LINE: Cryptosystem based on linear equations for logarithmic signatures

Gennady Khalimov[1], Yevgen Kotukh[2], Maksym Kolisnyk[1], Svitlana Khalimova[1], Oleksandr Sievierinov[1] and Maksym Korobchynskyi[2]

[1] *Kharkiv National University of Radioelectronics, Kharkiv, 61166, Ukraine*
[2] *Yevhenii Bereznyak Military Academy, Kyiv, 04050, Ukraine*

Abstract

The discourse herein pertains to a directional encryption cryptosystem predicated upon logarithmic signatures interconnected via a system of linear equations (henceforth referred to as LINE). A logarithmic signature serves as a foundational cryptographic primitive within the algorithm, characterized by distinct cryptographic attributes including nonlinearity, non-commutativity, unidirectionality, and factorizability by key. The confidentiality of the cryptosystem is contingent upon the presence of an incomplete system of equations and the substantial ambiguity inherent in the matrix transformations integral to the algorithm. Classical cryptanalysis endeavors are constrained by the potency of the secret matrix transformation and the indeterminacy surrounding solutions to the system of linear equations featuring logarithmic signatures. Such cryptanalysis methodologies, being exhaustive in nature, invariably exhibit exponential complexity. The absence of inherent group computations within the algorithm, and by extension, the inability to exploit group properties associated with the periodicity of group elements, serves to mitigate quantum cryptanalysis to Grover's search algorithm.

LINE, predicated upon an incomplete system of linear equations, embodies security levels ranging from 1 to 5, as stipulated by the National Institute of Standards and Technology (NIST), and thus presents a promising candidate for the construction of post-quantum cryptosystems.

Keywords

LINE, Post-quantum cryptosystem, Logarithmic signature, Directional encryption.

1. Introduction

Computationally complex problems, commonly referred to as "hard problems," encompass a wide array of issues for which a substantial, preferably insurmountable, allocation of resources is necessitated for resolution. Within the realm of cryptography, these problems serve as the foundational bedrock for secure cryptographic schemes. Typically, this is achieved by establishing a correlation between the scheme's security and the infeasibility of solving the associated complex problem. Historically, two predominant complex problems, or their derivatives, have held sway in public-key cryptography: integer factorization and discrete logarithmization. RSA integers and discrete logarithms within finite cyclic groups (DLOG) form the corner-stone of numerous cryptographic constructions [1,2,3,4,5]. Practical implementations of cryptographic schemes reliant on RSA and DLOG dilemmas are orchestrated such that the selection of parameters introduces convolution into the corresponding crypt-analysis endeavor. In 1994, Shor [6] elucidated that these conventionally arduous problems can be effortlessly resolved through the utilization of large-scale quantum computers. The trajectory of quantum computing development has increasingly materialized, with prognostications from entities such as Microsoft and IBM anticipating the advent of large-scale quantum computers boasting several thousand qubits by 2030. Such advancements portend a tangible menace to the efficacy of contemporary public-key cryptography in upholding security. Consequently, the cryptographic community, industry stakeholders, and numerous standardization bodies have initiated strategic maneuvers toward the adoption of a quantum-resistant alternative: post-quantum cryptography. Post-quantum cryptography, also known as quantum-resistant cryptography, emerges as a pivotal response to the impending vulnerability of

[1] *ICST-2024: Information Control Systems & Technologies, September , 23 – 25, 2024, Odesa, Ukraine*

Hennadii.khalimov@nure.ua (G. Khalimov); yevgenkotukh@gmail.com (Y. Kotukh); maksym.kolisnyk@nure.ua (M. Kolisnyk) ; Svitlana.khalimova@nure.ua (S. Khalimova); Oleksandr.Sievierinov@nure.ua (O. Sievierinov); maks_kor @ukr.net (M. Korobchynskyi);

0000-0002-2054-9186 (G. Khalimov); 0000-0003-4997-620X (Y. Kotukh); 0000-0002-1075-9470 (M. Kolisnyk) ; 0000-0001-7224-589X (S. Khalimova) ; 0000-0002-6327-6405 (O. Sievierinov) ; 0000-0001-8049-4730 (M. Korobchynskyi)

classical cryptographic systems in the face of quantum computational prowess. We delve into the fundamental principles, challenges, and promising avenues of post-quantum cryptographic research, elucidating its pivotal role in fortifying the security posture of digital communications and transactions. Amidst the exigency posed by the impending advent of quantum computing, the quest for cryptographic primitives impervious to quantum attacks has garnered substantial impetus. The landscape of quantum-resistant cryptographic primitives, spanning lattice-based, code-based, hash-based, and multivariate polynomial cryptographic schemes is changing almost day by day. Through a comprehensive analysis of their underlying mathematical structures, security properties, and implementation considerations, we aim to furnish readers with insights into the diverse arsenal of cryptographic tools poised to withstand the disruptive potential of quantum adversaries.

2. Motivation

Quantum-resistant cryptosystems, predicated on lattice-based structures, error-correcting linear codes, multidimensional polynomial equations, one-way functions, elliptic curve isogenies, and non-commutative groups, actively leverage computationally complex problems. This mosaic of cryptographic techniques engenders resilience against quantum threats, underpinning a diverse array of cryptographic schemes. The first category encompasses schemes such as FrodoKEM, Kyber, Saber, along with Dilithium, Falcon, and qTESLA signatures, which hinge on the arduous task of training with LWE errors and the short integer solution of SIS. These schemes find application in key encapsulation and directed encryption scenarios. The complexity of decoding linear noisy codes with a secret code is pivotal in schemes like BIKE, Classic McEliece, HQC, NTS-KEM, ROLLO, and CFS, Durandal, WAVE signatures. These schemes rely on the intricate process of deciphering linear noisy codes, thereby fortifying their cryptographic underpinnings [7,8,9,10]. Furthermore, the complexity inherent in solving multidimensional equations forms the cornerstone of signature schemes such as LUOV, MQDSS, Rainbow, and GeMSS. These schemes exploit the intricacies of multidimensional equations to bolster cryptographic robustness. Likewise, the challenges posed by unidirectional functions are harnessed in signature schemes like XMSS, SPHINCS+, and Picnic, contributing to their quantum resistance [11,12,13]. Moreover, the complexity entailed in searching for isogenic elliptic curves underscores the security of directional encryption schemes like SIKE and CSIDH, along with signature schemes such as CSI-FiSh and SQISign. Lastly, the complexity arising from the group factorization problem serves as a linchpin in directional encryption schemes. These schemes, spanning from [17,18,19,20,21,22,23,24], derive cryptographic strength from the intractability of the group factorization problem. The evaluation of quantum security for cryptosystems, submitted to the NIST competition and earmarked as candidates for post-quantum cryptography, undergoes continuous scrutiny and refinement. Recent advancements, detailed in literature [25], elucidate the construction of polynomial quantum algorithms for solving the LWE problem with polynomial modulus-noise relations. Despite identified algorithmic flaws, novel insights into leveraging complex Gaussian functions and windowed quantum Fourier transforms portend promising avenues for quantum computing applications or novel LWE problem-solving methodologies. As underscored by Bart Prinell's commentary, while the absence of large-scale quantum computers impedes empirical validation of quantum algorithms, the imperative of post-quantum encryption remains paramount to ensuring resilience against prospective quantum adversaries [26]. The current slate of NIST-standard candidates appears robust, albeit subject to refinement through parameter optimization and technological advancements. A fundamental reimagining of cryptosystem design is proposed, wherein the traditional paradigm of leveraging hard-to-solve problems is supplanted by a novel approach predicated on problems boasting a constellation of equivalent solutions devoid of regularities. Such a framework obviates vulnerability to quantum cryptanalysis, relegating adversaries to Grover's algorithm with exponential complexity. Exemplifying this approach, the Shamir threshold secret sharing scheme capitalizes on classical algebraic principles, wherein secrecy is predicated on the unavailability of a critical mass of function values required to reconstruct the overarching secret.

