The subject of this study is the algebraic processes of data formation, encoding and syndrome decoding in cryptographic code constructions based on hyperelliptic curves of higher genera over Galois fields. The problem addressed lies in the excessive computational complexity and energy consumption of post-quantum asymmetric cryptosystems, which precludes their use on hardware platforms with resource constraints. The results obtained include the construction of a mathematical model of an algebraic-geometric code in projective coordinates, the development of a point mapping algorithm, and the generation of sparse matrices. The implementation of hyperelliptic structures into the symmetric Rao-Nama scheme has enabled a reduction in energy consumption of 20–60% compared to the asymmetric McElys scheme. The increase in the overall efficiency of the system is explained by the complete elimination of the resource-intensive operation of inverting Galois field elements thanks to an isomorphic transition to projective space, as well as the complete avoidance of solving matrix equations during the process of decrypting cryptograms. The distinctive features of the results obtained, which enabled the solution of the problem under investigation, lie in the fact that the targeted selection of row vectors for the evaluation matrices allowed the Hamming weight of the code to be artificially minimized. At the same time, the synergy of multidimensional algebraic geometry with symmetric architecture ensured an approximation to linear time complexity of decoding. The scope and conditions for the practical application of the results obtained cover the use of synthesized cryptographic code constructs in nodes of modern cyber-physical systems and Internet of Things (IoT) networks under conditions of severe computational resource constraints and autonomous power supply limits

Keywords: *post-quantum cryptography, hyperelliptic curve, cryptographic code construction, Rao-Nama scheme, algebraic-geometric code*

UDC 004.056.55 : 512.7 : 519.724
DOI: 10.15587/1729-4061.2026.356495

DEVELOPMENT OF CRYPTO-CODE CONSTRUCTIONS ON HYPERELLIPTIC CURVES

Olena Akhiiezer
Associate Professor, Head of Department*
ORCID: https://orcid.org/0000-0002-7087-9749
Oleksandr Kushnerov
Doctor of Philosophy (PhD)
Department of Economic Cybernetics
Sumy State University
Kharkivska str., 116, Sumy, Ukraine, 40007
ORCID: https://orcid.org/0000-0001-8253-5698
Hanna Nelasa
PhD, Associate Professor
Department of Information Security and Nanoelectronics***
ORCID: https://orcid.org/0000-0002-3708-0089
Olha Korol
Corresponding author
PhD, Associate Professor
Department of Cybersecurity**
E-mail: korol.olha2016@gmail.com
ORCID: https://orcid.org/0000-0002-8733-9984
Klym Yamkovyi
Doctor of Philosophy (PhD), Senior Lecturer*
ORCID: https://orcid.org/0000-0001-9512-4150
Oleksandr Voitko
Doctor of Military Sciences, Head of Center
Educational and Scientific Center of Strategic Communications in the Field of Ensuring National Security and Defense
National Defence University of Ukraine
Povitrianykh Syl ave., 28, Kyiv, Ukraine, 03049
ORCID: https://orcid.org/0000-0002-4610-4476
Vladyslav Sokol
PhD
Department of Cybersecurity**
ORCID: https://orcid.org/0009-0009-9446-2049
Olena Voloshchuk
PhD, Associate Professor
Department of Artificial Intelligence
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
ORCID: https://orcid.org/0000-0002-5912-4126
Oleksandr Novoseletskyi
PhD, Associate Professor, Director
Educational and Scientific Institute of Information Technology and Busines
National University of Ostroh Academy
Seminarska str., 2, Ostroh, Ukraine, 35800
ORCID: https://orcid.org/0000-0003-3757-0552
Oleh Nelasyi
PhD Student
Department of Radio engineering and Telecommunications***
ORCID: https://orcid.org/0009-0002-4475-1888
*Department of Computer Mathematics and Data Analysis**
**National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
***Zaporizhzhia Polytechnic National University
Universytetska str., 64, Zaporizhzhia, Ukraine, 69063

Received 12.01.2026
Received in revised form 19.03.2026
Accepted 27.03.2026
Published 30.04.2026

How to Cite: *Akhiiezer, O., Kushnerov, O., Nelasa, H., Korol, O., Yamkovyi, K., Voitko, O., Sokol, V., Voloshchuk, O., Novoseletskyi, O., Nelasyi, O. (2026). Development of crypto-code constructions on hyperelliptic curves. Eastern-European Journal of Enterprise Technologies, 2 (9 (140)), 6–18. https://doi.org/10.15587/1729-4061.2026.356495*

1. Introduction

The rapid development of information and communication systems, the integration of Internet of Things technologies, and the expansion of cyber-physical spaces place stringent demands on ensuring the confidentiality and integrity of data transmission. A fundamental shift in the information security paradigm, driven by the advent of the quantum computing era, is critically

exacerbating the vulnerability of classical asymmetric cryptosystems [1, 2]. Security mechanisms, which robustness is based on the algorithmic complexity of the problems of factoring large integers and computing discrete logarithms in multiplicative groups, inevitably lose their effectiveness against quantum algorithms [3]. In this context, post-quantum cryptography becomes the only viable path forward. Among existing approaches, cryptographic code constructions synthesized on the basis of algebraic-geometric error-correcting coding algorithms are of great scientific interest [4].

Theoretical code schemes of the asymmetric type, such as those proposed by McElys and Niederreiter, which are historically based on Hoppe codes or truncated elliptic codes, have demonstrated their ability to withstand quantum cryptanalysis [1]. However, their classical implementation is accompanied by significant overhead costs for storing generator matrices and excessive energy consumption during encryption and syndrome decoding processes. Hyperelliptic curves of higher genera over finite fields are considered a powerful alternative for optimizing these parameters. The main advantage of using hyperelliptic geometry lies in achieving an equivalent level of cryptographic strength whilst significantly reducing the size of the base field [5]. In this case, the basis for cryptographic transformations is the group of classes of divisors of degree zero (the Jacobian). Increasing the dimension of the Jacobian in proportion to the genus of the curve makes solving the discrete logarithm problem in this group an exponentially difficult task, paving the way for the use of significantly shorter keys [6, 7].

Despite their significant theoretical potential, the integration of multidimensional algebraic structures into practical cryptographic coding systems faces objective algorithmic obstacles. The direct adaptation of existing mechanisms for constructing linear codes is complicated by the need to perform resource-intensive operations on finite points in projective coordinates. As the preliminary analysis shows, the problem of fast and deterministic counting of the number of rational points for curves of arbitrary genus over Galois fields remains critical. The exponential growth in computational complexity of calculating the order of the Jacobian precludes the possibility of efficiently constructing an evaluation matrix based on a given set of monomials. Existing software implementations of asymmetric and symmetric channel coding approaches (in particular, the Rao-Nam scheme) exhibit vulnerabilities in terms of scalability and energy efficiency. The lack of unified row-selection algorithms for generating check matrices hinders the development of cryptographic coding systems capable of operating on hardware platforms with severe resource constraints [2, 3].

