Iran J Sci Technol Trans Sci (2022) 46:323–332
https://doi.org/10.1007/s40995-021-01257-3

RESEARCH PAPER

Blind Signature Protocol Based on Hidden Discrete Logarithm Problem Set in a Commutative Algebra

M. H. Nguyen[1] · D. N. Moldovyan[2] · N. A. Moldovyan[2] · M. Q. Le[3] · G. L. Nguyen[4]

Received: 22 June 2021 / Accepted: 17 December 2021 / Published online: 4 January 2022

Abstract
A new blind signature scheme is proposed which is characterized in that it is based on a hidden discrete logarithm problem defined in a finite commutative associative algebra. The used algebraic support represents a 4-dimensional commutative associative algebra defined over the ground finite field $GF(p)$, commutative group of which possesses 4-dimensional cyclicity. The public key represents a triple of vectors contained in different cyclic subgroup of the multiplicative group. Correspondingly, three different blinding factors are used to insure the anonymity property of the introduced blind signature protocol.

Keywords Information security · Post-quantum cryptography · Blind signature · Finite associative algebra · Commutative algebra · Multi-dimensional cyclicity

1 Introduction

Digital signature (DS) schemes are widely used in information technologies for solving different tasks of insuring information security (Rivest et al. 1978, ElGamal 1985). A particular type of the signature schemes, called blind signatures (Chaum 1983, Chaum 1988), represent a special interest for application in electronic cash systems and in electronic secret-voting systems. Specific requirements to the blind DS protocols are: (1) the signer has no access to the document during the procedure of forming the signature; (2) the signer does not have the ability to find a correlation of the signed document with the act of signing (anonymity or untraceability requirement).

✉ M. H. Nguyen
hieuminhmta@gmail.com

[1] Institute of Cryptographic Science and Technology, Hanoi, Vietnam

[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia

[3] Information Technology Institute, National University, Hanoi (VNU-ITI), Vietnam

[4] Institute of Information Technology, Vietnam Academy of Science and Technology, Hanoi, Vietnam

A variety of different known DS schemes can be used to satisfy the first requirement. To do this, it is enough to accept the agreement that the signature to the document is formed as a signature to the hash function calculated from the document. The first requirement is a necessary condition for the feasibility of the second requirement. To implement a DS protocol satisfying the second requirement a specific method is used, that consists in using a blinding factor (or factors) during the process of the signature generation.

The participants of a blind DS protocol are the signer and the requester (client) who has prepared some electronic document for signing. Protocols of such type are supposed to be used in information technologies where the signer performs signing of many documents provided by many different clients. The intention of the requester is to obtain a genuine signature of the signer to the document in such a way that in the future, when the signed document is presented to the signatory, the latter will not be able to identify which of the clients is associated with this document.

The first blind signature protocol (Chaum 1983) was developed on the basis of the RSA signature scheme (Rivest et al. 1978) that is based on the computational difficulty of the factoring problem (FP). Subsequently, blind DS protocols based on the computational difficulty of the discrete logarithm problem (DLP) have

been proposed (Camenisch 1995). In the first case the anonymity of the requester is ensured by his introducing one blinding factors into the blind signature. In the second case the anonymity is ensured by requester's introducing two blinding factors into the blind signature. The protocols are designed so that after receiving a blind signature from the signer, the requester can possibility to remove the blinding factors, thereby obtaining a genuine signature.

Like in the case of modern DS standards and other DS schemes of wide use, which are based on computational difficulty of FP and DLP, the said blind signature protocols will be insecure in coming post-quantum era (Yan 2014, Ding and Steinwandt 2018) when quantum attacks will become possible in practice. An attack on a cryptographic scheme is called quantum, if it uses both the ordinary and quantum computers. A cryptoscheme is called post-quantum, if it performs efficiently on ordinary computers and resists quantum attacks.

Post-quantum cryptographic algorithms and protocols should be based on the computationally difficult problems that are different from the FP and the DLP, since for solving them there are known polynomial algorithms (Shor 1997, Smolin et al. 2013). Quantum method for solving FP and DLP exploits (1) extreme efficiency of performing a discrete Fourier transform of a periodic function taking on values in an explicitly given finite cyclic group and (2) reduction of each of the mentioned two problems to problem of finding a period length of a periodic function (Jozsa 1988, Ekert and Jozsa 1996).

A response to such a challenge in the field of applied and theoretical cryptography was the announcement by the US National Institute of Standards and Technology (NIST) in December 2016 of a program of adopting post-quantum cryptographic standards of public-key agreement and digital signature schemes by 2024 (NIST 2016). A worldwide competition for the development of post-quantum public-key cryptoschemes had been started as a core part of that program (NIST 2020). The NIST program does not provide for the development of post-quantum blind signature protocols. However, this task is quite important and interesting.

The present paper is devoted to development of a practical post-quantum blind signature scheme based on computational difficulty of so called hidden discrete logarithm problem (HDLP). Next Sect. 2 describes in brief the concept of HDLP as a post-quantum cryptographic primitive and finite associative algebras (FAAs) as algebraic support of the HDLP-based public key cryptoschemes. Section 3 introduces the initial HDLP-based signature scheme suitable for transformation into a blind signature scheme. A novel 4-dimensional FAA with 4-dimensional cyclicity is used as algebraic support of the developed signature scheme. Section 4 proposes a practical post-quantum blind signature protocol using four blinding factors and a public key representing a triple of 512-bit integers. Section 5 presents discussion and Sect. 6 concludes the paper.

2 Preliminaries

The HDLP appears to be one of attractive cryptographic primitives for development of practical post-quantum public-key cryptoschemes. On the base of the HDLP, public-key agreement protocols (Kuzmin et al. 2017, Moldovyan-Dmitriy 2019), commutative encryption algorithms (Modovyan-Dmitriy et al. 2020, Modovyan-Nikolay and Modovyan-Alexander 2019), and DS schemes (Modovyan-Nikolay and Abrosimov 2019, Modovyan-Nikolay and Modovyan-Alexander 2020) had been designed. To reveal the concept of HDLP, consider the definition of DLP.

