Quasigroups and Related Systems **18** (2010), 165 – 176

Non-commutative finite groups as primitive of public key cryptosystems

Dmitriy N. Moldovyan

Abstract. A new computationally difficult problem define over non-commutative finite groups is proposed as cryptographic primitive. Finite non-commutative rings of the four-dimension vectors over the ground field are defined with the vector multiplication operations of different types. Non-commutative multiplicative groups of the rings are applied to design public key cryptoschemes based on the proposed difficult problem.

1. Introduction

The most widely used in the public key cryptography difficult problems, factorization and finding discrete logarithm, can be solved in polynomial time on a quantum computer [5]. Quantum computing develops towards practical implementations therefore cryptographers look for some new hard problems that have exponential complexity while using both the ordinary computers and the quantum ones [1, 2]. Such new difficult problems have been defined over braid groups representing a particular type of infinite non-commutative groups. Using the braid groups as cryptographic primitive a number of new public key cryptosystems have been developed [3, 6].

Present paper introduces a new hard problem defined over finite non-commutative groups and public key cryptoschemes constructed using the proposed hard problem. It is also presented a theorem disclosing the local structure of the non-commutative group, which is exploited in the proposed hard problem. Then concrete type of the non-commutative finite groups is constructed over finite four-dimension vector space.

2010 Mathematics Subject Classification: 11G20, 11T71
Keywords: difficult problem, automorphism, non-commutative group, finite group, public key distribution, public encryption, commutative encryption.
The work was supported by the Russian Foundation for Basic Research grant # 08-07-00096-a.

2. New problem and its cryptographic applications

Suppose for some given finite non-commutative group Γ containing element Q possessing high prime order q there exists a method for easy selection of the elements from sufficiently large commutative subgroup $\Gamma_{comm} \in \Gamma$. One can select as private key a random element $W \in \Gamma_{comm}$ such that $W \circ Q \neq Q \circ W$ and a random number $x < q$ and then compute the public key $Y = W \circ Q^x \circ W^{-1}$ (note that it is easy to show that for arbitrary value x the inequality $W \circ Q^x \neq Q^x \circ W$ holds). Finding pair (W, x), while given Γ, Γ_{comm}, Q, and Y, is a computationally difficult problem that is suitable to design new public key cryptosystems. The problem suits also for designing commutative encryption algorithms.

The public key agreement protocols can be constructed as follows. Suppose two users have intension to generate a common secret key using a public channel. The first user generates his private key (W_1, x_1), computes his public key $Y_1 = W_1 \circ Q^{x_1} \circ W_1^{-1}$, and sends Y_1 to the second user. The last generates his private key (W_2, x_2), computes his public key $Y_2 = W_2 \circ Q^{x_2} \circ W_2^{-1}$, and sends Y_2 to the first user. Then the first user computes the value

$$K_{12} = W_1 \circ (Y_2)^{x_1} \circ W_1^{-1} = W_1 \circ \left(W_2 \circ Q^{x_2} \circ W_2^{-1}\right)^{x_1} \circ W_1^{-1} = W_1 \circ W_2 \circ Q^{x_2 x_1} \circ W_2^{-1} \circ W_1^{-1}.$$

The second user computes the value

$$K_{21} = W_2 \circ (Y_1)^{x_2} \circ W_2^{-1} = W_2 \circ \left(W_1 \circ Q^{x_1} \circ W_1^{-1}\right)^{x_2} \circ W_2^{-1} = W_1 \circ W_1 \circ Q^{x_1 x_2} \circ W_1^{-1} \circ W_2^{-1}.$$

The elements W_1 and W_2 belong to the commutative subgroup Γ_{comm}, therefore $K_{21} = K_{12} = K$, i.e. each of the users has generated the same secret K that can be used, for example, to encrypt confidential messages send through the public channel.

Suppose a public-key reference book is issued. Any person can send to some user a confidential message M using user's public key $Y = W \circ Q^x \circ W^{-1}$, where W and x are elements of user's private key. For this aim the following public key encryption scheme can be used, in which it is supposed using some encryption algorithm F_K controlled with secret key K representing an element of the group Γ.