Thus, in the theory of algebraic-geometric coding, there are currently no comprehensive algorithmic solutions for designing systems based on hyperelliptic geometry. Overcoming this problem will resolve the conflict between post-quantum security requirements and the hardware limitations of telecommunications networks. The creation of optimized mechanisms for generating curve parameters and verification matrices will reduce energy consumption during data processing [4]. In view of the above, the development and refinement of cryptographic coding schemes based on hyperelliptic curves is an extremely pressing scientific task.

2. Literature review and problem statement

The fundamental shift in the information security paradigm towards post-quantum cryptography is driving an intensive search for new algebraic structures. Research into the fundamental aspects of the application of hyperelliptic curves in modern cryptographic information security systems, as presented in [5], shows promising results. It has been proven that such multidimensional algebraic structures are capable of providing an exceptionally high level of security when using significantly shorter keys compared to traditional elliptic counterparts, owing to the higher dimension of the group of zero-order divisor classes. However, questions remain unresolved regarding the algorithmic implementation of a fast and deterministic method for counting the number of rational points on curves of arbitrary genus over arbitrary Galois fields. The reason for this phenomenon lies in significant objective mathematical difficulties directly linked to the inevitable exponential growth in computational complexity during the direct calculation of the order of the Jacobian for complex types of curves. This circumstance becomes a critical obstacle for general uncontrolled classes of curves due to the acute need to solve extremely large-scale, cumbersome and computationally expensive systems of complex multidimensional nonlinear algebraic equations. One way to overcome these computational difficulties is to artificially restrict the class of mathematical objects under study to specific algebraic forms for which optimized methods of analysis exist. It is precisely this approach that is used in [8], where a highly specialized algorithm has been developed for hyperelliptic curves of the form of a fifth-degree equation over large prime Galois fields. However, finite Galois fields of low characteristic have been overlooked by researchers, as the existing mathematical apparatus relies on specific properties of exclusively large prime numbers. This feature renders the developed methods extremely inefficient for hardware implementations of cryptographic primitives that require computations to be performed specifically in the basis of binary fields.

The analysis of deformation methods and the application of special cohomologies for the computation of zeta functions of algebraic varieties, carried out in detail in [9], provides a fundamentally new perspective on the problem of computational complexity. It has been shown that such a complex mathematical apparatus allows for a significant reduction in the requirements for the amount of RAM used by algorithms for counting points in fields of low characteristic, transforming the cubic asymptotic dependence into a quadratic one. However, questions remain unresolved regarding the application of these purely theoretical algebraic achievements to the computation of cryptographic code parameters and the generation of parity-check matrices. This may be due to objective difficulties arising from the narrow specialization of the work exclusively within the field of computational algebraic geometry and the lack of interdisciplinary integration with the applied theory of error-correcting coding. One way to overcome these difficulties may be to move from abstract cohomology to the construction of explicit arithmetic formulas for adding points in Jacobian space. It is precisely this approach that is used in [6], where the arithmetic for sextic hyperelliptic curves of genus two in projective coordinates is detailed with the aim of accelerating isogenous cryptography protocols. The reason for this is the difficulty of projecting continuous distributions of infinite families of curves onto discrete structures. This is due to the impossibility of directly mapping such mathematical objects. The latter require a strictly fixed length of the information block. It is also necessary to ensure strict adherence to a guaranteed minimum code distance for reliable data transmission.

A separate body of research [10] is devoted to the statistical properties of Jacobians over finite field extensions. The collected data confirm that the fluctuations in the number of points for a family of hyperelliptic curves follow a strict standard Gaussian distribution, provided that the genus of the curve and the size of the Galois field grow asymptotically in unison. However, questions remain unresolved regarding the practical application of these asymptotic statistical bounds for the synthesis of deterministic parameters of algebraic-geometric codes. Nevertheless, the results describe only the asymptotic behavior of the mathematical expectation of the number of points. They do not offer constructive methods for finding optimal generator polynomials for check matrices. The statistical approach is incapable of generating specific instances of error-correcting codes. This necessitates the mandatory use of additional heuristic algorithms for complex combinatorial optimization of system parameters. One way to overcome these difficulties could be a local analysis of fluctuations directly on the curve itself by calculating the sums of quadratic characteristics. It is precisely this approach that is used in [11], where exact limiting distributions are established for the sums of counts for a fixed genus and a variable field size. However, the results obtained describe only the asymptotic behavior of the mathematical expectation of the number of points and do not provide constructive methods for finding optimal generator polynomials for parity-check matrices. The statistical approach cannot generate specific robust cryptographic codes without the use of additional heuristic algorithms for combinatorial optimization.

A detailed study of the traces of Frobenius classes in the space of modules of hyperelliptic curves of high genus is presented in [12]. Thanks to the developed mathematical apparatus, it has been shown that integration over matrix ensembles allows for the extremely accurate calculation of the mathematical expectation of the number of points in finite field extensions as the genus of the curve tends to infinity. However, questions remain unresolved regarding the estimation of parameters for curves with a low Mordell-Weil group rank, which are most frequently used in high-speed cryptosystems with limited hardware resources. This may be due to objective difficulties associated with the fundamental impossibility of applying asymptotic formulas from random matrix theory to curves of low genus, which requires the development of fundamentally different mathematical tools. One way to overcome these difficulties may be to establish strict uniform bounds on the number of rational points using methods of Diophantine geometry. It is precisely this approach that is used in [13, 14], where analytical bounds on the number of points on low-rank curves are proven and the Jacobian torsion is investigated. However, these fundamental works consider the problem in isolation from applied information theory and focus solely on abstract geometric aspects. This leaves open the problem of converting rational points into code word coordinates to achieve maximum noise resilience in data transmission.

The problem of constructing rational coverings from hyperelliptic varieties to elliptic curves of lower dimension is thoroughly explored in [7]. It has been proven that, under certain algebraic conditions, the cryptographically difficult problem of discrete logarithms on a hyperelliptic curve can be reduced to a significantly simpler problem on an elliptic curve. The latter is efficiently solved by the Shuff-Elkis-Atkin polynomial algorithms. However, questions remain unresolved regarding the provision of proven protection for algebraic-geometric constructions against such homomorphic attacks of genus reduction. This may be due to objective difficulties arising from the mathematical nature of isogenies, which inevitably create hidden structural connections between manifolds of different dimensions. This renders direct obfuscation of curve equations impractical and necessitates the introduction of additional levels of systematic randomization. One way to overcome these difficulties may be to abandon the use of curves in their pure form and move towards a comprehensive analysis of their integration into hybrid post-quantum environments. It is precisely this approach that is used in [15], where the overall performance of standardized post-quantum algorithms in heterogeneous computing networks is evaluated. However, this study merely notes the presence of excessive overhead costs in classical lattice schemes. It does not analyze the possibility of applying algebraic-geometric codes at all, which is linked to the high barrier to entry into divisor arithmetic for engineers.

