UDC 512.552.18+003.26
MSC 16P10

Digital signature scheme on the 2×2 matrix algebra

N. A. Moldovyan, A. A. Moldovyan

St. Petersburg Federal Research Center of the Russian Academy of Sciences,
39, 14-ya liniya V. O., St. Petersburg, 199178, Russian Federation

For citation: Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2×2 matrix algebra. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2021, vol. 17, iss. 3, pp. 254–261. https://doi.org/10.21638/11701/spbu10.2021.303

The article considers the structure of the 2×2 matrix algebra set over a ground finite field $GF(p)$. It is shown that this algebra contains three types of commutative subalgebras of order p^2, which differ in the value of the order of their multiplicative group. Formulas describing the number of subalgebras of every type are derived. A new post-quantum digital signature scheme is introduced based on a novel form of the hidden discrete logarithm problem. The scheme is characterized in using scalar multiplication as an additional operation masking the hidden cyclic group in which the basic exponentiation operation is performed when generating the public key. The advantage of the developed signature scheme is the comparatively high performance of the signature generation and verification algorithms as well as the possibility to implement a blind signature protocol on its base.

Keywords: digital signature, post-quantum cryptoscheme, blind signature, hidden logarithm problem, finite associative algebra, matrix algebra.

1. Introduction. At present in the field of the public-key cryptography, considerable attention of the cryptographic community is paid to the development of post-quantum cryptoschemes [1–3]. Finite non-commutative associative algebras (FNAAs) represent significant interest as algebraic support of practical post-quantum digital signature schemes based on different forms of the hidden discrete logarithm problem (HDLP) [4, 5]. A unified method for setting FNAAs of arbitrary even dimensions is proposed in [6]. To get faster post-quantum signature algorithms, the latter are developed on 4-dimensional FNAAs [5, 7, 8].

A finite m-dimensional vector space defined over a finite field (for example, $GF(p)$), in which the vector multiplication operation (distributive at the left and at the right relatively addition operation) is set, is called finite algebra. A vector A is denoted as $A = (a_0, a_1, \ldots, a_{m-1})$ or as $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, 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 ($\circ$) of two m-dimensional vectors A and B is set as

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

here every of the products $\mathbf{e}_i \circ \mathbf{e}_j$ is to be substituted by a single-component vector $\lambda \mathbf{e_k}$, where $\lambda \in GF(p)$, indicated in the cell in the intersection of the i-th row and j-th column of so called basis vector multiplication table (BVMT). To define associative vector multiplication operation the BVMT should define associative multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$:

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

The 2×2 matrix algebra set over $GF(p)$ can be represented as the 4-dimensional FNAA defined by Table for the case $\lambda = 1$. This BVMT is sparse and the computational difficulty of the vector multiplication is two times lower than in the 4-dimensional FNAA presented in [5, 8]. Therefore development of the HDLP-based signature schemes on the matrix algebra potentially gives higher performance. In this connection, it is of interest to study the structure of the 2×2 matrix algebra from the point of view of identifying various types of commutative multiplicative groups contained in the algebra.

Table. **The BVMT setting the 4-dimensional FNAAs** ($\lambda \neq 0$) **and the 2×2 matrix algebra** ($\lambda = 1$)

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	0	0
$\mathbf{e}_1$	0	0	$\lambda\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\lambda\mathbf{e}_3$	0	0
$\mathbf{e}_3$	0	0	$\mathbf{e}_2$	$\mathbf{e}_3$

This paper considers the structure of the 2×2 matrix algebra and introduces a new post-quantum signature algorithm based on a novel form of the HDLP.

2. Structure of the 2×2 matrix algebra set over $GF(p)$**.** Consider the sructure of the FNAAs set by Table for different values of the structural coefficient λ. For an arbitrary fixed value of λ the algebra contains the global two-sided unit $E = (1, 0, 0, 1)$. The vectors $G = (g_0, g_1, g_2, g_3)$ satisfying the non-equality $g_0 g_3 \neq \lambda g_1 g_2$ are invertible. The vectors $N = (n_0, n_1, n_2, n_3)$ satisfying the condition $n_0 n_3 = \lambda n_1 n_2$ are non-invertible. From the latter equality one can easily show that the number of non-invertible vectors contained in the algebra is equal to $\eta_N = p^3 + p^2 - p$ and the number of invertible vectors (the order of the multiplicative group of the algebra) is equal to

