Quasigroups and Related Systems **17** (2009), 161 – 176

Secret-sharing schemes and orthogonal systems of k-ary operations

Galina B. Belyavskaya

Abstract. We suggest a general method of the construction of secret-sharing schemes based on orthogonal systems of partial (in particular, everywhere determined) k-ary operations which generalizes some known methods of the construction of such schemes by a finite fields and point the orthogonal systems of k-ary operations respecting to these known schemes. The different transformations of orthogonal systems of k-ary operations are reformulated and applied to orthogonal systems of polynomial k-ary operations over finite fields, in particular, to orthogonal systems corresponding to some known schemes.

1. Introduction

It is known that for receiving the secret information the secret key is used. The problem of construction of secret-sharing schemes is one of tasks of modern cryptography connected with partition of the secret (more exactly, with sharing the secret key). The method of sharing the secret key provides safety of the procedure of acceptance of decision in some critical situation. It consists in definition the group of person which have a right to accept decision. Every member of this group has a part of the secret key, only the full collection of these parts allows to restore the secret key giving access to the secret.

There are many applications for such schemes including communication networks, financial institutions and computing. One of the aspects of a such scheme is a possibility to share responsibility for acceptance of an important decision, concerning application of systems of weapon, signature of bank checks or of access to the bank depository. One example arises in the military where it would be necessary for several high-level officers to

2000 Mathematics Subject Classification: 94A60, 20N05, 20N15, 05B15

Keywords: secret-sharing scheme, k-ary operation, k-ary quasigroup, orthogonal system of partial k-ary operations, transformation of an orthogonal system.

reconstruct the necessary key required to release very important decision.

The problem of construction of a secret-sharing scheme can be generalized when a decision can be accepted not one but any of several distinct groups of users. In this case the secret key is distributed between all members of groups of users and every user obtains his part of the secret.

One of main aims of a such secret-sharing scheme is defence of a key away from loss. It is better to share a key between several users such that the possibility its restoration by a few groups with in advance defined participants, acting in agreement. That eliminates a risk of loss of a key. The possibility of restoration of a secret must appear when all or sufficiently great part of owners of the secret key was joined. But some of keepers of secret key can be absent with respect to different reasons so it need to restoration the secret if an incomplete collection of owners of the secret key but if their number is greater of some threshold value.

Let $1 < k \leqslant n$. A secret-sharing scheme between n users is called (n, k)-*threshold* if any group of k from n users can restore a secret but none group of the smaller number of users cannot obtain an information about the secret key [1].

Secret-sharing schemes were introduced in 1979 by A. Shamir [12]. Later his idea was generalized by other authors, which will be mentioned below. In [13] various secret-sharing schemes known at that time were surveyed.

We suggest a general secret-sharing scheme based on orthogonal systems of partial (in particular, everywhere determined) k-ary operations which generalizes some of the known schemes and find the orthogonal systems of k-ary operations respecting to these known schemes. Some little-known transformations of orthogonal systems of k-ary operations are recalled and are applied to orthogonal systems of polynomial k-ary operations over finite fields $GF(q)$, in particular, to orthogonal systems corresponding to known secret-sharing schemes.

2. Orthogonal systems of partial k-ary operations

At first we recall some necessary definitions and results. By x_i^j we will denote the sequence $x_i, x_{i+1}, \ldots, x_j$, $i \leqslant j$. Let Q be a finite or infinite set, $k \geqslant 2$ be a positive integer, and let Q^k denote the k-th Cartesian power of the set Q.

Let Q be a nonempty set and $D \subseteq Q^k$, $D \neq \emptyset$. If A is a mapping of D into Q, then A is said to be *a partial k-ary operation* (and (Q, A) to be a *partial k-ary groupoid*). If $D = Q^k$, we have a usual k-ary operation (or shortly, k-operation) given on the set Q (see, for example, [14]).

A *k-groupoid* (Q, A) *of order* n is a set Q with one k-ary operation A defined on Q, where $|Q| = n$.

A *k-ary quasigroup* or a *k-quasigroup* is a k-groupoid (Q, A) such that in the equality $A(x_1^k) = x_{k+1}$ each set of values of k elements from x_1^{k+1} uniquely defines the value of the $(k+1)$-th element. Sometimes a quasigroup k-operation A is itself considered as a k-quasigroup.

The k-operation E_i, $1 \leqslant i \leqslant k$, on Q with $E_i(x_1^k) = x_i$ is called the *i-th identity operation* (or the *i-th selector*) *of arity k*.

For $k \geqslant 2$, *an k-dimensional hypercube* (briefly, a *k-hypercube*) *of order* n is an $\underbrace{n \times n \times \cdots \times n}_{k}$ array with n^k points based upon n distinct symbols.

A *k-dimensional permutation cube of order n* [6]) is a k-dimentional $n \times n \times \cdots \times n$ matrix of n elements with the property that every column (that is, every sequence of n elements parallel to an edge of the cube) contains a permutation of the elements. In particular, a two-dimentional permutation cube is simply a latin square of order n which is an $n \times n$ array in which n distinct symbols are arranged so that each symbol occurs once in each row and column [6].

A k-operation (a k-quasigroup) defined on a set Q corresponds to every k-hypercube (to every permutation k-hypercube) with the elements of Q and vice versa (see, for example, [4]).

Definition 1. [14] Let $(Q, A_1), (Q, A_2), \ldots, (Q, A_k)$ be partial k-groupoids with the same domain $D = D(A_1) = D(A_2) = \ldots = D(A_k) \subseteq Q^k$. The k-tuple of k-operations $(A_1^k) = (A_1, A_2, ..., A_k)$ is called *orthogonal* if for every $(a_1, a_2, ..., a_k) \in Q^k$ for which the system $\{A_i(x_1^k) = a_i\}_{i=1}^k$ has a unique solution.

The k-tuple (A_1^k) of partial k-operations with the same domain D is orthogonal if and only if the mapping $(x_1^k) \rightarrow (A_1(x_1^k), A_2(x_1^k), \ldots, A_k(x_1^k))$ is a bijection when $(x_1^k) \in D$.

The set of different partial k-operations of the same domain D is said to be an *orthogonal system of partial k-operations* (a k-OSPO) if each k-tuple of the k-operations of this set is orthogonal [14].

For coding of information it is useful the following

Theorem 1. [14] *To every orthogonal system of k-ary partial operations $\sum = \{A_1, A_2, \ldots, A_t\}$, $t \geqslant k$, in which all partial operations are defined* *on a set of q elements, the set D has p elements and $q < p \leqslant q^k$, there corresponds a code of p t-sequences of code distance $t-(k-1)$ over an alphabet of q letters, $q < p \leqslant q^k$, and vise versa.*

An orthogonal system of k-ary operations (k-OSO) is a partial case of k-OSPOs. Such systems were studied in many works (see, for example, [6, 7]).

A k-OSPO, in particular, a k-OSO can be used for construction of secret-sharing systems in the following way.

