Quasigroups and Related Systems **18** (2010), 177 – 186

Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms

Dmitriy N. Moldovyan and Nikolay A. Moldovyan

Abstract. There are considered attacks on cryptoschemes based on the recently proposed hard problem called hidden conjugacy search problem (HCSP), defined over finite non-commutative groups. It is shown that using homomorphisms of the non-commutative finite group into finite fields $GF(p^s)$, $s \geqslant 1$, in some cases the HCSP can be reduced to two independent problems: discrete logarithm and conjugacy search problem. Two methods for preventing such attacks are proposed. In the first method there are used elements of the order p. The second method uses non-invertible elements and relates to defining the HCSP over the finite non-commutative ring.

1. Introduction

Since the factorization and finding discrete logarithm problems (DLP) can be solved in polynomial time on a quantum computer [6] new hard problems attracts attention of the researchers in the cryptology area. One of such problems called conjugacy search problem (CSP) [1, 2] is defined over finite non-commutative groups as follows. Suppose Γ is a finite non-commutative group, $G, Y \in \Gamma$, $X \in \Gamma_c$, where Γ_c is a commutative subgroup of Γ, and $Y = XGX^{-1}$. Given G and Y find $X \in \Gamma_c$. Recently [4] a novel hard problem that can be called the hidden conjugacy search problem (HCSP) has been applied to design the key agreement protocol, commutative encryption algorithm, and public-key encryption algorithm. The HCSP is defined as follows. Given G and Y recover integer x and element $X \in \Gamma_c$ such that $Y = XG^xX^{-1}$. If the value x is known, the HCSP is reduced to CSP. If the element X is known, the HCSP is reduced to DLP.

2010 AMS Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: difficult problem, finite group, homomorphism, non-commutative group, non-commutative ring, public-key cryptoscheme

Present paper introduces two attacks on the HCSP-based cryptoschemes that are implemented using finite non-commutative groups Γ of the m-dimensional vectors and matrices $m \times m$ defined over the finite ground field $GF(p)$. It is described a general homomorphism of the finite commutative and non-commutative groups of vectors into $GF(p)$. The first attack uses the homomorphism of the Γ into $GF(p)$ to reduce the HCSP to two independent problems, DLP and CSP. The second attack uses the hypothetic homomorphisms $\psi^{(s)}$ of the Γ into $GF(p^s)$, where $s \leqslant m$ to reduce the HCSP to two independent problems, DLP and CSP. Methods for preventing this attack are proposed. To prevent the both attacks there are two approaches. The first approach uses the element G possessing the order equal to p. The second approach uses the non-invertible element G of the finite ring $\mathbf{R}$ containing the group Γ. In the first case $\forall s \in \{1,\ldots,m\}$ the homomorphism $\psi^{(s)} : \Gamma \rightarrow GF(p^s)$ maps the element Y into the unity element of $GF(p^s)$ for all $s \leqslant m$. In the second case $\forall s \in \{1,\ldots,m\}$ the homomorphism $\psi^{(s)} : \mathbf{R} \rightarrow GF(p^s)$ maps the element Y into zero of $GF(p^s)$.

2. Homomorphisms of the finite groups and rings

Finite rings $\mathbf{R}$ of m-dimensional vectors are defined over the ground field $GF(p)$, where p is a prime. Suppose $\mathbf{e}$, $\mathbf{i}$, ..., $\mathbf{w}$ be some m basis vectors and $a, b, \ldots, z \in GF(p)$ are coordinates. Then the vectors are denoted as $a\mathbf{e} + b\mathbf{i} + \cdots + z\mathbf{w}$ or as $(a, b, \ldots, z)$. The terms like $\tau\mathbf{v}$, where $\tau \in GF(p)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \ldots, \mathbf{w}\}$, are called *components* of the vector. The addition of two vectors is defined in the natural way, the multiplication by the formula

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

where in the last expression each product of two basis vectors should be replaced by some basis vector $\mathbf{v}$ or by a vector $\tau\mathbf{v}$ in accordance with some given table called the *basis-vector multiplication table* (BVMT) such that operation $\circ$ is associative. There are possible different types of the BVMTs defining commutative [3] and non-commutative rings $\mathbf{R}$ [4]. In general case there exists the homomorphism $\mathbf{R} \rightarrow GF(p^s)$. Indeed, suppose the vector A is invertible, then the vector equation

$$A \circ X = V \tag{1}$$

with unknown X has unique solution for arbitrary vector V: $X = A^{-1} \circ V$. Equation (1) can be rewritten as a system of m linear equations over $GF(p)$ with m unknowns that are coordinates of the vector X. Let Δ_A be the main determinant of the system of equation relating to formula (1). The determinant Δ_A is completely defined by coordinates of the vector A.