The latter is usually set in a given finite cyclic group of prime order q as finding the unknown value of the integer x in the equation $Y' = G'^x$, where G' is a generator of the group. The HDLP is set in a finite algebraic structure containing a very large number of different cyclic groups as different subsets of algebraic elements. One of such groups is selected at random and is secret, for example, the cyclic group generated by an element G. A random non-negative integer $x < q$ is generated and the value $Y' = G^x$ is calculated. Then the values Y' and G are mapped into the elements $Y = \alpha(Y')$ and $Z = \beta(G)$, where $\alpha(\cdot)$ and $\beta(\cdot)$ are masking operations possessing property of mutual commutativity with the exponentiation operation. Parameters of the masking operations are secret. The HDLP consists in finding the value x when the elements Y and Z are given. Different forms of the HDLP are introduced for development of different public key. In some particular forms of the HDLP only one of the values Y' and G is masked (Kuzmin et al. 2017, Moldovyan-Dmitriy 2010).

Finite associative algebras are used as algebraic supports of the HDLP-based cryptoschemes. An arbitrary vector A of some finite m-dimensional vector space defined over a finite field, for example over a ground field $GF(p)$, can be written as an ordered set of elements of the field $GF(p)$: $A = (a_0, a_1, \ldots, a_{m-1})$ or as a sum of its component: $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, where $\mathbf{e}_i$ are basis vectors; $a_i \in GF(p)$ are coordinated of the vector. A vector space in which, in addition to the operations of addition of vectors and multiplication of a vector by a scalar, an operation of multiplication of two vectors (the vector multiplication) is defined, which has the property of distributivity with respect to the operation of addition, is called algebra.

The vector multiplication operation $A = \sum_{i=0}^{m-1} a_i \mathrm{e}_i$ and $B = \sum_{j=0}^{m-1} b_j \mathrm{e}_j$ is usually determined by the rule of multiplying each component of the first vector with each component of the second vector, namely, by the following formula:

$$A \circ B = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j (e_i \circ e_j), \tag{1}$$

in which every product of the form $\mathrm{e}_i \circ \mathrm{e}_j$ must be replaced by a one-component vector $\lambda \mathbf{e}_k$, selected from the so-called multiplication table of basis vectors (MTBV), where $\lambda \in GF(p)$ is called structural constant. In the case $\lambda = 1$ only basis vector $\mathbf{e}_k$ is indicated in the MTBV. Left multiplier in the product $\mathrm{e}_i \circ \mathrm{e}_j$ specifies the row and the right one specifies the column, the intersection of which indicates the cell containing the value $\lambda \mathbf{e}_k$.

Taking into account the formula (1) one can prove that the defined vector multiplication operation is associative, if the used MTBV is such that the following equality holds true:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) \tag{2}$$

for all possible triples ($\mathbf{e}_i$, $\mathbf{e}_j$, $\mathbf{e}_k$). Note also that the defined vector multiplication and scalar multiplication by a scalar ψ are mutually commutative: $\psi(A \circ B) = (\psi A) \circ B = A \circ (\psi B)$.

If the vector multiplication operation, defined by a MTBV, has the properties of non-commutativity and associativity, then the case of specifying a non-commutative FAA is realized. Most of the different known forms of the HDLP had been proposed for non-commutative algebras used as algebraic support of the developed cryptoschemes. The paper (Modovyan-Nikolay and Modovyan-Alexander 2019) introduced a unified method for setting non-commutative FAAs of arbitrary even dimensions $m \geq 2$. The paper (Modovyan-Nikolay 2020) introduced another unified method for setting other type non-commutative FAAs of arbitrary even dimensions $m > 4$. For the case $m > 4$, the latter method defines a commutative FAA possessing multidimensional cyclicity. That 4-dimensional FAA was used in the paper (Minh et al. 2020) to define for the first time the HDLP in commutative algebras. The concept of multidimensional cyclicity was proposed in (Modovyan-Nikolay and Modovyanu-Peter 2009) as follows: a commutative finite group generated by a minimum generator system containing $\mu \geq 2$ elements of the same order is called a group possessing μ-dimensional cyclicity.

In present paper another form of the HDLP is set in a commutative FAA for developing a post-quantum signature scheme that is suitable for developing on its base a post-quantum blind signature protocol. Like in the case of the DS scheme from (Minh et al. 2020), the proposed form of the HDLP exploits the multidimensional structure of the commutative FAA used as algebraic support. However, the proposed form implements another criterion of post-quantum security than that implemented in (Minh et al. 2020). This difference gives possibility to design a signature scheme that is free from doubling the verification equation. Due to the last one has possibility to develop a HDLP-based blind signature protocol, in addition the signature has a smaller size. Besides, a new 4-dimensional commutative FAA is used as algebraic support of the introduced HDLP and developed signature schemes.

3 Initial Signature Scheme

3.1 The Used Algebraic Support

The 4-dimensional commutative FAA used as algebraic support is defined over the ground field $GF(p)$ by MTBV shown as Table 1.

Proposition 1 *The vector multiplication operation defined by Table 1 is associative.*

Proof Note that the Table 1 is described by the following formula:

$$e_i \circ e_j = \begin{cases} e_{i+j-2 \bmod 4}, & \text{if } i \bmod 2 = 0; \\ e_{i-j+2 \bmod 4}, & \text{if } i \bmod 2 = 1. \end{cases} \tag{3}$$

Consider the product of arbitrary three vectors A, B and $C = \sum_{k=0}^{m-1} c_k \mathrm{e}_k$, which is performed in correspondence with Table 1:

$$\begin{aligned} (A \circ B) \circ C &= \left(\sum_{i=0}^{3} \sum_{j=0}^{3} a_i b_j \mathrm{e}_i \circ \mathrm{e}_j \right) \circ \sum_{k=0}^{3} c_k \mathrm{e}_k \\ &= \sum_{i=0}^{3} \sum_{j=0}^{3} \sum_{k=0}^{3} a_i b_j c_k (\mathrm{e}_i \circ \mathrm{e}_j) \circ \mathrm{e}_k; \end{aligned} \tag{4.1}$$

$$\begin{aligned} A \circ (B \circ C) &= \left(\sum_{i=0}^{3} a_i \mathrm{e}_i \right) \circ \left(\sum_{j=0}^{3} \sum_{k=0}^{3} b_j c_k \mathrm{e}_i \circ \mathrm{e}_j \right) \\ &= \sum_{i=0}^{3} \sum_{j=0}^{3} \sum_{k=0}^{3} a_i b_j c_k \mathrm{e}_i \circ (\mathrm{e}_j \circ \mathrm{e}_k). \end{aligned} \tag{4.2}$$

Table 1 Setting a 4-dimensional FAA possessing multidimensional cyclicity ($\lambda = 4$)