3. Our contribution

3.1 Definition of an incomplete cryptosystem of linear equations

The construction of the cryptosystem is predicated upon a well-established algebraic problem, wherein the existence of a unique solution is contingent upon a fully defined system of linear equations. However, when confronted with an incompletely defined system of equations, the enumeration of solutions is governed by the cardinality of the set of potential solutions. In our formulation, we establish linear equations relative to unknowns, utilizing values denoted by logarithmic subscripts. Notably, the number of equations pertaining to secret values of logarithmic signatures is typically fewer than the total number of unknowns. Consequently, this engenders an incomplete system of linear equations vis-à-vis the unknowns, precluding polynomial-time resolution. The crux of any potential attack on such a cryptosystem boils down to the task of sorting and defining variables. The security of a cryptosystem hinged upon a problem featuring incompletely defined equations is contingent upon the robustness of the set of solutions. Central to the algorithm is the concept of logarithmic signature, serving as a foundational cryptographic primitive imbued with distinctive cryptographic attributes, including non-linearity, non-commutativity, unidirectionality, and factorizability by key. Subsequently, we shall delve into a comprehensive exposition elucidating the salient aspects of cryptosystems integrating logarithmic signatures.

3.2 Logarithmic signature

The representation of logarithmic signatures is intricately linked to the positional numbering system, wherein the data array, constituting the logarithmic signature, is structured into subblocks. Each subblock comprises vectors or strings, which can be construed as numerical entities. The encryption process, or cryptogram, is determined by the summation of vectors selected by a designated key (numeric value). The computational security of the cipher hinges upon the formidable challenge of decomposing the cryptogram into constituent vectors in the absence of knowledge regarding the correspondence between vector positions and their respective values. An early instantiation of logarithmic signatures for finite permutation groups was introduced in [18] within the context of constructing a symmetric cryptosystem. A defining characteristic of such constructions lies in their susceptibility to factorization by key. Subsequent discourse on the algebraic properties of logarithmic signatures and associated cryptosystems was deliberated in depth in [19,20]. In 2002, Magliveras et al. [21] devised two public key cryptosystems, MST1 and MST2. Building upon this foundation, Lempken et al. [22] leveraged logarithmic signatures and random coverages to devise a generalized MST3 encryption scheme. Notably, the public key in this scheme encompasses ordinary logarithmic signatures alongside random numerical entities, while the secret key is constituted by random coverages and sandwich transformations [21]. The presumed intractability of this scheme hinges upon the group factorization problem within non-Abelian groups. Furthermore, spurred by insights gleaned from attacks detailed in [23], Svaba and van Trung refined an extended variant of the generalized scheme [24], denoted as eMST3 cryptosystems. This iteration incorporates a clandestine homomorphism to obfuscate the secret logarithmic signature via a random cover transformation. Subsequent advancements in the MST3 cryptosystem were predicated upon high-order groups encompassing generalized Suzuki groups, small Ree groups, three-parametric groups, automorphism groups of the Suzuki functional field, and automorphisms of the Ree functional field [27,28,29,30,31,32,33,34]. The efficacy of logarithmic signatures lies in their simplicity, as the computation of text ciphers is facilitated through elementary addition operations utilizing bitwise XOR. However, a notable drawback is the substantial size of logarithmic arrays, necessitating the employment of masking arrays to ensure a commensurately high level of secrecy.

Within the purview of the presented cryptosystem, the logarithmic signature assumes a pivotal role as a fundamental cryptographic primitive facilitating keyless encryption and factorization by means of the logarithmic signature's key.

3.3 Our proposal

Let's consider the main steps of the algorithm.

Step 1. Here we construct of a secret logarithmic signature over a field $F(2^m)$. The implementation of secret homomorphic transformations with calculations over the field $F(2^m)$

presented in [35] . Let's construct a logarithmic signature using the following set of secret homomorphic transformations:

$$\beta_1 \xrightarrow{\rho_1} \beta_2 \xrightarrow{\rho_2} \beta_3 \xrightarrow{\rho_3} \beta_4 \xrightarrow{\rho_4} \beta_5 \xrightarrow{\rho_5} \beta,$$

where β_1 - simple factorization logarithmic signature type $(r_1,...,r_s)_{\beta_1}$;

Transformation 1 (ρ_1). In this step we make a noise of s blocks of the β_1 signature. In this case the signature type does not change. As a result, we get β_2 signature. Transformation 2 (ρ_2). Next, we shuffling secretly all blocks of β_2 signature. As a result, we get β_3 signature. Transformation 3 (ρ_3). Then, we mix all records in signature blocks β_3. As a result, we get β_4 signature. Transformation 4 (ρ_4). Next, we proceed with secret homomorphic transformation of array strings in this way: $\beta_4(i) = \gamma \cdot \beta_3(i)$, $i = \overline{1, r_1 + r_2 + ... + r_s}$, $\gamma \in F(2^m)$. As a result, we get β_5 signature. Transformation 5 (ρ_5). Finally, we use secret homomorphic transformation of string array $\beta(i) = \beta_4(i) \cdot \omega_{m\times m}$, $i = \overline{1, r_1 + r_2 + ... + r_s}$. As a result, we get β signature. Note, that $\omega_{m\times m}$ is an invertible binary matrix of dimension $m \times m$.

We have a logarithmic signature $\beta = \beta(i)$ over m - bit strings as a result of all steps. The security estimation is determined taking to the account a high entropy of secret transformations. These estimates are discussed in [24,35 ÷ 37].

Step 2. Here we construct general parameters, public and secret keys. Let's construct $K = k \times k$ logarithmic signatures β_K. We present logarithmic signatures β_K in the form of a two-dimensional set of arrays with index $\beta_{k_1,k_2} \in \beta_K$, $k_1 = \overline{1,k}$, $k_2 = \overline{1,k}$ for given types $r_{k_1,k_2} = \left(r_1,...,r_{s(k_1,k_2)}\right)_{k_1,k_2}$, $r_{k_1,k_2} \in r_K$.

$$\beta_{k_1,k_2} = [B_1, B_2, ..., B_{s(k_1,k_2)}]_{k_1,k_2} := (\beta_{i,j})_{k_1,k_2},\ j = \overline{1, s(k_1,k_2)},\ i = \overline{1, r_j}.$$