$$\Omega = p^4 - \eta_N = p(p-1)\left(p^2 - 1\right).$$

Consider the set of the vectors X that are permutable with a fixed vector A. The vectors $X = (x_0, x_1, x_2, x_3)$ can be computed from the vector equation $A \circ X = X \circ A$ that can be reduced to the following system of three linear equations with the unknowns x_0, x_1, x_2, and x_3:

$$\begin{aligned} &\lambda a_2 x_1 - \lambda a_1 x_2 = 0,\\ &a_1 x_0 + (a_3 - a_0)\, x_1 - a_1 x_3 = 0,\\ &a_2 x_0 + (a_3 - a_0)\, x_2 - a_2 x_3 = 0. \end{aligned} \qquad (1)$$

Depending on the coordinates of the vector A, the cases should be considered.

I. Case $a_1 = a_2 = 0$. The system (1) reduces to

$$\begin{aligned} (a_3 - a_0)\, x_1 = 0,\\ (a_3 - a_0)\, x_2 = 0. \end{aligned}$$

If $a_3 \neq a_0$, then one gets the solution space

$$X = (x_0, x_1, x_2, x_3) = (d, 0, 0, h)\,, \qquad (2)$$

here $d, h = 0, 1, \ldots, p-1$. The set (2) describes a commutative subalgebra of order p^2 that contains $2p-1$ different non-invertible vectors of the forms $(d, 0, 0, 0)$ and $(0, 0, 0, h)$. Multiplicative group Γ_1 of this subalgebra is cyclic and has order $\Omega_1 = p^2 - (2p-1) = (p-1)^2$. One can show that the group Γ_2 possesses 2-dimensional cyclicity (in terms of [9]), i. e., its minimum generator system includes two vectors of the order $p-1$.

If $a_3 = a_0$, then A is a scalar vector and the solution space of the system (1) includes all vectors of the algebra.

II. Case $a_1 = 0,\ a_2 \neq 0$. The system (1) reduces to

$$\begin{aligned} &x_1 = 0, \\ &x_3 = x_0 + \frac{(a_3 - a_0)}{a_2} x_2 \end{aligned}$$

and the solution space of this system is described as follows:

$$X = (x_0, x_1, x_2, x_3) = \left(d,\ 0,\ h,\ d + \frac{(a_3 - a_0)}{a_2} h\right),$$

where $d, h = 0, 1, \ldots, p-1$. The latter set includes non-invertible vectors satisfying the condition $d\left(d + \frac{(a_3-a_0)}{a_2} h\right) = 0$. The latter condition sets the two subsets of non-invertible vectors: i) $X = \left(0,\ 0,\ h,\ \frac{(a_3-a_0)}{a_2} h\right)$ and ii) $X = \left(-\frac{(a_3-a_0)}{a_2} h,\ 0,\ h,\ 0\right)$, which intersect in the zero vector $(0, 0, 0, 0)$.

IIa. Case $a_0 \neq a_3$. This subcase corresponds to commutative subalgabra of order p^2 which includes $2p-1$ non-invertible vectors and multiplicative group Γ_1 of order $\Omega_1 = (p-1)^2$.

IIb. Case $a_0 = a_3$. This subcase corresponds to commutative subalgabra of order p^2 which includes p non-invertible vectors of the form $(0, 0, h, 0)$ and contains a multiplicative group Γ_2 of order $\Omega_2 = p^2 - p = p(p-1)$.

III. Case $a_1 \neq 0,\ a_2 = 0$. The system (1) reduces to

$$\begin{aligned} &x_2 = 0, \\ &x_3 = x_0 + \frac{(a_3 - a_0)}{a_1} x_1 \end{aligned}$$

and the solution space of this system is described as follows:

$$X = (x_0, x_1, x_2, x_3) = \left(d,\ h,\ 0,\ d + \frac{(a_3 - a_0)}{a_1} d\right),$$

where $d, h = 0, 1, \ldots, p-1$. The latter set includes non-invertible vectors satisfying the condition $d\left(d + \frac{(a_3-a_0)}{a_1} h\right) = 0$. The latter condition sets the two subsets of non-invertible vectors: i) $X = \left(0,\ h,\ 0,\ \frac{(a_3-a_0)}{a_1} h\right)$ and ii) $X = \left(-\frac{(a_3-a_0)}{a_1} h,\ h,\ 0,\ 0\right)$.