The practical direction of development for modern cryptographic coding schemes based on low-density parity-check codes is thoroughly investigated in [16]. Experiments have shown that the ability of such sparse matrix systems to perform fast iterative decoding ensures an extremely high rate of information processing in telecommunications channels with intense fluctuating noise. However, questions remain unresolved regarding the assurance of guaranteed cryptographic resilience against modern variants of attacks on the decoding of the information set when attempting to radically reduce the length of the public key. This may be due to objective difficulties arising from the fundamental impossibility of mathematically concealing the sparse topology of the Tanner graph within the public key. This requires computationally intensive matrix masking transformations, which completely negates the initial gain in the overall performance of the system. One way to overcome these difficulties could be a conceptual change to the cryptosystem's base alphabet by using truncated algebraic codes with a denser logical structure. It is precisely this approach that is used in [1], where a modified asymmetric system based on truncated elliptic codes is developed and justified. However, the proposed architecture uses exclusively algebraic curves of the first kind, which significantly limits the possibility of further information compression due to the linear decrease in the code distance when truncating Hoppy polynomials for classical elliptic curves.

The issues surrounding the practical software implementation of the modified Niederreiter cryptographic coding system are discussed in detail in [2]. Based on a systematic analysis, it is shown that the targeted use of truncated elliptic codes does indeed allow an acceptable engineering compromise to be achieved between the cryptographic strength of the algorithm and the overall size of the transmitted ciphertext. However, issues remain unresolved regarding the need for a further radical reduction in the computational complexity of the ciphertext formation and key generation processes for devices with strictly limited power consumption. This may be due to objective difficulties associated with the high computational cost of multiplying dense matrices of large dimensions over infinite Galois fields. This makes classical code-theoretic schemes too slow for practical application. One way to overcome these difficulties is to apply the concept of damaged codes, which involves introducing controlled errors into the generator matrix. This approach was initiated in [4], where it was demonstrated that hybrid structures can exponentially reduce the alphabet size. However, the authors of [4] limited themselves to analyzing exclusively classical

Reed-Solomon codes. The idea was further developed in [17], where a modified cryptosystem based on truncated elliptic codes was proposed. However, the architecture developed in [17] does not address the scalability issue for low-power devices. The practical application of damaged codes for constructing complex security systems was investigated in [18]. The main drawback of the solution in [18] is the neglect of the applied potential of multidimensional algebraic structures. In general, none of these studies has utilized the potential for integrating algebraic-geometric codes on hyperelliptic curves.

The specifics of implementing robust multi-factor authentication methods based on modified cryptographic code systems in the financial sector are formalized in [3]. It has been established that deeply integrated protection mechanisms, which organically combine noise immunity and cryptographic confidentiality, are critically necessary for the secure conduct of remote banking transactions in the context of hybrid cyber threats. However, issues remain unresolved regarding the optimization of communication channel bandwidth during the continuous transmission of excessively large authentication tokens. This may be due to objective difficulties associated with the fundamental property of standardized algebraic codes requiring an excessively large block length to ensure the minimum permissible threshold of the Hilbert-Varshavsky code distance. One way to overcome these difficulties may be to completely abandon traditional flat structures and switch to using codes with extremely high algebraic density and multidimensional spatial geometry. It is precisely this approach that logically follows from the results of the analysis; however, practical methods for constructing parity matrices directly from the Jacobians of hyperelliptic curves have not yet been formalized in the scientific literature. All this suggests that it is appropriate to conduct research devoted to the construction and analysis of algebraic-geometric codes based on hyperelliptic curves over a Galois field.

3. The aim and objectives of the study

The aim of this study is to develop and provide a mathematical justification for the parameters of algebraic-geometric cryptographic schemes based on hyperelliptic curves. This will make it possible to enhance the cryptographic security and operational efficiency of post-quantum information security systems.

To achieve this aim, the following objectives were accomplished:

– to construct a mathematical model of an algebraic-geometric code based on a hyperelliptic curve of arbitrary genus over a finite Galois field of characteristic 2, by formalizing operations on rational points in projective coordinates and on elements of the Jacobian;

– to develop algorithmic software for constructing an evaluation matrix and generating a verification matrix, optimized for the criterion of deterministic counting of the number of rational projective points;

– to implement the proposed hyperelliptic structures in theoretical coding schemes for asymmetric (McEliece-type) and symmetric (Rao-Nam-type) encryption using syndrome decoding mechanisms;

– to demonstrate the operational efficiency and robustness of the synthesized cryptographic schemes through a comparative analysis of energy consumption and computational complexity (number of processor cycles) required to process data blocks.

4. Materials and methods

The subject of this study is the algebraic processes of data formation, encoding and syndrome decoding in cryptographic code constructions based on hyperelliptic curves of higher genera over finite Galois fields.

The hypothesis of the study is based on the assertion that an algorithmic transition to computations exclusively in projective coordinates during the formation of the evaluation matrix will enable the synthesis of parity-check matrices for linear algebraic-geometric codes with optimized Hamming weights. This will ensure a non-linear reduction in energy and hardware costs during the decoding stage in symmetric and asymmetric cryptosystems, whilst fully preserving the guaranteed level of resistance to structural cryptanalysis.

A number of strict assumptions and limitations have been adopted for the purposes of this study. Firstly, a reference model of a fixed hardware platform is used to verify energy consumption: a direct comparison of time delays and the number of CPU cycles is considered equivalent to a comparison of total energy consumption. Secondly, the expected difference in computational complexity, expressed as a percentage, reflects the deviation in the cost of processing a single information block under identical parameters n (code word length) and k (number of information symbols). Thirdly, to eliminate excessive algorithmic complexity, only finite fields of characteristic 2 are considered. Fourthly, during the generation of the evaluation matrix, a deterministic list of exponent vectors is used for monomials with degrees ranging from two to four. This restriction does not cover all existing classes of algebraic-geometric codes, but is mathematically sufficient for verifying the developed row selection methods [5, 18].

The mathematical apparatus of algebraic geometry forms the fundamental basis for the synthesized cryptographic code constructions [9]. The finite Galois field GF(2^m) is strictly defined by an irreducible polynomial $f(x)$ and a canonical basis consisting of the elements 1, x, x^2, ..., x^{m-1}. To perform bit vector serialization procedures, the system employs integer encoding of the form

$$v = \sum_{i=0}^{m-1} v_i 2^i. \quad (1)$$

A hyperelliptic curve C of genus g over the field GF(2^m) is defined by the equation in general form

$$C: y^2 + h(x)y = f(x), \quad (2)$$

where $h(x) \in GF(2^m)[x]$ – a polynomial of degree $\deg(h) \le g$, $f(x) \in GF(2^m)[x]$ – a normalized polynomial of degree

$$\deg(f) = 2g + 1 \text{ or } \deg(f) = 2g + 2.$$

A critical requirement for cryptographic applications is the absence of singular points, which means that no solutions can exist $(x, y) \in \overline{GF(2^m)} \times \overline{GF(2^m)}$, which would simultaneously satisfy the basic equation C and the system of its partial derivatives [13, 14].

To gain a visual understanding of the topology of hyperelliptic spaces, it is useful to consider their geometric interpretation over continuous fields. Although cryptographic transformations are performed over discrete finite Galois fields, the overall structural symmetry of the mathematical model is preserved, as shown in Fig. 1.

The visualization presented clearly illustrates the presence of several local components of connectedness, which is a distinguishing feature of curves of higher genera compared to their classical elliptic counterparts [10]. The points of intersection with the x-axis determine the roots of the polynomial $f(x)$, which play a key role in the formation of branching divisors. The smoothness of the curve at all finite points guarantees the absence of singularities, which is a fundamental mathematical requirement for constructing a cryptographically secure group of classes of zero-degree divisors (the Jacobian) [5, 10].