The index j determines the number of the block and the index i determines the number of the record in j the block. Records of arrays $\beta_{i,j}$ are defined m - bitwise strings that we identify with the elements of the finite field $F(2^m)$. Let the set β_K consist of L factorizable logarithmic signatures β_L, $L < K$ і $K - L$ non-factorizable signatures υ_{K-L}. Factorized logarithmic signatures β_L will be constructed using secret transformations $\rho_1 \div \rho_5$. In two-dimensional indexing β_{k_1,k_2}, k_1 у k_2 we determine whether the logarithmic signature belongs to the set $\beta_{k_1,k_2} \in \beta_L$. We construct non-factorizable logarithmic signatures υ_{K-L} for type $\overbrace{(2,2,...,2)}^{m}$ by filling them with random m-bit strings $\nu_1(j)$ and $\nu_2(j)$, $j = \overline{1,m}$ of each block of the logarithmic signature $\beta_{k_1,k_2} \in \upsilon_{K-L}$. Values and indexes k_1 and k_2 determine belonging to a set of non-factorizable logarithmic signatures υ_{K-L}. For logarithmic signatures $\beta_{k_1,k_2} \in \beta_L$, we generate arrays $\alpha_{k_1,k_2} \in \alpha_L$ with random records $\alpha_{k_1,k_2} = [\mathrm{A}_1, \mathrm{A}_2, ..., \mathrm{A}_{s(k_1,k_2)}]_{k_1,k_2} := (a_{i,j})_{k_1,k_2}$, $a_{i,j} \in F(2^m)/0$, $j = \overline{1, s(k_1,k_2)}$, $i = \overline{1, r_j}$, $\left(r_1,...,r_{s(k_1,k_2)}\right)_{k_1,k_2}$. Let's the values of the string $\left[\nu_{1,j}, \nu_{2,j}\right]_{k_1,k_2} \in \beta_{k_1,k_2}$, $\left(\nu_{i,j}\right)_{k_1,k_2} \in F(2^m)/0$ $j = \overline{1,m}$, $\forall k_1, k_2$ for each block in $\beta_{k_1,k_2} \in \upsilon_{K-L}$ satisfy the following conditions: $\left(\nu_{1,j} + \nu_{2,j}\right)_{k_1,k_2} = \chi$, where $i = \overline{1,2}$, $j = \overline{1,m}$, $\chi \in F(2^m)/0$. We generate random sets

$$t_{k_1,k_2} \in t_K,\ t_{k_1,k_2} = (t_1,...,t_{s(k_1,k_2)})_{k_1,k_2} \in F(2^m)/0$$

$$\tau_{k_1,k_2} \in \tau_K,\ \tau_{k_1,k_2} = (\tau_1,...,\tau_{s(k_1,k_2)})_{k_1,k_2} \in F(2^m)/0$$

and let $\left(t_{i,j}\right)_{k_1,k_2} \neq \left(\tau_{i,j}\right)_{k_1,k_2}$, $(t_j)_{k_1,k_2} \neq 0$, $(\tau_j)_{k_1,k_2} \neq 0$, $i = \overline{1,r_j}$ - the number of the record in $j = \overline{1, s(k_1,k_2)}$ the block of the array, for the logarithmic β_{k_1,k_2} type signature $\left(r_1,...,r_{s(k_1,k_2)}\right)_{k_1,k_2}$

Let's set a secret binary matrix ψ with $m \times m$ dimensions and let's determine the arrays $\gamma_{k_1,k_2} \in \gamma_K$ and $\lambda_{k_1,k_2} \in \lambda_K$. For factorizable logarithmic signatures, $\beta_{k_1,k_2} \in \beta_L$ we define arrays $\gamma_{k_1,k_2} \in \gamma_L$ and $\lambda_{k_1,k_2} \in \lambda_L$ by following expressions:

$$(\gamma_{i,j})_{k_1,k_2} = (\beta_{i,j})_{k_1,k_2} + (t_j)_{k_1,k_2} + (\alpha_{i,j})_{k_1,k_2}\psi,\ (\lambda_{i,j})_{k_1,k_2} = (\alpha_{i,j})_{k_1,k_2} + (\tau_j)_{k_1,k_2}$$

and similarly, for non-factorable $\beta_{k_1,k_2} \in \upsilon_{K-L}$ we define the arrays $\gamma_{k_1,k_2} \in G_{K-L}$ and $\lambda_{k_1,k_2} \in \Lambda_{K-L}$ by following expressions:

$$(\gamma_{i,j})_{k_1,k_2} = (\beta_{i,j})_{k_1,k_2}\psi + (t_j)_{k_1,k_2}, (\lambda_{i,j})_{k_1,k_2} = (\beta_{i,j})_{k_1,k_2} + (\tau_j)_{k_1,k_2}$$

for $j = \overline{1, s(k_1,k_2)}$, $i = \overline{1, r_j}$. All calculations by $\gamma_{k_1,k_2} \in \gamma_K$ and $\lambda_{k_1,k_2} \in \lambda_K$ are determined by the rule below. Let the argument for γ_{k_1,k_2} be m-bit string R. Let's decompose the string R into values according to the type $\left(r_1,...,r_{s(k_1,k_2)}\right)_{k_1,k_2}$

$$R = (R_1, R_2, ..., R_{s(k_1,k_2)}) = 2^0 R_1 + 2^{\log r_1} R_2 + 2^{\log r_1 r_2} R_3 + ... = R_1 + \sum_{j=2}^{s(k_1,k_2)} 2^{\sum_{i=1}^{j-1} \log r_i} R_j .$$

The values R_j show the number of the record in j the block of the array $\gamma_{k_1,k_2} \in \gamma_K$. Calculations for the argument R are determined by bitwise summation of the array of strings $\gamma_{k_1,k_2} \in \gamma_K$

$$\gamma_{k_1,k_2}(R) = \gamma_{k_1,k_2}(R_1, R_2, ..., R_{s(k_1,k_2)}) = \sum_{j=1}^{s(k_1,k_2)} \gamma_{R_j,j} .$$

As a results we obtain general parameters and cryptosystems $K = k \times k$, $L < K$, m, r_K, secret keys β_K, t_K, τ_K, ψ and public keys γ_K, λ_K.

Step 3. On this step we construct of a cryptosystem based on an incomplete system of linear equations for logarithmic signatures $\beta_{k_1,k_2} \in \beta_K$. The fundamental objective underlying the construction of the cryptosystem is to compute L linear sums $\sum \gamma_{k_1,k_2}(R_{k_1,k_2}) = U_l$ by values $\gamma_{k_1,k_2}(R_{k_1,k_2})$. $l = \overline{1, L}$. Let's determine the sums U_l by expressions of the form

$$\sum_{j=1}^{k} \gamma_{ij}\left(R_{ij}\right) = U_i,\ i = \overline{1,k},$$

$$\sum_{j=1}^{k} \gamma_{ji}\left(R_{ji}\right) = U_{k+i},\ i = \overline{1,k},$$

$$\sum_{j=1}^{k} \gamma_{j\mu}\left(R_{j\mu}\right) = U_{2k+i},\ \mu = (k - j + i) \bmod k + 1,\ i = \overline{1,k}$$

$$\sum_{j=1}^{k} \gamma_{\mu j}\left(R_{\mu j}\right) = U_{3k+i},\ \mu = (k - i + j) \bmod k + 1,\ i = \overline{1,k}$$

Values $\gamma_{ij}\left(R_{ij}\right)$ are calculated by R_{ij}.

All expressions for U_l include only one value $\gamma_{k_1,k_2}(R_{k_1,k_2})$ from string and/or array column $\gamma_{k_1,k_2} \in \gamma_K$. The number of such expressions equal to $4k$. Relatively to $\gamma_{ij}\left(R_{ij}\right)$ we get a system of linear equations. Since the number of unknowns $\gamma_{k_1,k_2}(R_{k_1,k_2})$ is equal to $K = k^2$, and the number of knowns U_l is equal to $L < K$, the system of linear equations will be incomplete with respect to the unknowns $\gamma_{k_1,k_2}(R_{k_1,k_2})$. For K values of logarithmic signatures, $\gamma_{k_1,k_2}(R_{k_1,k_2})$ it is easy to calculate $L < K$ the values of U_l. The solution of the inverse problem regarding the finding $\gamma_{k_1,k_2}(R_{k_1,k_2})$ has an uncertainty of $2^{(K-L)m}$ possible solutions. The cryptosystem has potential $(K-L)m$ bit security.

