Quasigroups and Related Systems **18** (2010), 83 – 94

Fast signatures based on non-cyclic finite groups

Nikolay A. Moldovyan

Devoted to the memory of Valentin D. Belousov (1925-1988)

Abstract. Finite rings of the m-dimension vectors over the ground field are defined with the vector multiplication operations of different types. Non-cyclic multiplicative groups of the rings in particular cases possess structure described in terms of the multi-dimension cyclicity. The vector finite groups relating to such cases are applied to design fast digital signature algorithms.

1. Introduction

The cyclic finite groups of different types are widely used as primitives of the digital signature (DS) algorithms [7, 9]. A group is called cyclic, if there exists a group element G (called generator) such that all elements of the group can be generated as different powers of G. Usually in the DS schemes based on difficulty of the discrete logarithm problem (DLP) the public key is computed as a group element $Y = G^x$, where G is the $\omega(G)$ order group element, and x is the secret key ($x < \omega(G)$). Security of the DS scheme is provided by the necessary requirement that the value ω contains a large prime factor q such that $q \geqslant 2^{160}$ [2] and by some other requirements depending on type of the used group, the first requirement being a common one for all cyclic groups used as primitive of the DS algorithms. The upper security boundary is limited by the difficulty of the DLP. There are known the general-purpose methods for solving the DLP, which work in any type cyclic group [2]. Such methods have exponential complexity $W = O(\sqrt{q})$ group operations, where $O(\cdot)$ is the order notation, and q is the largest prime divisor of the group order. If $q \geqslant 2^{160}$, then solving the DLP with the general-purpose methods are computationally infeasible. For

2000 Mathematics Subject Classification: 11G20, 11T71
Keywords: digital signatures, non-cyclic groups, vector finite groups
Supported by the Russian Foundation for Basic Research grant # 08-07-00096-a.

some finite groups there are known specialized methods having subexponential difficulty. Such groups are also used in some DS schemes, however they do not provide sufficiently high performance of the signature generation and verification procedures.

At present finite groups of the elliptic curve (EC) points represent the most efficient primitive of the DS algorithms. In the DS schemes there are used properly defined ECs for which the most efficient methods for solving the DLP are the general-purpose ones. Therefore it is sufficient to use the EC defined over finite fields (FFs) having the order size 160 to 320 bits [1]. Due to sufficiently small size of the FF order the DS algorithms based on ECs [3] provide the high performance.

Unfortunately the performance of the EC-based DS algorithms is limited by the inversion operation in the underlying FF, which is included in the procedure implementing the operation of adding the EC points. To overcome this limitation the finite groups of vectors over the ground FFs have been proposed as primitives of the DS algorithms [5]. For detailed justification of this proposal it is required to consider the structure of the vector finite groups (VFGs) that in general case are not cyclic. Only in some particular cases the multiplicative VFGs have cyclic structure. Such cases relates to formation of the vector finite fields (VFFs) [4] that have been proposed to define ECs providing higher performance of the EC-based DS algorithms. Essentially higher performance is expected from the DS based on non-cyclic VFGs.

Present paper presents the results on investigation of the structure of the non-cyclic VFGs and describes peculiarities of designing the DS algorithm based on computations in the VFGs. Section 2 provides description of the finite rings of the m-dimension vectors and defines a class of the vector multiplication operations. Section 3 provides general description of the structure of the vector finite rings in terms of the multi-dimension cyclicity (MDC). The proposed formulas describing the group structure have been confirmed by computational experiments. Section 4 explains the features of designing the DS algorithms based on VFGs possessing the MDC and presents new DS schemes and a rough performance comparison with the well known DS algorithms. Section 5 concludes the paper.

2. Finite rings of the m-dimension vectors

Finite rings of m-dimension vectors are defined over the ground field $GF(p)$, where p is a prime. Suppose $\mathbf{e}$, $\mathbf{i}$, ..., $\mathbf{w}$ be some m formal basis vectors and $a, b, z \in GF(p)$, where $p \geqslant 3$, are coordinates. The set of vectors