$\circ$	e_0	e_1	e_2	e_3
e_0	$\lambda \mathrm{e}_2$	e_3	e_0	$\lambda \mathrm{e}_1$
e_1	e_3	e_2	e_1	e_0
e_2	e_0	e_1	e_2	e_3
e_3	$\lambda \mathrm{e}_1$	e_0	e_3	$\lambda \mathrm{e}_2$

The right parts in formulas (4.1) and (4.2) are equal, if equality (2) holds true for all possible triples of indices (i, j, k). Since the value of k does not influence on selection of one of two formulas in the right part of the expression (3), one should consider only the following four cases:

Case 1 i and j are even numbers.

$$\left.\begin{array}{l}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_{i+j-2} \circ \mathbf{e}_k = \mathbf{e}_{i+j-2+k-2} = \mathbf{e}_{i+j+k} \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ \mathbf{e}_{j+k-2} = \mathbf{e}_{i+j+k-2-2} = \mathbf{e}_{i+j+k}\end{array}\right\} \Rightarrow$$
$$\Rightarrow (\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k).$$

Case 2 i is odd; j is even.

$$\left.\begin{array}{l}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_{i-j+2} \circ \mathbf{e}_k = \mathbf{e}_{i-j+2-k+2} = \mathbf{e}_{i-j-k} \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ \mathbf{e}_{j+k-2} = \mathbf{e}_{i-j-k+2+2} = \mathbf{e}_{i-j-k}\end{array}\right\} \Rightarrow$$
$$\Rightarrow (\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k).$$

Case 3 i is even; j is odd.

$$\left.\begin{array}{l}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_{i+j-2} \circ \mathbf{e}_k = \mathbf{e}_{i+j-2-k+2} = \mathbf{e}_{i+j-k} \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ \mathbf{e}_{j-k+2} = \mathbf{e}_{i+j-k+2-2} = \mathbf{e}_{i+j-k}\end{array}\right\} \Rightarrow$$
$$\Rightarrow (\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k).$$

Case 4: i and j are odd numbers.

$$\left.\begin{array}{l}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_{i-j+2} \circ \mathbf{e}_k = \mathbf{e}_{i-j+2+k-2} = \mathbf{e}_{i-j+k} \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ \mathbf{e}_{j-k+2} = \mathbf{e}_{i-j+k-2+2} = \mathbf{e}_{i-j+k}\end{array}\right\} \Rightarrow$$
$$\Rightarrow (\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k).$$

Thus, for all possible triples $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$ the formula (2) holds true, i. e., the vector multiplication operation defined by Table 1 possesses the property of associativity. Proposition 1 is proven.

Proposition 2 *The 4-dimensional finite algebra set by Table 1 is commutative.*

Proof Note $\mathbf{e}_i \circ \mathbf{e}_j = \mathbf{e}_j \circ \mathbf{e}_i$, therefore, due to formula (1) we have $A \circ B = B \circ A$. Proposition 2 is proven.

Proposition 3 *The 4-dimensional FAA set by Table 1 contains a two-sided unit that is the vector $E = (0, 0, 1, 0)$.*

Proof Using formula (1) we have $A \circ E = \sum_{i=0}^{3} a_i(e_i \circ e_3) = \sum_{i=0}^{3} a_i e_i = A$ and $E \circ A = \sum_{j=0}^{3} a_j(\boldsymbol{e}_3 \circ \boldsymbol{e}_j) = \sum_{j=0}^{3} a_j \boldsymbol{e}_j = A$. Proposition 3 is proven.

A vector A for which the vector equation $A \circ X = E$ has a unique solution is called invertible vector. For a fixed invertible vector A the solution is denoted as A^{-1} and is called inverses of A. Evidently, $A \circ A^{-1} = A^{-1} \circ A = E$. To obtain invertibility condition one can consider the vector equation $A \circ X = E$ can be reduced to the following system of four equations with the unknown coordinates of the vector $X = (x_0, x_1, x_2, x_3)$:

$$\begin{cases} a_2x_0 + a_3x_1 + a_0x_2 + a_1x_3 = 1; \\ \lambda a_3x_0 + a_2x_1 + a_1x_2 + \lambda a_0x_3 = 0; \\ \lambda a_0x_0 + a_1x_1 + a_2x_2 + \lambda a_3x_3 = 0; \\ a_1x_0 + a_0x_1 + a_3x_2 + a_2x_3 = 0. \end{cases} \tag{5}$$

The main determinant of the system (5) is

$$\begin{aligned}\Delta &= \begin{vmatrix} a_2 & a_3 & a_0 & a_1 \\ \lambda a_3 & a_2 & a_1 & \lambda a_0 \\ \lambda a_0 & a_1 & a_2 & \lambda a_3 \\ a_1 & a_0 & a_3 & a_2 \end{vmatrix} = a_2 \begin{vmatrix} a_2 & a_1 & \lambda a_0 \\ a_1 & a_2 & \lambda a_3 \\ a_0 & a_3 & a_2 \end{vmatrix} - a_3 \begin{vmatrix} \lambda a_3 & a_1 & \lambda a_0 \\ \lambda a_0 & a_2 & \lambda a_3 \\ a_1 & a_3 & a_2 \end{vmatrix} \\ &\quad + a_0 \begin{vmatrix} \lambda a_3 & a_2 & \lambda a_0 \\ \lambda a_0 & a_1 & \lambda a_3 \\ a_1 & a_0 & a_2 \end{vmatrix} - a_1 \begin{vmatrix} \lambda a_3 & a_2 & a_1 \\ \lambda a_0 & a_1 & a_2 \\ a_1 & a_0 & a_3 \end{vmatrix} \\ &= a_2\left(a_2(a_2^2 - \lambda a_3^2) - a_1(a_1a_2 - \lambda a_0a_3) + \lambda a_0(a_1a_3 - a_0a_2)\right) \\ &\quad - a_3\left(\lambda a_3(a_2^2 - \lambda a_3^2) - a_1(\lambda a_0a_2 - \lambda a_1a_3) + \lambda a_0(\lambda a_0a_3 - a_1a_2)\right) \\ &\quad + a_0\left(\lambda a_3(a_1a_2 - \lambda a_0a_3) - a_2(\lambda a_0a_2 - \lambda a_1a_3) + \lambda a_0(\lambda a_0^2 - a_1^2)\right) \\ &\quad - a_1\left(\lambda a_3(a_1a_3 - a_0a_2) - a_2(\lambda a_0a_3 - a_1a_2) + a_1(\lambda a_0^2 - a_1^2)\right) = \ldots \\ &= \lambda^2(a_0^2 + a_3^2)^2 - 4\lambda a_0^2a_3^2 + (a_1^2 + a_2^2)^2 - 4\lambda a_0^2a_3^2 \\ &\quad - 2\lambda(a_0^2 + a_3^2)(a_1^2 + a_2^2) + 8\lambda a_0a_1a_2a_3 = \ldots \\ &= (\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2)^2 - 4(\lambda a_0a_3 - a_1a_2)^2.\end{aligned}$$