1. Sender generates a random element $U \in \Gamma_{comm}$ and a random number u, then computes the elements $R = U \circ Q^u \circ U^{-1}$ and $K = U \circ Y^u \circ U^{-1} = U \circ \left(W \circ Q^x \circ W^{-1}\right)^u \circ U^{-1} = U \circ W \circ Q^{xu} \circ W^{-1} \circ U^{-1}$.

2. Using the element K as encryption key and encryption algorithm E_K sender encrypts the message M into the cryptogramm $C = F_K(M)$. Then he sends the cryptogram C and element R to the user.

3. Using the element R the user computes the encryption key K as follows $K = W \circ R^x \circ W^{-1} = W \circ \left(U \circ Q^u \circ U^{-1}\right)^x \circ W^{-1} = W \circ U \circ Q^{ux} \circ U^{-1} \circ W^{-1}$. Then the user decrypts the cryptogram C as follows $M = F_K^{-1}(C)$, where F_K^{-1} is the decryption algorithm corresponding to the encryption algorithm F_K.

The proposed hard problem represents some combining the exponentiation procedure with the procedure defining group mapping that is an automorphism. These two procedures are commutative therefore their combination can be used to define the following commutative-encryption algorithm.

1. Represent the message as element M of the group Γ.

2. Encrypt the message with the first encryption key (W_1, e_1), where $W_1 \in \Gamma_{comm}$, e_1 is a number invertible modulo m, and m is the least common multiple of all element orders in the group Γ, as follows $C_1 = W_1 \circ M^{e_1} \circ W_1^{-1}$.

3. Encrypt the cryptogram C_1 with the second encryption key (W_2, e_2), where $W_2 \in \Gamma_{comm}$, e_2 is a number invertible modulo m, as follows

$$C_{12} = W_2 \circ C_1^{e_2} \circ W_2^{-1} = W_2 \circ W_1 \circ M^{e_1 e_2} \circ W_1^{-1} \circ W_2^{-1}.$$

It is easy to show the encrypting the message M with the second key (W_2, e_2) and then with the first key (W_1, e_1) produces the cryptogram $C_{21} = C_{12}$, i.e. the last encryption procedure is commutative.

3. On choosing elements

In the cryptoschemes described in previous section the first element of the private key should be selected from some commutative group. A suitable way to define such selection is the following one. Generate an element $G \in \Gamma$ having sufficiently large prime order g and define selection of the element W as selection of the random number $1 < w < g$ and computing $W = G^w$. Using this mechanism the private key is selected as two random numbers w and x and the public key is the element $Y = G^w \circ Q^x \circ G^{-w}$. One can easy show that for arbitrary values w and x the inequality $G^w \circ Q^x \neq Q^x \circ W^w$ holds.

For security estimations it represents interest haw many different elements are generated from two given elements G and Q having prime orders

g and q, respectively. The following theorem gives a positive answer to this question.

Theorem 1. *Suppose elements G and Q of some non-commutative finite group Γ have the prime orders g and q, correspondingly, and satisfy the following expressions $G \circ Q \neq Q \circ G$ and $K \circ Q \neq Q \circ K$, where $K = G \circ Q \circ G^{-1}$. Then all of elements $K_{ij} = G^j \circ Q^i \circ G^{-j}$, where $i = 1, 2, \ldots, q-1$ and $j = 1, 2, \ldots, g$, are pairwise different.*

Proof. It is evident that for some fixed value j the elements $K_{ij} = G^j \circ Q^i \circ G^{-j}$, where $i = 1, 2, \ldots, q$, compose a cyclic subgroup of the order q. Condition $K \circ Q \neq Q \circ K$ means that element K is not included in the subgroup Γ_Q generated by different powers of Q. Suppose that for some values i, $i' \neq i$, j, and $j' \neq j$ elements K_{ij} and $K_{i'j'}$ are equal, i.e. $G^j \circ Q^i \circ G^{-j} = G^{j'} \circ Q^{i'} \circ G^{-j'}$. Multiplying the both parts of the last equation at the right by element G^j and at the left by element G^{-j} one gets $Q^i = G^{j'-j} \circ Q^{i'} \circ G^{-(j'-j)}$. The subgroup Γ_Q has the prime order, therefore its arbitrary element different from the unity element is generator of Γ_Q, i.e. for $i' \leq q-1$ the element $P = Q^{i'}$ generates subgroup Γ_Q. Taking this fact into account one can write