$$a\mathbf{e} + b\mathbf{i} + \cdots + z\mathbf{w}$$

is a finite m-dimension vector space. A vector can be also represented as a set of its coordinates $(a, b, \ldots, z)$. The terms $\tau\mathbf{v}$, where $\tau \in GF(p^d)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \ldots, \mathbf{w}\}$, are called components of the vector. The addition and multiplication operations over the vectors are defined as follows. The addition of two vectors $(a, b, \ldots, z)$ and $(a', b', \ldots, z')$ is defined via addition of the coordinates corresponding to the same basis vector accordingly to the following formula

$$(a, b, \ldots, z) + (a', b', \ldots, z') = (a + a', b + b', \ldots, z + z').$$

The multiplication of two vectors $a\mathbf{e}+b\mathbf{i}+\cdots+z\mathbf{w}$ and $a'\mathbf{e}+b'\mathbf{i}+\cdots+z'\mathbf{w}$ is defined as pair-wise multiplication of all components of the vectors in correspondence with the following formula

$$\begin{gathered}(a\mathbf{e}+b\mathbf{i}+\cdots+z\mathbf{w})\circ(a'\mathbf{e}+b'\mathbf{i}+\cdots+z'\mathbf{w}) = aa'\mathbf{e}\circ\mathbf{e}+ba'\mathbf{i}\circ\mathbf{e}+\cdots+za'\mathbf{w}\circ\mathbf{e}+\\ +ab'\mathbf{e}\circ\mathbf{i}+bb'\mathbf{i}\circ\mathbf{i}+\cdots+cb'\mathbf{w}\circ\mathbf{i}+\ldots\\ \cdots+az'\mathbf{e}\circ\mathbf{w}+bz'\mathbf{i}\circ\mathbf{w}+\cdots+zz'\mathbf{w}\circ\mathbf{w},\end{gathered}$$

where $\circ$ denotes the vector multiplication operation. In the final expression each product of two basis vectors is to be replaced by some basis vector $\mathbf{v}$ or by a vector $\tau\mathbf{v}$ ($\tau \in GF(p)$) in accordance with some given table called basis-vector multiplication table (BVMT). There are possible different types of the BVMTs, but in this paper there is used the BVMT of some general type proposed in [6] (see Table 1). For arbitrary values m and τ Table 1 defines the vector multiplication that is a commutative and associative operation. Different values τ define different types of the vector multiplication operation that defines the structure of the multiplicative group of the vector finite ring (VFR).

$\circ$	$\overrightarrow{e}$	$\overrightarrow{i}$	$\overrightarrow{j}$	$\overrightarrow{k}$	$\overrightarrow{u}$	...	$\overrightarrow{w}$
$\overrightarrow{e}$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$	...	$\mathbf{w}$
$\overrightarrow{i}$	$\mathbf{i}$	$\epsilon\mathbf{j}$	$\epsilon\mathbf{k}$	$\epsilon\mathbf{u}$	$\epsilon\ldots$	$\epsilon\mathbf{w}$	$\epsilon\mathbf{e}$
$\overrightarrow{j}$	$\mathbf{j}$	$\epsilon\mathbf{k}$	$\epsilon\mathbf{u}$	$\epsilon\ldots$	$\epsilon\mathbf{w}$	$\epsilon\mathbf{e}$	$\mathbf{i}$
$\overrightarrow{k}$	$\mathbf{k}$	$\epsilon\mathbf{u}$	$\epsilon\ldots$	$\epsilon\mathbf{w}$	$\epsilon\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$
$\overrightarrow{u}$	$\mathbf{u}$	$\epsilon\ldots$	$\epsilon\mathbf{w}$	$\epsilon\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
...	...	$\epsilon\mathbf{w}$	$\epsilon\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$
$\overrightarrow{w}$	$\mathbf{w}$	$\epsilon\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$	...

Table 1. The basis-vector multiplication table of the general type [6].