The system (5) has unique solution, if $\Delta \neq 0$, and has no solution, if $\Delta = 0$. Therefore, we have the following invertibility condition:

$$(\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2)^2 - 4(\lambda a_0a_3 - a_1a_2)^2 \neq 0 \tag{6}$$

and the non-invertibility condition

$$(\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2)^2 = 4(\lambda a_0a_3 - a_1a_2)^2. \tag{7}$$

The set of all invertible vectors compose a finite commutative group called multiplicative group of the algebra.

Proposition 4 *If the structural constant λ is a quadratic non-residue, then the number of non-invertible vectors in the 4-dimensional FAA set by Table 1 is equal to $\eta = 2p^2 - 1$ and the order of the multiplicative group of the algebra is equal to $\Omega = (p^2 - 1)^2$.*

Proof Formula (7) sets the following two cases

$$\begin{aligned}\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 = 2\lambda a_0a_3 - 2a_1a_2 &\Rightarrow \lambda(a_0 - a_3)^2 \\ &= (a_1 - a_2)^2;\end{aligned}$$

$$\begin{aligned}\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 = -2\lambda a_0a_3 + 2a_1a_2 &\Rightarrow \lambda(a_0 + a_3)^2 \\ &= (a_1 + a_2)^2.\end{aligned}$$

Since the structural constant λ is a quadratic non-residue, in the first case the equality holds true only if $(a_0 - a_3)^2 = (a_1 - a_2)^2 = 0$. This gives p^2 different sets of coordinates a_0, a_1, a_2, and a_3, including (0, 0, 0, 0). In the second case the equality holds true only if $(a_0 + a_3)^2 = (a_1 + a_2)^2 = 0$. This gives other p^2 different sets of coordinates a_0, a_1, a_2, and a_3, including (0, 0, 0, 0). Therefore,

we have $\eta = 2p^2 - 1$ and $\Omega = p^4 - \eta = (p^2 - 1)^2$. Proposition 4 is proven.

Proposition 5 *If the structural constant λ is a quadratic residue in GF(p), then the number of non-invertible vectors in the 4-dimensional FAA set by Table 1 is equal to $\eta = 4p^3 - 6p^2 + 4p^2 - 1$ and the order of the multiplicative group of the algebra is equal to $\Omega = (p - 1)^4$.*

Proof Since the structural constant λ is a quadratic residue, formula (7) defines the following two cases

$$\left(a_0\sqrt{\lambda} - a_3\sqrt{\lambda}\right)^2 = (a_1 - a_2)^2 \Rightarrow a_0\sqrt{\lambda} - a_3\sqrt{\lambda} = \pm(a_1 - a_2);$$

$$\left(a_0\sqrt{\lambda} + a_3\sqrt{\lambda}\right)^2 = (a_1 + a_2)^2 \Rightarrow a_0\sqrt{\lambda} + a_3\sqrt{\lambda} = \pm(a_1 + a_2).$$

Sets of coordinates (a_0, a_1, a_2, a_3) satisfying four conditions defined by the said two cases represent non-invertible vectors. The following Table 2 shows the number of vectors coordinates of which satisfy every of the conditions.

Total number of non-invertible vectors equals to $\eta = p^2 + p^2 + 2p(p-1)^2 + 2p\ (p-1)^2 = 4p^3 - 6p^2 + 4p - 1$.

The order of the multiplicative group of the algebra is equal to $\Omega = p^4 - \eta = (p - 1)^4$. Proposition 5 is proven.

In the first case the equality holds true only if $(a_0 - a_3)^2 = (a_1 - a_2)^2 = 0$. This gives p^2 different sets of coordinates a_0, a_1, a_2, and a_3, including (0, 0, 0, 0). In the second case the equality holds true only if $(a_0 + a_3)^2 = (a_1 + a_2)^2 = 0$. This gives other p^2 different sets of coordinates a_0, a_1, a_2, and a_3, including (0, 0, 0, 0). Therefore, we have $\eta = 2p^2 - 1$ and $\Omega = p^4 - \eta = (p^2 - 1)^2$.

Like in the case of the commutative FAA introduced in (Minh et al. 2020), the said group has a 4-dimensional (2-dimensional) cyclicity, if the structural constant λ is equal to the quadratic residue (non-residue) in the field $GF(p)$. In the case of forming a group with 2-dimensional cyclicity, its basis includes two vectors, each of which has order equal to $p^2 - 1$, and order of the group is equal to $(p^2 - 1)^2$. Tables 3 and 4 present some examples of vectors V having the maximum possible order for the said two cases of the value of structural constant λ, when p = 14,377,379 (q = 7,188,689).

When developing the HDLP-based DS scheme in this section, we will consider the case of 4-dimensional cyclicity, when the basis of the multiplicative group Γ includes four vectors, each of which has order equal to $p - 1$, and order of the group is equal to $(p - 1)^4$. It is also assumed that $\lambda = 4$ and the characteristic p of the field $GF(p)$ is equal to a prime number having the structure $p = 2q + 1$, where q is a 512-bit prime. The generation of the required primes p is done by generating many different 512-bit primes q and testing the values $p = 2q + 1$ for primarily. Table 5 presents some examples of prime values of q of different size for which the value $2q + 1$ is prime.