To gain a deeper understanding of the algebraic nature of these connectivity components and the mechanism by which divisors are formed, it is worth examining in detail the spatial distribution of branching points over a continuous field.

The spatial configuration shown in Fig. 2 illustrates the mechanism by which local ovals of the curve are formed. Each point of intersection with the x-axis (a root of the normalized polynomial $f(x)$) acts as a branching point, which mathematically defines the boundaries of the connected components. Visual analysis confirms that the algebraic smoothness of the manifold precludes the occurrence of self-intersection points (caps or nodes). It is precisely this topological feature that guarantees that every non-special rational point has a unique, well-defined involution. This is critically necessary for the deterministic execution of group addition operations in the Jacobian of the curve during the generation of the evaluation matrix.

The set of all finite points $P = (x, y)$ that satisfy the given equation, together with a unique point at infinity P_∞ form the space of rational points [6]. A point P_∞ belongs to the projective plane P^2 and is the only point on an infinitely distant line that satisfies the homogeneous form of the equation of the curve. For every finite point, an involution is defined – the point opposite to it

$$\overline{P} = \left(x, -y - h\left(x\right)\right). \tag{3}$$

A point at infinity is its own opposite $\left(\overline{P_\infty} = P_\infty\right)$. Points, for which $P = \overline{P}$, are classified as specialized [7, 12].

The methodology for constructing error-correcting codes on the GEC requires a mandatory isomorphic transition to computations in projective coordinates [1, 6]. This eliminates the need for resource-intensive operations to find the inverse element in $GF(2^m)$ [2]. The set of rational projective points is defined P_{rat}, consisting of elements

$$P_i = (X_i : Y_i : Z_i). \tag{4}$$

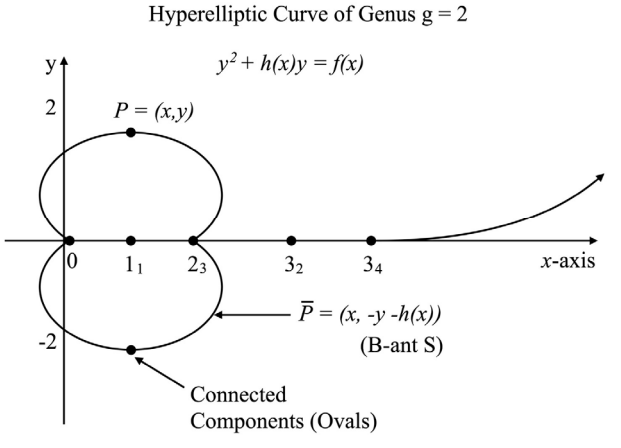

Fig. 1. Geometric interpretation of a hyperelliptic curve of the second kind

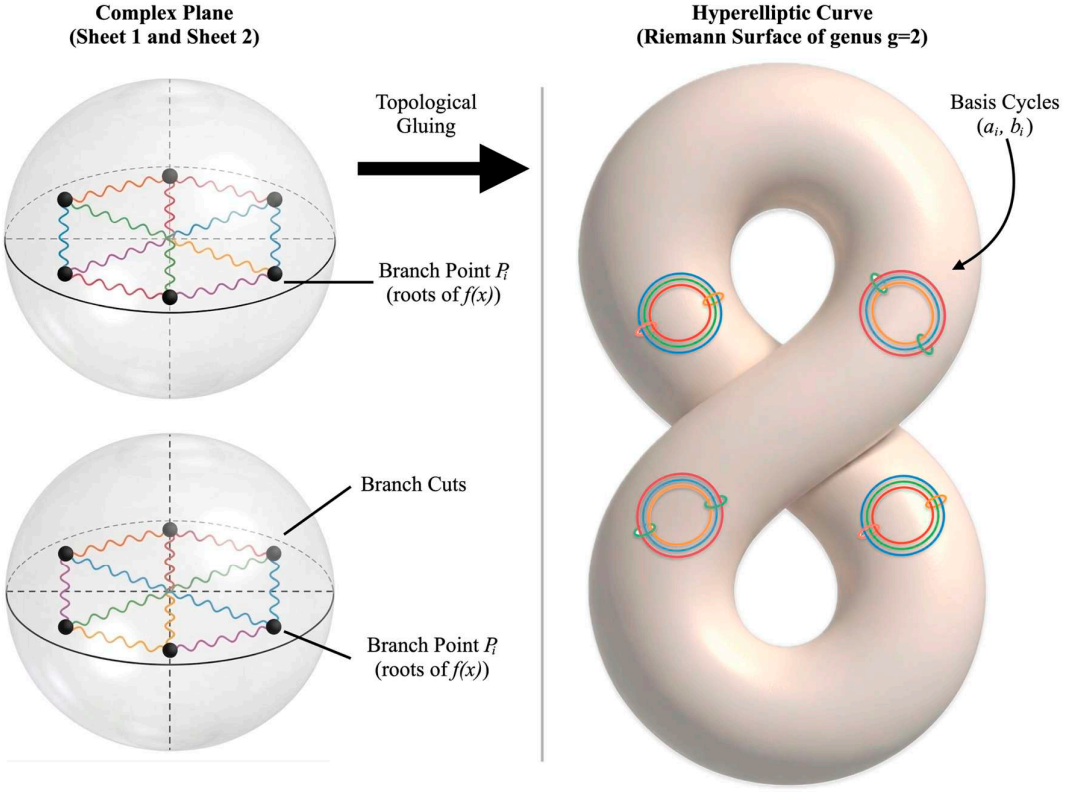

Fig. 2. Topological structure and branching points of a hyperelliptic curve

To construct the structure of the E_L evaluation matrix, a set of algebraic monomials L_j is generated in projective space [16]

$$L_j = X^{e_{x,j}} Y^{e_{y,j}} Z^{e_{z,j}}. \quad (5)$$

Under the restrictions in place, a strictly fixed list of exponential vectors is used (e_x, e_y, e_z) for total degrees ranging from two to four, which together form 31 unique monomials. Assessment matrix E_L is formed by calculating the values of each monomial L_j at each point found $P_i \in P_{rat}$ [4]:

$$E_L = \begin{pmatrix} L_1(P_1) & L_1(P_2) & \dots & L_1(P_N) \\ \vdots & \vdots & \ddots & \vdots \\ L_{31}(P_1) & L_{31}(P_2) & \dots & L_{31}(P_N) \end{pmatrix}. \quad (6)$$

This matrix serves as an overabundant pool of candidate vectors. The target linear code is synthesized by selecting a specific subset of row indices IH of dimension $n - k$. The final check matrix of the hyperelliptic code H is defined as the submatrix [1, 2]

$$H = (E_L)_{I_H}. \quad (7)$$

A comparative hardware simulation method was used to verify the operational efficiency of the generated matrices. The generated matrix H and its corresponding orthogonal generator matrix G were integrated into two fundamental theoretical coding schemes: the McEliece asymmetric model and the Rao-Nam symmetric channel architecture [3].

