-b_1d_2)j+(a_1d_2+d_1a_2+b_1c_2-c_1b_2)k;\\
2)\ \alpha_1\alpha_2 &=\left[(a_1+b_1i)+(c_1+d_1i)j\right]\left[(a_2+b_2i)+(c_2+d_2i)j\right]=\\
&=\left[(a_1+b_1i)(a_2+b_2i)-(c_1+d_1i)\left(\overline{c_2+d_2i}\right)\right]+\\
&+\left[(c_1+d_1i)\left(\overline{a_2+b_2i}\right)+(a_1+b_1i)(c_2+d_2i)\right]j;\\
3)\ \alpha_1\alpha_2 &=(a_1+\vec{\alpha}_1)(a_2+\vec{\alpha}_2)=\left[a_1a_2-(\vec{\alpha}_1,\vec{\alpha}_2)\right]+\left[a_1\vec{\alpha}_2+a_2\vec{\alpha}_1+\vec{\alpha}_1\times\vec{\alpha}_2\right].
\end{aligned}$$

The commutative property of multiplication does not hold for quaternion numbers. However, if the vector parts of quaternion numbers are parallel to each other, then their product is commutative.

Definition 3. *Let* $\alpha = a+bi+cj+dk\in\mathsf{H}(\mathbf{R})$ *be a quaternion (*$a,b,c,d\in\mathbf{R}$*). Then*

$$\bar{\alpha} = a-bi-cj-dk=a-(bi+cj+dk)\in\mathsf{H}(\mathbf{R})$$

is the conjugate of α, *and* $N^2(\alpha)=a^2+b^2+c^2+d^2=\alpha\bar{\alpha}=\bar{\alpha}\alpha$ *is the norm of* α, *and* $tr(\alpha)=2a=\alpha+\bar{\alpha}$ *is the trace of* α.

Therefore $\alpha^2-tr(\alpha)\alpha+N^2(\alpha)=0$. We define the special elements $\mathsf{i}=i+j+k,\quad \sigma=\dfrac{1+i+j+k}{2}$.

Proposition 1. *We have* $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ *and* $N(\alpha\beta) = N(\alpha)N(\beta)$ *for every* $\alpha, \beta \in \mathsf{H}(\mathbf{R})$. *We have* $N(\sigma) = 1$ *and* $\mathrm{i}^2 = -3,\ \sigma_1^2 = \sigma_1 - 1.$

4.2. Arithmetic of quaternion integers

Now we look at the number theory of integral quaternions. More information which is related with the arithmetic properties of $\mathsf{H}(\mathbf{Z})$ can be found in [21,22].

Definition 4. *Quaternions of the form* $\alpha = a\sigma + bi + cj + dk, \quad a,b,c,d \in \mathbf{Z}$ *are called integral quaternions, or Hurwitz integral quaternions (they form a ring* $\mathsf{H}(\sigma, \mathbf{Z})$*) and quaternions of the form* $\alpha = a + bi + cj + dk, \quad a,b,c,d \in \mathbf{Z}$ *shall be called quaternions with integer coefficients, or Lipschitz integral quaternions (they form subring* $\mathsf{H}(\mathbf{Z}) \subset \mathsf{H}(\sigma, \mathbf{Z})$*).*

We shall be working exclusively in the ring $\mathsf{H}(\sigma, \mathbf{R})$ of Hurwitz integral quaternions, and use the divisibility symbol "|" to denote divisibility on the left in $\mathsf{H}(\sigma, \mathbf{R})$.

Proposition 2. *A quaternion* $\alpha = a\sigma + bi + cj + dk$ *is Hurwitz if and only if either* a,b,c,d *are all integers, or all of them is the half of an odd integer. If* α *is such, then* $N^2(\alpha),\ tr(\alpha)$ *are integers.*

Proposition 3. *An integral quaternion is a unit (that is, divides every element of* $\mathsf{H}(\sigma, \mathbf{Z})$ *on the left) if and only if its norm is 1. These are exactly the 24 elements* $\pm 1,\ \pm i,\ \pm j,\ \pm k,\ \frac{\pm 1 \pm i \pm j \pm ik}{2}$, *which form a group under multiplication.*

Definition 4. *Two quaternions* $\alpha, \alpha' \in \mathsf{H}(\sigma, \mathbf{Z})$ *are associate if there exist unit quaternions* $\varepsilon, \varepsilon' \in \mathsf{H}(\sigma, \mathbf{Z})$ *such that* $\alpha' = \varepsilon\alpha\varepsilon'$

Theorem 1. *The ring* $\mathsf{H}(\sigma, \mathbf{Z})$ *is right Euclidean: for every* $\alpha, \beta \in \mathsf{H}(\sigma, \mathbf{Z})$ *with* $\beta \neq 0$ *there exist* $\omega, \rho \in \mathsf{H}(\sigma, \mathbf{Z})$ *such that*

$$\alpha = \beta\omega + \rho \tag{10}$$

and $N(\rho) < N(\omega)$.