3. Cyclicity of the multiplicative group of VFR

The fixed vector addition operation is used in the VFR described in Section 2. On the contrary, for the given values m and p different types of the multiplication operation are specified with different values of the "expansion" coefficient τ. In this section the structure of the multiplicative group is considered. There are possible a variety of different structures of the VFGs depending on selection of the value τ. The simplest example is provided by the example of the VFFs that are formed in the cases $m|p-1$, while usingle values τ such that the equation $x^m = \tau$ has no solution in the field $GF(p)$. In such cases the VFGs have the cyclic structure and the VFG order is equal to $\Omega = p^m - 1$. Majority of other cases (for some values m there are possible specific conditions of the VFFs formation) the VFGs possess non-cyclic structure. The known example are VFGs formed in the case $m|p-1$, while using value τ such that the equation $x^m = \tau$ has a solution in the field $GF(p)$. In the last case for $m = 2$ and $m = 3$ the order of the VFGs is expressed by the following formula derived theoretically [6] $\Omega = (p-1)^m$. However the last formula does not explain the VFG structure. In the case of non-cyclic VFGs the computational experiments appear to be required to reveal the structure. The computational experiments have shown that the last formula is correct for all values m and the structure of such non-cyclic groups can be described in terms of MDC. The experiment have also shown in all cases the multiplicative VFGs possess structure described in terms of the MDC, except the case of the VFFs while the VFGs possess one-dimension cyclicity.

3.1. Multi-dimension cyclicity of the VFG structure

Let us consider a hypothetic group Γ_μ of the order $\Omega(\Gamma_\mu) = q^\mu$, where q is a prime, in which there exist μ elements $G_1, G_2, \ldots, G_\mu$ possessing the same order q, such that any group element $G \in \Gamma_\mu$ can be represented as product $\prod_{i=1}^{\mu} G_i^{s_i}$ for some set of powers $(s_1, s_2, \ldots, s_\mu)$ and none of these elements, for example, G_j can be expressed as product $\prod_{i=1;i\neq j}^{\mu} G_i^{s_i}$.

Non-cyclic groups produced by the generator system in which all generators have the same order value are called in this paper groups possessing the structure with multi-dimension cyclicity (MDC). The value μ is called dimension of the MDC of the group structure. The term MDC is used to describe the VFG structures since it corresponds well to the fact that the elements of the considered groups are vectors, besides the term reflects the fact that in all cases the multiplicative groups of the VFRs can be described from a single position. Indeed, the cyclic structure of the multiplicative groups of the VFFs can be considered as a particular case of MDC, i.e., as one-dimension cyclicity.

Since the element order divides the group order, the minimum order of elements

G_i is value $\omega(G_i) = q$. It is easy to show that the basis $\{G_1, G_2, \ldots, G_\mu\}$ generates $\omega(G_1)\omega(G_2)\ldots\omega(G_\mu) \geqslant q^\mu$ different elements of the group Γ_μ. It is evident that $\Omega(\Gamma_\mu) \geqslant \omega(G_1)\omega(G_2)\ldots\omega(G_\mu)$. The number of different elements in the group Γ_μ is equal to $\Omega(\Gamma_\mu) = q^\mu$, therefore the last inequality holds, only if all elements of the basis have the minimum possible order q. The last means that all elements of the group, except the unity element, have the same order q.

Suppose the group Γ_μ contains $N_{\Omega'=q}$ different cyclic subgroups. Each of such subgroups contains $q-1$ non-unity elements, therefore $N_{\Omega'=q}(q-1) = q^\mu - 1$ and

$$N_{\Omega'=q} = \frac{q^\mu - 1}{q-1}. \tag{1}$$

There exist few real examples of such groups. Among vector finite groups we have the example relating to selection of the parameters $m = 2$, $p = 3$, and $\tau = 1$ that define the fourth order group containing three elements (0,1), (2,0), and (0,2) of the second order and the unity elements (1,0). Other example are provided by some subgroups in the groups considered below. It is a typical case that VFGs contains subgroups like Γ_μ. (Among the VFRs defined over the finite polynomial fields $GF(p^d)$, where $d \geqslant 2$, we have some more examples of the VFGs possessing the MDC structure and containing only elements having the same prime order.)

Note that in some group of the order q^d, where q is a prime, the dimension μ of the MDC satisfies the condition $\mu \leqslant d$. Let us consider a hypothetic group $\Gamma_{t\mu}$ of the order $\Omega = q^d$, where $d = t\mu$. Suppose the group $\Gamma_{t\mu}$ contains μ independent elements of the order $\omega = q^t$, composing a basis $\{G_1, G_2, \ldots, G_\mu\}$, then we have the following facts.

1. The group $\Gamma_{t\mu}$ contains μ exponentially independent elements of the order $\omega = q^j$ for each of the values $j = 1, 2, \ldots t$.