Let $\sum = \{A_1, A_2, \dots, A_t\}$ be a k-OSPO of partial k-operations given on a set Q of order q with $\mid D \mid = p$. Choose n, $k < n \leqslant t$, of partial k-operations $A_{i_1} = B_1, A_{i_2} = B_2, \dots, A_{i_n} = B_n$ of $\sum$, some k-tuple $a = (a_0, a_1, \dots, a_{k-1})$ of $D \subseteq Q^k$ and suppose that the element a_0 (or some elements of this k-tuple) is the secret. The k-tuple a we express in coded form as the n-tuple $b = (b_1, b_2, ..., b_n)$, where $b_j = B_j(a_0, a_1, ..., a_{k-1})$. As $\sum$ is a k-OSPO and $a = (a_0, a_1, ..., a_{k-1}) \in D \subseteq Q^k$, any k elements $b_{j_1}, b_{j_2}, ..., b_{j_k}$ of b define uniquely a k-tuple a, as by the definition of a k-OSPO the system $\{B_{j_1}(x_1^k) = b_{j_1}, B_{j_2}(x_1^k) = b_{j_2}, \dots, B_{j_k}(x_1^k) = b_{j_k}\}$ has a unique solution $(x_1, x_2, \dots, x_k) = (a_0, a_1, \dots, a_{k-1})$.

Taking that into account, one can suggest the following *construction of an (n,k)-threshold secret-sharing scheme between n users, any k of which can unlock the secret.*

1. Choose a k-OSPO $\sum = \{A_1, A_2, \dots, A_t\}$ with a great domain D the partial operations of which is given on a set Q of sufficiently great order q.
2. Choose a k-tuple $a = (a_0, a_1, \dots, a_{k-1})$ of D in which the element a_0 (or some elements) is (are) the secret.
3. Choose an n-tuple $(i_1, i_2, \dots, i_n)$ of $\{1, 2, \dots, t\}$, $k \leqslant n \leqslant t$.
4. Calculate the n-tuple $b = (b_1, b_2, \dots, b_n) =$
$(A_{i_1}(a_0^{k-1}), A_{i_2}(a_0^{k-1}), \dots, A_{i_n}(a_0^{k-1})) = (B_1(a_0^{k-1}), B_2(a_0^{k-1}), \dots, B_n(a_0^{k-1}))$.
5. The pairs $(i_1, b_1), (i_2, b_2), \dots, (i_n, b_n)$, which form the secret key, can be separated between n users which are the keepers of the secret.

Using this system any group of k from n users having k pairs $(i_{j_1}, b_{j_1}), \dots, (i_{j_k}, b_{j_k})$ unlocks the secret deciding the system $\{B_{j_1}(x_1^k) = b_{j_1}, B_{j_2}(x_1^k) = b_{j_2}, \dots, B_{j_k}(x_1^k) = b_{j_k}\}$ and none another group of smaller numbers of users cannot to receive an information about the secret.

This system allows to increase a number of keepers of the secret adding l elements $i_{n+1}, i_{n+2}, \ldots, i_{n+l}$, where $n + l \leqslant t$, in point 3.

If there is only one group of the keepers of the secret, then in item 3 we choose $n = k$.

The pointed algorithm is the same when we use an orthogonal system of k-ary operations (a k-OSO) given on a set Q. In this case $D = Q^k$.

As one variation on theme of secret-sharing schemes, we might want a scheme where some participants' share carry more weight than others. In this case we require that a share from participant i can be replaced by a collection of shares from participant of lower weights. Such a system is often called a multilevel scheme. For example, assume that in a bank, one wants to have a valid signature for transfer of a great sum of money only if the shares of two tellers and one vice-president or two vice-presidents are entered.

In such case we can in the suggested scheme to share secret $(i_1, b_1), (i_2, b_2), \ldots, (i_n, b_n)$ between $l < n$ keepers giving more parts of the secret key to the participants with more weight and less parts to the participants with lower weight.

3. Some known secret-sharing schemes

The following connection between k-OSOs and codes is well known.

Theorem 2. [15] *A code of q^k words of length t with the code distance $t - (k - 1)$ in an alphabet from q letters corresponds to every orthogonal system of k-ary operations $\sum = \{A_1, A_2, \ldots, A_t\}$, $t \geqslant k$, defined on a set Q of order q and vice versa.*

It is a partial case of Theorem 1 when $p = q^k$. In this case we have an MDS-code (that is a code with the maximal Hamming distance $n - (k - 1)$ between codewords).

In his book [16] W. W. Wu stated that all the secret-sharing schemes known at the time his book was written are connected with latin squares and provided some constructions of such schemes using orthogonal latin squares. All his examples construct secret-sharing schemes in which only two parts of the secret key are need to unlock the secret. J. Dénes and A. D. Keedwell [7, Chapter 9] made a more general observation that all these schemes can be constructed with the aid of Reed-Solomon codes.

A code of Reed-Solomon over $GF(q)$ is a code with codewords of length $q - 1$. The codes of Reed-Solomon over $GF(q)$ are MDS-codes [7, Ch. 9].

The scheme with the secret $(s_0, s_1, \ldots, s_{k-1})$ due to A. Shamir [12] based on a polynomial $q(x) = s_0+s_1x+\ldots+s_{k-1}x^{k-1}$ modulo p, where p is a prime greater than n and where the polynomial is so chosen that it has distinct values modulo p for n different values $x_1, x_2, \ldots, x_n$ of x. The secret key is the n different ordered pairs of integers $(x_i, q(x_i))$ for $i = 1, 2, \ldots, n$. The polynomial $q(x)$ is calculated by the Lagrange's interpolation formula

$$q(x) = \sum_{i-1}^{k} \frac{q(x_i)(x-x_1)(x-x_2)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_k)}{(x_i-x_1)(x_i-x_2)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_k)}$$

for polynomials where $x_1, x_2, \ldots, x_k$ are any k of n parts of the secret key.

The second scheme of such kind is due to R. J. McEliece and D. V. Sarwarte [11]. In this scheme a Reed-Solomon code over a finite field $GF(q)$ with words of length $q-1$ is defined by the following matrix G:

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_{q-1} \\ a_1^2 & a_2^2 & \cdots & a_{q-1}^2 \\ & \ldots & & \\ a_1^{k-1} & a_2^{k-1} & \cdots & a_{q-1}^{k-1} \end{pmatrix}$$

where $a_0 = 0, a_1 = 1, a_2, \ldots, a_{q-1}$ are the different elements of $GF(q)$ with $q = p^m$ (p is prime) elements. Every k-tuple $s = (s_0, s_1, \ldots, s_{k-1})$ in coded form is the $(q-1)$-tuple $b = (b_1, b_2, \ldots, b_{q-1})$, where $b = sG$. In this case $b_i = q(a_i)$, where $q(x) = s_0 + s_1x + \ldots + s_{k-1}x^{k-1}$, so this method is a generalization of that Shamir. The subset of $n \leqslant (q-1)$ pairs of the set $\{(i, b_i) \mid i = 1, 2, \ldots, q-1\}$, any k of which unlock the secret, can be the secret key.

J. W. Greene, M. E. Hellman and E. D. Karnin used the matrix $\overline{G}$ over a finite field to construct an extended Reed-Solomon code [8]:

$$\overline{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & a_1 & a_2 & \cdots & a_{q-1} \\ 0 & 0 & a_1^2 & a_2^2 & \cdots & a_{q-1}^2 \\ & & & \ldots & & \\ 0 & 1 & a_1^{k-1} & a_2^{k-1} & \cdots & a_{q-1}^{k-1} \end{pmatrix}.$$

Thus, the matrix $\overline{G}$ of *an extended Reed-Solomon code* is the matrix G with two first added columns. The first (the second) column contains the element 1 on the first (on the last) place and the element 0 on the rest places.