Definition 5. *A quaternion* $\beta \in \mathsf{H}(\sigma, \mathbf{Z})$ *is a right-hand divisor of* $\alpha \in \mathsf{H}(\sigma, \mathbf{Z})$ *if there is* $\omega \in \mathsf{H}(\sigma, \mathbf{Z})$ *such that* $\alpha = \beta\omega$.

Remark 1. The ring $\mathsf{H}(\sigma, \mathbf{Z})$ is also left Euclidean. In fact, $\alpha \to \overline{\alpha}$ is an isomorphism between $\mathsf{H}(\sigma, \mathbf{Z})$ and its dual $\overline{\mathsf{H}}(\sigma, \mathbf{Z})$, so every assertion that we prove for $\mathsf{H}(\sigma, \mathbf{Z})$ holds also if we replace "left" with "right" and vice versa.

Definition 6. *A quaternion* $\pi \in \mathsf{H}(\sigma, \mathbf{Z})$ *is prime (irreducible) if* α *is not a unit in* $\mathsf{H}(\sigma, \mathbf{Z})$, *and if, whenever* $\pi = \beta\gamma$ *in* $\mathsf{H}(\sigma, \mathbf{Z})$, *the either* β *or* γ *is a unit.*

Theorem 2. *Suppose that* $\alpha \in \mathsf{H}(\sigma, \mathbf{Z})$ *and* $p \in \mathbf{Z}$ *is a prime such that* $p \mid N(\alpha)$ *but* p *does not divide* α. *Then* α *can be written as* $\pi\omega$, *where* $N(\pi) = p$, *and this* π *is uniquely determined up to right association.*

Theorem 3. *For every odd, rational prime* $p \in \mathbf{N}$, *there exists a prime* $\pi \in \mathsf{H}(\mathbf{Z})$, *such that* $N(\pi) = p = \pi\overline{\pi}$. *In particular,* $p \in \mathbf{N}$ *is not prime in* $\mathsf{H}(\mathbf{Z})$.

Theorem 4. *An integral quaternion is irreducible in the ring* $\mathsf{H}(\sigma, \mathbf{Z})$ *if and only if its norm is a prime in* $\mathbf{Z}$. *The only elements of* $\mathsf{H}(\sigma, \mathbf{Z})$ *whose norm is 2 are* $\lambda = 1 + i$ *and its left associates. If* $p > 2$ *is a prime in* $\mathbf{Z}$, *then there exist exactly* $24(p+1)$ *integral quaternions whose norm is* p.

As $\mathsf{H}(\sigma, \mathbf{Z})$ is left Euclidean, every element can be written as a product of irreducible quaternions. This decomposition is unique in the following certain sense.

Theorem 5. *For any primitive Hurwitz integer* α *and any factorization of* $N^2(\alpha)$ *into a product* $p_0 p_1 \cdots p_k$ *of ordinary prime numbers, there is a factorization*

$$\alpha = \pi_0 \pi_1 \cdots \pi_k \tag{11}$$

of α *into a product of Hurwitz primes with* $N^2(\pi_i) = p_i^2$. *Moreover, given any factorization with this property, all the other factorizations with this property are of the form*

$$\alpha = \left(\pi_0 U_1\right)\left(U_1^{-1}\pi_1 U_2\right)\cdots\left(U_k^{-1}\pi_k\right), \tag{12}$$

where the U_i *are Hurwitz integers of norm 1|of which there are precisely 24, as we shall soon see. Conway and Smith call this `uniqueness up to unit-migration'* [23].

4.3. Modular arithmetic of quaternion integers

More information which is related with the modular arithmetic $\mathsf{H}(\sigma, \mathbf{Z})$ can be found in [24].

Definition 7. *Let* $\pi \neq 0$ *be a quaternion integer. If there exist* $\omega \in \mathsf{H}(\sigma, \mathbf{Z})$ *such that* $\alpha - \beta = \omega\pi$ *then* $\alpha, \beta \in \mathsf{H}(\sigma, \mathbf{Z})$) *are right congruent modulo* π *and it is denoted as* $\alpha = \beta \left(\mathrm{mod}\, \pi\right)$.