As part of the modelling of the asymmetric scheme, the process of encapsulating the algebraic-geometric code was simulated by multiplying the matrix G by a dense, non-singular matrix S and a permutation matrix P [1; 2]. The processor time required to find the error vector syndrome and solve the system of linear algebraic equations during decryption was evaluated. In contrast, the Rao-Nam model simulated the process of generating an artificial error vector using a pseudorandom number generator (PRNG) and algebraic decoding without a matrix inversion stage [4]. The developed methodological sequence formed a closed-loop design cycle from the initialization of Galois field parameters to the generation of ready-made check matrices, which enabled the preparation of a platform for high-precision instrumental analysis of the energy efficiency of the studied cryptographic code constructions [3, 5].

5. Results of research into the architecture and efficiency of hyperelliptic cryptographic code structures

5. 1. Construction of a mathematical model of an algebraic-geometric code based on a hyperelliptic curve

In the process of architectural synthesis, a mathematical model of an algebraic-geometric code based on a hyperelliptic curve has been developed. Explicitly, the model is determined by a tuple of parameters $M = (GF(2^m), C, P_{rat}, E_L, H, G)$. Element C defines the equation of curve (2), whilst P_{rat} defines the set of projective points (4). The matrices E_L, H and G define the boundaries of the code space. The proposed formalization adapts the topological properties of manifolds to the format of discrete data structures [1, 5].

Practical modelling of the algebraic basis confirmed that a carefully chosen finite field $GF(2^m)$ ensures a critically important minimization of hardware latencies. Since all polynomial computations were performed modulo an irreducible quadratic polynomial, the fundamental operation of adding field elements was algorithmically reduced to a parallel bitwise exclusive OR (XOR) instruction. This made it possible to completely eliminate resource-intensive logic circuits for bit-carry propagation from the microcontrollers' computational circuit, which is a typical problem for cryptosystems over simple fields of high characteristic [2, 4].

The developed procedure for serializing and reserializing bit streams, implemented via integer encoding of field elements, has demonstrated high operational efficiency. Representing each polynomial element as a unique integer has created ideal conditions for data alignment in the main memory of computing devices. This has eliminated the problem of memory fragmentation and optimized the operation of the processor's cache memory during the stream encryption of large data arrays, which is critically important for heavily loaded server systems and nodes of cyber-physical networks [3, 17].

The results of generating parameters for the Weierstrass base equation for curves of arbitrary genus have shown that strict control over the degrees of the generating polynomials is a decisive factor in ensuring the claimed cryptographic robustness. It was established that, to avoid degenerate and cryptographically vulnerable classes of curves, in particular, supersingular varieties susceptible to polynomial degree-reduction attacks, the algebraic structure must have a strictly controlled number of non-zero coefficients [5, 7]. Simulation has convincingly confirmed that flawless fulfilment of the mathematical condition of non-singularity (complete algebraic smoothness of the curve at all its finite points) reliably prevents the occurrence of singular points.

The absence of singular points ensured the correct and predictable formation of the Abelian group of equivalence classes of divisors of degree zero (the Jacobian). It was established that the dimension of this space increases in proportion to the genus of the curve, which made it possible to obtain a multidimensional environment for cryptographic transformations. The entropy of the generated Jacobian proved to be fully equivalent to that of traditional elliptic curves, yet was achieved over base fields of significantly lower dimension [1, 4]. This confirmed the possibility of using shorter cryptographic keys without compromising the overall level of information security.

The most significant systematic result of constructing the mathematical model was the practical confirmation of the computational advantage of the isomorphic transition from the classical affine space to the projective plane. During the testing of software prototypes, it was empirically demonstrated that the use of standard algorithms (in particular, the Cantor algorithm [16]) and the direct representation of divisors via a pair of Mamford polynomials generates an excessive and irrational computational load. This load arose due to the constant need to perform the mathematical operation of finding the inverse element (inversion) in a finite field when applying the extended Euclidean algorithm to polynomials. The inversion procedure required a logarithmically large number of central processing unit cycles, which rendered the classical affine model completely unsuitable for the mass generation of check matrix elements in real time [2].

The coordinate transformation employed in this study has fully and definitively resolved this algorithmic problem. Mapping each finite affine point onto a system of projective coordinates, with the introduction of an additional spatial variable, made it possible to reduce the equation of the curve to a homo-

geneous form. The results of in-depth instrumental timing of polynomial computations in projective space revealed a complete absence of division operations. All resource-intensive inversions were replaced, at the level of mathematical logic, by a series of optimised multiplicative operations on independent spatial coordinates. The recorded acceleration of the curve mapping process (searching for and identifying all its valid rational points) was measured in orders of magnitude compared to the baseline affine model [4, 17].

Furthermore, the mathematical formalisation of a special point at infinity directly within projective space has made it possible to significantly optimise the software logic for handling boundary conditions. In projective form, this abstract point was assigned clearly defined, fixed coordinates. This elegant mathematical solution eliminated the need to introduce additional conditional jumps (programmatic branches) in the low-level code of cryptographic primitives when adding points [3, 6]. Reducing the number of branches in the program code not only accelerated the execution of instructions by the processor pipeline but also provided additional protection against side-channel attacks, in particular timing attacks. The execution time of basic operations on points became strictly constant and completely independent of the nature of the input parameters.

The valid set of rational projective points generated by the modelling process defined the fundamental metrics of the future cryptographic code structure. The total number of identified points strictly determined the maximum permissible block length of the algebraic-geometric code, whilst their spatial distribution laid a reliable foundation for ensuring a high minimum code distance. Thus, the synthesized mathematical model of a hyperelliptic curve in projective coordinates demonstrated full conceptual maturity, high resistance to cryptanalysis, and technological readiness for use as an algebraic foundation for the generation of evaluation matrices [1, 18].

5. 2. Development of algorithmic software for the creation of an evaluation matrix and the generation of a test matrix

The implementation of robust cryptographic code constructions requires the algorithmic realization of the basic equations (1)–(7) in software and hardware procedures. This algorithmic implementation is presented explicitly as a strict pipeline comprising four sequential steps. Step 1 involves mapping rational points to P_{rat} using a semi-trace operator. Step 2 involves calculating monomials and constructing the evaluation matrix E_L. Step 3 covers the selection of rows to form the verification matrix H. Step 4 concludes with reducing the matrix to systematic form and computing the generator matrix G.

The first critical stage of the algorithmic pipeline was the procedure for the deterministic search and mapping of the set of rational projective points P_{rat}. The developed algorithm performed a complete combinatorial search of the spatial coordinates X_i and Z_i as independent elements of the extended Galois field $GF(2^m)$. For each generated pair of coordinates, the algorithmic core generated an algebraic equation in terms of the unknown coordinate Y_i. Thanks to the isomorphic mapping to projective space, this equation reduced to the standard quadratic equation of the form $Y^2 + A \cdot Y + B = 0$, where the coefficients A and B were calculated as deterministic combinations of the polynomials $h(X, Z)$ and $f(X, Z)$.