According to Theorem 5.1 [7] every extended Reed-Solomon code (and that means the corresponding secret-sharing scheme) with a generating matrix of two rows

$$\begin{pmatrix} 1 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 1 & a_1 & a_2 & \cdots & a_{q-1} \end{pmatrix}$$

which is defined over a field $GF(q)$ can be constructed from a complete set of orthogonal latin squares (binary quasigroups) of order q.

This result can be generalized to the k-ary case. At first we remind that an *i-invertible* k-operation A defined on Q is a k-operation for which the equation $A(a_1^{i-1}, x, a_{i+1}^k) = a_{k+1}$ has a unique solution for each fixed k-tuple $(a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_{k+1})$ of Q^k.

A k-ary quasigroup can be defined as a k-groupoid (Q, A) such that the k-operation A is i-invertible for each $i = 1, 2, \dots, k$.

A k-ary operation $A(x_1^k) = a_1x_1 + a_2x_2 + \ldots + a_kx_k$ over a field $GF(q)$ is i-invertible, if $a_i \neq 0$ and it is a k-quasigroup if and only if all its coefficients are different from 0.

Theorem 3. *Every secret-sharing system corresponding to the extended Reed-Solomon code over a field $GF(q)$ with the matrix $\overline{G}$ is equivalent to the orthogonal system $\sum = \{E_1, E_k, A_1, A_2, \dots, A_{q-1}\}$ of k-operations of order q, where $E_1(x_0^{k-1}) = x_0$, $E_k(x_0^{k-1}) = x_{k-1}$,*

$$A_i(x_0^{k-1}) = x_0 + a_ix_1 + a_i^2x_2 + \ldots + a_i^{k-1}x_{k-1}.$$

All k-operations A_i, $i = 1, 2, \dots, q-1$, are k-quasigroups.

Proof. Let us consider a secret-sharing scheme corresponding to the extended Reed-Solomon code over a field $GF(q)$ with the matrix $\overline{G}$. The determinant formed by any k of the columns of this matrix is nonsingular, so the system of k-operations $\sum = \{E_1, E_k, A_1, A_2, \dots, A_{q-1}\}$ defining by the columns of the matrix $\overline{G}$: $E_1(x_0^{k-1}) = x_0, E_k(x_0^{k-1}) = x_{k-1}$, $A_i(x_0^{k-1}) = x_0 + a_ix_1 + a_i^2x_2 + \ldots + a_i^{k-1}x_{k-1}$, $i = 1, 2, \dots, q-1$, is orthogonal. All k-operations A_i are k-quasigroups as $a_i \neq 0$ for any $i = 1, 2, \dots, q-1$, so a system of permutation k-hypercubes corresponds to these k-quasigroups.

The k-tuple $(s_0, s_1, \dots, s_{k-1})$, including the secret, is coded as

$$(s_0, s_{k-1}, A_1(s_0^{k-1}), A_2(s_0^{k-1}), \dots, A_{q-1}(s_0^{k-1})).$$

Converse is evident since the system $\sum = \{E_1, E_k, A_1, A_2, \dots, A_{q-1}\}$ of k-operations defines the columns of the matrix $\overline{G}$. So this system defines the secret-sharing scheme, corresponding to the extended Reed-Solomon code. □

Note that $A_i(s_0^{k-1}) = q(a_i)$, $i = 1, 2, \dots, q-1$, where $q(x)$ is the polynomial of Shamir over the field $GF(q)$.

It is easy to see that the system $\sum = \{E_1, E_2, A_1, A_2, \dots, A_{q-1}\}$ of orthogonal binary operations, where $E_1(x, y) = x$, $E_2(x, y) = y$, $A_i(x, y) = x + a_i y$, $i = 1, 2, \dots, q-1$, corresponds to the secret-sharing scheme, which respect to the matrix of two rows of Theorem 5.1 [7]. In this case all operations $A_i(x, y)$, $i = 1, 2, \dots, q-1$, are binary quasigroups.

In the case of the matrix G we have the following

Corollary 1. *Every secret-sharing system corresponding to the Reed-Solomon code over a field $GF(q)$ with the matrix G is equivalent to the orthogonal system $\sum = \{A_1, A_2, \dots, A_{q-1}\}$ of k-quasigroups of order q, where $A_i(x_0^{k-1}) = x_0 + a_i x_1 + a_i^2 x_2 + \dots + a_i^{k-1} x_{k-1}$, $i = 1, 2, \dots, q-1$.*

Note that instead of the matrix $\overline{G}$ one can take the matrix over a field $GF(q)$ with a primitive element (that is a generating element of the multiplicative group) a and with the following k-operations (corresponding to the columns of this matrix): $E_1(x_0^{k-1}) = x_0$, $E_k(x_0^{k-1}) = x_{k-1}$, $A_1(x_0^{k-1}) = x_0 + x_1 + \dots + x_{k-1}$, $A_{i+1}(x_0^{k-1}) = x_0 + a^i x_1 + a^{2i} x_2 + \dots + a^{(k-1)i} x_{k-1}$, $i = 1, 2, \dots, q-2$, where k-operations $A_1, A_2, \dots, A_{q-1}$ are k-quasigroups. We may take the matrix with the $q+1$ rows defined by these k-operations.

4. Transformations of orthogonal systems

With the point of view of ciphering of an information it is important to obtain many orthogonal systems from one system. In the connect with that we recall some transformations of orthogonal systems of k-operations known in the algebraic theory of orthogonal systems of k-operations with some additions.

At first we reremind some necessary information from [2] with respect to k-OSOs (for the case $k = 2$ see [3]).

Let $(A_1, A_2, \dots, A_k) = (A_1^k)$ be a k-tuple of k-operations defined on a set Q. This k-tuple defines the unique mapping $\bar{\theta} : Q^k \to Q^k$ in the following way: $\bar{\theta} : (x_1^k) \to (A_1(x_1^k), A_2(x_1^k), \dots, A_k(x_1^k))$, (or briefly, $\bar{\theta} : (x_1^k) \to (A_1^k)(x_1^k))$.

Conversely, any mapping Q^k into Q^k uniquely defines a k-tuple (A_1^k) of k-operations on Q: if $\bar{\theta}(x_1^k) = (y_1^k)$, then we define $A_i(x_1^k) = y_i$ for all $i = 1, 2, \ldots, k$ (or shortly, $i \in \overline{1,k}$). Thus, we obtain $\bar{\theta} = (A_1^k)$, where $\bar{\theta}(x_1^k) = (A_1^k)(x_1^k) = (A_1^k(x_1^k))$. If C is a k-operation on Q and $\bar{\theta}$ is a mapping Q^k into Q^k, then the operation $C\bar{\theta}$ defined by the equality $C\bar{\theta}(x_1^k) = C(\bar{\theta}(x_1^k))$ is also a k-operation. Let $C\bar{\theta} = D$ and $\bar{\theta} = (A_1^k)$, then $D(x_1^k) = C(A_1^k(x_1^k))$ or briefly, $D = C(A_1^k)$. If $\bar{\theta} = (B_1^k)$ and $\bar{\varphi} = (A_1^k)$ are mappings Q^k into Q^k, then $\bar{\varphi}\bar{\theta} = (A_1^k)\bar{\theta} = (A_1\bar{\theta}, A_2\bar{\theta}, \ldots, A_k\bar{\theta}) = ((A_i\bar{\theta})_{i=1}^k = (A_i(B_1^k))_{i=1}^k$.