Table 3 Vectors V having maximum order equal to $p - 1$ (λ is a quadratic residue)

λ	V
4	(10,372,179; 12,177,379; 13,377,372; 11,379,279)
9	(10,012,378; 7,869,534; 11,375,847; 10,957,689)
25	(12,939,641; 7,188,689; 7,188,689; 1,437,738)
3	(12,546,341; 7,321,689; 7,172,509; 1,070,538)
5	(12,546,341; 7,321,689; 7,172,509; 1,070,538)

Table 4 Vectors V having maximum order $p^2 - 1$ (λ is a quadratic non-residue)

λ	V
2	(9,070,865; 7,301,638; 7,130,538; 3,946,004)
7	(10,172,835; 9,301,504; 7,781,209; 3,559,757)
8	(10,182,970; 9,305,010; 1,155,039; 3,595,514)
11	(10,172,835; 9,303,505; 7,751,209; 3,555,757)
17	(13,132,970; 7,235,015; 1,355,089; 2,791,514)

Table 2 Number of subsets of non-invertible vectors for the case when λ is a quadratic residue

Condition	# of different combinations of coordinates (a_0, a_1, a_2, a_3)
$a_0\sqrt{\lambda} - a_3\sqrt{\lambda} = a_1 - a_2 = 0$	p^2 including (0, 0, 0, 0)
$a_0\sqrt{\lambda} + a_3\sqrt{\lambda} = a_1 + a_2 = 0$	p^2 including (0, 0, 0, 0)
$a_0\sqrt{\lambda} - a_3\sqrt{\lambda} = \pm(a_1 - a_2) \neq 0$	$2p(p - 1)^2$
$a_0\sqrt{\lambda} + a_3\sqrt{\lambda} = \pm(a_1 + a_2) \neq 0$	$2p(p - 1)^2$)

Table 5 Specially selected prime values of q

q (bit length of q)	p
1,156,112,201 (32)	2,312,224,403
6,785,973,453,813,842,891 (64)	13,571,946,907,627,685,783
15,777,278,116,070,701 3,851,236,586,330,907,166,231 (128)	31,554,556,232,141,402,770 2,473,172,661,814,332,463
294,376,761,264,963,048,730,708,277,251 2,639,408,627,270,785,989,333 5,935,514,953,423,851,321,991,519 (256)	5,887,535,225,299,260,974,614,165,545 0,252,788,172,545,415,719,786,671 871,029,906,847,702,643,983,039
35,687,538,543,572,407,882,858,303,216,507 61,155,407,334,331,566,376,142,966,145,846 64,045,696,352,628,128,923,744,450,422,769 90,309,175,242,333,397,008,877,768,843,061 17,702,415,790,074,075,810,133,363 (512)	71,375,077,087,144,815,765,716,606,433,015 2,231,081,466,866,313,275,228,593,229 169,328,091,392,705,256,257,847,488,900 84,553,980,618,350,484,666,794,017,755,537 68,612,235,404,831,580,148,151,620,266,727

3.2 Signature scheme

To develop a HDLP-base DS scheme we use the primary group of the order q^4 contained in the multiplicative group of the algebra. For generating a minimum generator system $< G_1, G_2, G_3, G_4 >$, the probabilistic method described in (Minh et al. 2020) can be used. That method involves the generation of random four vectors of order q, which with probability about $1 - q^{-1}$ form a minimum generator system of the mentioned primary group. Suppose that the four vectors G_1, G_2, G_3, and G_4 have been produced.

Procedure for generating a public key in the developed signature scheme includes the following steps:

1. Generate at random three non-negative integers $x < q$, $w < q$, and $\mu < p$, where μ is a primitive element modulo p.
2. Calculate the vector $Y = {G_1}^x \circ {G_2}^w$.
3. Calculate the vector $Z = \mu G_1 \circ {G_3}^{1/x}$.
4. Calculate the vector $U = G_2 \circ {G_3}^{-1/w}$.

The produced public key represents the triple (Y, Z, U) of 4-dimensional vectors contained in three different cyclic subgroups of the primary group.

The *signature generation algorithm* is as follows:

1. Generate at random non-negative integers $k < q$, and $\rho < p$.
2. Compute the integer $t = kwx^{-1} \bmod q$.
3. Compute the fixator $R = \rho G_1^k \circ G_2^t$.
4. Compute the first signature element $e = f_h(M, R)$, where f_h is a pre-agreed 512-bit collision-resistant hash function; M is a document to be signed.
5. Compute the second signature element $s = k - ex \bmod q$.
6. Compute the third signature element $d = t - ew \bmod q$.
7. Compute the fourth signature element $\psi = \rho\mu^{-s} \bmod p$.

This algorithm outputs the 2049-bit signature in the form of three 512-bit integers e, s, d and one 513-bit integer ψ.

The procedure for verifying the authenticity of the signature (e, s, d, ψ) to the document M is performed using the public key (Y, Z, U) as follows.

The signature verification algorithm:

1. Compute the vector $R^* = \psi Y^e \circ Z^S \circ U^d$.
2. Compute the hash value $e^* = f_h(M, R^*)$.
3. If $e^* = e$, then the signature is accepted as genuine one. Otherwise the signature is rejected as a false one.

Consider a signature (e, s, d, ψ) to a document M, which have been correctly computed in full correspondence with the signature generation algorithm. To prove correctness of the developed DS scheme we show that the said signature passes the verification procedure as a genuine signature:

$$
\begin{aligned}
R^* &= \psi Y^e \circ Z^s \circ U^d \\
&= \rho\mu^{-s} G_1^{ex} \circ G_2^{ew} \circ \mu^s G_1^s \circ G_3^{s/x} \circ G_2^d \circ G_3^{-d/w} \\
&= \rho G_1^{ex} \circ G_2^{ew} \circ G_1^{k-ex} \circ G_3^{(k-ex)/x} \circ \\
&\circ G_2^{t-ew} \circ G_3^{-(t-ew)/w} \\
&= \rho G_1^{ex} \circ G_2^{ew} \circ G_1^{k-ex} \circ G_3^{k/x-e} \circ \\
&\circ G_2^{t-ew} \circ G_3^{-t/w+e} \\
&= \rho G_1^{ex} \circ G_2^{ew} \circ G_1^{k-ex} \circ G_3^{k/x-e} \circ \\
&\circ G_2^{t-ew} \circ G_3^{-k/x+e} = \rho G_1^k \circ G_2^t = R \\
&\Rightarrow f_h(M, R^*) = f_h(M, R) \Rightarrow e^* = e
\end{aligned}
$$

One should note that the owner of the public key (Y, Z, U) has possibility to use an alternative method for computing the signature, which is the same as the described signature generation algorithm, except the steps 3 and

7. The latter in the alternative signature generation algorithm are as follows:

3. Compute the vector $R = \rho Z^k \circ U^t$

7. Compute the fourth signature element $\psi = \rho\mu^{k-s} \bmod p$.

Since $Z^k \circ U^t = \mu^k G_1^k \circ G_2^t$, the alternative algorithm for computing a signature performs correctly and allows one to use only two 512-bit integers x and w and 513-bit integer μ as a 1537-bit private key instead of using five private values x, w, μ, G_1, and G_2 as 5641-bit private key.