$$\begin{aligned}\left(Q^i\right)^z = \left(G^{j'-j} \circ Q^{i'} \circ G^{-(j'-j)}\right)^z &= G^{j'-j} \circ Q^{i'z} \circ G^{-(j'-j)} \\ &= G^{j'-j} \circ P^z \circ G^{-(j'-j)} \in \Gamma_Q.\end{aligned}$$

The last formula shows that mapping $\varphi_{G^{j'-j}}(P^z) = G^{j'-j} \circ P^z \circ G^{-(j'-j)}$ maps each element of Γ_Q on some element of Γ_Q. The mapping $\varphi_{G^{j'-j}}(\Gamma_Q)$ is bijection, since for $z = 1, 2, \ldots, q$ the set of elements $\left(Q^i\right)^z$ composes the subgroup Γ_Q. Thus, the mapping $\varphi_{G^{j'-j}}(\Gamma_Q)$ is a bijection of the subgroup Γ_Q onto itself.

Since order of the element G is prime, there exists some number $u = (j'-j)^{-1} \bmod g$ for which the following expressions hold $G = \left(G^{j'-j}\right)^u$ and

$$\varphi_G(\Gamma_Q) = \varphi_{\left(G^{j'-j}\right)^u}(\Gamma_Q) = \underbrace{\varphi_{G^{j'-j}}\left(\varphi_{G^{j'-j}}\left(\ldots \varphi_{G^{j'-j}}(\Gamma_Q)\ldots\right)\right)}_{u \text{ bijective mappings}},$$

where the mapping is represented as superposition of u mappings $\varphi_{G^{j'-j}}(\Gamma_Q)$. The superposition is also a bijection of the subgroup Γ_Q onto itself, since the mapping $\varphi_{G^{j'-j}}(\Gamma_Q)$ is the bijection Γ_Q onto Γ_Q. Therefore the following expression holds $K = G \circ Q \circ G^{-1} = \varphi_G(Q) \in \Gamma_Q$ and $K \circ Q = Q \circ K$.

The last formula conradicts to the condition $K \circ Q \neq Q \circ K$ of the theorem. This contradiction proves Theorem 1. □

According to Theorem 1 there exist $(q-1)g$ different elements $Z_{ij} \neq E$, where E is unity element of Γ. Together with the unity element E they compose g cyclic subgroups of the order q and each of elements $Z_{ij} \neq E$ belongs only to one of such subgroups.

4. Finite rings of four-dimension vectors

Different finite rings of m-dimension vectors over the ground field $GF(p)$, where p is a prime, can be defined using technique proposed in [4]. The non-commutative rings of four-dimension vectors are defined as follows. Suppose $\mathbf{e}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ be some formal basis vectors and $a, b, c, d \in GF(p)$, where $p \geqslant 3$, are coordinates. The vectors are denoted as $a\mathbf{e}+b\mathbf{i}+c\mathbf{i}+d\mathbf{k}$ or as (a, b, c, d). The terms $\tau\mathbf{v}$, where $\tau \in GF(p^d)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, are called components of the vector.

The addition of two vectors (a, b, c, d) and (x, y, z, v) is defined addition of the coordinates corresponding to the same basis vector accordingly to the following formula

$$(a, b, c, d) + (x, y, z, v) = (a + x, b + y, c + z, d + v).$$

The multiplication of two vectors $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + z\mathbf{w}$ and $x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + v\mathbf{k}$ is defined as multiplication of each component of the first vector with each component of the second vector in correspondence with the following formula

$$(a\mathbf{e}+b\mathbf{i}+c\mathbf{j}+z\mathbf{w}) \circ (x\mathbf{e}+y\mathbf{i}+z\mathbf{j}+v\mathbf{k}) = ax\mathbf{e}\circ\mathbf{e}+bx\mathbf{i}\circ\mathbf{e}+cx\mathbf{j}\circ\mathbf{e}+dx\mathbf{k}\circ\mathbf{e}+ \\ +az\mathbf{e}\circ\mathbf{j}+bz\mathbf{i}\circ\mathbf{j}+cz\mathbf{j}\circ\mathbf{j}+dz\mathbf{k}\circ\mathbf{j}+ av\mathbf{e}\circ\mathbf{k}+bv\mathbf{i}\circ\mathbf{k}+cv\mathbf{j}\circ\mathbf{k}+dv\mathbf{k}\circ\mathbf{k},$$

