Cryptosystems based on RS and BCH codes over finite noncommutative algebras

V.G. Labunets[1], **E. Osthaimer**[2]

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

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 and Fourier- Cayley-Dickson-Galois transforms.

Keywords: public key, linear code, finite Cayley-Dickson algebras, finite Clifford algebras, Fourier-Clifford-Galois transforms, Fourier-Cayley-Dickson-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 $\mathrm{GF}(p)$ that contains p elements. It is possible to extend $\mathrm{GF}(p)$ to a field of p^m elements, called an *extension field* of $\mathrm{GF}(p)$, and denoted by $\mathrm{GF}(q) := \mathrm{GF}(p^m)$, where m is a nonzero positive integer. Note that commutative Galois field $\mathrm{GF}(p^m)$ contains as a subset the elements of $\mathrm{GF}(p)$. Symbols from the extension field $\mathrm{GF}(p^m)$ are used in the construction of classical Reed-Solomon (R-S) codes.

An (n,k) linear code $Cod(n,k\,|\,\mathrm{GF}(q))$ is k D subspace of the vector space $\mathrm{GF}^n(q)$ of all n-tuples $\mathbf{c} = (c_0, c_1, ..., c_{n-1})$ over $\mathrm{GF}(q)$, *i.e.*,

$Cod(n,k\,|\,\mathrm{GF}(q)) \subset \mathrm{GF}^n(q)$ and $\mathrm{Dim}\{Cod(n,k\,|\,\mathrm{GF}(q))\} = k$.

Any k linearly independent codewords $(g_0, g_1, ..., g_{n-1})$ generate $Cod(n,k\,|\,\mathrm{GF}(q))$, in the sense that

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

Thus $Cod(n,k\,|\,\mathrm{GF}(q))$ 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. $\mathrm{RS}(n,k)$ 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 $\mathrm{RS}(n,k)$ code,

$$(n,k) = (2^m - 1, 2^m - 1 - 2t),$$

where t is the symbol-error correcting capability of the code, and $n - k = 2t$ 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 $\mathrm{GF}^k(q)$ of all n-tuples $\mathbf{m} = (m_0, m_1, ..., m_{k-1})$ (information symbols (massage)) over $\mathrm{GF}(q)$ to the set of codewords $Cod(n,k\,|\,\mathrm{GF}(q)) \subset \mathrm{GF}^n(q)$:

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

Definition 1. Let $\mathrm{GF}(q)$ be a finite field and $\mathrm{GF}(q)[X]$ denote the $\mathrm{GF}(q)$-space of univariate polynomials where all the coefficients of X are from $\mathrm{GF}(q)$. Pick $D = \{\beta_0, \beta_1, ..., \beta_{n-1}\}$ n different elements of $\mathrm{GF}(q)$ 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 $\mathrm{GF}(q)$. We define an encoding function for Reed-Solomon code as $\mathrm{RS}: \mathrm{GF}^k(q) \to \mathrm{GF}^n(q)$ in the following form. A message $\mathbf{m} = (m_0, m_1, ..., m_{k-1})$ with $m_i \in \mathrm{GF}(q)$ is mapped to a degree $k-1$ polynomial (it is called the information polynomial in the indeterminate X):

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

Obviously, $f_{\mathbf{m}}(X)$ is one of the q^k polynomials over $\mathrm{GF}(q)$ 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 $\beta_i \in \mathrm{GF}(p)$:

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

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

or

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

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

$\mathbf{g}_0 = \left(1,\ \varepsilon^{(b+0)\cdot 1},\ \varepsilon^{(b+0)\cdot 2},\ ...,\ \varepsilon^{(b+0)\cdot(n-1)}\right),$

$\mathbf{g}_1 = \left(1,\ \varepsilon^{(b+1)\cdot 1},\ \varepsilon^{(b+1)\cdot 2},\ ...,\ \varepsilon^{(b+1)\cdot(n-1)}\right),$