If $\bar{\theta} = (B_1^k)$ is a permutation of Q^k, then $B_i = E_i\bar{\theta}$ and $B_i\bar{\theta}^{-1} = B_i(B_1^k)^{-1} = E_i, \ i \in \overline{1,k}$.

Definition 2. [2] A k-tuple (A_1^k) of different k-operations on Q is called *orthogonal* if the system $\{A_i(x_1^k) = a_i\}_{i=1}^k$ has a unique solution for all $(a_1^k) \in Q^k$.

The k-tuple (E_1^k) of the selectors of arity k is the identity permutation of Q^k and is orthogonal.

There is a close connection between orthogonal k-tuples of k-operations on Q and permutations of Q^k (such permutations will be called *k-permutations*).

Proposition 1. [2] *A k-tuple (A_1^k) of k-operations is orthogonal if and only if the mapping $\bar{\theta} = (A_1^k)$ is a permutation of Q^k.*

In [2] it was introduced the notion of a strongly orthogonal system of k-operations.

Definition 3. [2] A system $\Sigma = \{A_1, A_2, \ldots, A_t\} = \{A_1^t\}$, $t \geqslant 1$, of k-operations, given on a set Q, is called *strongly orthogonal* if the system $\overline{\Sigma} = \{E_1^k, A_1^t\}$ is orthogonal.

In this case all k-operations of Σ are k-quasigroups since an i-invertible k-operation A defined on Q is i-invertible if and only if the mapping $(E_1, E_2, \ldots, E_{i-1}, A, E_{i+1}, \ldots, E_k)$ is a permutation of Q^k.

The system $\overline{\Sigma}$ is called the *orthogonal system of k-quasigroups* (k-OSQs).

A k-operation A is a k-quasigroup if and only if the set $\Sigma = \{A\}$ is strongly orthogonal. A set $\Sigma = \{A_1^t\}$ of k-quasigroups when $k > 2$, $t \geqslant k$, can be orthogonal but not strongly orthogonal in contrast to the binary case [2].

Note that in the case of a strongly orthogonal set $\Sigma = \{A_1, A_2, \ldots, A_t\} = \{A_1^t\}$ of k-operations the number t of k-operations in Σ can be less than arity k.

According to [2] if $\sum$ is a k-OSO given on a set Q, then $\sum' = \sum\overline{\theta} = \{A_1\overline{\theta}, A_2\overline{\theta}, \ldots, A_t\overline{\theta}\}$, where $\overline{\theta}$ is a permutation of Q^k, is also a k-OSO.

Two k-OSO $\sum$ and $\sum'$ given on a set Q are *conjugate* if there exists a permutation $\overline{\theta}$ of Q^k such that $\sum' = \sum\overline{\theta}$. They are called *parastrophic* if $\sum' = \sum\overline{\theta}^{-1}$ where $\overline{\theta} = (A_{i_1}, A_{i_2}, \ldots, A_{i_k})$, $A_{i_j} \in \sum$ for any $j \in \overline{1,k}$. In this case $\sum' = \sum\overline{\theta}^{-1} = \{E_1, E_2, \ldots, E_k, A_i\overline{\theta}^{-1} | i \in \overline{1,t}, i \neq i_j, j \in \overline{1,k}\}$.

By Theorem 1 of [2] every k-OSO is conjugate to a k-OSQ and by Lemma 3 of [2] two k-OSQs are conjugate if and only if they are parastrophic.

In [2] the transformation of isostrophy of k-OSOs described below (for $k = 2$ see [3]) which is more general than conjugation was also considered.

Let $\sum = \{A_1^t\}$ be a k-OSO given on a set Q, $T = (\alpha_1, \alpha_2, \ldots, \alpha_t)$ be a system of permutations of Q. The transformation $\sum \to \sum'$ where $\sum' = \{\alpha_1 A_1, \alpha_2 A_2, \ldots, \alpha_t A_t\}$, $A_i \in \sum$ is called *isotopy* of k-OSOs and denoted by $\sum' = \sum^T$.

Remark 1. Note that if a k-OSO $\sum = \{A_1^t\}$ is strongly orthogonal and $T = (\alpha_1, \alpha_2, \ldots, \alpha_{t+k})$, then $\overline{\sum}^T = \{\alpha_1 E_1, \alpha_2 E_2, \ldots, \alpha_k E_k, B_1, B_2, \ldots, B_t\}$ where $B_j = \alpha_{k+j} A_j$, $j \in \overline{1,t}$, are k-quasigroups.

It is true [2] that $(\sum\overline{\theta})^T = (\sum^T)\overline{\theta}$, i.e., if $B_i \in \sum' = (\sum\overline{\theta})^T$, $i \in \overline{1,t}$, then

$$B_i(x_1^k) = (\alpha_i(A_i\overline{\theta}))(x_1^k) = (\alpha_i A_i)\overline{\theta}(x_1^k). \tag{1}$$

The transformation $\sum \to (\sum\overline{\theta})^T = \sum'$ is called in [2] *isostrophy*.

The system $\sum'$ is also orthogonal. Indeed, any k-tuple with different k-operations of $\sum'$ defines a permutation of Q^k: $(B_{i_1}, B_{i_2}, \ldots, B_{i_k}) = ((\alpha_{i_1} A_{i_1})\overline{\theta}, (\alpha_{i_2} A_{i_2})\overline{\theta}, \ldots, (\alpha_{i_k} A_{i_k})\overline{\theta}) = (\alpha_{i_1} E_1, \alpha_{i_2} E_2, \ldots, \alpha_{i_k} E_k)(A_{i_1}, A_{i_2}, \ldots, A_{i_k})\overline{\theta}$. Thus, this k-tuple is the product of three permutations of Q^k, so it is orthogonal.

In addition, we consider the following case of the transformation of isostrophy of a k-OSO, namely, $\sum' = (\sum\overline{\theta}_1)^T$, where $\overline{\theta}_1 = \overline{\theta}\,\overline{\theta}_0$, $\overline{\theta}_0 = (\beta_1 E_1, \beta_2 E_2, \ldots, \beta_k E_k)$, $\beta_1, \beta_2, \ldots, \beta_k$ are permutations of Q, that is $\overline{\theta}_0(x_1^k) = (\beta_1 E_1, \beta_2 E_2, \ldots, \beta_k E_k)(x_1^k) = (\beta_1 x_1, \beta_2 x_2, \ldots, \beta_k x_k)$.