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 or by a vector containing only one non-zero coordinate in accordance with the basis-vector multiplication table (BVMT) defining associative and non-commutative multiplication. There are possible different types of the BVMTs, but in this paper there is used the BVMT of some particular type shown in Table 1, where $\mu \neq 0$. For arbitrary combination of the values $\mu \in GF(p)$ and $\tau \in GF(p)$ Table 1 defines formation of the non-commutative finite ring of four-dimension vectors.

Table 1: The basis-vector multiplication table

$\circ$	$\overrightarrow{e}$	$\overrightarrow{i}$	$\overrightarrow{j}$	$\overrightarrow{k}$
$\overrightarrow{e}$	$\mu\mathbf{e}$	$\mu\mathbf{i}$	$\mu\mathbf{j}$	$\mu\mathbf{k}$
$\overrightarrow{i}$	$\mu\mathbf{i}$	$-\mu^{-1}\tau\mathbf{e}$	$\mathbf{k}$	$-\tau\mathbf{j}$
$\overrightarrow{j}$	$\mu\mathbf{j}$	$-\mathbf{k}$	$-\mu^{-1}\mathbf{e}$	$\mathbf{i}$
$\overrightarrow{k}$	$\mu\mathbf{k}$	$\tau\mathbf{j}$	$-\mathbf{i}$	$-\mu^{-1}\tau\mathbf{e}$

In the defined ring the vector $(\mu^{-1},0,0,0)$ plays the role of the unity element. For implementing the cryptoschemes described in Section 2 it represents interest the multiplicative group Γ of the constructed non-commutative ring. To generate the elements Q and G of sufficiently large orders it is required computing the group order Ω that is equal to the number of invertible vectors. If some vector $A=(a,b,c,d)$ is invertible, then there exists its inverses $A^{-1}=(x,y,z,v)$ for which the following formula holds $A\circ A^{-1}=E=(\mu^{-1},0,0,0)$. This vector equation defines the following system of four linear equations with four unknowns x, y, z, and v:

$$\left\{\begin{array}{rcl} \mu ax-\mu^{-1}\tau by-\mu^{-1}cz-\mu^{-1}\tau dv &=& \mu^{-1} \\ \mu bx+\mu ay-dz+cv &=& 0 \\ \mu cx+\mu az-\tau bv+\tau dy &=& 0 \\ \mu dx-cy+bz+\mu av &=& 0. \end{array}\right.$$

If this system of equations has solution, then the vector (a,b,c,d) is invertible, otherwise it is not invertible. The main determinant of the system is the following one

$$\Delta(A)=\left|\begin{array}{cccc} \mu a & -\mu^{-1}\tau b & -\mu^{-1}c & -\mu^{-1}\tau d \\ \mu b & \mu a & -d & c \\ \mu c & \tau d & \mu a & -\tau b \\ \mu d & -c & b & \mu a \end{array}\right|$$

Computation of the determinant gives

$$\Delta(A)=\left(\mu^2a^2+\tau b^2+c^2+\tau d^2\right)^2.$$

Counting the number of different solutions of the congruence $\Delta(A)\equiv 0 \bmod p$ one can define the number N of non-invertible vectors and then define the

group order $\Omega = p^4 - N$. The indicated congruence has the same solutions as the congruence

$$\mu^2 a^2 + \tau b^2 + c^2 + \tau d^2 \equiv 0 \bmod p. \tag{1}$$

Statement 1. *For prime $p = 4k + 1$, where $k \geqslant 1$, $\mu \neq 0$, and $\tau \neq 0$, the order of the non-commutative group of the four-dimension vectors is equal to $\Omega = p(p-1)(p^2-1)$.*