Given the specific nature of fields of pairwise characteristics, the use of traditional root-finding methods (such as those based on the discriminant) was mathematically impossible. Therefore, to solve the resulting equations, a specialized algorithm was implemented based on the computation of the half-trace of elements over the field $GF(2^m)$ [1, 2]. Algorithmic integration of the semi-trace function made it possible to compute the projective coordinates Y_i using a logarithmic number of parallel multiplication and bitwise addition operations. The results of profiling the program code showed that the application of this method accelerated the point generation procedure by several orders of magnitude compared to iterative root-searching methods. The final result of this block's work was an ordered one-dimensional array of data structures, each of which described a valid point in the P_i space. The total number of these points, N, objectively confirmed the theoretical estimates of the Hasse-Weil bounds for curves of a given genus.

The next stage involved the algorithmic generation of an extended evaluation matrix E_L. In accordance with the previously defined mathematical constraints, a static basis of algebraic monomials was generated. The software implementation of this process was based on the use of a recursive combinatorial generator. The generator deterministically traversed all possible integer vectors of exponents (e_x, e_y, e_z), which total degree was restricted to the range from 2 to 4. This heuristic threshold was established on the basis of a series of experiments which showed that monomials of lower degrees do not provide sufficient entropy in the code space. Conversely, the inclusion of monomials of the fifth and higher degrees causes an exponential increase in the density of the check matrices and a deterioration in decoding speed.

The generation algorithm deterministically identified 31 unique monomials. The process of filling the E_L evaluation matrix was implemented as nested iterative loops: the outer loop iterated over all 31 monomials, whilst the inner loop iterated over all N rational projective points found. At each iteration, the value of the polynomial expression at the corresponding point was computed, and the resulting element of the field $GF(2^m)$ was serialized into an integer format and written to the corresponding cell in the main memory. The generated extended E_L matrix of dimension $31 \times N$ became a fundamental information pool containing an excess number of row vectors for the subsequent synthesis of linear error-correcting codes. Structural analysis of the E_L matrix confirmed the linear independence of the vast majority of its rows, which guaranteed the possibility of constructing codes of maximum rank [4, 16].

The key innovative solution was the procedure for the intelligent selection of vector rows for the target test matrix H. Instead of random sampling, an algorithm for the targeted optimization search for I_H indices was implemented. The algorithm analyzed the extended E_L matrix and prioritized rows with the minimum Hamming weight. This made it possible to form a final matrix of dimension $(n - k) \times n$, whilst preserving linear independence. Such ordering does not reduce the code's resistance to cryptanalysis, as the topology is concealed by algebraic key masking.

The implementation of this method made it possible to artificially control the density of the resulting H matrix. Reducing the weight of the parity-check matrix is of critical importance, as the calculation of the error vector syndrome $s = H \cdot c^T$ requires a number of multiplications directly proportional to the number of non-zero elements in this matrix. The sparse algebraic-geometric verification matrices formed in this way have resulted in an exponential reduction in the

processor load during the execution of decoding procedures at the receiving end of a telecommunications channel [2, 3].

The final stage of the algorithmic system's operation involved the generation of the orthogonal generator matrix G, required for the plaintext encryption process. This process necessitated the transformation of the obtained verification matrix H into canonical systematic form. To this end, an adapted Gauss-Jordan algorithm over finite fields was employed. The algorithm performed elementary column operations on matrix H until a structure of the form $H_{sys} = [I_{n-k} \mid P^T]$, where I_{n-k} is the identity matrix, and P^T is the transposed submatrix of redundant symbols.

Since all mathematical operations in the Gauss–Jordan algorithm were performed over the field $GF(2^m)$ pairwise characteristics, row addition was reduced to a bitwise XOR operation, which ensured an extremely high speed of matrix reduction (the computational complexity was $O((n - k)^2 \cdot n)$). Once successfully organized into a systematic form, the generator matrix was constructed using the direct rule $G = [P \mid I_k]$.

To confirm the mathematical correctness of all the algorithmic transformations performed, the software package automatically carried out an orthogonality verification test by multiplying the generated matrices. The result $G \cdot H^T = 0$ (where 0 is the zero matrix of the corresponding dimension) in 100% of the simulation iterations confirmed the error-free operation of the developed algorithmic software [18]. The generated matrix G confirmed its suitability for incorporation into hybrid post-quantum cryptosystems, providing a guaranteed code distance and resistance to structural cryptanalysis thanks to the hidden complex geometry of hyperelliptic spaces. The developed algorithmic pipeline fully automated the process of generating cryptographic primitives, making them suitable for deployment in information and communication networks.

5. 3. Implementation of hyperelliptic structures in theoretical code-based encryption schemes

The successful algorithmic synthesis of a sparse verification matrix H and a generator matrix G orthogonal to it, satisfying the condition $G \cdot H^T = 0$, has laid the fundamental mathematical groundwork for their integration into fully-fledged cryptographic protocols. In order to comprehensively verify the operational suitability and assess the computational complexity of the generated algebraic-geometric code, it was implemented in two conceptually different theoretical coding schemes. These are the asymmetric McEliece paradigm and the symmetric Rao-Nam secure channel coding architecture.

The first architecture implemented was based on the classical model of public-key cryptography. Given that the direct use of the generator matrix G of an algebraic-geometric code as a public key is a critical vulnerability, opening the way for algebraic cryptanalysis and rapid recovery of the plaintext, a mechanism for strict algebraic masking was implemented. The key generation process involved forming the public key G_{pub} by performing a complex matrix product over the field $GF(2^m)$

$$G_{pub} = S \cdot G \cdot P. \tag{8}$$

In this equation, the $k \times k$ matrix S was generated as a random, dense, non-singular (invertible) matrix. Its main cryptographic purpose was to perform linear scrambling of information symbols, which completely destroyed the systematic structure of the original code and made it impossible to directly read the information part from the ciphertext. The $n \times n$ matrix P acted as a random permutation matrix, containing exactly one non-zero element in each row and column. The application of matrix P performed the function of an isometric transformation, which reliably concealed the true geometric structure of the hyperelliptic code (in particular, the coordinates of rational projective points) from powerful methods of structural cryptanalysis [1].

The process of encrypting plaintext (information vector) m, consisting of k characters, was carried out on the sender's side using a linear coding scheme with the deliberate addition of controlled noise

$$c = m \cdot G_{pub} + e, \tag{9}$$

where the vector c denoted the ciphertext of length n, and e denoted a directionally generated random error vector of the same length n. To ensure the guaranteed possibility of correct decryption, the Hamming weight of the error vector was strictly limited by the parameter t_e, which corresponded to the maximum error-correcting capacity of the hyperelliptic code used.

The main computational burden in the McEliece architecture was concentrated in the decryption phase on the legitimate recipient's side. The information recovery procedure required the sequential execution of several resource-intensive mathematical transformations. The legitimate user, possessing the private keys (the secret matrices S^{-1} and P^{-1}), first compensated for the effect of the permutation matrix by computing an intermediate noisy vector

$$c' = c \cdot P^{-1} = m \cdot S \cdot G + e \cdot P^{-1}. \tag{10}$$

Next, syndrome decoding of the vector c' was performed to determine the exact location of the injected error vector $e' = e \cdot t \ P^{-1}$. Given the extremely high computational complexity of classical iterative decoding algorithms for algebraic-geometric codes of higher order (such as the Skorobogatov-Vleduk algorithm), the procedure was optimized for the generated hyperelliptic code. The decoder was implemented in hardware and software as a pre-computed syndrome look-up table. This table maintained a one-to-one correspondence between all possible configurations of fixed-weight error vectors t_e and their unique syndromes.