In this case, if $B_i \in \sum'$, then

$$B_i(x_1^k) = (\alpha_i A_i)\overline{\theta}_1(x_1^k) = (\alpha_i A_i)\overline{\theta}\,\overline{\theta}_0(x_1^k) = ((\alpha_i A_i)\overline{\theta})\overline{\theta}_0(x_1^k). \tag{2}$$

Let $\overline{\theta} = (C_1, C_2, \ldots, C_k)$, then (2) can be written as

$$B_i(x_1^k) = \alpha_i A_i(C_1(\beta_j x_j)_{j=1}^k, C_2(\beta_j x_j)_{j=1}^k, \ldots, C_k(\beta_j x_j)_{j=1}^k), \tag{3}$$

where $(\beta_j x_j)_{j=1}^k = (\beta_1 x_1, \beta_2 x_2, \ldots, \beta_k x_k)$.

Transformation (3) of a known k-OSO $\sum = \{A_1^t\}$ is realized with the help of a tuple of permutations α_i, $i \in \overline{1,t}$, some known orthogonal k-tuple of k-operations $(C_1, C_2, \ldots, C_k) = \overline{\theta}$ and k permutations β_j, $j \in \overline{1,k}$, of Q.

Remark 2. The transformation (3) can be represented by conjugations and isotopy of k-operations. Remind that two k-operations (Q, A) and (Q, B) are *isotopic* if there exists a $(k+1)$-tuple $T = (\beta_1, \beta_2, \ldots, \beta_k, \alpha)$ of permutations of Q such that $\alpha B(x_1^k) = A(\beta_1 x_1, \beta_2 x_2, \ldots, \beta_k x_k)$ for any $x_1^k \in Q^k$ or, shortly, $B = A^T$. Any k-operation isotopic to a k-quasigroup is a k-quasigroup. Using isotopic k-operations transformation (2) can be written as $\sum' = \{B_1, B_2, \ldots, B_t\} = \{(A_1\overline{\theta})^{T_1}, (A_2\overline{\theta})^{T_2}, \ldots, (A_t\overline{\theta})^{T_t}\} = \{\alpha_1(A_1\overline{\theta})^{T_0}, \alpha_2(A_2\overline{\theta})^{T_0}, \ldots, \alpha_t(A_t\overline{\theta})^{T_0}\}$, where $T_i = (\beta_1, \beta_2, \ldots, \beta_k, \alpha_i^{-1})$, α_i, $i \in \overline{1,t}$, β_j, $j \in \overline{1,k}$, are permutations of Q, $T_0 = (\beta_1, \beta_2, \ldots, \beta_k, 1)$ (1 is the identity permutation of Q).

If $Q(A)$ is a k-quasigroup, then the system $\sum = \{E_1, E_2, \ldots, E_k, A\}$ is orthogonal and $\bar{\theta} = (E_2, \ldots, E_k, A)$ is a k-permutation of Q^k.

By Proposition 3 of [9] the systems

$\sum \bar{\theta} = \{E_2, E_3, \ldots, E_k, A, A\bar{\theta}\}$, $\sum \bar{\theta}^2 = \{E_3, E_4, \ldots, E_k, A, A\bar{\theta}, A\bar{\theta}^2\}, \ldots,$
$\sum \bar{\theta}^k = \{A, A\bar{\theta}, A\bar{\theta}^2, \ldots, A\bar{\theta}^k\}$ and $\sum \bar{\theta}^s = \{A\bar{\theta}^{s-k}, A\bar{\theta}^{s-k-1}, \ldots, A\bar{\theta}^s\}$

are orthogonal for every $s \geqslant k+1$. Each of these systems contains $k+1$ operations, any k of which define a k-permutation of Q^k.

The transformation of isotopy, conjugation or isostrophy of a k-OSO $\sum$, described above, corresponds to the transformation of the secret-sharing scheme, based on the k-OSO $\sum$, which it is possible to call the transformation of isotopy, conjugation or isostrophy of the secret-sharing scheme respectively.

5. Transformations of orthogonal systems

Consider transformations of k-OSOs which consist *polynomial k-operations*, i.e., k-operations of the form

$$A(x_1^k) = a_1x_1 + a_2x_2 + \ldots + a_kx_k$$

over a field $GF(q)$. Any selector E_i of arity k can be considered as a polynomial k-operation: $E_i(x_1^k) = a_1x_1 + a_2x_2 + \ldots + a_ix_i + \ldots + a_kx_k$ where $a_i = 1, a_j = 0, i, j \in \overline{1,k}$, $j \neq i$.

Let $\Sigma = \{A_1, A_2, \ldots, A_t\}$, $k \geqslant 2$, $t \geqslant k$, be a set of k-operations each of which is a polynomial k-operation over a field $GF(q)$, that is

$$\begin{array}{c} A_1(x_1^k) = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1k}x_k, \\ A_2(x_1^k) = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2k}x_k, \\ \ldots \\ A_t(x_1^k) = a_{t1}x_1 + a_{t2}x_2 + \ldots + a_{tk}x_k. \end{array} \tag{4}$$

Let $\overline{A}$ be the matrix $t \times k$ defined by (4). The system $\sum = \{A_1^t\}$, $k \geqslant 2$, $t \geqslant k$, of polynomial k-operations from (4) is orthogonal if and only if all k-minors of the matrix $\overline{A}$, defined by these k-operations, are different from 0 (Proposition 1 of [5]).

Consider the transformations of isotopy, conjugation and isostrophy of k-OSOs which consist of polynomial k-operations over a finite field $GF(q)$, in particular, when the k-OSOs are defined by the columns of the matrix G or $\overline{G}$.

Denote by $\sum_{\overline{A}}$, $\sum_G$ and $\sum_{\overline{G}}$ the k-OSOs of polynomial k-operations defined by (4), by the columns of the matrix G and by the columns of the matrix $\overline{G}$ respectively. In the following statements the definitions of corresponding transformations of these k-OSOs described in the previous item (which give new k-OSOs) are applied for the polynomial k-operations.

We will consider only these k-OSOs over a field $GF(q)$ which contain t k-operations $A_1, A_2, \ldots, A_t$.

Proposition 2. *Let $B_i \in \sum_{\overline{A}}^T$, where $T = (\alpha_1, \alpha_2, \ldots, \alpha_t)$, α_i is a permutation of a set Q for $i \in \overline{1,t}$, then*

$$B_i(x_1^k) = \alpha_i(a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{ik}x_k), \quad i \in \overline{1,t}.$$

Indeed, $B_i(x_1^k) = \alpha_i A_i(x_1^k) = \alpha_i(a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{ik}x_k)$, $i \in \overline{1,t}$.

For the polynomial k-operations defined by the matrix G or $\overline{G}$ we have

Corollary 2. *If $B_i \in \sum_G^T$, $T = (\alpha_1, \alpha_2, \ldots, \alpha_{q-1})$, then $B_i(x_0^{k-1}) = \alpha_i(x_0 + a_ix_1 + a_i^2x_2 + \ldots + a_i^{k-1}x_{k-1})$, $i \in \overline{1, q-1}$, and $B_1 = \alpha_1 E_1$, $B_2 = \alpha_2 E_k$, $B_i(x_0^{k-1}) = \alpha_i(x_0 + a_ix_1 + a_i^2x_2 + \ldots + a_i^{k-1}x_{k-1})$, $i \in \overline{3, q+1}$, if $B_i \in \sum_{\overline{G}}^T$.*

Proposition 3. *Let $B_i \in \sum_{\overline{A}} \overline{\theta}$, where $\overline{\theta} = (C_1, C_2, \ldots, C_k)$, then*

$$B_i(x_1^k) = a_{i1}C_1(x_1^k) + a_{i2}C_2(x_1^k) + \ldots + a_{ik}C_k(x_1^k), \quad i \in \overline{1,t}.$$

Indeed, $B_i(x_1^k) = A_i\overline{\theta}(x_1^k) = a_{i1}C_1(x_1^k) + a_{i2}C_2(x_1^k) + \ldots + a_{ik}C_k(x_1^k)$ for all $i \in \overline{1,t}$.