$\mathbf{g}_2 = \left(1,\ \varepsilon^{(b+2)\cdot 1},\ \varepsilon^{(b+2)\cdot 2},\ ...,\ \varepsilon^{(b+2)\cdot(n-1)}\right),$

... .,

$\mathbf{g}_{k-1} = \left(1, \varepsilon^{(b+k-1)\cdot 1}, \varepsilon^{(b+k-1)\cdot 2}, ..., \varepsilon^{(b+k-1)\cdot(n-1)}\right).$

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 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

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

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 GF(p^m)) we are going to use in the construction of generalized Reed-Solomon codes.

3.1. Reed-Solomon and Bose codes over noncommutative algebras

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 $[\sigma]$

$$a^{[\sigma]}(X):=\begin{cases}a\circ X, & \sigma=0,\\ X\circ a, & \sigma=1\end{cases}\qquad a^{[\sigma_k]}\left(X^k\right):=X^{\sigma}aX^{k-\sigma},\quad \text{for}\quad \sigma^k=0,1,...,k.$$

Now, let

$$f^{[\boldsymbol{\sigma}]}(X)=f^{[(\sigma_0,\sigma_1,...,\sigma_{n-1})]}(X)=\sum_{i=0}^{n-1}a_i^{[\sigma_i]}\left(X^i\right)=\sum_{i=0}^{n-1}X^{\sigma_i}a_iX^{i-\sigma_i},$$

are polynomials with a bunch of keys $\boldsymbol{\sigma}=(\sigma_0,\sigma_1,...,\sigma_{n-1})\in\mathbf{Z}_1\times\mathbf{Z}_2\times...\times\mathbf{Z}_{n-1}\times\mathbf{Z}_n:=\mathsf{Z}_n$. For example,

1) $\sigma_0\in\{0\}=\mathbf{Z}_1$, it is trivial case: $a^{[0]}\left(X^0\right)\equiv a$;

2) $\sigma_1\in\{0,1\}=\mathbf{Z}_2$, in this case we have two variants:

$$a^{[0]}\left(X^1\right)=aX^1,\ a^{[1]}\left(X^1\right)=X^1a;$$

3) $\sigma_2\in\{0,1,2\}=\mathbf{Z}_3$, in this case we have three variants:

$$a^{[0]}\left(X^2\right)=aX^2,\ a^{[1]}\left(X^2\right)=X^1aX^1,\ a^{[2]}\left(X^2\right)=X^2a;$$

4) $\sigma_3\in\{0,1,2,3\}=\mathbf{Z}_4$, for this case we obtain four variants

$$a^{[0]}\left(X^3\right)=aX^3,\ a^{[1]}\left(X^3\right)=X^1aX^2,\ a^{[2]}\left(X^3\right)=X^2aX^1,\ a^{[3]}\left(X^3\right)=X^3a.$$

There are $n!=1\cdot2\cdot3\cdots n$ similar bunch of keys $\boldsymbol{\sigma}=(\sigma_0,\sigma_1,...,\sigma_{n-1})$.

Example 1. For $\boldsymbol{\sigma}=(0,0,...,0)$ and $\boldsymbol{\sigma}=(0,1,2,3,...,n-1)$ we obtain right- and left-side polynomials

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

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

Let

$$Alg_{2^m}^{[\boldsymbol{\sigma}]}(p)[X] = Alg_{2^m}^{[(\sigma_0,\sigma_1,...,\sigma_{n-1})]}(p)[X] :=$$
$$= \left\{ f^{[\boldsymbol{\sigma}]}(X) = \sum_{i=0}^{n-1} a_i^{[\sigma_i]} \left(X^i \right) | \left(\forall a_i \in Alg_{2^m}(p) \right) \& \left(\boldsymbol{\sigma} \in \mathsf{Z}_n \right) \right\},$$

denote the rings of univariate polynomials over $Alg_{2^m}(p)$ with a bunch of keys $\boldsymbol{\sigma} = (\sigma_0, \sigma_1, ..., \sigma_{n-1})$.