2. For all values $j = 1, 2, \ldots t$ the group Γ_t contains $N_{\omega=q^j}$ elements G of the order $\omega(G) = q^j$, which is equal to the value

$$N_{\omega=q^j} = q^{\mu(j-1)}(q^\mu - 1). \tag{2}$$

3. For each of the values $j = 1, 2, \ldots t$ the group Γ_t contains $N_{\Omega'=q^j}$ different cyclic subgroups of the order $\Omega' = q^j$, which is equal to the value

$$N_{\Omega'=q^j} = q^{(\mu-1)(j-1)}\frac{q^\mu - 1}{q-1}. \tag{3}$$

The VFGs provide sufficient number of real examples of groups of the $\Gamma_{t\mu}$ type, which relates to the cases $m = 2, 4, \ldots 2^d$ $(d = 1, 2, 3\ldots)$ and primes p having the structure $p = 2^k + 1$ $(k = 4, 8, 16)$. Table 2 presents experimental results.

$m=2;\ p=257;\ \tau=169$		$m=4;\ p=257;\ \tau=81$		$m=8;\ p=17;\ \tau=1$	
ω	N_ω	ω	N_ω	ω	N_ω
2	3	2	15	2	255
4	12	4	240	4	65280
8	48	8	3840	8	16711680
16	192	16	61440	16	4278190080
32	768	32	983040	-	-
64	3072	64	15728640	-	-
128	12288	128	251658240	-	-
256	49152	256	4026531840	-	-

Table 2. Some particular variants of the vector finite groups of order $(p-1)^m$.

3.2. Vector groups having multi-dimension cyclicity structure

Let us consider a hypothetic group Γ of the order $\Omega = \left(\prod_{i=1}^{z} q_i^{t_i}\right)^{\mu}$, where q_i is a prime for all $i \in \{1,2,\dots z\}$. Suppose for all $i = 1,2,\dots z$ the group Γ contains μ exponentially independent elements of the order $\omega = q_i^{t_i}$, which compose the basis $\{G_1^{(i)}, G_2^{(i)}, \dots, G_\mu^{(i)}\}$. Such assumption leads to the following facts.

1. The group Γ contains μ exponentially independent elements of the order $\omega = \prod_{i=1}^{z} q_i^{t_i}$, that generate all of the group elements.

2. The group Γ contains μ exponentially independent elements of the order $\omega = D$, where D is a divisor of the group order.

3. For each divisor D of the group order such that $D = q_i^{t'_i}$, where $i \in \{1,2,\dots z\}$ and $0 \leqslant t'_i \leqslant t_i$, the group Γ contains the number of elements $N_{\omega=q_i^{t'_i}}$ of the order D, which is equal to

$$N_{\omega=q_i^{t'_i}} = q_i^{\mu(t'_i-1)}(q_i^{\mu}-1). \tag{4}$$

4. For each divisor D of the group order such that $D = \prod_{i=1}^{z'} q_i^{t'_i}$, where $i = 1,2,\dots z$ and $1 \leqslant t'_i \leqslant t_i$, the group Γ contains the number of elements $N_{\omega=D}$ of the order D, which is equal to

$$N_{\omega=D} = \prod_{i=1}^{z'} q_i^{\mu(t'_i-1)}(q_i^{\mu}-1). \tag{5}$$

5. For each divisor $D|\Omega$ of the group order such that $D = \prod_{i=1}^{z'} q_i^{t'_i}$, where $i = 1,2,\dots z$ and $1 \leqslant t'_i \leqslant t_i$, the group Γ contains the number $N_{\Omega'=D}$ of cyclic subgroups of the order $\Omega' = D$, which equals to

$$N_{\Omega'=D} = \prod_{i=1}^{z'} q_i^{(\mu-1)(t'_i-1)} \frac{q_i^{\mu}-1}{q_i-1}. \tag{6}$$

Among different types of the multiplicative groups of VFRs the VFGs possessing the MDC structure are more attractive as primitive of the DS algorithms, some other particular types of the non-cyclic VFGs also represent interest for public key cryptography though. In the VFGs possessing the MDC for each prime divisor q_i of the group order Ω there exist subgroups of the orders $\Omega' = \left(q_i^{t'_i}\right)^{\mu}$, where $t'_i = 1, 2, \ldots t_i$, which possess the MDC structure with the same dimension value μ. In particular for some large prime q there exists the q^{μ}-order subgroup all elements of which have the same order q, except the unity element. Such subgroups play important role in the DS algorithms proposed below. Examples confirming the facts and formulas presented above are given in the next section.