Corollary 3. *If* $B_i \in \sum_G \overline{\theta}$, *where* $\overline{\theta} = (C_1, C_2, \ldots, C_k)$, *then* $B_i(x_0^{k-1}) = C_1(x_0^{k-1}) + a_i C_2(x_0^{k-1}) + a_i^2 C_3(x_0^{k-1}) + \ldots + a_i^{k-1} C_k(x_0^{k-1})$, $i \in \overline{1, q-1}$. *The* k*-operations of* $\sum_{\overline{G}} \overline{\theta}$ *have the form:* $B_1 = C_1$, $B_2 = C_k$, $B_i(x_0^{k-1}) = C_1(x_0^{k-1}) + a_i C_2(x_0^{k-1}) + a_i^2 C_3(x_0^{k-1}) \ldots + a_i^{k-1} C_k(x_0^{k-1})$, $i \in \overline{3, q+1}$.

Indeed, $B_1 = E_1 \overline{\theta} = C_1$, $B_2 = E_k \overline{\theta} = C_k$ by the definition.

Corollary 4. *Let* A_{i_0} *be a* k*-operation from* $\sum_G$ *(from* $\sum_{\overline{G}}$, $A_{i_0} \neq E_1, E_k$*)*, $\overline{\theta} = (E_1, E_2, \ldots, E_{k-1}, A_{i_0})$. *If* $B_i \in \sum_G \overline{\theta}$, $i \in \overline{1, q-1}$, $i \neq i_0$, *then* $B_i(x_0^{k-1}) = (1 + a_i^{k-1}) x_0 + (a_i + a_i^{k-1} a_{i_0}) x_1 + \ldots + (a_i^{k-2} + a_i^{k-1} a_{i_0}^{k-2}) x_{k-2} + a_i^{k-1} a_{i_0}^{k-1} x_{k-1}$ *and* $B_{i_0}(x_0^{k-1}) = (1 + a_{i_0}^{k-1}) x_0 + a_{i_0}(1 + a_{i_0}^{k-1}) x_1 + \ldots + a_{i_0}^{k-2}(1 + a_{i_0}^{k-1}) x_{k-2} + a_{i_0}^{2k-2} x_{k-1}$. *If* $B_i \in \sum_{\overline{G}} \overline{\theta}$, *then* $B_1 = E_1$, $B_2 = A_{i_0}$ *and* B_i, $i \in \overline{3, q+1}$, *have the same form as above.*

Proof. $\overline{\theta} = (E_1, E_2, \ldots, E_{k-1}, A_{i_0})$ is a k-permutation, A_{i_0} is a k-quasigroup, so by Corollary 3 $B_i(x_0^{k-1}) = E_1(x_0^{k-1}) + a_i E_2(x_0^{k-1}) + a_i^2 E_3(x_0^{k-1}) + \ldots + a_i^{k-2} E_{k-1}(x_0^{k-1}) + a_i^{k-1} A_{i_0}(x_0^{k-1}) = x_0 + a_i x_1 + a_i^2 x_2 + \ldots + a_i^{k-2} x_{k-2} + a_i^{k-1}(x_0 + a_{i_0} x_1 + \ldots + a_{i_0}^{k-1} x_{k-1}) = (1 + a_i^{k-1}) x_0 + (a_i + a_i^{k-1} a_{i_0}) x_1 + \ldots + (a_i^{k-2} + a_i^{k-1} a_{i_0}^{k-2}) x_{k-2} + a_i^{k-1} a_{i_0}^{k-1} x_{k-1}$, $i \in \overline{1, q-1}$, if $B_i \in \sum_G \overline{\theta}$. For $i = i_0$ we obtain B_{i_0}.

When $B_i \in \sum_{\overline{G}} \overline{\theta}$, then $B_1 = E_1(E_1, E_2, \ldots, E_{k-1}, A_{i_0}) = E_1$, $B_2 = E_k(E_1, E_2, \ldots, E_{k-1}, A_{i_0}) = A_{i_0}$. The rest k-operations has the form as in the first part of the corollary. □

Note that the transformation of Corollary 4 corresponds to the following transformation of the matrix G (or $\overline{G}$): the last row (that is the k-th row) multiplied by $a_{i_0}^{j-1}$ is added to the j-th row, $j = 1, 2, \ldots, k-1$, the last row is multiplied by $a_{i_0}^{k-1}$ (assume $a_{i_0}^0 = 1$). The k-operation B_i is defined by the i-th column of the obtained matrix.

Let $\overline{\theta} = (E_1, E_2, \ldots, E_{k-1}, A)$, where the k-operation A is k-invertible. In this case $\overline{\theta}$ is a k-permutation and $\overline{\theta}^{-1} = (E_1, E_2, \ldots, E_{k-1}, {}^{(k)}A)$, where ${}^{(k)}A$ is the k-operation such that $A(x_1, x_2, \ldots, x_{k-1}, {}^{(k)}A(x_1^k)) = E_k(x_1^k) = x_k$. If A is a polynomial k-operation, that is $A(x_1^k) = a_1 x_1 + a_2 x_2 + \ldots + a_k x_k$, where $a_k \neq 0$, then ${}^{(k)}A(x_1^k) = a_k^{-1}(-a_1 x_1 - a_2 x_2 - \ldots - a_{k-1} x_{k-1} + x_k)$.

Corollary 5. *Let* $A_{i_0} \in \sum_G$, $B_i \in \sum_G \overline{\theta}^{-1}$, $\overline{\theta} = (E_1, E_2, \ldots, E_{k-1}, A_{i_0})$. *Then* $B_i(x_0^{k-1}) = (1 - a_i^{k-1}(a_{i_0}^{k-1})^{-1}) x_0 + a_i(1 - a_i^{k-2}(a_{i_0}^{k-2})^{-1}) x_1 + \ldots + a_i^{k-2}(1 - a_i(a_{i_0})^{-1}) x_{k-2} + a_i^{k-1}(a_{i_0}^{k-1})^{-1} x_{k-1}$, *if* $i \in \overline{1, q-1}$, $i \neq i_{i_0}$ *and* $B_{i_0} = E_k$. *All* B_i *for* $i \neq i_0$ *are polynomial* k*-quasigroups.*