Reed-Solomon codes with the bunch of keys $\boldsymbol{\sigma} = (\sigma_0, \sigma_1, ..., \sigma_{n-1})$ are obtained by evaluating certain subspaces of $Alg_{2^m}^{[\boldsymbol{\sigma}]}(p)[X]$ in set of points $D = \{x_0, x_1, ..., x_{n-1}\}$ which are subsets of $Alg_{2^m}(p)$. Specifically, a Reed-Solomon codes $Code\left\{D, k \mid f^{[\boldsymbol{\sigma}]}(X), Alg_{2^m}(p)\right\}$ of length n and dimension k over $Alg_{2^m}(p)$ are defined as follows:

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

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 $\mathbf{s} \in Code\left\{D, k \mid f^{[\boldsymbol{\sigma}]}(X), Alg_{2^m}(p)\right\}$ 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 $\mathbf{v} \in Code\left\{D, k \mid f^{[\boldsymbol{\sigma}]}(X), Alg_{2^m}(p)\right\}$ 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.*,

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

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

$$c_j = f^{[\boldsymbol{\sigma}]}(x_j) = \sum_{i=0}^{k-1} u_i^{[\sigma_i]} x_j^i = \sum_{i=0}^{k-1} x_j^{\sigma_i} \cdot u_i \, x_j^{i-\sigma_i}$$

or in matrix form

$$\begin{bmatrix} c_0 \\ c_1 \\ ... \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} x_0^0 & x_0^1 & ... & x_0^{k-1} \\ x_1^0 & x_1^1 & ... & x_1^{k-1} \\ ... & ... & ... & ... \\ x_{n-1}^0 & x_{n-1}^1 & & x_{n-1}^{k-1} \end{bmatrix} \begin{bmatrix} u_0^{[(\sigma_0,\sigma_1,...,\sigma_{k-1})]} \\ u_1^{[(\sigma_0,\sigma_1,...,\sigma_{k-1})]} \\ ... \\ u_{k-1}^{[(\sigma_0,\sigma_1,...,\sigma_{k-1})]} \end{bmatrix} =$$

$$\begin{bmatrix} x_0^0(\circ) & x_0^{\sigma_1} \cdot (\circ) \cdot x_0^{1-\sigma_1} & ... & x_0^{\sigma_{k-1}} \cdot (\circ) \cdot x_0^{k-\sigma_{k-1}} \\ x_1^0(\circ) & x_1^{\sigma_1} \cdot (\circ) \cdot x_1^{1-\sigma_1} & ... & x_1^{\sigma_{k-1}} \cdot (\circ) \cdot x_1^{k-\sigma_{k-1}} \\ ... & ... & ... & ... \\ x_{n-1}^0(\circ) & x_{n-1}^{\sigma_1} \cdot (\circ) \cdot x_{n-1}^{1-\sigma_1} & ... & x_{n-1}^{\sigma_{k-1}} \cdot (\circ) \cdot x_{n-10}^{k-\sigma_{k-1}} \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ ... \\ u_{k-1} \end{bmatrix}.$$

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. 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

$$c_j = f^{[\sigma]}(x_j)\Big|_{x_j=\varepsilon^{j-1}} = f^{[(\sigma_0,\sigma_1,...,\sigma_{k-1})]}(\varepsilon^{j-1}) = \sum_{i=1}^{k-1} \varepsilon^{\sigma_i(j-1)} \cdot u_i \cdot \varepsilon^{(i-\sigma_i)(j-1)},$$

This has the form of discrete Fourier-Clifford-Galois or Fourier-Caley-Dickson-Galois transforms (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 $\boldsymbol{\sigma} = (0,0,...,0)$ and $\boldsymbol{\sigma} = (0,1,2,3,...,n-1)$ we have right- and left-side transforms

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

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. 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.