4. Experimental confirmation

For values $m = 2$ and $m = 3$ in the case $m|p-1$ it has been theoretically derived [6] the following formula

$$\Omega = (p-1)^m. \tag{7}$$

In all our experiments relating to the case $p > m$ and $m|p-1$ the group order is described with formula (7), if the coefficient τ is the mth power of some element $x \in GF(p)$. To determine the real structure of the VFGs we have computed the order of all elements in the VFGs involved in experiments (multiplying the group elements G many times, the order $\omega(G)$ has been calculated). Experimental results are presented in Table 3. The results are completely described by formulas (4) and (5).

$m = 10;\ p = 11;\ \tau = 1$		$m = 7;\ p = 29;\ \tau = 28$		$m = 6;\ p = 19;\ \tau = 1$	
ω	N_ω	ω	N_ω	ω	N_ω
2	1023	2	127	2	63
5	9765624	4	16256	3	728
10	9990233352	7	823542	6	45864
-	-	14	104589834	9	530712
-	-	28	13387498752	18	33434856

Table 3. Structure of the VFGs possessing the order $\Omega = (p-1)^{\mu}$, where $\mu = m$ (N_ω is the number of the group elements having the order ω).

Thus, performing many different computational experiments in all cases, when τ can be represented as the mth degree of some element of the ground field $GF(p)$ and $m|p-1$, we have get the vector group structure that is described in terms of the MDC with $\mu = m$. The experiments have also revealed different other conditions under which there are formed the VFG possessing the MDC structure described by formula (5). From the results for the case $m|p-1$ the following formula for the VFG order have been derived

$$\Omega = (p^{\nu} - 1)^{\mu}, \tag{8}$$

where μ is the dimension of MDC, $\mu|m$, $\nu = m/\mu$, which describes the VFG structure when the parameter τ is such that the equation $\tau = x^{\mu}$ has solutions in $GF(p)$, and the equation $\tau = x^{\mu\delta}$ has no solutions in $GF(p)$ for each divisor $\delta|\nu$, $\delta > 1$. Examples of the VFGs relating to such cases are presented in Table 4. In the next section formula (8) is used to define the VFGs suitable to implementation of the DS algorithms. In Table 4 the formulas describing the group order Ω for cases $m \leqslant 8$ have been obtained from experiments on finding the order ω for each group element, like experiments used to obtain results of Table 3. For cases $m > 8$ the formulas have been preliminary composed and then experimentally proved.

The cases $\mu = 1$ relates to VFRs that are extension FFs $GF(p)$, when the VFGs are cyclic. Such VFFs are very attractive for application in EC-based DS algorithms [4] due to sufficiently fast multiplication operation and possibility of the efficient parallelization of the vector multiplication. In this paper only non-cyclic VFGs ($\mu \geqslant 2$) are discussed as primitives of the DS algorithms.

$m,\ p,\ \tau$	Ω	μ	$m,\ p,\ \tau$	Ω	μ
10, 11, 4	$\left(p^5-1\right)^{\mu}$	2	24, 1201, 729	$(p-1)^{\mu}$	24
10, 11, 10	$\left(p^2-1\right)^{\mu}$	5	24, 1201, 49	$\left(p^2-1\right)^{\mu}$	12
9, 13, 1	$\left(p^3-1\right)^{\mu}$	3	24, 1201, 16	$\left(p^3-1\right)^{\mu}$	8
9, 19, 1	$(p-1)^{\mu}$	9	24, 1201, 19	$\left(p^4-1\right)^{\mu}$	6
8, 17, 4	$\left(p^2-1\right)^{\mu}$	4	24, 1201, 61	$\left(p^6-1\right)^{\mu}$	4
8, 5, 4	$\left(p^4-1\right)^{\mu}$	2	24, 1201, 23	$\left(p^8-1\right)^{\mu}$	3
6, 19, 8	$\left(p^2-1\right)^{\mu}$	3	24, 1201, 289	$\left(p^{12}-1\right)^{\mu}$	2
6, 19, 16	$\left(p^3-1\right)^{\mu}$	2	24, 1201, 101	$\left(p^{24}-1\right)^{\mu}$	1
42, 421, 67	$(p-1)^{\mu}$	42	42, 421, 29	$\left(p^2-1\right)^{\mu}$	21
42, 421, 277	$\left(p^3-1\right)^{\mu}$	14	42, 421, 73	$\left(p^6-1\right)^{\mu}$	7
42, 421, 7	$\left(p^7-1\right)^{\mu}$	6	42, 421, 19	$\left(p^{14}-1\right)^{\mu}$	3
42, 421, 79	$\left(p^{21}-1\right)^{\mu}$	2	42, 421, 2	$\left(p^{42}-1\right)^{\mu}$	1

Table 4. Analytic description of the experimental results on investigation of the VFG structure (cases $\mu \leqslant m$).