IIIa. Case $a_0 \neq a_3$. This subcase corresponds to commutative subalgabra of order p^2 which includes $2p-1$ non-invertible vectors and multiplicative group Γ_1 of order $\Omega_1 = (p-1)^2$.

IIIb. Case $a_0 = a_3$. This subcase corresponds to commutative subalgabra of order p^2 which includes p non-invertible vectors of the form $(0, h, 0, 0)$ and contains a multiplicative group Γ_2 of order $\Omega_2 = p(p-1)$. It is easy to show that Γ_2 is a cyclic group.

IV. Case $a_1 \neq 0,\ a_2 \neq 0$. The system (1) reduces to

$$
\begin{gathered}
x_2 = \frac{a_2}{a_1} x_1, \\
x_3 = x_0 + \frac{(a_3 - a_0)}{a_1} x_1
\end{gathered}
$$

and the solution space of the system (1) is described as follows:

$$
X = (x_0, x_1, x_2, x_3) = \left(d,\ h,\ \frac{a_2}{a_1} h,\ d + \frac{(a_3 - a_0)}{a_1} h \right), \tag{3}
$$

here $d, h = 0, 1, \ldots, p-1$. Taking into account the non-invertibility condition, for vectors from the set (3) one can write

$$
\begin{gathered}
d^2 + \frac{(a_3 - a_0)}{a_1} hd - \lambda \frac{a_2}{a_1} h^2 = 0, \\
d = \frac{(a_3 - a_0) \pm \sqrt{\Delta}}{2a_1} h,
\end{gathered}
$$

where $\Delta = (a_3 - a_0)^2 + 4\lambda a_1 a_2$.

IVa. Case $\Delta \neq 0$ is a quadratic residue in $GF(p)$. The number of non-invertible vectors in the set (3) equals to $2p-1$ and the commutative subalgebra set by (3) includes multiplicative group of the Γ_1 type.

IVb. Case $\Delta \neq 0$ is a quadratic non-residue in $GF(p)$. The commutative subalgebra set by (3) includes the single non-invertible vector $(0,0,0,0)$ and represents the field $GF(p^2)$ with cyclic multiplicative group Γ_3 of order $\Omega_3 = p^2 - 1$.

IVc. Case $\Delta = 0$. The number of non-invertible vectors in the set (3) equals to p and the commutative subalgebra set by (3) includes multiplicative group Γ_2 of order $\Omega_2 = p(p-1)$.

Thus, the studied 4-dimensional FNAA contains exactly three types of commutative subalgebras of order p^2, which are characterized in type of multiplicative group. Arbitrary two of the subalgebras intersect exactly in the subset on scalar vectors. Indeed, each of the vectors that is not a scalar vector defines a single commutative subalgebra of order p^2. Each of the subalgebras contains $p^2 - p$ unique non-scalar vectors and the 4-dimensional FNAA contains $p^4 - p$ different non-scalar vectors, therefore for number η of the commutative subalgebras of all three types we get the following formula:

$$
\eta = \frac{p^4 - p}{p^2 - p} = p^2 + p + 1.
$$

Suppose k, t, and u denote number of different commutative groups of the types Γ_1, Γ_2, and Γ_3 correspondingly. Then we have $\eta = k + t + u$ and

$$
k + t + u = p^2 + p + 1. \tag{4}
$$

Taking into account that the set of scalar vectors includes $p-1$ invertible vectors, one can write

$$
\begin{gathered}
(\Omega_1 - (p-1))\, k + (\Omega_2 - (p-1))\, t + (\Omega_3 - (p-1))\, u = \Omega - (p-1), \\
\left((p-1)^2 - (p-1)\right) k + (p(p-1) - (p-1)t + \left(p^2 - 1 - (p-1)\right) u = \\
= p(p-1)(p^2 - 1) - (p-1), \\
(p-2)k + (p-1)t + pu = p^3 - p - 1.
\end{gathered} \tag{5}
$$