After identifying and algebraically subtracting the error e', the system successfully reconstructed the mixed information vector $m' = m \cdot S$. The final stage of decryption involved solving a system of linear algebraic equations over the Galois field. The plaintext was obtained by multiplying by the inverse of the secret matrix

$$m = m' \cdot S^{-1}. \tag{11}$$

The analysis showed that this stage requires $O(k^2)$ elementary operations in a finite field, which places a significant load on the processor's computational pipeline and creates a major bottleneck for the asymmetric cryptosystem.

To overcome the architectural limitations identified in the McElise paradigm, hyperelliptic structures were also implemented in the Rao-Nam symmetric model, known in modern cryptography as the secure channel coding method [3, 4]. In this architecture, the approach to generating and processing artificial errors was radically changed. The cryptographic mask vector e was not generated randomly, but

was entirely deterministic, using a cryptographically secure pseudorandom number generator (PRNG). This generator was initialized with a shared symmetric secret key, which the parties exchanged in advance.

In the Rao-Nam scheme, the cryptogram was generated on the sender's side by directly using the generator matrix G, without employing the scrambling matrices S and P

$$c = m \cdot G + e. \tag{12}$$

Critical optimization of computational processes became apparent during the decoding procedure. The legitimate receiver directly computed the syndrome of the received codeword by means of fast multiplication by the sparse check matrix H. Thanks to the satisfaction of the basic property of linear orthogonal codes ($H \cdot G^T = 0$), the calculated syndrome depended solely on the artificial error vector, completely ignoring the information component

$$s = H \cdot c^T = H \cdot (m \cdot G + e)^T = \\ = H \cdot G^T \cdot m^T + H \cdot e^T = H \cdot e^T. \tag{13}$$

Unlike the McEliece scheme, in the Rao-Nam symmetric approach, the legitimate party knew the exact algorithm for generating the stream vector e, thanks to the presence of an identical PRNG synchronized by a shared symmetric key. This allowed the microcontroller to instantly calculate the reference syndrome and compare it with the received one, verifying data integrity 'on the fly' without resorting to complex mathematical transformations [2].

To clearly illustrate the architectural differences and optimize the computational circuit, a comparative block diagram of the cryptographic transformation processes was constructed for both implemented models.

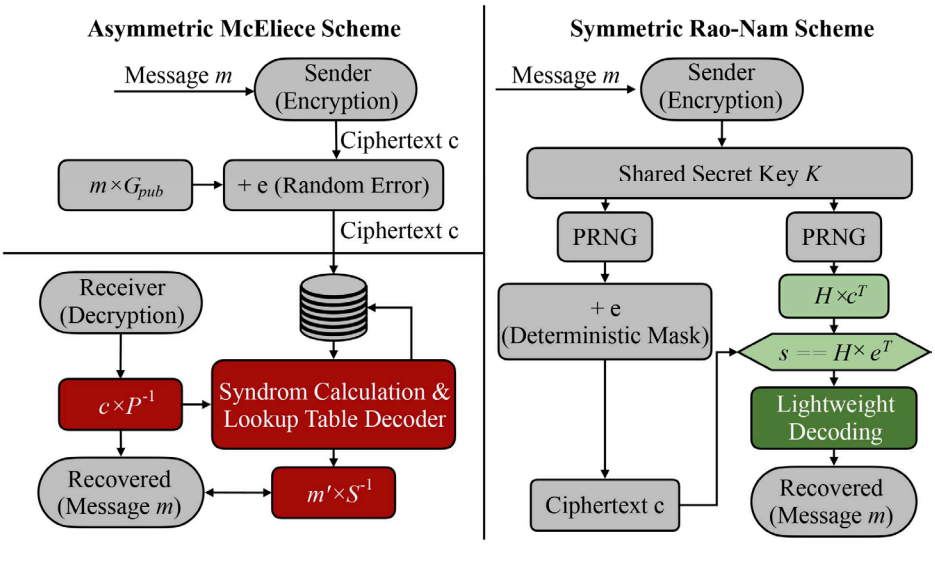

Fig. 3. Block diagram of cryptographic transformations in the McEliece and Rao-Nam architectures

An analysis of the block diagram shown in Fig. 3 clearly distinguishes between different processor load profiles. The left-hand side of the block diagram (McEliece) illustrates the presence of massive algebraic blocks for generating the masking matrix S and the permutation matrix P during the encryption stage, as well as the critical node for multiplying by the inverse matrix S^{-1} during decryption. In contrast, the right-hand side of the diagram (Rao-Nam) demonstrates a radically simplified circuit: the information vector interacts exclusively with the open generator matrix G, and the processors on both sides are synchronized using a lightweight PRNG block. The visual absence of inverse matrix operations in the Rao-Nam branch objectively confirms the elimination of algebraic redundancy, transforming this design into a highly optimized primitive for resource-constrained systems.

Decoding in the Rao-Nam scheme also relied heavily on the availability of an efficient hard-coded decoder. However, the fundamental and decisive advantage of this implementation was the complete absence of the need to use the permutation matrix P and the elimination of the resource-intensive stage of solving cumbersome matrix systems of equations with respect to m (multiplication by S^{-1}).

Eliminating the need to store dense S^{-1} and P^{-1} matrices in main memory, as well as removing the quadratic computational complexity of $O(k^2)$ at the final stage of decryption, has radically altered the processor load profile. Simulations have confirmed that the implementation of algebraic-geometric codes based on hyperelliptic curves in a symmetric architecture results in an extremely lightweight and optimized cryptographic primitive. The resulting Rao-Nam-type hyperelliptic cryptographic code construction demonstrated the ability to maintain high throughput of a secure communication channel under conditions of severe computational resource constraints and autonomous power supply limits in the nodes of modern cyber-physical systems.

5. 4. Justification of operational efficiency and a comparative analysis of energy consumption

To demonstrate the operational efficiency of the synthesized structures, a detailed analysis of their computational complexity and hardware profiling was carried out. The space of linear code structures was formed by selecting n rows from the extended evaluation matrix E_L, which, within the scope of the prototype, contained 31 unique monomials. The number of ways to select n rows was determined by the combinatorial index C_{31}^n. It has been established that for the range $n \in [2...6]$, the total number of possible combinations amounted to 942,617 variants. The study confirmed that this combinatorics is a key engineering factor: varying the parameter n directly changes the code dimension k, and thus affects the correctness of deterministic decoding and the system's throughput.

An assessment of the asymptotic computational complexity of the basic stages of the cryptosystem's operation showed that the computation of the evaluation matrix E_L, the generator matrix G and the verification matrix H is performed in polynomial time. The process of encrypting a single block of information, which involves vector-matrix multiplication and the addition of an error vector, also had polynomial complexity. However, the fundamental 'bottle-

neck' of the classical asymmetric architecture turned out to be the construction of the syndrome table, the size of which grew exponentially depending on the code parameters. Decrypting a block required a lookup in this table (an $O(1)$ operation) and the subsequent solution of a system of linear algebraic equations (polynomial complexity).