Theorem 1. *The determinant Δ_A defines the multiplicative homomorphism $\psi(A) = \Delta_A$ of the ring $\mathbf{R}$ into the field $GF(p)$.*

Proof. If A is not invertible, then $\Delta_A = 0$, i.e., all non-invertible vectors are mapped into zero of $GF(p)$. Let us consider the vector equation (1) with invertible vector A and arbitrary vector V. For all vectors $V \in \{V\}$, where $\{V\}$ denotes the considered vector space, equation (1) has unique solution, therefore $\Delta_A \neq 0$ and multiplication of the vector A by all vectors V of the considered vector space $\{V\}$ defines a linear transformation T_A of $\{V\}$. The matrix M_A of coefficients of the system of linear equations corresponding to the vector equation (1) can be put into correspondence to T_A. Another invertible vector B defines the transformation T_B corresponding to analogous matrix M_B. The vector multiplication operation in $\mathbf{R}$ is associative, therefore we have

$$(A \circ B) \circ V = A \circ (B \circ V). \tag{2}$$

The left part of (2) represents the linear transformation $T_{A \circ B}$ corresponding to the matrix $M_{A \circ B}$. The right part of (2) is the superposition $T_B * T_A$ of linear transformations T_B and T_A, therefore we have

$$T_{A \circ B} = T_B * T_A \Rightarrow M_{A \circ B} = M_A M_B \Rightarrow \Delta(A \circ B) = \Delta_A \Delta_B.$$

The last expression means that the mapping $\psi : A \to \Delta_A$ is the multiplicative homomorphism of the multiplicative group Γ of the ring $\mathbf{R}$ into the field $GF(p)$. Since for arbitrary non-invertible vectors A and B we have $\Delta_A = 0$ and $\Delta_B = 0$, the last fact means that $\psi : A \to \Delta_A$ is the multiplicative homomorphism of $\mathbf{R}$ into $GF(p)$. Theorem 1 is proved. □

In a particular case when the ring $\mathbf{R}$ is a vector finite field $GF(p^m)$ [5] the homomorphism defined by Theorem 1 is the same mapping as norm homomorphism defined for the extension finite fields. Below it is also used the following well known fact. If $\mathbf{R}$ is a finite ring of matrices M defined over $GF(p)$, then mapping ψ' such that $\forall M : \ \psi'(M) \to \Delta_M$, where Δ_M is the determinant of the matrix M, represents the multiplicative homomorphism $\psi' : \ \mathbf{R} \to GF(p)$.

3. The fist attack

Using the homomorphism ψ in the case of the group of vectors (or ψ' in the case of group of matrices) described in Section 2 the following attack on cryptoschemes based on the HCSP [4] is possible. The homomorphism ψ maps the equation over the non-commutative group Γ used for computing the public key $Y = XG^xX^{-1}$, where X and x are the secret key, into the following equation over the field $GF(p)$

$$\psi(Y) = \psi(X)\,(\psi(G))^x\,(\psi(X))^{-1} = (\psi(G))^x\,. \tag{3}$$

There are possible the following three cases.

1. The order of the value $\psi(G) \in GF(p)$ is equal to the order of the element $G \in \Gamma$. In this case the secret value x can be found solving the DLP in $GF(p)$. Then the secret element X can be found solving the CSP. Thus, in this case the HCSP is reduced to two independent well known hard problems and the attack can be considered as successful one.

2. The order of the value $\psi(G) \in GF(p)$ is less than the order of the element $G \in \Gamma$. In this case the partial information about the secret value x can be found solving the DLP in $GF(p)$, i.e., solving the equation $\psi(Y) = (\psi(G))^{x'}$ one can found the value $x' \equiv x \bmod \omega_{\psi(G)}$, where $\omega_{\psi(G)}$ is the order of the value $\psi(G) \in GF(p)$. The last means that the difficulty of the HCSP is reduced.