To find the value t, consider the number of non-invertible vectors A relating to the Case IVc, i. e. $a_1 \neq 0,\ a_2 \neq 0, \Delta = 0$, which define the commutative subalgebras containing multiplicative groups of the Γ_2 type. Such vectors satisfy the conditions $a_0a_3 - \lambda a_1 a_2 \neq 0$ and $\Delta = (a_3 - a_0)^2 + 4\lambda a_1 a_2 = 0$. From the condition $\Delta = 0$ we have $(a_3 + a_0)^2 = 0$ and $a_3 = -a_0$. Thus, the Case IVc gives $(p-1)^2$ different vectors A that set the subalgebras containing the Γ_2 type groups. Each of the subcases IIb and IIIb gives other $p-1$ unique vectors A setting the subalgebras containing the Γ_2 type groups. Totally, we have $(p-1)^2+2(p-1) = (p-1)(p+1)$ of the said vectors A. Every of the said subalgebras contains $p-1$ of the said vectors A and t algebras contain $t(p-1) = (p-1)(p+1)$ of the said non-invertible vectors, therefore,

$$t = p + 1.$$

From (4) and (5) we have

$$k = \frac{p(p+1)}{2}, \quad u = \frac{p(p-1)}{2}.$$

3. The proposed post-quantum signature scheme. Suppose a 2×2 matrix algebra is defined over the field $GF(p)$ with prime $p = 2q + 1$, where q is a 256-bit prime. Generation of the public key in the form of matrices (Y, T, Z) is performed as follows:

1) select at random an invertible 2×2 matrix G contained in a cyclic group of the Γ_1 type (using results of Section 2 one can easily to propose a method for implementing this step);

2) generate a uniformly random invertible 2×2 matrix A and integer $x < q$ and compute the matrix $Y = AG^xA^{-1}$;

3) generate a uniformly random invertible 2×2 matrix B and integer $\lambda < p$ and compute the matrix $Z = BGB^{-1}\lambda$;

4) compute the matrix $T = AG^uB^{-1}$.

The size of public key equals approximately to 384 bytes. The private key corresponding to the calculated public key represents three matrices G, A, B, and two integers x and λ. The size of private key equals to about 448 bytes.

Procedure for generation of the signature (e, s, σ) to the electronic document M:

• select at random integers $k < q$, $\rho < p$ and calculate matrix $R = AG^kB^{-1}\rho$;

• using some specified 256-bit hash-function f_h compute the hash value e from the document M to which the matrix R is concatenated: $e = f_h(M, R)$. The value e is the first signature element;

• calculate the second signature element $s = k - u - ex \bmod q$ and the third signature element $\sigma = \rho\lambda^{-s}$.

The signature size equals near to 96 byte. Computaional difficulty of the signature generation can be estimated as one exponentiation operation in the 2×2 matrix algebra (approximately 3072 multiplications in $GF(p)$).

Signature verification procedure includes the three steps:

• compute the matrix $R' = Y^eTZ^s\sigma$;

• compute the value $e' = f_h\left(M, R\right)$;

• if $e' = e$, then the signature is accepted as genuine, else it is rejected.

Computaional difficulty of the signature verification can be estimated as 2 exponentiations in the 2×2 matrix algebra (about 6142 multiplications in $GF(p)$).

Correctness proof of the signature scheme is as follows:

$$R' = Y^e T Z^s \sigma = \left(AG^x A^{-1}\right)^e \left(AG^u B^{-1}\right) \left(BGB^{-1}\lambda\right)^s \sigma =$$
$$= AG^{xe+u+s} B^{-1} \lambda^s \left(\rho\lambda^{-s}\right) = AG^{xe+u+k-u-ex} B^{-1} \rho = R,$$
$$\{R' = R\} \Rightarrow f_h\left(M, R'\right) = f_h\left(M, R\right) \Rightarrow e' = e.$$

Thus, the correctly computed signature (e, s, σ) passes the verification procedure as a genuine signature.

4. Blind signature protocol. Blind digital signature is used to solve problems of ensuring the anonymity (non-traceability) of users that arise in some special information technologies [10, 11], for example, electronic money systems and secret electronic voting. Blind signature is computed by a signer in the process of interacting with some user (client). The signer uses his personal private key to calculate the blind signature and transfers it to the client. Using the blind signature, the client computes an authentic signature of the signer to some document to which the signer does not have access during the protocol execution. In addition, the anonymity of the client is ensured by the fact that during the protocol he introduces one or two random blinding factors into the blind signature. After receiving a blind signature from the signer, the client removes the blinding factors, thereby calculating the true signature.