5. Designing the DS algorithms based on the VFGs

In the standard case of the DS algorithm design based on cyclic groups the group order Ω should contain a large prime divisor $q|\Omega$ such that $q \geqslant 2^{160}$ [2, 7]. However taking into account the MDC of the VFG structure it can be shown that for VFGs the standard cryptographic requirement is essentially excessive. If the prime divisor q of the VFG order relates to the MDC subgroup of the order q^{μ}, then the general security requirement can be specified as $q \geqslant 2^{160/\mu}$, where μ is the dimension of the cyclicity of the group structure. However to make use of this essential correction some changes in the design of the DS algorithms should be introduced.

First, the public key is to be generated as μ vectors $Y_1, Y_2, ..., Y_\mu$ in accordance with the following formula

$$Y_i = G_1^{x_{1i}} \circ G_2^{x_{2i}} \cdots \circ G_\mu^{x_{\mu i}} = \prod_{j=1}^{\mu} G_j^{x_{ji}},$$

where $\omega(G_i) = q \ \forall i \in \{1, 2, \ldots, \mu\}$, $G_1, G_2, \ldots G_\mu$ is the generator system of the subgroup having the order q^μ, and the set $\{x_{ji}\}$ is the secret key ($i, j \in \{1, 2, \ldots, \mu\}$). Computation of the secret key defines a problem of finding multi-dimension logarithm at the basis $G_1, G_2, \ldots G_\mu$. This problem can be solved using some modifications of the general-purpose methods for finding discrete logarithms in cyclic groups [2]. The difficulty of such modified methods is $O(\sqrt{q^\mu})$ exponentiation operations in the used VFG, therefore the minimum security (corresponding to difficulty of breaking the DS algorithm, which is equal to 2^{80} exponentiation operations) can be provided with the condition $|p| \approx |q| \geqslant 160/\mu$ bits.

Second, the DS scheme should be modified in accordance with the modified public key. All parts of the public key $(Y_1, Y_2, \ldots, Y_\mu)$ should be used in the DS verification procedure. The following DS schemes takes into account the mentioned modifications.

Generation of the DS corresponding to the message M is performed as follows:

1. Select μ random values $k_1, k_2, \ldots, k_\mu$ such that for all $i = 1, 2, \ldots, \mu$ it holds $k_i < q$.

2. Calculate vector $R = (r_1, r_2, \ldots, r_m) = G_1^{k_1} \circ G_2^{k_2} \cdots \circ G_\mu^{k_\mu}$.

3. Using some specified hash function F_h (different examples see in [2]) calculate the hash value h from the message to which the vector R is concatenated: $h = F_h(M \| r_1 \| r_2 \| \ldots \| r_m)$.

4. Represent the value h as some concatenation of μ elements: $h = h_1 \| h_2 \| ... \| h_\mu$ and compute the second element of the DS as the set of μ values $\{s_1, s_2, \ldots s_\mu\}$:

$$s_j = t_j + \sum_{i=1}^{i=\mu} x_{ji} h_i \bmod q,$$

where $j = 1, 2, \ldots \mu$.

Verification of the DS corresponding to the message M is performed as follows:

1. Compute the vector $R' = Y_1^{-h_1} \circ Y_2^{-h_2} \cdots \circ Y_\mu^{-h_\mu} \circ G_1^{s_1} \circ G_2^{s_2} \cdots \circ G_m^{s_\mu}$.

2. Compute the value $h' = F_h(M \| r'_1 \| r'_2 \| \ldots \| r'_m)$.

3. Compare the values h' and h. If $h' = h$, then the DS is valid.

There are possible different variants of the values m and μ that provide fast generation and verification of the DS, the values $\mu = 2$ (for $m = 2, 6, 10, 14$ and 22) and $\mu = 3$ (for $m = 3, 9, 15$, and 21) are the most interesting for practical applications though. Values $\mu > 3$ lead to comparatively large size of the public key. The values m corresponding to $\mu = 2$ and $\mu = 3$, which are indicated in brackets, provides possibility to select the values p providing faster procedures for DS generation and verification.