3. The homomorphism ψ maps the element G to the unity element of the field $GF(p)$ and equation (3) degenerates into trivial equation $1 = 1^x$, from which no information about the secret value can be obtained. In this case the considered attack is not efficient to reduce the HCSP.

Thus, in the design of the cryptoschemes based on the HCSP it should be used the element G such that $\psi(G) = 1$ and the order $\omega_{\psi(G)}$ is a sufficiently large prime [4]. Selection of such element G depends on the order of the concrete group used for constructing a cryptoscheme based on the HCSP. The following theorem is very useful to select the suitable element G.

Theorem 2. *If the element G has the order ω_G such that* $\gcd(\omega_G, p-1) = 1$, *then* $\psi(G) = 1$.

Proof. Suppose E is the unity element of the group Γ and $\psi(G) \neq 1$. Then $\psi\left(G^{\omega_G}\right) = \psi(E) = 1$ and $\psi\left(G^{\omega_G}\right) = (\psi(G))^{\omega_G}$ imply $(\psi(G))^{\omega_G} = 1$. Thus $\gcd(\omega_G, p-1) \neq 1$, which contradicts to the assumption. □

We use Theorem 2 for a selection of the element G in the finite non-

commutative group Γ of four-dimensional vectors with multiplication defined by BVMT presented in Table 1.

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

Table 1. The basis-vector multiplication table ($m = 4$) [4].

The order of this group is $\Omega = p(p-1)^2(p+1)$ (cf. [4]). In this case it is possible to generate a 90-bit prime $p = 2q - 1$ such that q is a prime. Then we can generate the vector G having sufficiently large prime order $\omega_G = q$ satisfying the condition $\gcd(\omega_G, p-1) = 1$ (cf. [4]). In the case of groups Γ corresponding to matrices $m \times m$ and m-dimensional vectors the choice of G satisfying Theorem 2 is relatively simple. Such choice prevents the attacks using the considered homomorphism. However there are potentially possible some other ways for reducing the HCSP to independent DLP and CSP, which use multiplicative homomorphisms $\psi^{(s)} : \Gamma \to GF(p^s)$, where $s \leqslant m$.

4. The second attack

Taking into account possibility to define the HCSP over different variants of the finite non-commutative groups it is reasonable to consider some attack on the HCSP-based cryptoschemes, in which some other potentially possible multiplicative homomorphisms can be exploited. Such attacks are also oriented to reducing the HCSP to two independent hard problems each of which is significantly less difficult than HCSP. In the second type of attacks there is assumed existence of some hypothetic multiplicative homomorphisms $\psi^{(s)} : \Gamma \to GF(p^s)$, where the cases $s \leqslant m$ provide sufficient generality for finite groups of vectors and matrices over the field $GF(p)$. Indeed, in the case of matrices the order group is described by the formula

$$\Omega_{m\times m} = \prod_{i=0}^{m-1} p^i \left(p^{m-i} - 1\right). \tag{4}$$

Since order of the multiplicative group of $GF(p^s)$ is equal to $p^s - 1$, the values $s = 1, 2, \ldots, m$ cover all cases that can be used in the second attack.

Like in the case of the first attack described in Section 3 one can formulate the following statement.

Theorem 3. *If the element G has the order ω_G such that* $\gcd(\omega_G, r) = 1$, *where* $r = \prod_{i=1}^{m} (p^m - 1)$, *then* $\forall s \leqslant m$ *the following formula holds* $\psi^s(G) = 1$.

Proof. The proof is analogous to the proof of Theorem 2. □

It is remarkable that order of the non-commutative group Γ in the case of matrices and in many cases of vectors contains the divisor p. This fact provides the first method to provide security of the HCSR-based cryptoschemes against attacks of the second type. The method consists in using element G having the order $\omega_G = p$. Then, accordingly to Theorem 3 for all $s \leqslant m$ the following mappings hold: $\psi^{(s)}(G) = 1$ and $\psi^{(s)}(Y) = 1$, therefore the considered hypothetic homomorphisms become inefficient to reduce the difficulty of the HCSP.