Security of the described signature scheme is based on the particular form of the HDLP that is supposedly hard and can be defined as follows: *for the given triple of vectors* (Y, Z, U) *find the triple of integers* (x, w, μ) *such that* $Y = \mu^{-x} Z^x \circ U^w$.

Security of the proposed signature algorithm Security definition of the proposed signature scheme we formulate as follows: *to forge a signature is computationally infeasible*.

Like in the case of the Schnorr signature scheme (Schnorr 1991) the first signature element e is the hash-function value computed from the document M to which the fixator value R is concatenated and the right part of the verification equation (indicated in item 1 of the signature verification algorithm) is equal to R, if the signature is valid (genuine). We suppose the hash function used in the proposed signature scheme is secure and possesses no weaknesses that can be used to forge a signature. Therefore, a forging algorithm is an algorithm that computes a valid signature after computing the fixator value R and the hash value e. The fixator value R is defined by the randomization integers $k < q$ and $\rho < p$.

Proposition 6 *Existence of a polynomial algorithm for forging a signature means existence of a polynomial algorithm for solving the underlying HDLP.*

Argumentation. The supposed forging algorithm uses no weakness of the hash function, therefore, it works equally well for different hash functions and different values of the fixator R. Suppose the forging algorithm computes two signatures (e_1, s_1, d_1, ψ_1) and (e_2, s_2, d_2, ψ_2) for two different hash functions, but the same value of the fixator R, i. e., we have two different verification equations with the same value of the left part. Therefore, one can write

$$
\begin{aligned}
&R^* = \psi_1 Y^{e_1} \circ Z^{s_1} \circ U^{d_1} = \psi_2 Y^{e_2} \circ Z^{s_2} \circ U^{d_2} \\
&\Rightarrow \frac{\psi_1}{\psi_2} Y^{e_1-e_2} \circ Z^{s_1-s_2} \circ U^{d_1-d_2} = E \\
&\Rightarrow \frac{\psi_1}{\psi_2} G_1^{x(e_1-e_2)} \circ G_2^{w(e_1-e_2)} \circ \mu^{s_1-s_2} G_1^{s_1-s_2} \circ \\
&\circ G_3^{(s_1-s_2)/x} \circ G_2^{d_1-d_2} \circ G_3^{-(d_1-d_2)/w} = E \\
&\Rightarrow \frac{\psi_1}{\psi_2} \mu^{s_1-s_2} G_1^{x(e_1-e_2)+s_1-s_2} \circ G_2^{w(e_1-e_2)+d_1-d_2} \circ \\
&\circ G_3^{(s_1-s_2)x^{-1}-(d_1-d_2)w^{-1}} = E
\end{aligned}
$$

$$
\Rightarrow \left\{ \begin{array}{c} \frac{\psi_1}{\psi_2} \mu^{s1-s2} \equiv 1 \bmod p \\ x(e_1 - e_2) + s_1 - s_2 \equiv 0 \bmod q \\ w(e_1 - e_2) + d_1 - d_2 \equiv 0 \bmod q \\ (s_1 - s_2)x^{-1} - (d_1 - d_2)w^{-1} \equiv 0 \bmod q \end{array} \right\}.
$$

If the value $s_2 - s_1$ is even, then repeat the forging signature procedure for another fixator value (generate new random values k and ρ and compute a new value of R), until the odd value $s_2 - s_1$ is obtained. Then one can easily get the following:

$$x = (s_2 - s_1)(e_1 - e_2)^{-1} \bmod q,$$

$$w = (d_2 - d_1)(e_1 - e_2)^{-1} \bmod q, \text{ and}$$

$$\mu = (y_1^{-1} y_2)(s_2 - s_1)^{-1} \bmod p - 1 \bmod p$$

Thus, taking into account that operation of finding odd-degree roots in $GF(p)$, where $p = 2q + 1$, has polynomial computational complexity, one can conclude that a polynomial algorithm for forging a signature is reducible to a polynomial algorithm of solving the HDLP underlying the introduced signature scheme.

One can note that the described security proof is based on the ideas of the reductionist security proof (Pointcheval and Stern 2000, Koblitz and Menezes 2007) that was applied to the Schnorr signature algorithm (Schnorr 1991).

4 Blind signature protocol

Like in the known DLP-base signature schemes, in the developed HDLP-based signature the main contribution to the security is introduced by the exponentiation operations performed during the procedures for generating the public key, computing the signature, and verifying the signature. However, the fundamental difference of the latter is the following two points: i) when calculating the public key, the exponentiation operations are performed in two different finite cyclic groups, and 2) these two groups are hidden due to masking multiplications by the vectors $G_3^{1/x}$

and $G_3{}^{-1/w}$ belonging to the third cyclic group and masking scalar multiplication by integer ψ. Due to the marked differences of the developed DS scheme, the elements of the public key (Y, Z, U) belong to three different cyclic groups.

The proposed signature verification equation $R^* = \psi Y^e \circ Z^S \circ U^d$ includes factors of four types, therefore in the blind signature protocol based on the developed HDLP-based signature scheme one should use blinding factors of four different types: β, Y^{ε}, Z^{σ}, and U^{τ}. Thus, like in the case of known DLP-based blind DS protocols (Camenisch et al. 1995, Pointcheval and Stern 2000), a requester participating in process of generating a blind signature is to execute generation of four uniformly random integers $\beta < p$, $\varepsilon < q$, $\sigma < q$, and $\tau < q$, followed by computing the said four blinding factors.

The proposed HDLP-based blind digital signature protocol includes the following steps:

1. The signer generates two random non-negative integers $k < q$ and $\rho < p$ and computes the integer $t = kwx^{-1}$ - mod q. Then he calculates the vector $\overline{R} = \rho Z^{k} \circ U^{t}$. Then he sends the value of $\overline{R}$ to the requester who wish to obtain a genuine signer's signature to the document M (that is unknown to the signer).
2. The requester generates four uniformly random natural numbers $\beta < p$, $\varepsilon < q$, $\sigma < q$, and $\tau < q$, calculates the vector $R = \beta\overline{R} \circ Y^{\varepsilon} \circ Z^{\sigma} \circ U^{\tau}$ and the first element e of genuine signature: $e = f_h(M,R)$.
3. The requester then calculates the first element of the blind signature $\overline{e} = e - \varepsilon \bmod q$ and sends it to the signer.
4. Using his private key (x, w, μ), the signer calculates the second $\overline{s}$, the third $\overline{d}$, and the fourth $\overline{\psi}$ elements of blind signature: $\overline{S} = k - \overline{e}\,x \bmod q$, $\overline{d} = t - \overline{e}\,w \bmod q$, and $\overline{\psi} = \rho\ \mu^{-s\overline{e}} \bmod p$. He then sends the values $\overline{s}$, $\overline{d}$, and $\overline{\psi}$ to the requester.
5. Using the value $\overline{s}$, $\overline{d}$, and $\overline{\psi}$,the requester calculates the second s, third d and fourth ψ elements of genuine signer's signature to the document M: $s = \overline{s} + \sigma \bmod q$, $d = \overline{d} + \tau \bmod q$, and $\psi = \overline{\psi}\ \beta$.