Let us consider some particular variants of the DS scheme described above.

Example 1. $m = 6$, $p = 3112656501667$, and $\tau = 3229543499124319810093519$. These parameters define formation of the VFG having the order $\Omega = \left(p^5 - 1\right)^{\mu}$ and dimension of the cyclicity $\mu = 2$. The largest prime divisor of Ω is $q = 3229543499124319810093519$. The subgroup of the order q^{μ} is generated by the following pair of the q-order vectors

$G_1 =$
(2461700031734, 482034324490, 156834270570, 1324447431161, 2740416991343, 1220868764310),
$G_2 =$
(2538171306005, 283399862632, 192519072375, 891592729264, 760409728893, 2653262071023).

Example 2. $m = 10$, $p = 14152871$, and $\tau = 9$. These parameters define formation of the VFG having the order $\Omega = \left(p^5 - 1\right)^{\mu}$ and dimension of the cyclicity $\mu = 2$. The largest prime divisor of Ω is $q = 802431962411491058379600 4541$. The subgroup of the order q^{μ} is generated by the following pair of the q-order vectors

$G_1 =$
(6283401, 4259768, 6598451, 3709261, 8444571, 82053, 6685050, 10303674, 9996976, 10471343),
$G_2 =$
(1523659, 5587678, 3962704, 8694664, 3478222, 2379965, 4305324, 860257, 4524271, 8938870).

Example 3. $m = 14$, $p = 8093$, and $\tau = 9$. These parameters define formation of the VFG having the order $\Omega = \left(p^7 - 1\right)^{\mu}$ and dimension of the cyclicity $\mu = 2$. The largest prime divisor of Ω is $q = 40143281293465596069349$. The subgroup of the order q^{μ} is generated by the following pair of the q-order vectors

$G_1 = (6324, 3153, 1575, 5913, 3701, 5665, 3268, 5171, 4816, 1661, 1926, 4203, 678, 4187)$,
$G_2 = (5992, 4360, 4442, 2341, 6950, 2525, 921, 1565, 2120, 3592, 6668, 248, 399, 6214)$.

Example 4. $m = 2$, $p = 691789104238168962670253 9$, and $\tau = 2^{32} = 4294967296$. These parameters define formation of the VFG having the order $\Omega = (p-1)^{\mu}$ and dimension of the cyclicity $\mu = 2$.

The largest prime divisor of Ω is $q = 3458945521190844813351269$. The subgroup of the order q^{μ} is generated by the following pair of the q-order vectors

$$G_1 = (3, 0), \quad G_2 = (1, 5).$$

Example 5. $m = 3$, $p = 275352871102525507$, and $\tau = 2^{24} = 16777216$. These parameters define formation of the VFG having the order $\Omega = (p-1)^{\mu}$ and dimension of the cyclicity $\mu = 3$. The largest prime divisor of Ω is $q = 45892145183754251$. The subgroup of the order q^{μ} is generated by the following three of the q-order vectors

$G_1 = (21, 0, 0)$,
$G_2 = (217941963753891151,\ 239089986535147009,\ 109899378481277797)$,
$G_3 = (158846680700738144,\ 28761476487049241,\ 144620654759850124)$.

Example 6. $m = 4$, $p = 11780627332037$, and $\tau = 2^{24} = 16777216$. These parameters define formation of the VFG having the order $\Omega = (p-1)^{\mu}$ and dimension

of the cyclicity $\mu = 2$. The largest prime divisor of Ω is $q = 2945156833009$. The subgroup of the order q^μ is generated by the following four of the q-order vectors

$G_1 = (17, 0, 0, 0)$,
$G_2 = (872502753155,\ 6114625095567,\ 4745624761713,\ 4690788873292)$,
$G_3 = (11269823703275,\ 5374465446130,\ 6550130852697,\ 7523825764505)$,
$G_4 = (9996654190922,\ 7883587942021,\ 9910063088313,\ 272051995111)$.