Proof. For primes $p = 4k + 1$ the number -1 is a quadratic residue, since $(-1)^{(p-1)/2} = (-1)^{2k} \equiv 1 \bmod p$. Therefore there exists number λ such that $\lambda^2 \equiv -1 \bmod p$ and congruence (1) can be represented as follows

$$\begin{aligned} (\mu a)^2 - (\lambda c)^2 &\equiv \tau \left((\lambda b)^2 - d^2\right) \bmod p, \\ (\mu a - \lambda c)(\mu a + \lambda c) &\equiv \tau \left((\lambda b)^2 - d^2\right) \bmod p, \\ \alpha\beta &\equiv \tau \left((\lambda b)^2 - d^2\right) \bmod p, \end{aligned}$$

where $\alpha \equiv \mu a - \lambda c \bmod p$ and $\beta \equiv \mu a + \lambda c \bmod p$. It is easy to see that for each pair of numbers (α, β) satisfying the last congruence correspond unique pair of numbers (a, c) satisfying congruence (1). Therefore the number of solutions of congruence (1) can be computed as number of solutions of the last equation. Two cases can be considered. The first case correspond to condition $(\lambda b)^2 - d^2 \not\equiv 0 \bmod p$ and there exist $(p-1)^2$ of different pairs (b, d) satisfying this condition. For each of such pairs (b, d) for all $(p-1)$ values $\alpha \not\equiv 0 \bmod p$ there exists exactly one value β such that the last congruence holds. Thus, the first case gives $N_1 = (p-1)^3$ different solutions of congruence (1).

The second case correspond to condition $(\lambda b)^2 - d^2 \equiv 0 \bmod p$ which is satisfied with $2p-1$ different pairs (b, d). The left part of the last congruence is equal to zero modulo p in the following subcases i) $\alpha \not\equiv 0 \bmod p$ and $\beta \equiv 0 \bmod p$ ($p-1$ different variants), ii) $\alpha \equiv 0 \bmod p$ and $\beta \not\equiv 0 \bmod p$ ($p-1$ different variants), and iii) $\alpha \equiv 0 \bmod p$ and $\beta \equiv 0 \bmod p$ (one variant). Thus, the subcases gives $2p-1$ different variants of the pairs (a, c), therefore the second case gives $N_2 = (2p-1)^2$ different solutions of congruence (1). In total we have $N = N_1 + N_2 = (p-1)^3 + (2p-1)^2 = p^3 + p^2 - p$ solutions. The value N is equal to the number of non-invertible vectors and defines the group order $\Omega = p^4 - N = p^4 - p^3 - p^2 + p = p(p-1)(p^2-1)$. □

Statement 2. *Suppose prime $p = 4k + 3$, where $k \geqslant 1$, $\mu \neq 0$, $\tau \neq 0$, and the value τ is a quadratic non-residue modulo p. Then the order of the non-commutative group of four-dimension vectors is equal to $\Omega = p(p-1)(p^2-1)$.*

Proof. For primes $p = 4k+3$ the number -1 is a quadratic non-residue, since $(-1)^{(p-1)/2} = (-1)^{2k+1} \equiv -1 \bmod p$. Since the value τ is quadratic non-residue the following formulas hold $\tau^{(p-1)/2} \equiv -1 \bmod p$ and $(-\tau)^{(p-1)/2} \equiv 1 \bmod p$. The last formula shows that there exists number λ such that $\lambda^2 \equiv -\tau \bmod p$ and congruence (1) can be represented as follows

$$\begin{aligned}(\mu a)^2 - (\lambda b)^2 &\equiv (\lambda d)^2 - c^2 \bmod p,\\ (\mu a - \lambda b)(\mu a + \lambda b) &\equiv (\lambda d)^2 - c^2 \bmod p,\\ \gamma\delta &\equiv (\lambda d)^2 - d^2 \bmod p,\end{aligned}$$

where $\gamma \equiv \mu a - \lambda b \bmod p$ and $\delta \equiv \mu a + \lambda b \bmod p$. Then, counting different solutions of the last equation is analogous to counting solutions in the proof of Statement 1. This gives $N = p^3 + p^2 - p$ different solutions of congruence (1) and the group order $\Omega = p(p-1)(p^2-1)$. □