5. 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".

6. References

[1] New directions in cryptography / W. Diffie, M.E. Hellman // IEEE Trans. Inform. Theory. – 1976. – Vol. 22. – P. 644-654.

[2] Cao, Z. Conic analog of RSA cryptosystem and some improved RSA cryptosystems / Z. Cao // Journal of Natural Science of Heilongjiang University. – 1999. – Vol. 16(4).

[3] Cao, Z. The multi-dimension RSA and its low exponent security / Z. Cao // Science in China (E Series). – 2000. – Vol. 43(4). – P. 349-354,

[4] Cao, Z. A threshold key escrow scheme based on public key cryptosystem / Z. Cao // Science in China (E Series). – 2001. – Vol. 44(4). – P. 441-448.

[5] Komaya, K. New public-key schemes bases on elliptic curves over the ring Z_n / K. Komaya, U. Maurer, T. Okamoto, S. Vanston // Crypto'91, LNCS 576, Springer-Verlag, 1992. – P. 252-266.

[6] Rabin, M.O. Digitized signatures and public-key functions as intractible as factorization // MIT Laboratory for Computer Science Technical Report, LCS/TR-212, 1979.

[7] Rackoff, C. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack / C. Rackoff, D. Simon // CRYPTO'91, LNCS 576, Springer-Verlag, 1992. – P. 433-444.

[8] Rivest, R.L. A method for obtaining digital signatures and public key cryptosystems / R.L. Rivest, A. Shamir, L. Adleman // Communications of the ACM 21. – 1978. – P. 120-126.

[9] Smith, P. LUC: A new public key system / P. Smith, M. Lennon // Proceedings of the IFIPTC11 Ninth International Conference on Information Security, IFIP/Sec 93. – North-Holland, 1993. – P. 103-117.

[10] Williams, H.C. A Modification of the RSA Public-Key Encryption Procedure / H.C. Williams // IEEE Transactions on Information Theory. – 1980. – Vol. IT-26(6). – P. 726-729.

[11] Williams, H.C. Some public-key crypto-functions as intractable as factorization / H.C. Williams, G.R. Blakley, D. Chaum // CRYPTO'84, LNCS 196. – Springer-Verlag, 1985. – P. 66-70.
[12] Anshel, I. An algebraic method for public-key cryptography / I. Anshel, M. Anshel, D. Goldfeld // Math. Research Letters. – 1999. – Vol. 6. – P. 287-291.
[13] Bohli, J.-M. Towards provable secure group key agreement building on group theory / J.-M. Bohli, B. Glas, R. Steinwandt // Cryptology e-Print Archive: Report 2006/079, 2006.
[14] Dehornoy, P. Braid-based cryptography / P. Dehornoy // Contemporary Mathematics. – 2004. – Vol. 360. – P. 5-33.
[15] Ko, K.H. New Public-Key Cryptosystem Using Braid Groups / K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han // CRYPTO 2000, LNCS 1880. – Springer-Verlag, 2000. – P. 166-183.
[16] Eick, B. Polycyclic groups: a new platform for cryptography / B. Eick, D. Kahrobaei // Preprint arXiv: math.GR/0411077, 2004.
[17] Paeng, S.-H. New public key cryptosystem using finite Non Abelian Groups / S.-H. Paeng, K.-C. Ha, J.-H. Kim, S. Chee, C. Park // CRYPTO 2001, LNCS 2139. – Springer-Verlag, 2001. – P. 470-485.
[18] Thmposon's group and public key cryptography / V. Shpilrain, A. Ushakov // Preprint arXir: math.GR/0505487, 2005.
[19] Reed, I.S. Polynomial Codes Over Certain Finite Fields / I.S. Reed, G. Solomon // SIAM Journal of Applied Math. – 1960. – Vol. – P. 300-304.