Let $\mathsf{H}_\pi(\sigma, \mathbf{Z})$ be residue class of $\mathsf{H}(\sigma, \mathbf{Z})$ modulo π, where π is prime quaternion integer. The set obtained from the elements of $\mathsf{H}_\pi(\sigma, \mathbf{Z})$ obtains the elements which by the remainders from right dividing (or left dividing) the elements of $\mathsf{H}(\sigma, \mathbf{Z})$ by the element π. Thus, the quotient ring of the quaternion integers modulo this equivalence is denoted as $\mathsf{H}_\pi(\sigma, \mathbf{Z}) = \mathsf{H}(\sigma, \mathbf{Z}) / \left\langle \mathsf{H}(\sigma, \mathbf{Z})\pi \right\rangle$.

Theorem 6. *Let* $\pi \in \mathsf{H}(\sigma, \mathbf{Z})$). *Then* $\mathsf{H}_\pi(\sigma, \mathbf{Z})$ *has* $N^2(\pi)$ *element.*

Define $\mathsf{H}(\mathrm{i}, \mathbf{Z})$ as follows: $\mathsf{H}(\mathrm{i}, \mathbf{Z}) := \left\{\alpha = a + b(i + j + k) \middle| a, b \in \mathbf{Z}\right\}$ which is a subset of quaternion integers. The commutative property of multiplication holds over $\mathsf{H}(\mathrm{i}, \mathbf{Z})$, *i.e,*. for $\alpha_1, \alpha_2 \in \mathsf{H}(\mathrm{i}, \mathbf{Z})$ $\alpha_1\alpha_2 = \alpha_2\alpha_1$, but if $\alpha_1 \in \mathsf{H}(\mathrm{i}, \mathbf{Z})$ and $\alpha_2 \in \mathsf{H}(\mathbf{Z}) \setminus \mathsf{H}(\mathrm{i}, \mathbf{Z})$ then $\alpha_1\alpha_2 \neq \alpha_2\alpha_1$. Indeed,

$$\alpha_1\alpha_2 = \left[a_1 + b_1(i + j + k)\right]\left[a_2 + \vec{\alpha}_2\right] = \left[a_1 a_2 - \left(\vec{\alpha}_1, \overrightarrow{i + j + k}\right)\right] + \left[a_1\vec{\alpha}_2 + a_2\overrightarrow{(i + j + k)} + \overrightarrow{(i + j + k)} \times \vec{\alpha}_2\right],$$

$$\alpha_2\alpha_1 = \left[a_2 + \vec{\alpha}_2\right]\left[a_1 + b_1(i + j + k)\right] = \left[a_1 a_2 - \left(\vec{\alpha}_1, \overrightarrow{i + j + k}\right)\right] + \left[a_1\vec{\alpha}_2 + a_2\overrightarrow{(i + j + k)} - \overrightarrow{(i + j + k)} \times \vec{\alpha}_2\right].$$

Obviously, $\mathsf{H}(\mathrm{i}, \mathbf{Z}) \supset \mathbf{Z}[i]$ and it is the ring of Gaussian integers.

Theorem 7. *If* a *and* b *are relatively prime integers then* $\mathsf{H}(\mathrm{i}, \mathbf{Z}) / \left\langle a + b(i + j + k) \right\rangle$ *is isomorphic to* $\mathbf{Z}_{a^2 + 3b^2}$ [24].

Theorem 8. *Let* $\mathsf{H}(\mathrm{i}, \mathbf{Z}) / \left\langle \pi^m \right\rangle$ *be the residue class of* $\mathsf{H}(\mathrm{i}, \mathbf{Z})$ *modulo* π^k, *where* k *is any positive integer and* $\pi \in \mathsf{H}(\mathbf{Z})$ *is a prime quaternion integer. According to the modulo function* $\rho: \mathbf{Z}_{p^m} \to \mathsf{H}(\mathrm{i}, \mathbf{Z}) / \left\langle \pi^m \right\rangle$ *defined by*

$$g \to \tilde{g} = g - \left]\frac{g\overline{\pi}}{\pi\overline{\pi}}\right[\pi \left(\mathrm{mod}\, \pi^m\right) \tag{13}$$

$\mathsf{H}(\mathrm{i}, \mathbf{Z}) / \left\langle \pi^m \right\rangle$ *is isomorphic to* $\mathbf{Z}_{p^m}$, *where* $p = \pi\overline{\pi}$ *and* p *is an odd prime.*

The symbol of $]\cdot[$ in (13) is rounding to the closest integer. The rounding of Gaussian integer can be done by rounding the real and imaginary parts separately to the closest integer.

