Quasigroups and Related Systems **30** (2022), 287 – 298

https://doi.org/10.56415/qrs.v30.24

Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations

Nikolay A. Moldovyan

Abstract. A new-type algebraic digital signature schemes on non-commutative associative algebras are developed using technique of performing exponentiation operations in a hidden group. The signature contains two elements: a randomization integer e and a vector S. The used verification equations are characterized in multiple entries of the signature element S. The post-quantum security of the introduced signature algorithms is provided by the computational difficulty of solving a system of many quadratic equations in many variables, like in the public-key multivariate cryptosystems. However in the former case the quadratic equations are set over the finite fields having the order of significantly larger size.

1. Introduction

One of current challenges in the area of post-quantum cryptography reates to the development of practical digital signature algorithms [15, 2]. Recently [6, 10, 13] several signature schemes on finite non-commutative associative algebras (FNAAs) had been propsed. In that schemes, which are based on computational complexity of so called hidden discrete logarithm problem (HDLP), the exponentiation operations in a hidden group are performed, when generating the public key and the signature. Since there is a discrete logarithm problem, although in a hidden group, there are certain difficulties in justifying post-quantum security. The latter are associated

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50

Keywords: non-commutative algebra, finite associative algebra, hidden group, post-quantum cryptography, multivariate cryptography, public-key cryptoscheme, signature scheme.

This work was partially supported by RFBR (project No. 21-57-54001-Viet_a) and by the budget theme No. FFZF-2022-0007.

with the potential opportunity to find algebraic methods for reducing the HDLP to the usual discrete logarithm problem that can be solved in polynomial time on a quantum computer [4, 17].

Multivariate cryptography [3, 18] suggests various public-key cryptosystems that are based on the hardness of solving systems of many quadratic equations in many variables. The hypothetic quantum computer is not efficient to solve the latter type problems, therefore the multivariate public-key cryptographic algorithms are post-quantum. However, the maltivariate signature algorithms are not practical because of very large sizes of public and seret keys.

The present paper introduces a new signature algorithms with a hidden group in which the exponentiation operations are executed. However, the proposed signature algorithm is not attributed to the HDLP-based cryptoschemes, since its security is based on the computational hardness of solving the systems of many quadratic equations with many unknowns.

2. The used FNAAs

Suppose in a finite m-dimensional vector space over the field $GF(p)$ an additional operation, namely, the vector multiplication that is distributive at the right and at the left relatively the addition operation, is defined. Then one gets a finite m-dimensional algebra. Some algebra element (m-dimensional vector) A can be denoted in the following two forms: $A = (a_0, a_1, \ldots, a_{m-1})$ and $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, where $a_0, a_1, \ldots, a_{m-1} \in GF(p)$ are called coordinates; $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are basis vectors.

The vector multiplication operation of two m-dimensional vectors A and B is defined as follows:

$$AB = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j (\mathbf{e}_i \mathbf{e}_j),$$

where every of the products $\mathbf{e}_i \mathbf{e}_j$ is to be replaced by a single-component vector $\lambda \mathbf{e}_k$, where $\lambda \in GF(p)$, indicated in the cell at the intersection of the ith row and jth column of so called basis vector multiplication table (BVMT) like Tables 1 and 2. To define associative vector multiplication operation the BVMT should define associative multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$:

$$(\mathbf{e}_i \mathbf{e}_j)\, \mathbf{e}_k = \mathbf{e}_i\, (\mathbf{e}_j \mathbf{e}_k)\,.$$

Table 1: The BVMT for defining the 4-dimensional FNAA ($\lambda \neq 1$).

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\lambda\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\lambda\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_3$

In the developed signature algorithms, the FNAAs defined by Tables 1 and 2 are used as algebraic supports. The 4-dimensional FNAA had been used earlier in [12] as algebraic support of a HDLP-based signature scheme. This algebra contains the two-sided global unit

$$E = \left(\frac{1}{1-\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{1}{\lambda-1}\right).$$

A 4-dimensional vector A of the algebra, coordinates of which satisfy the condition

$$a_0 a_1 \neq a_2 a_3, \tag{1}$$

is invertible, i.e., for a vector of such a kind there exists the vector A^{-1} such that the condition $A \circ A^{-1} = A^{-1} \circ A = E$ holds true. If $a_0 a_1 = a_2 a_3$, then the vector A is non-invertible.