Proof. If $A_{i_0} \in \sum_G$, then A_{i_0} is a k-quasigroup and ${}^{(k)}A_{i_0}(x_0^{k-1}) = (a_{i_0}^{k-1})^{-1} (-x_0 - a_{i_0}x_1 - \ldots - a_{i_0}^{k-2}x_{k-2} + x_{k-1})$, so $B_i(x_0^{k-1}) = A_i\overline{\theta}^{-1}(x_0^{k-1}) = E_1(x_0^{k-1}) + a_iE_2(x_0^{k-1}) + a_i^2E_3(x_0^{k-1}) + ... + a_i^{k-2}E_{k-1}(x_0^{k-1}) + a_i^{k-1}\, {}^{(k)}A_{i_0}(x_0^{k-1}) = x_0 + a_ix_1 + a_i^2x_2 + \ldots + a_i^{k-2}x_{k-2} + a_i^{k-1}(a_{i_0}^{k-1})^{-1}(-x_0 - a_{i_0}x_1 - \ldots - a_{i_0}^{k-2}x_{k-2} + x_{k-1}) = (1 - a_i^{k-1}(a_{i_0}^{k-1})^{-1})x_0 + (a_i - a_i^{k-1}(a_{i_0}^{k-1})^{-1}a_{i_0})x_1 + \ldots + (a_i^{k-2} - a_i^{k-1}(a_{i_0}^{k-1})^{-1}a_{i_0}^{k-2})x_{k-2} + a_i^{k-1}(a_{i_0}^{k-1})^{-1}x_{k-1} = (1 - a_i^{k-1}(a_{i_0}^{k-1})^{-1})x_0 + (a_i - a_i^{k-1}(a_{i_0}^{k-2})^{-1})x_1 + \ldots + (a_i^{k-2} - a_i^{k-1}(a_{i_0})^{-1})x_{k-2} + a_i^{k-1}(a_{i_0}^{k-1})^{-1}x_{k-1} = (1 - a_i^{k-1}(a_{i_0}^{k-1})^{-1})x_0 + a_i(1 - a_i^{k-2}(a_{i_0}^{k-2})^{-1})x_1 + \ldots + a_i^{k-2}(1 - a_i(a_{i_0})^{-1})x_{k-2} + a_i^{k-1}(a_{i_0}^{k-1})^{-1}x_{k-1}$, $i \in \overline{1, q-1}$, if $B_i \in \sum_G \overline{\theta}^{-1}$. From this expression it follows that $B_{i_0} = E_k$ and all k-operations B_i, $i \neq i_0$, are polynomial k-quasigroups since all coefficients are different from 0. □

Proposition 4. *If in Proposition* 3 $\overline{\theta} = (A_{i_1}, A_{i_2}, \ldots, A_{i_k})$, $A_{i_l} \in \sum_{\overline{A}}$, $l \in \overline{1,k}$, $\overline{\theta}^{-1} = (D_1, D_2, \ldots, D_k)$, *then* $\sum_{\overline{A}}\overline{\theta}^{-1}$ *is a k-OSQ and* $B_{i_l} = E_l$, $l \in \overline{1,k}$, $B_i(x_1^k) = a_{i1}D_1(x_1^k) + a_{i2}D_2(x_1^k) + \ldots + a_{ik}D_k(x_1^k)$, $i \in \overline{1,t}$, $i \neq i_l$, $l \in \overline{1,k}$, *if* $B_i \in \sum_{\overline{A}}\overline{\theta}^{-1}$.

Proof. If $i \in \overline{1,t}$, $i \neq i_1, i_2, \ldots, i_k$, then $B_i = A_i(D_1, D_2, \ldots, D_k)$. But $A_{i_l} = E_l\overline{\theta}$ and $A_{i_l}\overline{\theta}^{-1} = E_l$, so $B_{i_l} = A_{i_l}\overline{\theta}^{-1} = E_l$ and the system $\sum_{\overline{A}}\overline{\theta}^{-1} = \{E_1, E_2, \ldots, E_k, B_i | i \in \overline{1,t}, i \neq i_1, i_2, \ldots, i_k\}$ is an orthogonal system of k-quasigroups (k-OSQ). □

Let $\sum \to (\sum \overline{\theta}\,\overline{\theta}_0)^T = (\sum \overline{\theta})^T\overline{\theta}_0$. Then, using (3), we obtain

Proposition 5. *Assume that* $B_i \in (\sum_{\overline{A}}\overline{\theta})^T\overline{\theta}_0$, *where* $\overline{\theta} = (C_1, C_2, \ldots, C_k)$, $\overline{\theta}_0 = (\beta_1E_1, \beta_2E_2, \ldots, \beta_kE_k)$ *and* $T = (\alpha_1, \alpha_2, \ldots, \alpha_t)$, *then* $B_i(x_1^k) = \alpha_i(a_{i1}C_1(\beta_jx_j)_{j=1}^k + a_{i2}C_2(\beta_jx_j)_{j=1}^k + \ldots + a_{ik}C_k(\beta_jx_j)_{j=1}^k)$, $i \in \overline{1,t}$.

Indeed, according to (3) $B_i(x_1^k) = \alpha_iA_i(C_1(\beta_jx_j)_{j=1}^k, C_2(\beta_jx_j)_{j=1}^k, \ldots, C_k(\beta_jx_j)_{j=1}^k) = \alpha_i(a_{i1}C_1(\beta_jx_j)_{j=1}^k + a_{i2}C_2(\beta_jx_j)_{j=1}^k + \ldots + a_{ik}C_k(\beta_jx_j)_{j=1}^k)$, $i \in \overline{1,t}$.

Corollary 6. *If* $B_i \in (\sum_G \overline{\theta})^T\overline{\theta}_0$, $\overline{\theta} = (C_1, C_2, \ldots, C_k)$, $\overline{\theta}_0 = (\beta_0E_1, \beta_1E_2, \ldots, \beta_{k-1}E_k)$, *then* $B_i(x_0^{k-1}) = \alpha_i(C_1(\beta_jx_j)_{j=0}^{k-1} + a_iC_2(\beta_jx_j)_{j=0}^{k-1} + \ldots + a_i^{k-1}C_k(\beta_jx_j)_{j=0}^{k-1})$, $i \in \overline{1, q-1}$. *If* $B_i \in (\sum_{\overline{G}}\overline{\theta})^T\overline{\theta}_0$, *then* $B_1(x_0^{k-1}) = \alpha_1C_1(\beta_jx_j)_{j=0}^{k-1}$, $B_2(x_0^{k-1}) = \alpha_2C_k(\beta_jx_j)_{j=0}^{k-1}$, $B_i(x_0^{k-1}) = \alpha_i(C_1(\beta_jx_j)_{j=0}^{k-1} + a_iC_2(\beta_jx_j)_{j=0}^{k-1} + \ldots + a_i^{k-1}C_k(\beta_jx_j)_{j=0}^{k-1})$, $i \in \overline{3, q+1}$.

Indeed, if $B_i \in (\sum_{\overline{G}}\overline{\theta})^T\overline{\theta}_0$, then

$$B_1(x_0^{k-1}) = \alpha_1E_1(C_1, C_2, \ldots, C_k)(\beta_jx_j)_{j=0}^{k-1} = \alpha_1C_1(\beta_jx_j)_{j=0}^{k-1},$$

$$B_2(x_0^{k-1}) = \alpha_2 E_k(C_1, C_2, \ldots, C_k)(\beta_j x_j)_{j=0}^{k-1} = \alpha_2 C_k(\beta_j x_j)_{j=0}^{k-1}.$$

Now let $\sum \to (\sum \overline{\theta}^{-1}\overline{\theta}_0)^T = (\sum \overline{\theta}^{-1})^T \overline{\theta}_0$ (see (1)).