5. Computational experiments and illustrations

Numerous computational experiments have shown that in the case $p = 4k+3$, where $k \geqslant 1$, $\mu \neq 0$, $\tau \neq 0$, when the value τ is a quadratic residue modulo p, the group order also equals to $\Omega = p(p-1)(p^2-1)$. However the formal proof of the last fact have not been found. The experiments have also shown that for given modulus p the structure of the non-commutative group of four-dimension vectors is the same for all non-zero values of the structural coefficients μ and τ. Here under structure of the group it is supposed a table showing the number of different vectors having the same order ω for all possible values ω. In the case of the commutative finite groups of four-dimension vectors the group structure changes with changing values of structural coefficients. The experiments have been performed using different other variants (than Table 1) of the BVMTs defining non-commutative groups of four-dimension vectors and in all cases the same structure and the same group order have been get, for all non-zero values of the structural coefficients.

Defining a group of four-dimension vectors with Table 1 and parameters $\mu = 1$, $\tau = 1$, and $p = 234770281182692326489897$ (it is a 82-bit number) one can easily generate the vectors Q and G having the prime orders $q = g = 117385140591346163244949$ (it is a 81-bit number) and then generate vector $K = G \circ Q \circ G^{-1}$:

$Q = (197721689364623475468796, 104620049500285101666611,$
$913406634520287022930 61, 190338950319800446198610);$

$$G = (44090605376274898528561, 33539251770968357905908,$$
$$628494189939543161994 14, 12193107612899947703 0014);$$
$$G^{-1} = (44090605376274898528561, 20123102941172396858 3989,$$
$$171920862188738010290483, 11283920505369284945 9883);$$
$$K = (19772168936462347546 8796, 12732429403871572708 0605,$$
$$205837389432865711027118, 16940283110252090588 9980).$$

The vectors satisfy the conditions $G \circ Q \neq G \circ Q$ and $K \circ Q \neq Q \circ K$ (see Theorem 1), therefore they can be used to implement the cryptoschemes presented in Sections 2 and 3. It is easy to generate many other different pairs of the vectors Q and G possessing 81-bit prime orders q and g and satisfying the condition of Theorem 1. The least common multiple of all element orders in the constructed group is

$$m = 12939853526188313144336212835389396459316$$
$$92060964758959029747196964 7376.$$

The exponent e of the encryption key for commutative encryption algorithm can be selected as $e = 7364758519536461719117$. Then the exponent of the decryption key is computed using formula $d = e^{-1} \bmod p$:

$$d = 89694276304164823519044988689552324310903862 02$$
$$188967381064403670926661.$$

Accordingly to the algorithm for computing the private key from the public one, which is described in the next section, the 80-bit security of the proposed cryptoschemes is provided in the case of 80-bit primes q and g. In this case the difficulty of the computation of the public key from the private one does not exceed 5800 multiplications modulo 80-bit prime. In the corresponding cryptoschemes of the public encryption and of the public key agreement, which are based on elliptic curves, the difficulty of computing the public key from the private one is equal to about 2400 multiplications modulo 160 prime. Taking into account that difficulty of the modulo multiplication is proportional to squared length of the modulus one can estimate that the proposed cryptoschemes are about 1.6 times faster than analogous schemes implemented using elliptic curves. Besides, performance of the proposed cryptoschems can be significantly enhanced defining computation of the secrete element W as a sum of small powers of G, for example, $W = \sum_{s=1}^{6} \rho_s G^{t_s}$, where $\rho_s \in GF(p)$, $t_s \leqslant 15$, $s = 1, 2, \ldots, 6$.

6. Algorithm for computing the private key

Using the known parameters Q and G having the orders q and $g = q$ the following algorithm finds the private key (w, x) from the public one $Y = G^w \circ Q^x \circ G^{-w}$.