The 6-dimensional FNAA is obtained as a particular case defined by the unified method for constructing the FNAAs of arbitrary even dimensions, which had been proposed in [5]. The used 6-dimensional FNAA contains the global two-sided unit $E = (1, 0, 0, 0, 0, 0)$. The scalar vectors have the form $(j, 0, 0, 0, 0, 0)$, where $j = 1, 2, \ldots p-1$. A vector $G = (g_0, g_1, g_2, g_3, g_4, g_5)$ is invertible, if its coordinates satisfy the following invertibility condition [5]:

$$\begin{aligned} &\frac{1}{4}((g_0 + g_2 + g_4)^2 - \lambda\,(g_1 + g_3 + g_5)^2)\times \\ &\times ((g_0 - g_2)^2 + (g_0 - g_4)^2 + (g_2 - g_4)^2 - \\ &- \lambda\,(g_1 - g_3)^2 - \lambda\,(g_1 - g_5)^2 - \lambda\,(g_3 - g_5)^2)^2 \neq 0. \end{aligned} \tag{2}$$

Each of the used FNAAs contains sufficiently large number of commutative groups of orders $(p-1)^2$, $p^2 - 1$, and $p(p-1)$. The developed signature schemes are not based on the HDLP, therefore, the existance of a prime divisor of the order of the hidden group is not a strict requirement that is

Table 2: The BVMT setting the used 6-dimensional FNAA ($\lambda \neq 0$).

$\cdot$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$

critical for providing security. However, to have possibility to reduce the computational complexity of the signature generation procedure the used FNAAs are defined over the ground finite field $GF(p)$ with the prime order $p = 2q+1$, where q is also a prime. In the case $m = 4$ ($m = 6$) it is supposed to use the prime q having the size 128 bits (96 bits).

In each of two developed signature algorithms selection of a commutative hidden group is performed as generation of a random minimum generator system $<G, H>$, which includes two mutually permutable vectors of the same order equal to q, as follows:

1. Using the invertibility condition (1) in the case $m = 4$ or (2) in the case $m = 6$, select at random an invertible vector R.

2. Compute the vector $G' = R^{p(p+1)}$.

3. If the vector G' is a scalar vector, then go to step1.

4. Select a random non-negative integer k ($k < q$) and generate a primitive element α modulo p. Then compute the scalar vector $L = \alpha E$ and the vector $H' = G'^k L$.

5. Compute the vectors $G = G'^2$ and $H = H'^2$ each of which has order q.

6. Output the pair of vectors $<G, H>$ as a minimum generator system of a hidden group possessing 2-dimensonal cyclicity and having order q^2.

3. The first signature scheme

The public key is generated as a set of four 4-dimensional vectors Y, Z, U, and W as follows:

1. Generate at random a minimum generator system $<G, H>$ of a hidden group $\Gamma_{<G,H>}$ of the order q^2.

2. Using the invertibility condition (1), generate random invertible vectors A and B satisfying the following inequalities $AB \neq BA$, $AG \neq GA$, and $BG \neq GB$. Then calculate the vectors A^{-1} and B^{-1}.

3. Generate random integers $x_1, x_2 \in GF(p)$ and calculate the vectors Y, Z, U, and W as follows:

$$\begin{aligned} Y &= AGB, \quad & Z &= AG^{x_1}B; \\ U &= AHB, \quad & W &= AH^{x_2}A^{-1}. \end{aligned} \tag{3}$$

Since the size of the prime p equals to 129 bits, the size of public key is equal to ≈ 2064 bits (258 bytes). The integers x_1, and x_2 and the vectors G, H, A^{-1}, and B^{-1} represent a private key having the size equal to ≈ 2320 bits (≈ 290 bytes).

Using the private key $\left(x_1, x_2, G, H, A^{-1}, B^{-1}\right)$ and some specified 384-bit hash-function f, one can generate a signature to the electronic document M as follows:

The signature generation procedure.

1. Generate a random natural numbers k ($k < q$) and t ($t < q$). Then calculate the vector

$$R = AG^kH^tA^{-1}.$$

2. Compute the hash-function value $e = e_1||e_2||e_3$ (the first signature element), where $||$ denotes the concatenation operation, from the document M to which the vector R is concatenated: $e = e_1||e_2||e_3 = f\left(M, R\right)$, where e_1, e_2, and e_3 are 128-bit integers.