Example. Let $k = 4$. The arrays γ_{k_1,k_2} which define expressions for U_i $i = \overline{1,4k}$ are marked in orange. Please see Fig. 1.). We form L equations of U_L that are linearly independent relative to the desired ones $\gamma_{k_1,k_2} \in \gamma_L$. We do it to construct the cryptosystem with $(K-L)m$ bits security. Let $L = 8$. Let's choose the following eight equations $U_L = \{U_1, U_2, U_3, U_5, U_9 \div U_{12}\}$.

Expressions for relatively unknown amounts $\gamma_{k_1,k_2} \in \gamma_K$ have the following form

$$\gamma_{11}\left(R_{11}\right) + \gamma_{21}\left(R_{21}\right) + \gamma_{31}\left(R_{31}\right) + \gamma_{41}\left(R_{41}\right) = U_1$$

$$\gamma_{12}\left(R_{12}\right) + \gamma_{22}\left(R_{22}\right) + \gamma_{32}\left(R_{32}\right) + \gamma_{42}\left(R_{42}\right) = U_2$$

$$\gamma_{13}\left(R_{13}\right) + \gamma_{23}\left(R_{23}\right) + \gamma_{33}\left(R_{33}\right) + \gamma_{43}\left(R_{43}\right) = U_3$$

$$\gamma_{11}\left(R_{11}\right) + \gamma_{12}\left(R_{12}\right) + \gamma_{13}\left(R_{13}\right) + \gamma_{14}\left(R_{14}\right) = U_5$$

$$\gamma_{11}(R_{11})+\gamma_{24}(R_{24})+\gamma_{33}(R_{33})+\gamma_{42}(R_{42})=U_9$$
$$\gamma_{12}(R_{12})+\gamma_{21}(R_{21})+\gamma_{34}(R_{34})+\gamma_{43}(R_{43})=U_{10}$$
$$\gamma_{13}(R_{13})+\gamma_{22}(R_{22})+\gamma_{31}(R_{31})+\gamma_{44}(R_{44})=U_{11}$$
$$\gamma_{14}(R_{14})+\gamma_{23}(R_{23})+\gamma_{32}(R_{32})+\gamma_{41}(R_{41})=U_{12}$$

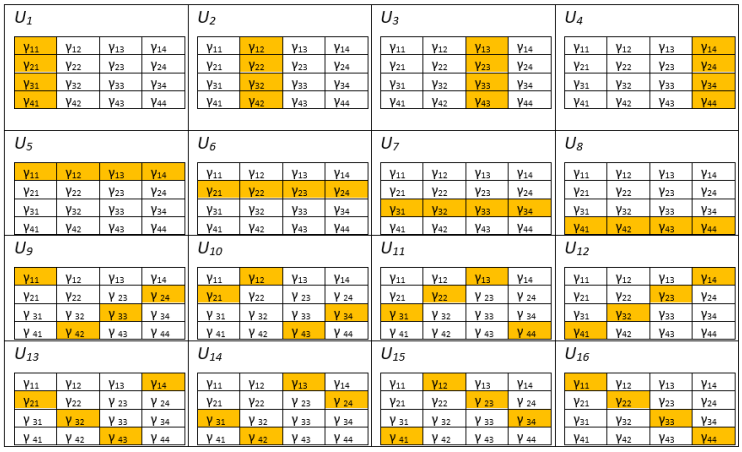

Figure 1: The arrays γ_{k_1,k_2}

The solution for the unknowns $\gamma_{k_1,k_2}\in\gamma_L$ can be expressed in the following expressions:

$$\gamma_{11}(R_{11})=U_9+\gamma_{24}(R_{24})+\gamma_{33}(R_{33})+\gamma_{42}(R_{42})$$
$$\gamma_{12}(R_{12})=(U_3+U_5+U_9+U_{12})+\gamma_{24}(R_{24})+\gamma_{32}(R_{32})+\gamma_{41}(R_{41})+\gamma_{42}(R_{42})+\gamma_{43}(R_{43})$$
$$\gamma_{13}(R_{13})=(U_1+U_2+U_9+U_{10}+U_{11})+\gamma_{24}(R_{24})+\gamma_{32}(R_{32})$$
$$+\gamma_{33}(R_{33})+\gamma_{34}(R_{34})+\gamma_{41}(R_{41})+\gamma_{43}(R_{43})+\gamma_{44}(R_{44})$$
$$\gamma_{14}(R_{14})=(U_1+U_2+U_3+U_9+U_{10}+U_{11}$$
$$+U_{12})+\gamma_{24}(R_{24})+\gamma_{34}(R_{34})+\gamma_{44}(R_{44})$$
$$\gamma_{21}(R_{21})=(U_3+U_5+U_9+U_{10}+U_{12})+\gamma_{24}(R_{24})$$
$$+\gamma_{32}(R_{32})+\gamma_{34}(R_{34})+\gamma_{41}(R_{41})+\gamma_{42}(R_{42})$$
$$\gamma_{22}(R_{22})=(U_2+U_3+U_5+U_9+U_{12})+\gamma_{24}(R_{24})+\gamma_{41}(R_{41})+\gamma_{43}(R_{43})$$
$$\gamma_{23}(R_{23})=(U_1+U_2+U_3+U_9+U_{10}+U_{11})+\gamma_{24}(R_{24})$$
$$+\gamma_{32}(R_{32})+\gamma_{34}(R_{34})+\gamma_{41}(R_{41})+\gamma_{44}(R_{44})$$
$$\gamma_{31}(R_{31})=(U_1+U_3+U_5+U_{10}+U_{12})+\gamma_{32}(R_{32})+\gamma_{33}(R_{33})+\gamma_{34}(R_{34})$$

Thus, to calculate the values, $\{\gamma_{11},\gamma_{12},\gamma_{13},\gamma_{14},\gamma_{21},\gamma_{22},\gamma_{23},\gamma_{31}\}\in\gamma_L$ one should define $\{\gamma_{24},\gamma_{32},\gamma_{33},\gamma_{34},\gamma_{41},\gamma_{42},\gamma_{43},\gamma_{44}\}\in G_{K-L}$.

Step 4. Encryption. To implement encryption we consider the following input parameters: x long Lm bit message, public keys γ_K, λ_K, hash function h. Encryption step consists of the following routines. We divide the message x into m-bit strings, which are converted into a set of L input parameters R_{ij} for L factorizable logarithmic signatures $\beta_{k_1,k_2}\in\beta_L$ according to their type $\left(r_1,...,r_{s(k_1,k_2)}\right)_{k_1,k_2}$. Next, we calculate the hash value $h(x)$ for Lm the bit string of the message x that can be present with $K-L$ m-bit strings with subsequent transformation $\sigma(h(x))=R_{k_1,k_2}$ into a set of input parameters R_{ij} for $K-L$ non- factorable logarithmic signatures $\beta_{k_1,k_2}\in\upsilon_{K-L}$ in accordance with the type $\overbrace{(2,2,...,2)}^{m}$. The hash function $h(x)$ is unidirectional and sensitive to bit changes in the message x. We can also add a session key to the display $\sigma(h(x))=R_{k_1,k_2}$ to randomize the cipher text in the case of low entropy of the message x. Then, we calculate the values of $\gamma_{k_1,k_2}(R_{k_1,k_2})$ and $\lambda_{k_1,k_2}(R_{k_1,k_2})$ $k_1=\overline{1,k}$, $k_2=\overline{1,k}$. Then, we calculate L the values of linear sums for $\sum\gamma_{k_1,k_2}(R_{k_1,k_2})=U_l$, $U_l\in U_L$. Finally, we calculate L sums of $\sum\lambda_{k_1,k_2}(R_{k_1,k_2})=V_l$, $V_l\in V_L$ using similar expressions for U_L.