Proposition 6. *If $B_i \in (\sum_{\overline{A}} \overline{\theta}^{-1})^T \overline{\theta}_0$, where $\overline{\theta} = (A_{i_1}, A_{i_2}, \ldots, A_{i_k})$,$A_{i_l} \in \sum_{\overline{A}}$, $l \in \overline{1,k}$, $\overline{\theta}^{-1} = (D_1, D_2, \ldots, D_k)$, $\overline{\theta}_0 = (\beta_1 E_1, \beta_2 E_2, \ldots, \beta_k E_k)$, then $B_{i_l} = \alpha_{i_l}\beta_l E_l$, $l \in \overline{1,k}$, $B_i(x_1^k) = \alpha_i(a_{i1}D_1(\beta_j x_j)_{j=1}^k + a_{i2}D_2(\beta_j x_j)_{j=1}^k + \ldots + a_{ik}D_k(\beta_j x_j)_{j=1}^k)$, $i \in \overline{1,t}$, $i \neq i_1, i_2, \ldots, i_k$, where B_i, $i \neq i_1, i_2, \ldots, i_k$, are k-quasigroups.*

This proposition is a consequence of Proposition 4, Proposition 5 and Remark 1 since
$B_{i_l}(x_1^k) = (\alpha_{i_l} A_{i_l} \overline{\theta}^{-1})\overline{\theta}_0(x_1^k) = (\alpha_{i_l} E_l)\overline{\theta}_0(x_1^k) = \alpha_{i_l} E_l(\beta_j x_j)_{j=1}^k = \alpha_{i_l}\beta_l E_l(x_1^k)$, $l \in \overline{1,k}$.

Corollary 7. *If $\sum_{\overline{G}} = \{E_1, E_k, A_1, A_2, \ldots, A_{q-1}\} = \{P_1, P_2, \ldots, P_{q+1}\}$, $\overline{\theta} = (P_{i_1}, P_{i_2}, \ldots, P_{i_k})$, $i_1, i_2, \ldots, i_k \in \overline{1, q+1}$, $\overline{\theta}^{-1} = (D_1, D_2, \ldots, D_k)$, $\overline{\theta}_0 = (\beta_0 E_1, \beta_1 E_2, \ldots, \beta_{k-1} E_k)$, $B_i \in (\sum_{\overline{G}} \overline{\theta}^{-1})^T \overline{\theta}_0$, then $B_{i_l} = \alpha_{i_l}\beta_{l-1} E_l$, $l \in \overline{1,k}$, $B_i(x_0^{k-1}) = \alpha_i(D_1(\beta_j x_j)_{j=0}^{k-1} + a_i D_2(\beta_j x_j)_{j=0}^{k-1} + \ldots + a_i^{k-1} D_k(\beta_j x_j)_{j=0}^{k-1})$, $i \in \overline{1, q+1}$, $i \neq i_1, i_2, \ldots, i_k$. All B_i, $i \neq i_1, i_2, \ldots, i_k$, are k-quasigroups.*

Indeed, in this case $B_{i_l}(x_0^{k-1}) = (\alpha_{i_l} P_{i_l} \overline{\theta}^{-1})\overline{\theta}_0(x_0^{k-1}) = (\alpha_{i_l} E_l)\overline{\theta}_0(x_0^{k-1}) = \alpha_{i_l} E_l(\beta_j x_j)_{j=0}^{k-1} = \alpha_{i_l}\beta_{l-1} E_l(x_0^{k-1})$, $l \in \overline{1,k}$. The rest k-operations are k-quasigroups by Remark 1.

If $\overline{\theta}^{-1} = (D_1, D_2, \ldots, D_k)$, then the k-operations B_i of $(\sum_G \overline{\theta}^{-1})^T \overline{\theta}_0$, $i \in \overline{1, q-1}$, where $\sum_G = \{A_1, A_2, \ldots, A_t\}$, $\overline{\theta} = (A_{i_1}, A_{i_2}, \ldots, A_{i_k})$, $A_{i_l} \in \sum_G$, $l \in \overline{1,k}$, have the same form as in Corollary 7.

The transformations of k-OSOs, given above, allow to construct new secret-sharing schemes or to renew (to renovate secret keys) the known secret-sharing schemes, in particular, based on a Reed-Solomon or an extended Reed-Solomon code in the pointed numerous ways.

Acknowledgements. The research in this article was made in part by support of the Russian Fond of Fundamental Research (Grant 08.820.08.08 RFFI).

References

[1] **A. P. Alferov, A. Yu. Zubov, A. S. Kuz'min, F. V. Cheremushkin**, *Foundations of cryptography*, (Russian), Gelios ARV, 2005.

[2] **A. S. Bektenov and T. Yakubov**, *Systems of orthogonal n-ary operations*, (Russian), Izvestiya AN Mold. SSR, Ser. fiz.-mat. nauk **3** (1974), 7 – 14.

[3] **V. D. Belousov**, *Systems of orthogonal operations*, (Russian), Matem. Sbornik **77 (119)** (1968), 38 – 58.

[4] **G. B. Belyavskaya and G. L. Mullen**, *Orthogonal hypercubes and n-ary operations*, Quasigroups and Related Systems **13** (2005), 73 – 86.

[5] **G. Belyavskaya and G. L. Mullen**, *Strongly orthogonal and uniformly orthogonal many-placed operations*, Algebra Discr. Math. **1** (2006), 1 – 17.

[6] **J. Dénes and A. D. Keedwell**, *Latin squares and their applications*, Acadèmiai Kiado, Budapest and Academic Press, New York, 1974.

[7] **J. Dénes and A. D. Keedwell**, *Latin squares. New Developments in the Theory and Applications*, Annals of Discrete Math. 46, North-Holland, 1991.

[8] **J. W. Greene, M. E. Hellman and E. D. Karnin**, *On secret sharing systems*, IEEE Trans. Information Theory IT-29 (1983), 35 – 41.

[9] **V. I. Izbash and P. Syrbu**, *Recursively differentiable quasigroups and complete recursive codes*, Comm. Math. Univ. Carolinae **45** (2004), 257 – 263.

[10] **C. F. Laywine, G. L. Mullen, and G. Whittle**, *D-dimensional hypercubes and the Euler and MacNeish conjectures*, Monatsh. Math. **111** (1995), 223 – 238.

[11] **R. McEliece and D. V. Sarwarte**, *On sharing secrets and Reed Solomon codes*, Comm. ACM **24** (1981), 583 – 584.

[12] **A. Shamir**, *How to share a secret*, Comm. ACM **22** (1979), 612 – 613.

[13] **G. L. Simmons (ed.)**, *Contemporary Cryptology – The Science of Information Integrity*, IEEE Press, New-York, 1992.

[14] **Z. Stojaković and J. Ušan**, *Orthogonal systems of partial operations*, Univ. u Novom Sadu, Zb. Rad. Prirod.-Mat. Fak. **8** (1978), 47 – 51.

[15] **J. Ušan**, *Orthogonal systems of n-ary operations and codes*, Mat. Vesnik **2** (1978), 91 – 93.

[16] **W. W. Wu**, *Elements of Digital Satellite Communication*, Computer Science Press, New York, 1985.

Received May 19, 2009

Institute of Mathematics and Computer Science, Academy of Sciences, Academiei str. 5,
MD-2028 Chisinau, Moldova
E-mail: gbel1@rambler.ru