Procedure for verifying a signature (e, s, d, ψ) to the document M is executed using the public key (Y, Z, U) and the signature verification algorithm of the initial HDLP-based signature scheme (see Sect. 3).

The correctness of the described blind signature protocol can be proved by substituting the signature for the input of the specified verification procedure and demonstrating that it passes verification as a genuine signature.

The proof of correctness of the blind digital signature protocol based on computational difficulty of the HDLP:

$$\begin{aligned} R* &= \psi Y^e \circ Z^s \circ U^d \\ &= \overline{\psi}\beta Y^{\overline{e}+\varepsilon} \circ Z^{\overline{s}+\sigma} \circ U^{\overline{d}+\tau} \\ &= \beta\overline{\psi} Y^{\overline{e}} \circ Z^{\overline{s}} \circ U^{\overline{d}} \circ Y^{\varepsilon} \circ Z^{\sigma} \circ U^{\tau} \\ &= \beta\overline{R} \circ Y^{\varepsilon} \circ Z^{\sigma} \circ U^{\tau} \\ \Rightarrow f_h(M,R*) &= f_h(M,R) \Rightarrow e* = e \end{aligned}$$

To demonstrate that that anonymity is provided, consider a blind signature $(\overline{e}, \overline{s}, \overline{\psi})$ computed correctly and an arbitrary genuine signature (e, s, d, ψ).

$$\left.\begin{array}{l} R = \psi Y^e \circ Z^s \circ U^d \\ \overline{R} = \overline{\psi} Y^{\overline{e}} \circ Z^{\overline{s}} \circ U^{\overline{d}} \end{array}\right\} \Rightarrow\ R = \frac{\psi}{\overline{\psi}}\overline{R} \circ Y^{e-\overline{e}} \circ Z^{s-\overline{s}} \circ U^{d-\overline{d}}.$$

Thus, the signatures $\left(\overline{e}, \overline{s}, \overline{d}, \overline{\psi}\right)$ and (e, s, d, ψ) are connected via some random values $\varepsilon = e - \overline{e}$; $\sigma = s - \overline{s}$ and $\tau = d - \overline{d}$, $\beta = \psi\overline{\psi}^{-1}$, therefore, having a given genuine signature, the signer is unable to distinguish the blind signature associated with the given authentic signature.

5 Discussion

For the first time, the implementation of a HDLP-based signature schemes on commutative FAAs was proposed in the paper (Minh et al. 2020). The main common features of the DS schemes presented in Sect. 3 and in (Minh et al. 2020) are:

(1) A commutative FAA multiplicative group of which has 4-dimensional cyclicity is used as algebraic support of the signature scheme;
(2) Computational difficulty of the HDLP is used to provide resistance to quantum attacks.

These two DS schemes have a number of significant differences, which are due to the use of different criteria for ensuring post-quantum resistance. The signature scheme from (Minh et al. 2020) satisfies the general criterion of post-quantum resistance introduced in (Moldovyan-Dmitriy et al. 2020), which can be formulated as follows: *the signature scheme should be constructed so that setting periodic functions based on public parameters of the scheme, which contain a period with the length depending on the value of discrete logarithm, is a computationally difficult problem*.

To satisfy the said design criterion, which is oriented to ensuring resistance to the both known and possible future quantum algorithm for finding a period length of periodic functions, the signature scheme (Minh et al. 2020) uses the method of doubling the verification equation, like that described in (Moldovyan-Dmitriy et al. 2020). In that method one of the signature elements represents an element of the algebra. Because of the latter, the public key size and signature size in (Minh et al. 2020) are quite large. Besides,

Table 6 Comparison with some known HDLP-based signature schemes (for the case of 512-bit value p)

Signature scheme	Signature size, byte	Public key size, byte	Computational complexity of signature generation, multiplications in $GF(p)$	Computational complexity of signature verification, multiplications in $GF(p)$
(Minh et al. 2020)	384	1024	4,608	3,072
(Moldovyan-Dmitriy et al. 2020)	384	1024	2,303	3,072
Proposed in Sect. 3	$\approx$ 256	$\approx$ 768	$\approx$ 2,304	$\approx$ 2,304
Proposed blind DS protocol	$\approx$ 256	$\approx$ 768	$\approx$ 4,608	$\approx$ 2,304

it is not evident how to develop a blind signature protocol on the base of the DS scheme from (Minh et al. 2020).

In the proposed signature scheme, we use a particular design criterion of post-quantum resistance that is oriented to ensuring security to the known quantum attacks (Shor 1997, Ekert and Jozsa 1996), that was used in (Moldovyan-Nikolay and Moldovyan-Alexander 2019, Moldovyan-Nikolay and Abrosimov 2019) for developing HDLP-based signature schemes on non-commutative FAAs. One can propose the following formulation of the used particular criterion: *a periodic function f set on the base of public parameters of the signature scheme and containing a period with the length depending on the discrete logarithm value should take on values in different finite cyclic groups contained in the algebraic support of the signature scheme and no cyclic group can be pointed out as a preferable cyclic group for the values of the function f.*

You can specify a periodic function from three integer variables i, j, and k with contains periods with the lengths (hx^{-1}, h, hxw^{-1}) depending on the values of x and of $w : F(i,j,k) = Y^i \circ Z^j \circ U^k$. However, the values of the function $F(i,j,k)$ lie in many different cyclic groups contained in the primary subgroup of order q^3, which is generated by the minimum generator system $< G_1, G_2, G_3 >$. At the same time, it is impossible to distinguish any fixed cyclic group, which with a significant probability includes the values of the function $F(i, j, k)$. This circumstance does not allow one to apply the quantum Shor algorithm (Shor 1997) to find the length of a period of the function $F(i, j, k)$ and then to find the values of x and of w.