3. Calculate the integers n and u:

$$n = \frac{k - x_1e_2e_3 - e_3}{e_3 + e_1e_3 + e_2e_3} \bmod q; \quad u = \frac{t - x_2e_2e_3 - e_1e_3}{e_3 + e_1e_3 + e_2e_3} \bmod q.$$

4. Calculate the second signature element S:

$$S = B^{-1}G^nH^uA^{-1}.$$

The size of the output signature (e, S) is equal to ≈ 900 bits (≈ 113 bytes). Computational difficulty w of the signature generation procedure is roughly equal to four exponentiation operations in the 4-dimensional FNAA used as algebraic support of the signature scheme, i. e., to $w \approx 12,288$ multiplications modulo a 129-bit prime. The verification of the signature (e, S) to the document M is performed using the public key (Y, Z, U, W) as folows:

The signature verification procedure.

1. Calculate the vector R':

$$R' = (YS\,(US)^{e_1}\,(ZSW)^{e_2})^{e_3}\,.$$

2. Compute the hash-function value e' from the document M to which the vector R' is concatenated: $e' = f\,(M, R')\,.$

3. If $e' = e$, then the signature is genuine. Otherwise reject the signature.

At the first step of the signature verification algorithm the computations are performed in accordance with a verification equation with 3 entries of the signature element S. The computational complexity w' of the signature verification procedure is roughly equal to three exponentiation operations in the 4-dimensional FNAA used as algebraic support of the signature scheme, i. e., we have $w' \approx 9,216$ multiplications modulo a 129-bit prime.

Correctness proof.
Taking into account that the vectors G and H are permutable and have order q, one can show that the correctly computed signature (e, S) passes the verification procedure as genuine signature:

$$\begin{aligned}
&R'_1 = (YS\,(US)^{e_1}\,(ZSW)^{e_2})^{e_3} = \\
&= \left(AGBB^{-1}G^nH^uA^{-1}\left(AHBB^{-1}G^nH^uA^{-1}\right)^{e_1}\times\right. \\
&\qquad \left.\times\left(AG^{x_1}BB^{-1}G^nH^uA^{-1}AH^{x_2}A^{-1}\right)^{e_2}\right)^{e_3} = \\
&= \left(AGG^nH^uA^{-1}\left(AHG^nH^uA^{-1}\right)^{e_1}\left(AG^{x_1}G^nH^uH^{x_2}A^{-1}\right)^{e_2}\right)^{e_3} = \\
&= \left(AG^{n+1}H^uA^{-1}AH^{e_1(u+1)}G^{e_1n}A^{-1}AG^{e_2(x_1+n)}H^{e_2(u+x_2)}A^{-1}\right)^{e_3} = \\
&= \left(AG^{n+1+e_1n+e_2(x_1+n)}H^{u+e_1(u+1)+e_2(u+x_2)}A^{-1}\right)^{e_3} = \\
&= AG^{e_3n+e_3+e_3e_1n+e_3e_2(x_1+n)}H^{e_3u+e_3e_1(u+1)+e_3e_2(u+x_2)}A^{-1} = \\
&= AG^{n(e_3+e_1e_3+e_2e_3)+e_3+x_1e_2e_3}H^{u(e_3+e_1e_3+e_2e_3)+e_1e_3+x_2e_2e_3}A^{-1} = \\
&= AG^{\frac{k-x_1e_2e_3-e_3}{e_3+e_1e_3+e_2e_3}(e_3+e_1e_3+e_2e_3)+e_3+x_1e_2e_3}\times \\
&\qquad \times H^{\frac{t-x_2e_2e_3-e_1e_3}{e_3+e_1e_3+e_2e_3}(e_3+e_1e_3+e_2e_3)+e_1e_3+x_2e_2e_3}A^{-1} = \\
&= AG^kH^tA^{-1} = R \;\;\Rightarrow\;\; f(M,R') = f(M.R) \;\Rightarrow\; e' = e.
\end{aligned}$$

4. The second signature scheme

The public key is calculted as a set of three 6-dimensional vectors Y, Z, and U in accordance with the public-key generation procedure of the first signature scheme (see Section 3) with exception that at step 3 only the following three vectors are computed:

$$Y = AGB, \quad Z = AG^{x_1}B, \quad U = AHB. \tag{4}$$

Since in the case $m = 6$ we use a 97-bit (96-bit) prime p (prime q) The size of public key is equal to ≈ 1746 bits (≈ 219 bytes). The integer x_1 and the vectors G, H, A^{-1}, and B^{-1} represent a private key having the size equal to ≈ 2424 bits (≈ 303 bytes).