The encryption result is recognized as a L m-bit values $U_l\in U_L$ and $V_l\in V_L$.

Step 5. Decryption. To implement decryption we consider the following input parameters: a cipher text $U_l \in U_L$, $V_l \in V_L$, secret keys β_K, t_K, τ_K, ψ. It is necessary to calculate $\gamma_{k_1,k_2} \in \gamma_L$ and to calculate $R_{k_1,k_2} \in R_L$ and restore x through the factorizable signatures $\beta_{k_1,k_2} \in \beta_L$. To calculate, $\gamma_{k_1k_2}\left(R_{k_1k_2}\right) \in \gamma_L$ you need to subtract the values $\gamma_{k_1,k_2} \in G_{K-L}$ from the sums of the set U_L. Decryption consists of the following steps. First, we calculate $D_l = U_l + V_l\psi + t_l + \tau_l\psi$, $l = \overline{1,L}$. The values U_l contain sums for subsets of factorizable and non-factorizable signatures $\gamma_{k_1,k_2} \in \gamma_L$ $\gamma_{k_1,k_2} \notin \gamma_L$

$$U_l = \sum_{\gamma_{k_1,k_2} \in \gamma_L} \gamma_{k_1,k_2}(R_{k_1,k_2}) + \sum_{\gamma_{k_1,k_2} \notin \gamma_L} \gamma_{k_1,k_2}(R_{k_1,k_2}).$$

The values V_l contain similar sums for subsets $\lambda_{k_1,k_2} \in \lambda_L$ and $\lambda_{k_1,k_2} \notin \lambda_L$

$$V_l = \sum_{\lambda_{k_1,k_2} \in \lambda_L} \lambda_{k_1,k_2}(R_{k_1,k_2}) + \sum_{\lambda_{k_1,k_2} \notin \lambda_L} \lambda_{k_1,k_2}(R_{k_1,k_2}).$$

Indices $k_1 = \varsigma(j,l)$ are $k_2 = \zeta(j,l)$ determined by the serial number j of the logarithmic signature in the equation for U_l and the number of the equation l. Substituting U_l and V_l into the expression for D_l, we get

$$D_l = \left(\sum_{\gamma_{k_1,k_2} \in \gamma_L} \gamma_{k_1,k_2}(R_{k_1,k_2}) + \sum_{\gamma_{k_1,k_2} \notin \gamma_L} \gamma_{k_1,k_2}(R_{k_1,k_2}) \right) + \left(\sum_{\lambda_{k_1,k_2} \in \lambda_L} \lambda_{k_1,k_2}(R_{k_1,k_2}) + \sum_{\lambda_{k_1,k_2} \notin \lambda_L} \lambda_{k_1,k_2}(R_{k_1,k_2}) \right)\psi$$

$$+ \sum_{k_1,k_2 \in K} t_{k_1,k_2} + \sum_{k_1,k_2 \in K} \tau_{k_1,k_2}\psi = \left(\begin{array}{l} \sum\limits_{\gamma_{k_1,k_2} \in \gamma_L} \beta_{k_1,k_2}(R_{k_1,k_2}) + \sum\limits_{\gamma_{k_1,k_2} \in \gamma_L} t_{k_1,k_2} \\ \alpha_{k_1,k_2}(R_{k_1,k_2})\psi \\ + \sum\limits_{\gamma_{k_1,k_2} \in \gamma_L} + \sum\limits_{\gamma_{k_1,k_2} \notin \gamma_L} \beta_{k_1,k_2}(R_{k_1,k_2})\psi \sum\limits_{\gamma_{k_1,k_2} \notin \gamma_L} t_{k_1,k_2} \end{array} \right) +$$

$$\left(\sum_{\lambda_{k_1,k_2} \in \lambda_L} \alpha_{k_1,k_2}(R_{k_1,k_2}) + \sum_{k_1,k_2 \in \lambda_L} \tau_{k_1,k_2} + \sum_{\lambda_{k_1,k_2} \notin \lambda_L} \beta_{k_1,k_2}(R_{k_1,k_2}) + \sum_{k_1,k_2 \notin \lambda_L} \tau_{k_1,k_2} \right)\psi$$

$$+ \sum_{k_1,k_2 \in K} t_{k_1,k_2} + \sum_{k_1,k_2 \in K} \tau_{k_1,k_2}\psi = \sum_{\gamma_{k_1,k_2} \in \gamma_L} \beta_{k_1,k_2}(R_{k_1,k_2})$$

As a result, we get L equations relative to the unknowns $\beta_{k_1,k_2}(R_{k_1,k_2})$

$$\sum_{\gamma_{k_1,k_2} \in \gamma_L} \beta_{k_1,k_2}(R_{k_1,k_2}) = D_l, \; l = \overline{1,L}.$$

Then, we solve the system of linear equations relatively $\beta_{k_1,k_2}(R_{k_1,k_2})$

$$\sum_{\gamma_{k_1,k_2} \in \gamma_L} \beta_{k_1,k_2}(R_{k_1,k_2}) = D_l \quad , \; l = \overline{1,L}.$$

Finally, we find factorization $R_{k_1,k_2} = \beta_{k_1,k_2}^{-1}(R_{k_1,k_2})$ and restore the message x.

3.4 Security analysis

There are several brute force attacks are considered as follows. First one is a brute-force of the input message x within an encryption and verification for the coincidence of ciphertexts. The complexity of this attack equals $N_1 = 2^{Lm}$. Next is a brute-force of ciphertexts U_l, V_l, $l = \overline{1,L}$ via solving of a system of linear equations relative to logarithmic signatures and the subsequent attack on logarithmic signatures. The complexity of this attack equals $N_2 = 2^{2Lm}$. Then, we consider brute-force of a secret homomorphic transformation ψ, calculation D_l and attack on logarithmic signatures. The secret transformation ψ is based on matrix multiplication. A brute force attack by selection ψ has a complexity 2^{m^2} where m the dimension of the matrix is $\psi_{m\times m}$. Also, analytical attacks on secret transformation ψ can be proposed as follows: Arrays of $\gamma_{k_1,k_2} \in \gamma_L$ and $\lambda_{k_1,k_2} \in \lambda_L$ for factorizable logarithmic signatures $\beta_{k_1,k_2} \in \beta_L$ are defined by expressions:

$$(\gamma_{i,j})_{k_1,k_2} = (\beta_{i,j})_{k_1,k_2} + (t_j)_{k_1,k_2} + (\alpha_{i,j})_{k_1,k_2}\psi, \quad (\lambda_{i,j})_{k_1,k_2} = (\alpha_{i,j})_{k_1,k_2} + (\tau_j)_{k_1,k_2}$$

where $(\beta_{i,j})_{k_1,k_2} \neq 0$, $(t_j)_{k_1,k_2} \neq 0$, $(\tau_j)_{k_1,k_2} \neq 0$ $i = \overline{1,r_j}$ is the record`s number in $j = \overline{1,s(k_1,k_2)}$ the array block, for a logarithmic signature β_{k_1,k_2} of the type $\left(r_1,...,r_{s(k_1,k_2)}\right)_{k_1,k_2}$. Let $(\beta_{i,j})_{k_1,k_2} + (t_j)_{k_1,k_2} \neq 0$. The values $(\beta_{i,j})_{k_1,k_2}$, $(t_j)_{k_1,k_2}$, $(\tau_j)_{k_1,k_2}$ are considered secret and there is no mapping

$$(\alpha_{i,j})_{k_1,k_2}\psi = (\gamma_{i,j})_{k_1,k_2} + (\beta_{i,j})_{k_1,k_2} + (t_j)_{k_1,k_2}$$

and it is impossible to construct equations relatively ψ

$$(\lambda_{i,j})_{k_1,k_2}\psi = (\gamma_{i,j})_{k_1,k_2} + (\beta_{i,j})_{k_1,k_2} + (t_j)_{k_1,k_2}.$$