The signature schemes described in Sect. 3 is characterized in the following features:

1. the signature scheme is set in a hidden commutative group with 2-dimensional cyclicity, therefore the discrete logarithm represents a pair of integers x and w (the hidden group is set by secret vectors G_1 and G_2);
2. the public key elements Z and U represent the masked forms of the vectors G_1 and G_2 representing a minimum generator system of the hidden group (the masking is performed as scalar multiplication by the integer ψ and multiplications by the vectors ${G_3}^{1/x}$ and ${G_3}^{-1/w}$ contained in the cyclic group generated the vector G_3 that together with the vectors G_1 and G_2 composes a minimum generator system of a primary group of order q^3 which has 3-dimensional cyclicity);
3. the powers of the masking factors ${G_3}^{1/x}$ and ${G_3}^{-1/w}$ are chosen so that their contribution to the left part of the verification equation is reduced to the multiplication by the unit element of the algebra (this is also due to specific generation of the signature randomization integers k and t; note also that due to the used scalar multiplication by the integer ψ the vectors Y, Z, and U compose a generator system of some group containing a primary subgroup possessing 3-dimensional cyclicity and order q^3).

The developed HDLP-based signature scheme and blind signature protocol are candidates for practical post-quantum public-key cryptoschemes due to sufficiently small size of public key and signature (see Table 6).

The developed DS scheme and protocol use a novel 4-dimensional commutative FAA, however they can be implemented using the 4-dimensional commutative FAA described in (Minh et al. 2020).

6 Conclusion

A novel HDLP-based signature scheme on a commutative FAA is proposed and used to develop a practical post-quantum blind signature protocol. The advantages of the introduced scheme and protocol are comparatively small size of public key and signature.

Acknowledgements We would like to express our sincere gratitude to the anonymous referee for his/her helpful comments that will help to improve the quality of the manuscript.

Author contributions Minh N.H and Moldovyan N.A has directed the conceptualization, formal analysis, writing—original draft preparation, writing—review & editing. Modovyan D.N, Minh L.Q and

Giang N.L have directed the conceptualization, formal analysis, writing—review & editing. All authors reviewed and approved the final manuscript.

Funding This research is supported by RFBR (project # 21–57-54001-Вьет_а) and by Vietnam Academy of Science and Technology (project # QTRU01.13/21–22).

Declarations

Conflict of interest The authors declare that they have no competing interests.

Availability of data and material Not applicable.

Code availability Not applicable.

Ethical approval Not applicable.

Consent to participate Not applicable.

Consent for publication Not applicable.

References

Rivest RL, Shamir A, Adleman LM (1978) A method for obtaining digital signatures and public key cryptosystems. Commun ACM 21(2):120–126

ElGamal T (1985) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inform Theory 31(4):469–472

Chaum D (1988) Blind Signature Systems. U.S. Patent # 4,759,063

Chaum D (1983) Blind signatures for untraceable payments. advances in cryptology: Proc. of CRYPTO'82. Plenum Press, pp. 199–203

Camenisch JL, Piveteau JM, Stadler MA (1995) Blind Signatures Based on the Discrete Logarithm Problem. Advances in Cryptology - EUROCRYPT '94 volume 950 of LNCS, Springer Verlang, pp 428–432

Yan SY (2014) Quantum attacks on public-key cryptosystems. Springer, US, p 207

Ding J, Steinwandt R (2018) Post-Quantum Cryptography. 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019, Proceedings. Lecture Notes in Computer Science series. Springer, vol. 11505

Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. SIAM J Comput 26:1484–1509

Smolin JA, Smith G, Vargo A (2013) Oversimplifying quantum factoring. Nature 499(7457):163–165

Jozsa R (1988) Quantum algorithms and the Fourier transform. Proc Royal Soc A 454:323–337

Ekert A, Jozsa R (1996) Quantum computation and Shor's factoring algorithm. Rev Mod Phys 68:733–752

NIST (2016) Federal Register. announcing request for nominations for public-key post-quantum cryptographic algorithms. Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (accessed January 10, 2021)

NIST (2020) Post-Quantum Cryptography. Round 3 Submissions. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (accessed January 10, 2021)

Kuzmin AS, Markov VT, Mikhalev AA, Mikhalev AV, Nechaev AA (2017) Cryptographic algorithms on groups and algebras. J Math Sci 223(5):629–641

Moldovyan-Dmitriy N (2019) Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem. Comput Sci J Moldova 27(79):56–72

Moldovyan-Dmitriy N, Moldovyan-Nikolay A, Moldovyan-Alexander A (2020) Commutative encryption method based on hidden logarithm problem. Bullet South Ural State Univ Ser Math Model Programm Comput Softw 13(2):54–68

Moldovyan-Nikolay A, Moldovyan-Alexander A (2019) Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem. Bullet South Ural State Univ Ser Math Model Programm Comput Softw 12(1):66–81

Moldovyan-Nikolay A, Abrosimov IK (2019) Post-quantum electronic digital signature scheme based on the enhanced form of the hidden discrete logarithm problem. Vestnik Saint Petersburg Univ Appl Math Comput Sci Control Process 15(2):212–220 (**(In Russian)**)

Moldovyan-Nikolay A, Moldovyan-Alexander A (2020) Candidate for practical post-quantum signature scheme. Vestnik Saint Petersburg Univ Appl Math Comput Sci Control Process 16(4):455–461

Moldovyan-Dmitriy N (2010) Non-commutative finite groups as primitive of public-key cryptoschemes. Quasigroups Relat Syst 18:165–176

Moldovyan-Nikolay A (2020) Unified method for defining finite associative algebras of arbitrary even dimensions. Quasigroups Relat Syst 26(2):263–270

Minh NH, Moldovyan-Alexander A, Moldovyan-Nikolay A, Canh HN (2020) A new method for designing post-quantum signature schemes. J Commun 15(10):747–754

Moldovyan-Dmitriy N, Moldovyan-Alexander A, Moldovyan-Nikolay A (2020) Digital signature scheme with doubled verification equation. Comput Sci J Moldova 28(82):80–103

Moldovyan-Nikolay A, Moldovyanu-Peter A (2009) New primitives for digital signature algorithms. Quasigroups Relat Syst 17(2):271–282

Pointcheval D, Stern J (2000) Security arguments for digital signatures and blind signatures. J Cryptol 13:361–396

Koblitz N, Menezes AJ (2007) Another look at "provable security." J Cryptol 20:3–37

Schnorr CP (1991) Efficient signature generation by smart cards. J Cryptol 4:161–174