The number of elements possessing the order equal to p is comparatively small and some special properties of the groups Γ are to be exploited to find the elements of such order. In the case of finite non-commutative group of four-dimensional vectors with the group operation defind with Table 1 different elements having order p can be computed (and applied as element G) using the following statement.

Statement 1. *Suppose Γ is the finite group of four-dimensional vectors over the field $GF(p)$ and the group operation is defined with Table 1. Then the vectors (μ^{-1}, b, c, d) have order equal to p, if the coordinates $b, c,$ and d satisfy condition*

$$\tau b^2 + c^2 + \tau d^2 \equiv 0 \bmod p. \tag{5}$$

Proof. Squaring the vector (μ^{-1}, b, c, d) gives

$$(\mu^{-1}\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^2 = \left(\mu^{-1} - \mu^{-1}(\tau b^2 + c^2 + \tau d^2)\right)\mathbf{e} + 2b\mathbf{i} + 2c\mathbf{j} + 2d\mathbf{k}.$$

Taking into account condition (5) we get $(\mu^{-1}, b, c, d)^2 = (\mu^{-1}, 2b, 2c, 2d)$. Suppose for integer $k > 1$ the following formular holds

$$(\mu^{-1}, b, c, d)^k = (\mu^{-1}, kb, kc, kd). \tag{6}$$

Then

$(\mu^{-1}, b, c, d)^{k+1} = (\mu^{-1}, b, c, d)^k \circ (\mu^{-1}, b, c, d)$

$= (\mu^{-1}, kb, kc, kd) \circ (\mu^{-1}, b, c, d) = \left(\mu^{-1}, (k+1)b, (k+1)c, (k+1)d\right)$.

Therefore formula (6) holds for all $k > 1$. If $k = p$, then $(\mu^{-1}, b, c, d)^p = (\mu^{-1}, pb, pc, pd) = E$, where $E = (\mu^{-1}, 0, 0, 0)$ is the unity element of Γ. If $k < p$, then $(\mu^{-1}, b, c, d)^k \neq E$. Therefore the value p is the order of the vector (μ^{-1}, b, c, d). Statement 1 is proved. □

Another method preventing attacks of the second type consists in using non-invertible elements N of the finite ring $\mathbf{R}$ containing the group Γ, where as G is used some non-invertible element N such that the set $\{N, N^2, \ldots, N^i, \ldots\}$ contains sufficiently large number of different elements $N^i \in \mathbf{R}$. Actually it is considered the variant of the HCSP defined over the finite non-commutative ring and it is supposed the HCSP-based cryptosystems exploit the public key Y computed as $Y = XN^xX^{-1}$. Applying the homomorphisms $\psi^{(s)}$ to the last equation gives $\psi^{(s)}(Y) = 0$, since $\psi^{(N)} = 0$. Thus, this method is also efficient to prevent attacks of the second type.

Existence of the elements N suitable for defining the HCSP over finite non-commutative rings and designing the public key cryptosystems is demonstrated in the case of the 2×2 matrices by the following statement.

Statement 2. *For the 2×2 matrix $N_{2\times 2}$ defined over the ground field $GF(p)$ for all positive integers $i \geqslant 2$ the following formula holds*

$$N_{2\times 2}^i = \begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix}^i = \begin{pmatrix} \lambda^{i-1}a & \lambda^{i-1}b \\ \lambda^{i-1}c & \lambda^{i-1}(\lambda - a) \end{pmatrix}, \tag{7}$$

where $a = \lambda/2 \pm \sqrt{(\lambda/2)^2 - bc}$.

Proof. It is easy to show that $\begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix}^2 = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda(\lambda - a) \end{pmatrix}$.
If (7) holds for some $i \geqslant 2$, then for $i + 1$ we have

$$\begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix}^{i+1} = \begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix}^i \begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix}$$
$$= \begin{pmatrix} \lambda^{i-1}a & \lambda^{i-1}b \\ \lambda^{i-1}c & \lambda^{i-1}(\lambda - a) \end{pmatrix} \begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix} = \begin{pmatrix} \lambda^i a & \lambda^i b \\ \lambda^i c & \lambda^i(\lambda - a) \end{pmatrix},$$

which completes the proof. □

Suppose the order of $\lambda \in GF(p)$ is ω_λ. Then powers of the matrix $N_{2\times 2}$ generate ω_λ different non-invertible matrices. Selecting a prime p such that $p = 2q + 1$, where q is a prime, and λ having the order $\omega_\lambda = q$ one can define different variants of the matrix $N_{2\times 2}$ suitable for application in the method for preventing attacks of the second type.