Using the described signature scheme and applying a scalar blinding factor μ and the left Y^ϵ and right Z^τ blinding factors in the form of two matrices, one can propose the blind sinature protocol.

1. The signer selects at random integers $k < q$, $\rho < p$ and calculate matrix $R^* = AG^k B^{-1}$. The latter is send to the client.

2. The client generates random non-negative integers $\epsilon < q$, $\tau < q$, and $\mu < p$ and calculates the matrix $R = Y^\epsilon R^* Z^\tau \mu$. Then he computes the first signature element of a valid signer's signature $e = f_h(M, R)$ and the first element of the blind signature $e^* = e - \epsilon \bmod q$. The value e^* is sent to the signer. (The document M is prepared by the client.)

3. The signer calculates other elements of the blind signature: the second $s^* = k - u - e^* x \bmod q$ and the third $\sigma^* = \rho\lambda^{-s^*}$ elements. Then he sends the values s^* and σ^* to the client.

4. The client calculates the second and third elements of the valid signer's signature: $s = s^* + \tau \bmod q$ and $\sigma = \sigma^* \mu$.

Correctness proof of this blind signature protocol is performed as proving that the output signature (e, s, σ) passes the verification procedure of the proposed signature scheme as a genuine signature:

$$R' = Y^e T Z^s \sigma = Y^{e^* + \epsilon} T Z^{s^* + \tau} \sigma^* \mu =$$
$$= Y^\epsilon Y^{e^*} T Z^{s^*} \sigma^* Z^\tau \mu = Y^\epsilon R^* Z^\tau \mu = R \Rightarrow$$
$$\Rightarrow f_h\left(M, R'\right) = f_h\left(M, R\right) \Rightarrow e' = e.$$

5. Discussion and conclusion. The private value x can be considered as a logarithm in a hidden cyclic group generated by the secret matrix G. Therefore, the signature scheme introduced in Section 3 can be called a HDLP-based scheme, like the signature algorithms described in [5, 7, 8]. The main contribution to the security of the proposed signature scheme is introduced by the exponentiation operation G^x performed in the hidden group generated by the matrix G. The value G^x is contained in a hidden form in the first element of the public key $Y = AG^xA^{-1}$.

An important point of the proposed signature scheme is the use of the scalar multiplication as an additional masking operation, when computing the element $Z = BGB^{-1}\lambda$. Due to scalar multiplication, the permutable matrices Y and TZT^{-1} are contained in different cyclic groups. Therefore, construction of periodic functions on the base of public key elements leads to the formation of periods with a length determined by the values q (order of the matrix G) and $p-1$ (order of scalar value λ) and the use of quantum algorithms [12–14] to calculate the value of x does not seem computationally possible. Thus, due to scalar multiplication and selecting the matrix G from one of the Γ_1-type groups, the post-quantum security design criterion proposed in [15] is satisfied by the proposed signature scheme. In the signature schemes [5, 8, 15] technique of doubling the verification equation was applied to satisfy that criterion. The said techniques defines larger sizes of public key and signature and lower performance of signature schemes.

Due to using the the $2{\times}2$ matrix algebra as algebraic support and a new design, the proposed signature scheme possesses significantly higher performance and smaller signature size than the HDLP-based schemes presented in [5, 8, 15]. In addition, the introduced signature scheme can be used to implement a blind signature protocol.

One can suppose that Table presents a particular case of sparse BVMTs which set various 4-dimensional FNAAs with computationally efficient vector multiplication, which represent interest as algebraic support of the HDLP-based signature schemes. Search of other sparse BVMTs and investigation of the structure of the FNAA defined by them represents a topic of a further research.

References

1. Post-quantum cryptography. *10th International conference.* Chongqing, China, May 8–10, 2019 (PQCrypto 2019). *Proceedings. Lecture Notes in Computer Science Series.* Berlin, Springer Publ., 2019, vol. 11505, pp. 1–421.

2. Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme. *Designs, codes and cryptography*, 2017, vol. 82, no. 1–2, pp. 469–493.

3. Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A. Cryptographic algorithms on groups and algebras. *Journal of Mathematical Sciences*, 2017, vol. 223, no. 5, pp. 629–641.