Using the private key $\left(x_1, G, H, A^{-1}, B^{-1}\right)$ and some specified 384-bit hash-function f, one can generate a signature to the electronic document M as follows:

The signature generation procedure.

1. Generate random natural numbers k ($k < q$) and t ($t < q$). Then calculate the vector

$$R = B^{-1}G^kH^tB.$$

2. Compute the hash-function value $e = e_1||e_2||e_3||e_4$ (the first signature element) from the document M to which the vector R is concatenated: $e = e_1||e_2||e_3||e_4 = f\left(M, R\right)$, where e_1, e_2, e_3, and e_3 are 96-bit integers.

3. Calculate the integers n and u:

$$n = \frac{k - e_4 - e_1e_4 - x_1e_3e_4}{e_1e_4 + e_2e_4 + e_3e_4 + e_4} \bmod q; \quad u = \frac{t - e_2e_4}{e_1e_4 + e_2e_4 + e_3e_4 + e_4} \bmod q.$$

4. Calculate the second signature element S:

$$S = B^{-1}G^nH^uA^{-1}.$$

The size of the output signature (e, S) is equal to ≈ 966 bits (≈ 121 bytes). Computational difficulty w of the signature generation procedure is roughly equal to four exponentiation operations in the 6-dimensional FNAA used as algebraic support of the signature scheme, i. e., $w \approx 20,736$ multiplications modulo a 97-bit prime or $w \approx 11,720$ multiplications modulo a 129-bit prime. The verification of the signature (e, S) to the document M is performed using the public key (Y, Z, U) as folows:

The signature verification procedure.

1. Calculate the vector R':

$$R' = \left((SY)^{e_1}\, S\, (US)^{e_2}\, (ZS)^{e_3}\, Y\right)^{e_4}.$$

2. Compute the hash-function value e' from the document M to which the vector R' is concatenated: $e' = f\left(M, R'\right)$.

3. If $e' = e$, then the signature is genuine. Otherwise reject the signature.

At the first step of the signature verification algorithm the computations are performed in accordance with a verification equation with 4 entries of the signature element S. The computational complexity w' of the signature verification procedure is roughly equal to four exponentiation operations in the 6-dimensional FNAA used as algebraic support of the signature scheme, i. e., we have $w' \approx 20,736$ multiplications modulo a 97-bit prime or $w' \approx 11,720$ multiplications modulo a 129-bit prime.

Correctness proof.
Taking into account that the vectors G and H are permutable and have order q, one can show that the correctly computed signature (e, S) passes the verification procedure as genuine signature:

$$
\begin{aligned}
R'_1 &= ((SY)^{e_1} S (US)^{e_2} (ZS)^{e_3} Y)^{e_4} = \\
&= \left(\left(B^{-1}G^nH^uA^{-1}AGB\right)^{e_1} B^{-1}G^nH^uA^{-1} \left(AHBB^{-1}G^nH^uA^{-1}\right)^{e_2} \times \right. \\
&\qquad \left. \times \left(AG^{x_1}BB^{-1}G^nH^uA^{-1}\right)^{e_3} AGB\right)^{e_4} = \\
&= \left(\left(B^{-1}G^nH^uGB\right)^{e_1} B^{-1}G^nH^uA^{-1} \left(AHG^nH^uA^{-1}\right)^{e_2} \times \right. \\
&\qquad \left. \times \left(AG^{x_1}G^nH^uA^{-1}\right)^{e_3} AGB\right)^{e_4} = \\
&= \left(B^{-1}G^{e_1(n+1)}H^{e_1u}G^nH^uH^{e_2(1+n)}G^{e_2n}A^{-1}AG^{e_3(x_1+n)}H^{e_3u}GB\right)^{e_4} = \\
&= \left(B^{-1}G^{e_1(n+1)+n+e_2n+e_3(x_1+n)+1}H^{e_1u+u+e_2(1+n)+e_3u}B\right)^{e_4} = \\
&= B^{-1}G^{e_4e_1(n+1)+e_4n+e_4e_2n+e_4e_3(x_1+n)+e_4}H^{e_4e_1u+e_4u+e_4e_2(1+n)+e_4e_3u}B = \\
&= B^{-1}G^{n(e_1e_4+e_2e_4+e_3e_4+e_4)+e_4+e_1e_4+e_3e_4x_1}H^{u(e_1e_4+e_2e_4+e_3e_4+e_4)+e_2e_4}B = \\
&= B^{-1}G^{\frac{k-e_4-e_1e_4-x_1e_3e_4}{e_1e_4+e_2e_4+e_3e_4+e_4}(e_1e_4+e_2e_4+e_3e_4+e_4)+e_4+e_1e_4+e_3e_4x_1} \times \\
&\qquad \times H^{\frac{t-e_2e_4}{e_1e_4+e_2e_4+e_3e_4+e_4}(e_1e_4+e_2e_4+e_3e_4+e_4)+e_2e_4}B = \\
&= B^{-1}G^kH^tB = R \quad \Rightarrow \quad f(M,R') = f(M.R) \;\Rightarrow\; e' = e.
\end{aligned}
$$