4.4. Quaternion codes

There are two cases. In the first case we have $\mathbf{GF}(p)$-valued massage $\mathbf{m} = (m_0, m_1, ..., m_{k-1}) \in \mathbf{GF}(p)$ - k-tuples of information symbols over $\mathbf{GF}^k(p)$ and quaternion Fourier-Galois transform. In this case we use procedure (13) for embedding $\mathbf{m}$ into $\mathsf{H}^k(\mathrm{i}, \mathbf{Z}) / \left\langle \pi \right\rangle$: $\rho\left\{\mathbf{GF}^k(p)\right\} \to \mathsf{H}^k(\mathrm{i}, \mathbf{Z}) / \left\langle \pi \right\rangle$, *i.e.*,

$$\rho(m_0, m_1, ..., m_{k-1}) = \left(\rho(m_0), \rho(m_1), ..., \rho(m_{n-1})\right) = (\tilde{m}_0, \tilde{m}_1, ..., \tilde{m}_{k-1}) = \tilde{\mathbf{m}}.$$

Let ε be an element of $\mathsf{H}(\sigma,\mathbf{Z})$ such that $\varepsilon^{p-1}=1$ and let p be a prime in $\mathbf{Z}$, where π is a quaternion prime number and $N(\pi)=p=\pi\overline{\pi}$. Then $\mathsf{F}=\left[\varepsilon^{kn}\right]_{k,n-0}^{p-2}$ is the quaternion Fourier-Hamilton-Galois transform. The most natural definition of quaternion RS code is in terms of such transform with a bunch of keys $\left[\downarrow\boldsymbol{\kappa}\right]=\left[\downarrow\left(\kappa_0,\kappa_1,...,\kappa_{n-1}\right)\right]$:

$$\mathbf{c}=\mathsf{F}^{\left[\downarrow\boldsymbol{\kappa}\right]}\tilde{\mathbf{m}}=\sum_{i=1}^{k-1}\varepsilon^{\kappa_i(j-1)}\cdot m_i\cdot\varepsilon^{(i-\kappa_i)(j-1)}. \tag{14}$$

As result we obtain RS code with the bunch of keys $\left[\downarrow\boldsymbol{\kappa}\right]=\left[\downarrow\left(\kappa_0,\kappa_1,...,\kappa_{n-1}\right)\right]$.

In the second case we have $\mathsf{H}(\sigma,\mathbf{Z})$-valued massage $\mathbf{m}=(m_0,m_1,...,m_{k-1})\in\mathsf{H}(\sigma,\mathbf{Z})$ - k-tuples of information symbols over quaternion ring $\mathsf{H}(\sigma,\mathbf{Z})$ and Fourier-Galois transform $\mathsf{F}=\left[\varepsilon^{kn}\right]_{k,n-0}^{p-2}$ over $\mathbf{GF}(p)$, where ε be an element of $\mathbf{GF}(p)$ such that $\varepsilon^{p-1}=1\ (\mathrm{mod}\ p)$. In this case we use procedure (13) for quaternization of Fourier-Galois transform

$$\rho(\mathsf{F})=\left[\rho(\varepsilon)^{kn}\right]_{k,n-0}^{p-2}=\left[\tilde{\varepsilon}^{kn}\right]_{k,n-0}^{p-2}=\tilde{\mathsf{F}}. \tag{15}$$

A quaternion RS with a bunch of keys $\left[\downarrow\boldsymbol{\kappa}\right]=\left[\downarrow\left(\kappa_0,\kappa_1,...,\kappa_{n-1}\right)\right]$ is defined as the following transform

$$\mathbf{c}=\tilde{\mathsf{F}}^{\left[\downarrow\boldsymbol{\kappa}\right]}\mathbf{m}=\sum_{i=1}^{k-1}\tilde{\varepsilon}^{\kappa_i(j-1)}\cdot m_i\cdot\tilde{\varepsilon}^{(i-\kappa_i)(j-1)}. \tag{16}$$