It is possible to try to strengthen the attack based on the addition of records $(\gamma_{i,j})_{k_1,k_2}$ within $(\lambda_{i,j})_{k_1,k_2}$ the block of arrays. Since the value of the secret parameter $(t_j)_{k_1,k_2}$ is constant for the entries $(\gamma_{i,j})_{k_1,k_2}$ in j the block of the array γ_{k_1,k_2} and the secret parameter $(\tau_j)_{k_1,k_2}$ is constant for the entries $(\lambda_{i,j})_{k_1,k_2}$ in the corresponding j block of the array, λ_{k_1,k_2} it is possible to consider the sums $(\gamma_{i,j})_{k_1,k_2}$ and $(\lambda_{i,j})_{k_1,k_2}$

$(\gamma_{i_1,j})_{k_1,k_2} + (\gamma_{i_2,j})_{k_1,k_2} = (\beta_{i_1,j})_{k_1,k_2} + (\beta_{i_2,j})_{k_1,k_2} + \left((\alpha_{i_1,j})_{k_1,k_2} + (\alpha_{i_1,j})_{k_1,k_2}\right)\psi$ without $(t_j)_{k_1,k_2}$,

$(\lambda_{i_1,j})_{k_1,k_2} + (\lambda_{i_2,j})_{k_1,k_2} = (\alpha_{i_1,j})_{k_1,k_2} + (\alpha_{i_1,j})_{k_1,k_2}$ without $(\tau_j)_{k_1,k_2}$.

Since $(\beta_{i_1,j})_{k_1,k_2} \neq (\beta_{i_2,j})_{k_1,k_2}$, there is no mapping

$$\left((\alpha_{i_1,j})_{k_1,k_2} + (\alpha_{i_1,j})_{k_1,k_2}\right)\psi = (\gamma_{i_1,j})_{k_1,k_2} + (\gamma_{i_2,j})_{k_1,k_2} + (\beta_{i_1,j})_{k_1,k_2} + (\beta_{i_2,j})_{k_1,k_2}$$

and it is impossible to obtain a solution to the equation

$$\left((\lambda_{i_1,j})_{k_1,k_2} + (\lambda_{i_1,j})_{k_1,k_2}\right)\psi = (\gamma_{i_1,j})_{k_1,k_2} + (\gamma_{i_2,j})_{k_1,k_2} + (\beta_{i_1,j})_{k_1,k_2} + (\beta_{i_2,j})_{k_1,k_2}$$

relatively to ψ. Also, there are following analytical attacks on ψ non-factorizable logarithmic signatures $\beta_{k_1,k_2} \notin \beta_L$ are considered. The first attack on ψ is based on the analysis of records in arrays $\gamma_{k_1,k_2} \notin \gamma_L$ and $\lambda_{k_1,k_2} \notin \lambda_L$ $(\gamma_{i,j})_{k_1,k_2} = (\beta_{i,j})_{k_1,k_2}\psi + (t_{i,j})_{k_1,k_2}$, $(\lambda_{i,j})_{k_1,k_2} = (\beta_{i,j})_{k_1,k_2} + (\tau_{i,j})_{k_1,k_2}$, $i = \overline{1,2}$. The values $(t_{i,j})_{k_1,k_2}$ and $(\tau_{i,j})_{k_1,k_2}$ are considered as a secret ones $(t_{1,j})_{k_1,k_2} = (t_{2,j})_{k_1,k_2} = (t_j)_{k_1,k_2}$, $(\tau_{1,j})_{k_1,k_2} = (\tau_{2,j})_{k_1,k_2} = (\tau_j)_{k_1,k_2}$ and it is impossible to obtain ratios $(\lambda_{i,j})_{k_1,k_2}\psi + (\tau_{i,j})_{k_1,k_2}\psi = (\gamma_{i,j})_{k_1,k_2} + (t_{i,j})_{k_1,k_2}$ to compute ψ. The second attack on ψ is based on the observation that the values of the secret parameters $(t_j)_{k_1,k_2}$ and $(\tau_j)_{k_1,k_2}$ are constant in each j block of the array of records $(\gamma_{i,j})_{k_1,k_2}$ and $(\lambda_{i,j})_{k_1,k_2}$. It is possible to strengthen the attack on ψ, if we consider the sum of records $(\gamma_{1,j})_{k_1,k_2} + (\gamma_{1,j})_{k_1,k_2}$ and $(\lambda_{1,j})_{k_1,k_2} + (\lambda_{2,j})_{k_1,k_2}$ within blocks of arrays $(\gamma_{i,j})_{k_1,k_2}$ and $(\lambda_{i,j})_{k_1,k_2}$

$$(\gamma_{1,j})_{k_1,k_2} + (\gamma_{2,j})_{k_1,k_2} = \left((\beta_{1,j})_{k_1,k_2} + (\beta_{1,j})_{k_1,k_2} + (\alpha_{1,j})_{k_1,k_2} + (\alpha_{1,j})_{k_1,k_2}\right)\psi,$$

$$(\lambda_{1,j})_{k_1,k_2} + (\lambda_{2,j})_{k_1,k_2} = (\beta_{1,j})_{k_1,k_2} + (\beta_{1,j})_{k_1,k_2} + (\alpha_{1,j})_{k_1,k_2} + (\alpha_{1,j})_{k_1,k_2}.$$

It is possible to obtain an equation for calculation ψ

$$\left((\lambda_{1,j})_{k_1,k_2} + (\lambda_{2,j})_{k_1,k_2}\right)\psi = (\gamma_{1,j})_{k_1,k_2} + (\gamma_{2,j})_{k_1,k_2}.$$

Taking into account the requirement $\left(\nu_{1,j} + \nu_{2,j}\right)_{k_1,k_2} = \chi$ for the values of the strings $\left[\nu_{1,j}, \nu_{2,j}\right]_{k_1,k_2} \in \beta_{k_1,k_2}$, $j = \overline{1,m}$, $\forall k_1, k_2$ we obtain a unique equation for all blocks of the array of records $(\gamma_{i,j})_{k_1,k_2}$

$$\chi\psi = (\gamma_{1,j})_{k_1,k_2} + (\gamma_{2,j})_{k_1,k_2}\, z.$$

Since the equation is written only for one m bit string, and the number of required values of the binary matrix ψ is equal to m^2, there remains uncertainty in $m^2 - m$ bits regarding the coefficients of the matrix ψ. Complexity of the attack $N_3 = 2^{m^2-m}$.