5.Disscussion

In each of the two introduced signature algorithms with a hidden group, the used exponentiation operations are a part of the technique that provides possibility (when using the private key) to compute the randomization vector R and the signature element S that satisfy the verification equation. It can be noted that the knowledge of the x_1 and x_2 values does not make it possible to develop a polynomial algorithm for computing a signature

until the secret vectors G and H are also known. Actually, the values x_1 and x_2 are used only to select some random vectors from the hidden group and to reduce the computational complexity of the signature generation procedure. It is easy to show that using a precomputed large set of the vectors contained in the group $\Gamma_{<G,H>}$ allows one to compute the public key, for example, in the first signature algorithm in the form of four vectors $Y = AG_1B$, $Z = AG_2B$, $U = AG_3B$, and $W = AG_4A^{-1}$, where $G_1, G_2, G_3, G_4 \in \Gamma_{<G,H>}$ are random vectors selected from the said set of pairwise permutable vectors. For this method of generating a public key, a modified signature generation procedure (computational complexity of which is roughly equal to eight exponentiation operations) can be used , while the source signature verification procedure is saved. Thus, the developed sihnature algorithms with a hidden group are not HDLP-based schemes.

We suppose that the most efficient attack on the proposed first algorithm is to find the vectors A', B', G_1, G_2, G_3, and G_4 which express the public-key in the form of formulas (3). The formulas (3) define the following system of seven quadratic vector equations with the said six unknowns:

$$\begin{cases} A'^{-1}Y = G_1B', & A'^{-1}Z = G_2B'; & A'^{-1}U = G_3B', & WA'^{-1} = A'G_4 \\ G_1G_2 = G_2G_1, & G_1G_3 = G_3G_1, & G_1G_4 = G_4G_1. \end{cases} \tag{5}$$

The last three vector equations in (5) reflect the requirement of pairwise permutability of the vectors G_1, G_2,G_3, and G_4. Thus we have a system of 7 quadratic vector equations with 6 unknowns. The system (5) reduces to the system of 28 equations with 24 unknowns over the field $GF(p)$ of 129-bit order.

A similar attack on the second proposed signature algorithm leads to the system of 5 quadratic vector equations with 5 unknowns, which reduces to the system of 30 quadratic equations with 30 unknowns, which is set over the field $GF(p)$ of 97-bit order.

From the multivariate cryptography [1, 3, 18] it is known that finding a solution of such systems is a computationally hard problem and the quantum computer is not efficient to solve it. Like the multivariate public-key cryptosystems, the developed algorithms are attributed to the post-quantum signature schemes. The latter represent significant practical interest due to significantly lower sizes of the public key, private key, and signature. A merit of the introduced algorithms is a significantly higher order of the finite field over which the system of quadratic equations is set.

Table 3: Comparison of the proposed and known multivariate signature schemes.

Signature scheme	signature size, bytes	public-key size, bytes	η	ρ	ω
[18]	–	–	27	27	2^{16}
Rainbow [1]	33	16,065	27	33	2^8
Rainbow [16] (3 versions)	66... 204	>150,000... >1,900,000	64... 128	96... 204	$2^4, 31,$ 2^8
QUARTZ [3]	16	72,704	100	107	2^4
Proposed ($m = 4$)	160	768	28	24	$>2^{128}$
Proposed ($m = 6$)	112	576	30	30	$>2^{96}$

Table 3 (where η (ρ) is the number of equations (unknowns) in the system of quadratic equations; ω is the order of the finite field) provides some comparison of the introduced post-quantum signature algorithms with some multivariate sinature algorithms. Table 4, where a procedure execution time* is estimated in multiplications in $GF(p)$ with 129-bit characteristic, compares the introduced signature algorithms with some HDLP-base ones.