The quaternion Fourier-Hamilton-Galois transform $\mathsf{F}_{2^n}=\left[\varepsilon^{kn}\right]_{k,n-0}^{2^n-1}$ is represented as a weakly filled matrices product:

$$\mathsf{F}_{2^n}=\prod_{j=1}^{n}\left[I_{2^{j-1}}\otimes\Delta\left(\varepsilon^{2^{j-1}}\right)\right]\cdot\left[I_{2^{j-1}}\otimes\begin{bmatrix}1&1\\1&-1\end{bmatrix}\otimes I_{2^{n-j}}\right], \tag{17}$$

where $\Delta\left(\varepsilon^{2^{j-1}}\right)=\mathrm{diag}\left(1,\varepsilon^{1\cdot2^{j-1}},\varepsilon^{2\cdot2^{j-1}},...,\varepsilon^{(2^{n-j}-1)\cdot2^{j-1}}\right)$. Then

$$\mathbf{c}=\mathsf{F}_{2^n}\mathbf{m}=\prod_{j=1}^{n}\left[I_{2^{j-1}}\otimes\Delta\left(\varepsilon^{2^{j-1}}\right)\right]\cdot\left[I_{2^{j-1}}\otimes\begin{bmatrix}1&1\\1&-1\end{bmatrix}\otimes I_{2^{n-j}}\right]\mathbf{m}. \tag{18}$$

All variables in (18) are assumed to be $\mathbf{GF}(p)$-valued variables, obeying the arithmetic laws of a Galois field $\mathbf{GF}(p)$. From (18) for c_{2k}^{j+1} and c_{2k+1}^{j+1} we have

$$\begin{bmatrix}c_{2k}^{j+1}\\c_{2k+1}^{j+1}\end{bmatrix}=\begin{bmatrix}\varepsilon^{2k\cdot2^{j-1}}&\\&\varepsilon^{(2k+1)\cdot2^{j-1}}\end{bmatrix}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}c_{2k}^{j}\\c_{2k+1}^{j}\end{bmatrix}=\begin{bmatrix}\varepsilon^{2k\cdot2^{j-1}}\cdot(c_{2k}^{j}+c_{2k+1}^{j})\\\varepsilon^{(2k+1)\cdot2^{j-1}}\cdot(c_{2k}^{j}+c_{2k+1}^{j})\end{bmatrix} \tag{19}$$

Engineers often represent this transformation as a picture and call it the “butterfly operation”.

For quaternion Fourier-Hamilton-Galois transform $\mathsf{F}_{2^n}^{\left[\downarrow\boldsymbol{\kappa}\right]}$ with a bunch of keys $\left[\downarrow\boldsymbol{\kappa}\right]$ we use the following expression

$$\mathbf{c}=\mathsf{F}_{2^n}^{\left[\downarrow\boldsymbol{\kappa}\right]}\mathbf{m}=\prod_{j=1}^{n}\left[I_{2^{j-1}}\otimes\Delta\left(\varepsilon^{\kappa_j}(\circ)\varepsilon^{2^{j-1}-\kappa_j}\right)\right]\cdot\left[I_{2^{j-1}}\otimes\begin{bmatrix}1&1\\1&-1\end{bmatrix}\otimes I_{2^{n-j}}\right]\mathbf{m} \tag{20}$$

From (20) for c_{2k}^{j+1} and c_{2k+1}^{j+1} we have

$$\begin{bmatrix} c_{2k}^{j+1} \\ c_{2k+1}^{j+1} \end{bmatrix} = \begin{bmatrix} \varepsilon^{\kappa_j}(\circ)\varepsilon^{2k\cdot 2^{j-1}-\kappa_j} & \\ & \varepsilon^{\kappa_j}(\circ)\varepsilon^{(2k+1)\cdot 2^{j-1}-\kappa_j} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} c_{2k}^{j} \\ c_{2k+1}^{j} \end{bmatrix} = \begin{bmatrix} \varepsilon^{\kappa_j}\cdot(c_{2k}^{j}+c_{2k+1}^{j})\cdot\varepsilon^{2k\cdot 2^{j-1}-\kappa_j} \\ \varepsilon^{\kappa_j}\cdot(c_{2k}^{j}+c_{2k+1}^{j})\cdot\varepsilon^{(2k+1)\cdot 2^{j-1}-\kappa_j} \end{bmatrix}. \quad (21)$$

Obviously, it is the "butterfly operation" with key $\left[\downarrow \kappa_j\right]$. Fast quaternion Fourier-Hamilton-Galois transform contain $n2^{n-1}$ "butterfly blocks" and every block can has unique key.