The computational difficulty of the DS generation and verification procedures is approximately equal to difficulty of three modulo exponentiation operations like $g^s \bmod n$, where $|s| = \mu|q|$ and $|n| = m|p|$. As it has been shown above in the case $m = \mu$ the characteristic of the field $GF(p)$ can be selected such that $|p| \approx |q| \geqslant 160/\mu$ bits. This provides high performance of the proposed algorithm. Comparison with the performance (in arbitrary unites) of some widely used DS algorithms is presented in Table 6, where the performance is estimated for the size of the DS parameters providing supposed security of 2^{80} group operations.

DS scheme	DL problem in ...	$\|p\|$, bits	Public key size, bits	DS size, bits	Rate, arb. un.
GOST 1994 [10]	$GF(p)$	1024	1024	1024	1
DSA [11]	$GF(p)$	1024	1024	320	3
Shnorr [8]	$GF(p)$	1024	1024	320	3
GOST 2001 [10]	EC	256	512	512	6
ECDSA [11]	EC	160	320	320	10
Proposed ($m = 6$; $\mu = 2$)	VFG	42	512	320	70
Proposed ($m = 10$; $\mu = 2$)	VFG	21	420	320	80
Proposed ($m = \mu = 2$)	VFG	82	328	320	100
Proposed ($m = \mu = 3$)	VFG	56	504	320	100
Proposed ($m = \mu = 4$)	VFG	43	688	320	100

Table 5. Rough performance comparison of different DS schemes based on difficulty of the DL problem (EC denotes elliptic curve defined over $GF(p)$).

6. Conclusion

Using specially introduced BVNTs to define the vector multiplication operation in the finite vector spaces over the finite ground fields leads to formation of the VFRs containing the multiplicative group possessing the MDC structure. The MDC is a common feature for such VFGs. The dimension of the structure cyclicity μ is equal to some divisor of the vector dimension m. Using different values of the expansion coefficient τ that is the flexible parameter of the used BVMT different values μ are assigned. The particular case of the VFFs formation corresponds to value $\mu = 1$.

The VFGs relating to cases $\mu = 2$ and $\mu = 3$ are very attractive as primitives for fast DS algorithms. It has been proposed a DS scheme in which some design features have been applied taking into account the MDC structure of the VFGs.

Several concrete VFGs suitable to application in the frame of the proposed DS scheme have been described. An algorithm for finding two-dimension algorithms has been described and used to estimate the security of the DS algorithms based on computations in FVGs possessing the structure with two-dimension cyclicity. Performance comparison with the known fast DS schemes shows the proposed ones provides significantly higher rate. Besides, the vector multiplication operation suite well to parallelization therefore the propose DS scheme is significantly more efficient in parallelized hardware implementation than other known DS algorithms, especially when the VFGs with sufficiently large value m are applied.

References

[1] **N. Koblitz**, *A course in number theory and cryptography*, Springer-Verlag. Berlin, 2003.

[2] **A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone**, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997.

[3] **A. J. Menezes and S. A. Vanstone**, *Elliptic curve cryptosystems and their implementation*, J. Cryptology **6** (1993), 209 – 224.

[4] **N. A. Moldovyan**, *A method for generating and verifying electronic digital signature certifying an electronic document*, Russian patent application # 2008140403. October 14, 2008.

[5] **N. A. Moldovyan and D. N. Moldovyan**, *A method for computing and verifying electronic digital signature certifying an electronic document*, Russian patent application # 2008130759. July 24, 2008.

[6] **N. A. Moldovyan and P. A. Moldovyanu**, *New primitives for digital signature algorithms*, Quasigroups and Related Systems **17** (2009), 271 – 282.

[7] **J. Pieprzyk, Th. Hardjono and J. Seberry**, *Fundamentals of computer security*, Springer-Verlag. Berlin, 2003.

[8] **C. P. Schnorr**, *Efficient signature generation by smart cards*, J. Cryptology **4** (1991), 161 – 174.

[9] **N. Smart**, *Cryptography: an Introduction*, McGraw-Hill Publication, London, 2003.

[10] GOST R 34.10-94 (and GOST R 34.10-2001). Russian Federation Standard. Information Technology. Government Committee of the Russia for Standards.

[11] International Standard ISO/IEC 14888-3:2006(E).

Received January 26, 2009

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, 14 Linya str. 39, St. Petersburg 199178, Russia, E-mail: nmold@mail.ru