The third attack on ψ is determined by the possibility of constructing sums from $n > 2$ entries on arrays of logarithmic signatures $\beta_{k_1,k_2} \notin \beta_L$, so that $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (t_{i,j})_{k_1,k_2} = 0$ and $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\tau_{i,j})_{k_1,k_2} = 0$, then we obtain a relatively solvable ψ equation

$$\sum_{i\in1,2,\, j\in(j_1,\dots,j_n 0} (\gamma_{i,j})_{k_1,k_2} = \sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\beta_{i,j})_{k_1,k_2}\psi,$$

$$\sum_{i\in1,2,\, j\in(j_1,\dots,j_n 0} (\lambda_{i,j})_{k_1,k_2} = \sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\beta_{i,j})_{k_1,k_2}.$$

A system of m linear equations allows you to find a solution relatively ψ

$$\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\lambda_{i,j})_{k_1,k_2}\psi = \sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\gamma_{i,j})_{k_1,k_2}.$$

The system of equations is based on the selection of m bit records from the arrays of values of logarithmic signatures in the sets $(\gamma_{i,j})_{k_1,k_2}$ и $(\lambda_{i,j})_{k_1,k_2}$, the sums of the entries in which contain $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (t_{i,j})_{k_1,k_2} = 0$ и $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\tau_{i,j})_{k_1,k_2} = 0$. Since the values of $(t_{i,j})_{k_1,k_2}$ and $(\tau_{i,j})_{k_1,k_2}$ are considered secret, the values of the sums $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (t_{i,j})_{k_1,k_2}$ cannot $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\tau_{i,j})_{k_1,k_2}$ be predicted and can be assumed with probability 2^{-2m}, what the selected entries in sets $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\gamma_{i,j})_{k_1,k_2}$ and $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\lambda_{i,j})_{k_1,k_2}$ will be equal to zero. To build a system of equations, ψ it is necessary to have m cases of equality of zero $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (t_{i,j})_{k_1,k_2}$ both $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\tau_{i,j})_{k_1,k_2}$ in the sums $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\gamma_{i,j})_{k_1,k_2}$ and $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\lambda_{i,j})_{k_1,k_2}$ for each calculation ψ. The probability of such an event can be estimated by the value of 2^{-2m^2}. An important issue is establishing the fact that the matrix calculated ψ by the system of equations for a random set $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\gamma_{i,j})_{k_1,k_2}$ is $\sum_{i\in1,2,\, j\in(j_1,\dots,j_n)} (\lambda_{i,j})_{k_1,k_2}$ the desired one. Representations of arrays $\gamma_{k_1,k_2} \notin \gamma_L$ and $\lambda_{k_1,k_2} \notin \lambda_L$ do not allow verification $(\lambda_{i,j})_{k_1,k_2}\psi = (\gamma_{i,j})_{k_1,k_2}$ due to secrecy $(t_{i,j})_{k_1,k_2}, (\tau_{i,j})_{k_1,k_2}$.

Finally, we can evaluate of the quantum secrecy of directional encryption based on a cryptosystem with an incomplete system of linear equations. The cryptosystem security for directional encryption is based on the secrecy of the homomorphic matrix transformation and the incompleteness of the linear equations relative to the values of the logarithmic signatures. The impossibility of an algebraic solution regarding the uncertainty of the matrix transformation is determined by the incomplete definition of systems of linear equations for matrix equations and a probabilistic assessment of the possibility of constructing such a system of equations. The absence of a mechanism for verifying the truth of solutions for an attack on a secret matrix transformation based on random samples of records of logarithmic signatures indicates a probabilistic assessment of the success of the attack. It is not possible to formulate a target function for a quantum algorithm for such an attack. A similar attack on the algebraic solution relative to the values of the logarithmic signatures due to the indeterminacy of the linear equations also cannot be formalized with a target function for the quantum algorithm. A quantum attack based on Grover's algorithm with exponential complexity is possible for the search attack of the input text based on the given cipher text. It appears that polynomial attacks on the algorithm are not possible, since the data in the algorithm (records of arrays γ_{k_1,k_2} and λ_{k_1,k_2}) are structured as random sets without regularities. Simple logarithmic signatures are well structured, however, secret transformations used to construct protected logarithmic signatures introduce strong randomization in array records.

3.5 Security parameters evaluation

We consider the general parameters of the cryptosystem as follows: m-bit length of logarithmic signatures; K as a number of logarithmic signatures in the cryptosystem; L as a number of factorizable logarithmic signatures in the cryptosystem; r_K types of logarithmic signatures. Below

are the sizes of keys for building a cryptosystem with parameters $k = 4$, $K = k \times k = 16$, $L = 8$, $r_{k_1,k_2} = \overbrace{(2,2,...,2)}^{m}$.

Table 1
Secret keys costs

m	Costs for secret keys				
	$\lvert\beta_K\rvert = 2Km$ byte	$\lvert t_K\rvert = Km$ byte	$\lvert\tau_K\rvert = Km$ byte	$\lvert\psi\rvert = m^2$ byte	$\lvert\beta_K\rvert + \lvert t_K\rvert + \lvert\tau_K\rvert + \lvert\psi\rvert$ byte
8	256	128	128	8	520
16	1024	512	512	32	1080
32	4096	2048	2048	128	8320
64	16384	8192	8192	512	33280

Table 2
Public keys costs

Public key costs		
$\lvert\gamma_K\rvert = \lvert\beta_K\rvert$ byte	$\lvert\lambda_K\rvert = \lvert\alpha_K\rvert$ byte	$\lvert\gamma_K\rvert + \lvert\lambda_K\rvert$ byte
256	32	288
1024	32	1056
4096	32	4128
16384	32	16416

Table 3
Decryption costs

m	The size of the cipher text is U beat	The size of the cipher text is V beat	The number is multiplied λ_K by the binary ψ dimension matrix $m \times m$	The number is complex $\gamma_K + \lambda_K$ m-everyday words L	Number added $\gamma_K + \lambda_K$ with words $t_K + \tau_K$	The number is added when reducing the system of linear equations $L(K-L)/2$	The number is calculated β_K^{-1}
8	64	64	8	8	8	32	8
16	128	128	8	8	8	32	8
32	256	256	8	8	8	32	8
64	512	512	8	8	8	32	8

Table 4
Security estimation

m	Guessing attack through selection of input text 2^{-Lm}	A brute force guessing attack ψ 2^{-m^2}	A brute force guessing attack ψ through entries in a block $2^{-(m^2-m)}$	Attacking the matrix ψ through a system of equations 2^{-2m^2}
8	2^{-64}	2^{-64}	2^{-56}	2^{-128}
16	2^{-128}	2^{-256}	2^{-240}	2^{-512}
32	2^{-256}	2^{-1024}	2^{-992}	2^{-2048}
64	2^{-512}	2^{-4096}	2^{-4032}	2^{-8192}

It should also be noted that the arrays λ_K are generated as random entries and can be generated based on the initial value.

The secret keys of the cryptosystem are β_K, t_K, τ_K, ψ.

Public keys are defined as γ_K, λ_K.

4. Conclusions

A cryptosystem based on an incomplete system of linear equations with respect to logarithmic signatures is a good candidate for post-quantum cryptography. The incompleteness implemented in the algorithm for systems of linear equations guarantees undecidability with respect to secret logarithmic signatures and secret matrix transformation. Quantum secrecy is based on the high randomization of records in arrays of logarithmic signatures and the absence of regularities in the structured data of the algorithm. The directional encryption algorithm is well-scalable with respect to computing costs, memory, and limitations of hardware platforms without reducing the high level of secrecy. Due to the selection of the general parameters of the cryptosystem, the declared NIST levels of secrecy of 128, 192, 256 bits are realized. The cost of public keys when calculating over words of 16, 32 bits is in the range of 1 ÷ 4 Kbytes and is comparable to implementations for the best candidates for post-quantum cryptography. The basic computational operation of the algorithm is bitwise XOR over the words of logarithmic arrays.