Using the ring $\mathbf{R}_{2\times 2} \supset \Gamma$ of the 2×2 matrices and the matrix $N_{2\times 2}$ defined over the ground field with characteristic $p > 2^{80}$ one can define the key agreement scheme as follows. Some uses A and B computes their public keys $Y_A = X_A N_{2\times 2}^{x_A} X_A^{-1}$ and $Y_B = X_B N_{2\times 2}^{x_B} X_B^{-1}$, where (X_A, x_A) is the private key of the user A and (X_B, x_B) is the private key of the user B. Then the first and second users compute the values K_{AB} and K_{BA}, correspondingly, as follows

$$K_{AB} = X_A Y_B^{x_A} X_A^{-1} = X_A \left(X_B N_{2\times 2}^{x_B} X_B^{-1}\right)^{x_A} X_A^{-1} = X_A X_B N_{2\times 2}^{x_B x_A} X_B^{-1} X_A^{-1}.$$

$$K_{BA} = X_B Y_A^{x_B} X_B^{-1} = X_B \left(X_A N_{2\times 2}^{x_A} X_A^{-1}\right)^{x_B} X_B^{-1} = X_B X_A N_{2\times 2}^{x_A x_B} X_A^{-1} X_B^{-1}.$$

In this scheme it is assumed that X_A and X_B are selected from some specified commutative subgroup $\Gamma_c \subset \Gamma \subset \mathbf{R}_{2\times 2}$, therefore $K_{21} = K_{12} = K$, i.e., each of the users computes the same secret value K. Security of the described cryptoscheme is defined by difficulty of the HCSP over $\mathbf{R}_{2\times 2}$, which cannot be reduced with attacks of the second type (note that the second type attacks cover the case of the fist attack described in Section 3).

5. Discussion and conclusion

Consideration of the multiplicative homomorphisms of the non-commutative finite rings $\mathbf{R} \supset \Gamma$ (or groups Γ) is an important item of the investigation of the difficulty of the HCSP defined over $\mathbf{R}$ (or over Γ), which relates to security estimation of the HCSP-based cryptoschemes. Using the matrices and vectors defined over the field $GF(p)$ for implementing the HCSP-based cryptoschemes is very attractive. In the case of matrices M the multiplicative homomorphism $\psi' : M \to \Delta_M$ is well known. A general multiplicative homomorphism ψ of the vector finite rings into $GF(p)$ have been described. If the ring of m-dimensional vectors represents the field $GF(p)$ [5] the homomorphism ψ coincide with the norm homomorphism, more detailed consideration of this fact is out of the scope of this paper though. In Section 3 the mentioned homomorphisms have been used in the first attack proposed against the HCSP-based cryptoschemes. To prevent this attack the condition for selecting parameters of the HCSP have been proposed.

The considered attacks of the second type relates to using hypothetic homomorphisms $\psi^{(s)} : \mathbf{R} \to GF(p^s)$, where $s \leqslant m$. These attacks are more powerful and cover the case of the first attack. While designing concrete cryptoschemes their parameters are selected depending on the order Ω of the multiplicative group Γ of the ring $\mathbf{R}$. In the case of matrices the formula

describing the order Ω is known. However using the $m \times m$ matrices is limited by sufficiently small values m, since the size $|Y|$ of the public key Y increases approximately as $m^2|p|$, where $|p|$ denotes the size of p, and to provide the security of the HCSP-based cryptoschemes the order Ω should contain the prime divisor q having the size $|q| \geqslant 80$ bits. The value of q is limited by p^{m-1}, therefore $|q|(m-1)|p|$ and $|Y| \approx m^2(m-1)^{-1}|q|$ (the last holds for prime m; for composite m the increase of $|Y|$ is more significant).