5. Conclusion

According to Berlekamp, McEliece, and van Tilborg maximum-likelihood decoding of linear codes is NP-complete over all finite fields $\mathbf{GF}(p)$. In this paper, we have shown a new unified approach to the Reed-Solomon and Bose-Chaudhuri-Hocquenghem codes over finite noncommutative algebras. The approach is based on a bunch of keys for discrete Fourier-Clifford-Galois or Fourier-Caley-Dickson-Galois transforms. Cardinality of the set of bunch of keys is equal to $k!$ for (n,k)-code.

6. References

[1] Diffie W and Hellman M E 1976 New directions in cryptography *IEEE Trans. Inform. Theory* **22** 644-654
[2] Cao Z 1999 Conic analog of RSA cryptosystem and some improved RSA cryptosystems *Journal of Natural Science of Heilongjiang University* **16(**4**)** 15-18
[3] Cao Z 2000 The multi-dimension RSA and its low exponent security *Science in China (E Series)* **43(4)** 349-354
[4] Cao Z 2001 A threshold key escrow scheme based on public key cryptosystem *Science in China (E Series)* **44(4)** 441-448
[5] Komaya K, Maurer U, Okamoto T and Vanston S 1992 New public-key schemes bases on elliptic curves over the ring Z_n *Crypto'91 LNCS* (Berlin: Springer-Verlag) **576** 252-266
[6] Rabin M O 1979 *Digitized signatures and public-key functions as intractible as factorization MIT Laboratory for Computer Science Technical Report* LCS/TR **212** p 16
[7] Rackoff C and Simon D 1992 Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack *Crypto'91, LNCS* (Berlin: Springer-Verlag) **576** 433-444
[8] Rivest R L, Shamir A and Adleman L 1978 A method for obtaining digital signatures and public key cryptosystems *Communications of the ACM* **21** 120-126
[9] Smith P and Lennon M 1993 LUC: A new public key system *Proceedings of the IFIPTC11 Ninth International Conference on Information Security, IFIP/Sec 93* 103-117
[10] Williams H C 1980 A Modification of the RSA Public-Key Encryption Procedure *IEEE Transactions on Information Theory* IT **26(6)** 726-729
[11] Williams H C 1985 Some public-key crypto-functions as intractable as factorization *Crypto'84, LNCS* (Berlin: Springer-Verlag) **196** 66-70
[12] Anshel I, Anshel M and Goldfeld D 1999 An algebraic method for public-key cryptography *Math. Research Letters* **6** 287-291
[13] Bohli J M, Glas B and Steinwandt R 2006 Towards provable secure group key agreement building on group theory *Cryptology* e-Print Archive: Report 2006/079
[14] Dehornoy P 2004 Braid-based cryptography *Contemporary Mathematics* **360** 5-33
[15] Ko K H, Lee S J, Cheon J H and Han J W 2000 New Public-Key Cryptosystem Using Braid Groups *Crypto 2000, LNCS* (Berlin: Springer-Verlag) **1880** 166-183
[16] Eick B and Kahrobaei D 2004 Polycyclic groups: a new platform for cryptography *Preprint arXiv: math.GR/0411077*
[17] Paeng S H, Ha K C, Kim J H, Chee S and Park C 2001 New public key cryptosystem using finite Non Abelian Groups *Crypto 2001, LNCS* (Berlin: Springer-Verlag) **2139 4**70-485
[18] Shpilrain V and Ushakov A 2005. Thmposon's group and public key cryptography *Preprint math.GR/0505487*
[19] Reed I S and Solomon G 1960 Polynomial Codes Over Certain Finite Fields *SIAM Journal of Applied Math.* **8** 300-304

[20] Hurwitz A 1919 *Vorlesungen uber die Zahlentheorie der Quaternionen* (Berlin: Verlag-Springer) p 88
[21] Pall G 1940 On the arithmetic of quaternions *Tran. Amer. Math. Soc.* **47** 487-500
[22] Chernov V M 2015 Quasiparallel algorithm for error-free convolution computation using reduced Mersenne–Lucas codes *Computer Optics* **39** 241-248
[23] Conway J H and Sloane N J A 1993 Sphere Packings, Lattices and Groups (Berlin: Verlag-Springer) p 573
[24] Hurwitz A 1896 Uber die Zahlentheorie der Quaternione *Math.-Phys. Klasse* (Gottingen: Nachr. Ges. Wiss.) 303-330, 313-340

Acknowledgments
This work was supported by grants the RFBR № 17-07-00886 and by Ural State Forest Engineering's Center of Excellence in "Quantum and Classical Information Technologies for Remote Sensing Systems".