References

[1] R. L. Rivest, A. Shamir, L. M. Adlemanб A method for obtaining digital signatures and public-key cryptosystems. Communications of the Association for Computing Machinery, 21 2 (1978) 120–126.

[2] M. O. Rabin, Digital signatures and public key functions as intractable as factorization. Technical Report MIT/LCS/TR-212, Massachusetts Institute of Technology, January 1979.

[3] H. C. Williams, Some public key crypto-functions as intractable as factorization, in: GR Blakley and David Chaum , editors, CRYPTO'84, Springer, Heidelberg, volume 196 of LNCS, 1984, pp. 66–70.

[4] S. Goldwasser, S. Micali, Probabilistic encryption and how to play mental poker keeping secret all partial information, in :14th ACM STOC, ACM Press, 1982, pp. 365–377.

[5] P. Paillier, Public-key cryptosystems based on composite degree residue classes, in Jacques Stern, editor, EURO-CRYPT'99, Springer, Heidelberg, volume 1592 of LNCS, 1999, pp.223–238.

[6] P.W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in: 35th FOCS IEEE Computer Society Press, 1994, pp. 124–134.

[7] R. J. McEliece, A public-key cryptosystem based on algebraic coding theory. The deep space network progress report 42-44, Jet Propulsion Laboratory, California Institute of Technology, January/February 1978.

[8] N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. A. Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich, G. Zémo, V. Vasseur, S. Ghosh, BIKE. Technical report, National Institute of Standards and Technology, 2020.

[9] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, J. Bos, HQC. Technical report, National Institute of Standards and Technology, 2020.

[10] M. R. Albrecht, D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurich, R. Misoczki, R. Niederhagen, K. G. Paterson, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C. Jung Tjhai, M. Tomlinson, W. Wang, Classic McEliece. Technical report, National Institute of Standards and Technology, 2020.

[11] L. Lamport, Constructing digital signatures from a one-way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, October 1979.

[12] R. C. Merkle, A certified digital signature, in: Gilles Brassard, editor, CRYPTO'89, Springer, Heidelberg, volume 435 of LNCS, 1990, pp. 218–238.

[13] J. Rompel, One-way functions are necessary and sufficient for secure signatures, in: 22nd ACM STOC, ACM Press, 1990, pp. 387–394.

[14] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D. Urbanik, G. Pereira, K. Karabina A. Hutchinson, SIKE. Technical report, National Institute of Standards and Technology, 2020.

[15] W. Beullens, T. Kleinjung, F. Vercauteren, CSI- FiSh : Efficient isogeny based signatures through class group computations, in: Steven D. Galbraith and Shiho Moriai, editors, ASIACRYPT 2019, Springer, Heidelberg, Part I, volume 11921 of LNCS, 2019, pp. 227–247.

[16] L. De Feo, D. Kohel, A. Leroux, C. Petit, B. Wesolowski, SQISign : Compact post-quantum signatures from quaternions and isogenies, in: Shiho Moriai and Huaxiong Wang, editors, ASIACRYPT 2020, Springer, Heidelberg, Part I, volume 12491 of LNCS, 2020, pp. 64–93.
[17] N.R. Wagner, M.R. Magyarik, A public-key cryptosystem based on the word problem, in: Proc. Advances in Cryptology - CRYPTO 1984, LNCS 196, Springer-Verlag, 1985, pp. 19–36.
[18] S.S. Magliveras, A cryptosystem from logarithmic signatures of finite groups, in: Proceedings of the 29th Midwest Symposium on Circuits and Systems, Elsevier Publishing, Amsterdam, The Netherlands, 1986, pp. 972–975.
[19] S. S. Magliveras, N.D. Memon, Algebraic properties of cryptosystem PGM, Journal of Cryptology 5 3 (1992)167–183.
[20] A. Caranti, F. Dalla Volta, The round functions of cryptosystem PGM generate the symmetric group, Designs, Codes and Cryptography 38 1 (2006) 147–155.
[21] S. Magliveras, D. Stinson, T. van Trung, New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups, Journal of Cryptology 15 4 (2002) 285–297.
[22] W. Lempken, S.S. Magliveras, T. van Trung and W. Wei, A public key cryptosystem based on non-abelian finite groups, J. of Cryptology, 22 (2009) 62–74.
[23] S. S. Magliveras, P. Svaba, T. van Trung, P. Zajac, On the security of a realization of cryptosystem MST3, Tatra Mountains Mathematical [16 1] Publications 41 (2008) 65– 78.
[24] P. Svaba, T. van Trung, Public key cryptosystem MST3 cryptanalysis and realization, Journal of Mathematical Cryptology 4 3 (2010) 271–315.
[25] Y. Chen Quantum Algorithms for Lattice Problems April 18, 2024. URL: https://eprint.iacr.org/2024/555.pdf.
[26] B. Prinell, Social Network Post. URL: https://www.linkedin.com/posts/bart-preneel-4451412_lattice-based-cryptography-no-panic-but-activity-7184684082159603713-pxkX?utm_source=share&utm_medium=member_desktop.
[27] G. Khalimov, Y. Kotukh, S. Khalimova, Encryption scheme based on the automorphism group of the Ree function field, in: 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), IEEE, 2020, pp. 1–8.
[28] G. Khalimov, I. Didmanidze , O. Sievierinov, Y. Kotukh, O. Shonia, Encryption scheme based on the automorphism group of the Suzuki function field, in: 2020 IEEE International Conference on PROBLEMS OF INFOCOMMUNICATIONS. SCIENCE AND TECHNOLOGY PIC ST2020 October 6-9, 2020.
[29] G. Khalimov, Y. Kotukh, S. Khalimova, Improved encryption scheme based on the automorphism group of the Ree function field, in: 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) , IEEE Xplore: 14 May 2021, DOI: 10.1109/ IEMTRONICS52119.2021.9422514.
[30] G. Khalimov, Y. Kotukh, O. Sievierinov, S. Khalimova, S.-Y. Chang, Y. Balytskyi, Strong Encryption Based on the small Ree groups, in: International Conference "Problems of Infocommunications . Science and Technology" (PIC S&T'2022) October 10 – 12, 2022.
[31] G. Khalimov, Y. Kotukh, S. Khalimova, O. Marukhnenko, D. Tsyplakov, Towards advance encryption based on a Generalized Suzuki 2-groups, in: International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME 2021, 2021.
[32] G. Khalimov, Y. Kotukh, S. Khalimova, Encryption scheme based on the automorphism group of the Ree function field, in: 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2020, pp. 1–8.
[33] G. Khalimov, Y. Kotukh, S. Khalimova, MST3 cryptosystem based on a generalized Suzuki 2 – groups, in: CEUR Workshop Proceedings, 2020, 2711, 2020, pp. 1–15.
[34] G. Khalimov, Y. Kotukh, S. Khalimova, MST3 cryptosystem based on the automorphism group of the Hermitian function field, in: 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 2019, pp. 865–868.
[35] P. Svaba, Covers and logarithmic signatures of finite groups in cryptography, Dissertation, 2022.
[36] S. R. Blackburn, C. Cid, C. Mullan, Cryptanalysis of the mst3 public key cryptosystem. Journal of Mathematical Cryptology, 3 4 (2009) 321.
[37] W. Lempken, T. van Tran, S. S. Magliveras, W. Wei, A public key cryptosystem based on non-abelian finite groups. Journal of Cryptology, 22 1 (2009) 62–74.