In the case of the m-dimensional vectors the parameters of the ring $\mathbf{R}$ can be selected so that the secure size of the public key is approximately equal to $4|q| \approx 320$ bits for small ($m = 4$) and large ($m = 8, 16, 32$) values of m. Table 2 presents the comparison of the size of public key in the case of diferent dimensions of the matrices and vectors. Practical interest to use the large values m is connected with the fact that in the case of vectors the computational difficulty of the multiplication operation decreases significantly with increasing value of m. However construction of the non-commutative finite vector groups for large values of m relates to less investigated problem. Table 3 presents an example of the BVMT for the case $m = 8$. If structural coefficient $\tau \in GF(p)$ is such that equation $x^2 = \tau$ has no solution in $GF(p)$, then the order of the group Γ of eight-dimensional vectors, which is defined with this BVMT, contains divisor $p^2 + 1$. It is easy to generate values p such that $q = \left(p^2 + 1\right)/2$ is prime (for example, for $p = 307970789149$ and $\tau = 2$ we have $q = 47423003484528908072101$). Investigation of different variants of the vector groups Γ for $m = 6, 8, 12, 16, 20, 28, 32$ relates to a separate problem.

Elements of Γ	dimension	$\lvert p\rvert$, bits	$\lvert Y\rvert$, bits
matrices	2×2	80	320
matrices	3×3	40	360
matrices	4×4	40	640
matrices	5×5	20	500
matrices	6×6	20	720
matrices	7×7	14	686
vectors	4	80	320
vectors	8	40	320
vectors	16	21	336
vectors	32	11	352

Table 2. A rough estimation of the public-key size of the HCSP-based cryptoschemes possessing the 80-bit security.

$\circ$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$	$\mathbf{v}$	$\mathbf{w}$	$\mathbf{x}$
$\mathbf{e}$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$	$\mathbf{v}$	$\mathbf{w}$	$\mathbf{x}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{e}$	$\mathbf{k}$	$-\mathbf{j}$	$\mathbf{v}$	$-\mathbf{u}$	$\mathbf{x}$	$-\mathbf{w}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$-\mathbf{e}$	$\mathbf{i}$	$\mathbf{w}$	$-\mathbf{x}$	$-\mathbf{u}$	$\mathbf{v}$
$\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	$-\mathbf{e}$	$\mathbf{x}$	$\mathbf{w}$	$-\mathbf{v}$	$-\mathbf{u}$
$\mathbf{u}$	$\mathbf{u}$	$\mathbf{v}$	$\mathbf{w}$	$\mathbf{x}$	$\tau\mathbf{e}$	$\tau\mathbf{i}$	$\tau\mathbf{j}$	$\tau\mathbf{k}$
$\mathbf{v}$	$\mathbf{v}$	$-\mathbf{u}$	$\mathbf{x}$	$-\mathbf{w}$	$\tau\mathbf{i}$	$-\tau\mathbf{e}$	$\tau\mathbf{k}$	$-\tau\mathbf{j}$
$\mathbf{w}$	$\mathbf{w}$	$-\mathbf{x}$	$-\mathbf{u}$	$\mathbf{v}$	$\tau\mathbf{j}$	$-\tau\mathbf{k}$	$-\tau\mathbf{e}$	$\tau\mathbf{i}$
$\mathbf{x}$	$\mathbf{x}$	$\mathbf{w}$	$-\mathbf{v}$	$-\mathbf{u}$	$\tau\mathbf{k}$	$\tau\mathbf{j}$	$-\tau\mathbf{i}$	$-\tau\mathbf{e}$

Table 3. The basis-vector multiplication table for case $m = 8$.

References

[1] **D. Grigoriev, V. Shpilrain**, *Authentication from matrix conjugation*, Groups-Complexity-Cryptology **1** (2009), 199 – 205.

[2] **Ko Kihyoung, Lee Sangjin, Cha Jaechoon, Choi Dooho**, *Cryptosystems based on non-commutativity*, Patent Application # WO2001KR01283. Publication # WO03013052 (A1), February 13, 2003.

[3] **N. A. Moldovyan**, *Fast signatures based on non-cyclic finite groups*, Quasigroups and Related Systems **18** (2010), 83 – 94.

[4] **D. N. Moldovyan**, *Non-commutative finite groups as primitive of public-key cryptoschemes*, Quasigroups and Related Systems **18** (2010), 165 – 176.

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

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

Received January 18, 2010

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