6. Conclusion

The proposed two post-quantum signature algorithms, using FNAAs as algebraic support, can be attributed to the cryptoschemes with a hidden group and to the multivariate public key cryptosystems, however not to the HDLP-based signature algorithms. For the first time it is proposed a method for development of the signature schemes on FNAAs, which are based on the computational difficulty of solving systems of many quadratic equations with many unknowns. The introduced post-quantum signature algorithms are more practical than the known multivariate signature algorithms and can serve as an attractive starting point for preparing a new proposal for participating in the NIST competition on developing a standard on a post-quantum signature algorithm (NIST is going to consider new proposals at the fourth round of its competition [14]).

Table 4: Comparison of the proposed and known HDLP-based signature schemes.

Signature scheme	signature size, bytes	public-key size, bytes	signature generation time*	signature verification time*
[7]	96	384	$\approx 49,200$	$\approx 36,800$
[9]	96	384	$\approx 12,400$	$\approx 24,800$
[8]	192	768	$\approx 221,200$	$\approx 221,200$
[11]	96	576	$\approx 221,200$	$\approx 165,900$
Proposed ($m = 4$)	113	290	$\approx 12,288$	$\approx 9,216$
Proposed ($m = 6$)	121	219	$\approx 27,648$	$\approx 13,824$

References

[1] **J. Ding, D. Schmidt**, *Rainbow, a new multivariable polynomial signature scheme*, Lecture Notes in Computer Sci., **3531** (2005), 164 – 175.

[2] Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms, (2016) [on line] https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (May 10, 2022)

[3] **D. Jintai, S. Dieter**, *Multivariable Public Key Cryptosystems*, (2004) https://eprint.iacr.org/2004/350.pdf (May 10, 2022)

[4] **R. Jozsa**, *Quantum algorithms and the fourier transform*, Proc. Roy. Soc. London Ser A, **454** (1998), 323 – 337.

[5] **N.A. Moldovyan**, *Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions*, Quasigroups and Related Systems, **26** (2020), 263 – 270.

[6] **N.A. Moldovyan**, *Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security*, Bull. Acad. Sci. Moldova, Math., **2(93)** (2020), 62 – 67.

[7] **D.N. Moldovyan**, *A practical digital signature scheme based on the hidden logarithm problem*, Computer Sci. J. Moldova, **29** (2021), no. 2(86), 206−226.

[8] **N.A. Moldovyan, A.A. Moldovyan**, *Candidate for practical post-quantum signature scheme*, Vestnik of Saint Petersburg Univ. Applied Math., Computer Sci., Control Processes, **16** (2020), 455 – 464.

[9] **N.A. Moldovyan, A.A. Moldovyan**, *Digital signature scheme on the 2x2 matrix algebra*, Vestnik of Saint Petersburg Univ. Applied Math., Computer Sci., Control Processes, **17** (2021), 254 – 261.

[10] **D.N. Moldovyan, A.A. Moldovyan, N.A. Moldovyan**, *Digital signature scheme with doubled verification equation*, Computer Sci. J. Moldova, **28** (2020), no. 1(82), 80 – 103.

[11] **D.N. Moldovyan, A.A. Moldovyan, N.A. Moldovyan**, *An enhanced version of the hidden discrete logarithm problem and its algebraic support*, Quasigroups and Related Systems, **29** (2021), 97 – 106.

[12] **A.A. Moldovyan, N.A. Moldovyan**, *Post-quantum signature algorithms based on the hidden discrete logarithm problem*, Computer Sci. J. Moldova, **26** (2018), no. 3(78), 301 – 313.

[13] **A.A. Moldovyan, N.A. Moldovyan**, *Finite Non-commutative Associative Algebras as Carriers of Hidden Discrete Logarithm Problem*, Bull. South Ural State Univ., Ser. Mathematical Modelling, Programming & Computer Software, **12** (2019), no. 1, 66 – 81.

[14] **D. Moody**, *NIST Status Update on the 3rd Round*, (2021). Available at: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf (May 10, 2022).

[15] *Post-Quantum Cryptography*, Lecture Notes in Computer Sci., **11505**, (2019).

[16] Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. https://www.pqcrainbow.org/ (May 10, 2022)

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

[18] **Q. Shuaiting, H. Wenbao, Li Yifa, J. Luyao**, *Construction of Extended Multivariate Public Key Cryptosystems*, Intern. J. Network Security, **18** (2016), 60 – 67.

Received November 22, 2021

St. Petersburg Federal Research Center
of the Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg, Russia
e-mail: nmold@mail.ru