1. For all values $j = 1, 2, \ldots, q$ compute vectors $T(j) = G^j \circ Y \circ G^{-j}$ (difficulty of this step is $2q$ vector multiplications).
2. Order the table computed at the step 1 accordingly to the values $T(j)$ (difficulty of this step is $q \log_2 q$ comparison operations).
3. Set counter $i = 1$ and initial value of the vector $V = (\mu^{-1}, 0, 0, 0)$.
4. Compute the vector $V \leftarrow V \circ Q$.
5. Check if the value V is equal to some of the vectors $T(j)$ in the ordered table. If there is some vector $T(j') = V$, then deliver the private key $(w, x) = (j', i)$ and STOP. Otherwise go to step 6.
6. If $i \neq q$, then increment counter $i \leftarrow i + 1$ and go to step 4. Otherwise STOP and output the message INCORRECT CONDITION. (Difficulty of steps 5 and 6 does not exceed q vector multiplication operations and $q \log_2 q$ comparison operations.)

Overall the time complexity of this algorithm is about $3q$ vector multiplication operations and $2q \log_2 q$ comparison operations, i.e. the time complexity is $O(q)$ operations, where $O(\cdot)$ is the order notation. The algorithm requires storage for q vectors and for the same number of $|p|$-bit numbers, i.e. the space complexity is $O(q)$.

This algorithm shows that the 80-bit security of the proposed cryptosystems can be provided selecting 80-bit primes q and g. Such prime orders of the vectors Q and G can be get using 81-bit primes p.

Is seems that element G having composite order can be used in the cryptoschemes described above and this will give higher security, while using the given fixed modulus p. However this item represents interest for independent research.

7. Conclusions

Results of this paper shows that finite non-commutative groups represent interest for designing fast public key agreement schemes, public encryption

algorithms, and commutative encryption algorithms. Such cryptoschemes are fast and the hard problem they are based on is expected to have exponential difficulty using both the ordinary computers and the quantum ones.

Theorem 1 is useful for justification of the selection elements Q and G while defining parameters of the cryptoschemes. The proposed non-commutative finite group of the four-dimension vectors seems to be appropriate for practical implementation of the proposed schemes. We have proved the formulas for computing the order of such groups in majority of cases. Unfortunately for a quarter of cases the formal proof have not been found and this item remains open for future consideration. However the proved cases covers the practical demands while implementing the proposed cryptoscheme in the case of using the constructed non-commutative groups of four-dimension vectors.

It is easy to show that there exists multiplicative homomorphism of the proposed groups of four-dimension vectors into the finite field over which the vector space is defined. Therefore in the case of using the constructed finite non-commutative group in the proposed cryptoschemes one should take into account the existing homomorphism. To prevent attacks using this homomorphism the large prime orders g and q of the elements G and Q should satisfy conditions $g|p+1$ and $q|p+1$ (i.e., $g \not| p-1$ and $q \not| p-1$, since $g > 2$ and $q > 2$).

References

[1] **I. Anshel, M. Anshel and D. Goldfeld**, *An algebraic method for public key cryptography*, Math. Research Letters **6** (1999), 287 – 291.

[2] **K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang and C. Park**, *New public-key cryptosystems using Braid groups*, Advances in Cryptology – CRYPTO 2000, Lecture Notes Computer Sci. **1880** (2000), 166 – 183.

[3] **E. Lee and J. H. Park**, *Cryptanalysis of the public key encryption based on Braid groups*, Advances in Cryptology – EUROCRYPT 2003, Lecture Notes Computer Sci. **2656** (2003), 477 – 489.

[4] **N. A. Moldovyan and P. A. Moldovyanu**, *New primitives for digital signature algorithms: vector finite fields*, Quasigroups and Related Systems **18** (2010), 11 – 20.

[5] **P. W. Shor**, *Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer*, SIAM J. Computing **26** (1997), 1484−1509.

[6] **G. K. Verma**, *A proxy blind signature scheme over Braid groups*, Int. J. Network Security **9** (2009), 214 – 217.

Received January 18, 2010

St. Petersburg Institute for Informatics and Automation
Russian Academy of Sciences
14 Liniya, 39
St. Petersburg 199178
Russia
E-mail: mdn.spectr@mail.ru