4. Moldovyan N. A., Moldovyan A. A. Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem. *Bulletin of the South Ural State University. Series Mathematical Modelling, Programming & Computer Software*, 2019, vol. 12, no. 1, pp. 66–81. https://doi.org/10.14529/mmp190106

5. Moldovyan N. A., Moldovyan A. A. Candidate for practical post-quantum signature scheme. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2020, vol. 16, iss. 4, pp. 455–461. https://doi.org/10.21638/11701/spbu10.2020.410

6. Moldovyan N. A. A unified method for setting finite non-commutative associative algebras and their properties. *Quasigroups and Related Systems*, 2018, vol. 26, no. 2, pp. 263–270.

7. Moldovyan D. N. New form of the hidden logarithm problem and its algebraic support. *Bulletin of Academy of Sciences of Moldova. Mathematics*, 2020, no. 2 (93), pp. 3–10.

8. Moldovyan N. A. Signature schemes on algebras, satisfying enhanced criterion of post-quantum security. *Bulletin of Academy of Sciences of Moldova. Mathematics*, 2020, no. 2 (93), pp. 62–67.

9. Moldovyan N. A., Moldovyan P. A. New primitives for digital signature algorithms. *Quasigroups and Related Systems*, 2009, vol. 17, no. 2, pp. 271–282.

10. Chaum D. Security without identification. Transaction systems to make big brother obsolete. *Communications of the AMS*, 1985, vol. 28, no. 10, pp. 1030–1044.

11. Camenisch J. L., Piveteau J.-M., Stadler M. A. Blind signatures based on the discrete logarithm problem. *Advances in Cryptology (EUROCRYPT'94). Proceedings. Lecture Notes in Computer Science.* Berlin, Springer Verlang Publ., 1995, vol. 950, pp. 428–432.

12. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484–1509.

13. Jozsa R. Quantum algorithms and the fourier transform. *Proceedings of the Royal Society of London. Series A*, 1998, vol. 454, pp. 323–337.

14. Yan S. Y. *Quantum attacks on public-key cryptosystems.* Boston, Springer Publ., 2013, 207 p.

15. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Digital signature scheme with doubled verification equation. *Computer Science Journal of Moldova*, 2020, vol. 28, no. 1 (82), pp. 80–103.

Received: January 18, 2020.
Accepted: June 04, 2021.

Authors' information:

Nikolay A. Moldovyan — Dr. Sci. in Technics, Professor, Chief Researcher; nmold@mail.ru

Alexandr A. Moldovyan — Dr. Sci. in Technics, Professor, Chief Researcher; maa1305@yandex.ru

Схема цифровой подписи на алгебре матриц 2×2

Н. А. Молдовян, А. А. Молдовян

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук,
Российская Федерация, 199178, Санкт-Петербург, 14-я линия В. О., 39

Для цитирования: *Moldovyan N. A., Moldovyan A. A.* Digital signature scheme on the 2×2 matrix algebra // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т. 17. Вып. 3. С. 254–261.
https://doi.org/10.21638/11701/spbu10.2021.303

Рассматривается структура матричной алгебры 2×2, заданной над основным конечным полем $GF(p)$. Показано, что эта алгебра содержит три типа коммутативных подалгебр порядка p^2, которые различаются между собой значением порядка их мультипликативной группы. Выведены формулы, описывающие количество подалгебр каждого типа. Создана новая схема постквантовой цифровой подписи, основанная на новой форме скрытой задачи дискретного логарифмирования. Схема отличается использованием скалярного умножения в качестве дополнительной операции, маскирующей скрытую циклическую группу, в которой выполняется базовая операция возведения в степень при генерации открытого ключа. Достоинствами разработанной схемы подписи являются сравнительно высокая производительность алгоритмов генерации и проверки подписи и возможность реализации на ее основе протокола слепой подписи.

Ключевые слова: цифровая подпись, постквантовая криптосхема, слепая подпись, скрытая задача логарифмирования, конечная ассоциативная алгебра, алгебра матриц.

Контактная информация:

Молдовян Николай Андреевич — д-р техн. наук, проф., гл. науч. сотр.; nmold@mail.ru

Молдовян Александр Андреевич — д-р техн. наук, проф., гл. науч. сотр.; maa1305@yandex.ru