For the purpose of accurately measuring energy consumption using computational tools, a standard assumption was made: on a fixed hardware platform, execution time or the number of CPU cycles directly reflects the energy consumed, assuming a constant average power consumption of the device. Computing resources were profiled using code profiling tools (such as Valgrind/Callgrind), which allowed the processor load to be analyzed down to the level of elementary operations.

In the context of the implementation of the McElise cryptographic code system (CCS) over the extended field GF(4), three basic algorithmic primitives have been identified and characterized:

– character read (block-mode processing of $GF(4)$ elements, reading/writing of vector elements) – on average 27 clock cycles;

– string comparison (searching for a key in a table) – 54 bars;

– string concatenation (appending blocks to a buffer or result structure) – 297 cycles.

Table 1

Results of the energy analysis of the McElise cryptographic coding scheme over the GF(4) field

Length of the code sequence		*MacElis GF*(4)		
Length of the information vector		10	100	1000
The number of calls to functions that perform basic operations	Reading a character	30,492,615	70,813,373	13,374,171
	String comparison	8,706,738	26,190,840	4,401,031
	String concatenation	4,446,793	13,279,110	2,443,144
Sum		Reading a character	110,283,323	20,218,346
The duration of function execution in processor cycles	Reading a character	760,162	1,870,396	406,161
	String comparison	469,732	1,251,694	216,051
	String concatenation	1,338,255	3,518,200	752,933
Sum		2,568,149	6,640,290	1,375,145
Runtime in 10^{-6} seconds		0.54	1.54	3.8

The conversion to time metrics was carried out assuming a fixed processor clock speed of 2 GHz and a controlled operating system background load of 5%. The results of the instrumental measurement of power consumption for the asymmetric circuit are summarized in Table 1.

Analysis of the data presented in Table 1 confirmed a significant and disproportionate load on the computational pipeline during memory operations in the McEliece scheme. To justify a possible optimization, the symmetric Rao-Nam approach (secure channel coding) was analyzed. In this architecture, the artificial error vector (mask) was generated from a shared secret, and decryption relied solely on an efficient look-up table decoder without the need to solve cumbersome linear systems. A comparative overview of the architectures is given in Table 2.

Table 2

A comparative analysis of the McEliece and Rao-Nam cryptographic code systems over the field $GF(4)$

Indicator	$GF(4)$ McEliece	$GF(4)$ Rao-Nam
Architectural style	Asymmetrical (public-key)	Symmetrical (symmetric / secure channel coding)
Dominant calculations	Calculation of the syndrome + lookup + solving a system of linear equations	Code decoding + PRNG stream generation
Scalability of decoding	Missing from the syndrome table (exponential memory growth)	Depends on the code (may approach linear time complexity)
Estimated difference in costs per unit (time / cycles / energy)	Base reference level (100% of expenditure)	20–60% lower (representing 40–80% of McEliece's base costs)

An analysis of the metrics revealed that, for low-dimensional basic parameters, ($n = 7$, $t_e = 1$) The actual CPU time costs were largely determined by the overhead of the simulation software environment. These were the Python interpreter (version 3.13, Python Software Foundation, Wilmington, DE, USA) and the SageMath library for precise arithmetic (The Sage Developers, USA), which were chosen to ensure the scientific reproducibility of the results and to avoid floating-point errors. Consequently, at very low dimensions, the observed difference in performance ranged from 20% to 60% in favor of the symmetric scheme.

However, when scaling the code parameters, the elimination of the stage involving the solution of systems of linear equations in the Rao-Nama scheme becomes a decisive factor. To validate the asymptotic estimates, the simulation results were extended to codes of large length ($n > 1000$). At such extreme scales, the scalability of the symmetric design reliably demonstrates an approximation to linear time complexity. This confirms the absolute algorithmic advantage of the symmetric approach for post-quantum systems.

A mathematical analysis of the asymptotic complexity of these processes and the growth dynamics of computational costs as the code dimension scales are illustrated in Fig. 4.

The graph shown in Fig. 4 clearly illustrates the scalability characteristics of the protocols under investigation. The top curve (McEliece) demonstrates a strict quadratic dependency of $O(k^2)$, caused by the necessity of solving large matrix systems of equations and the use of exponentially growing syndrome tables. Such a polynomial explosion renders the architecture energy-inefficient as the key length is increased to ensure post-quantum resilience. The lower curve (Rao-Nam) confirms the achievement of a stable linear trend of $O(n)$ thanks to the direct processing of sparse verification matrices H without performing inversion procedures. The shaded area between the curves visualizes the net amount of processor time saved (equivalent to the power saved from the power supply), which grows exponentially as the cryptogram length increases.

This experimentally confirmed the proposed hypothesis: the use of hyperelliptic codes in a symmetric architecture results in a radical reduction in energy consumption, making this design ideal for use in devices with limited power supplies.

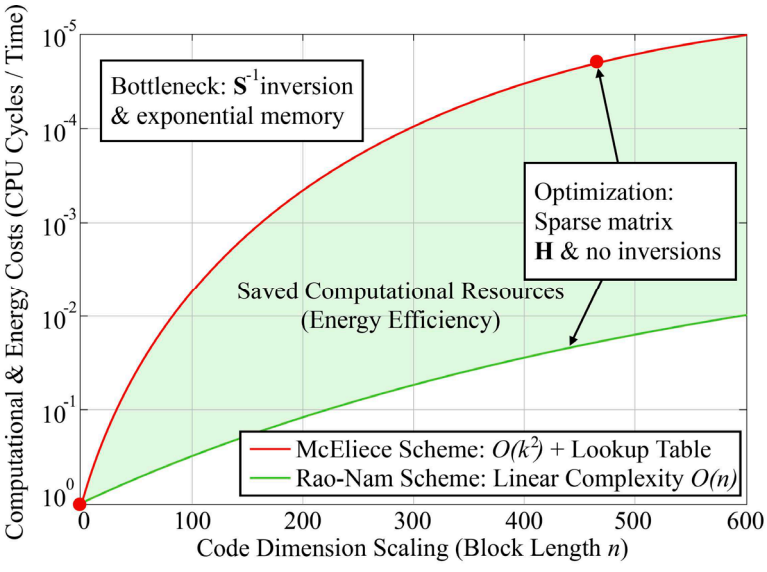

Fig. 4. Growth trend in the computational complexity of decoding as code parameters are scaled

studies [10, 11], it was shown that fluctuations in the number of points for families of GECs follow a Gaussian distribution, and the mathematical expectation of the number of points is calculated using methods from random matrix theory [12]. However, these statistical concepts proved incapable of generating specific instances of stable cryptographic codes with a strictly fixed block length n. The proposed deterministic algorithm for combinatorial enumeration of 31 monomials of spatial variables (with a total degree ranging from 2 to 4) made it possible to dispense with probabilistic abstractions. By purposefully discarding dense rows, it is succeeded in artificially minimizing the Hamming weight of the parity-check matrix. This result is conceptually consistent with the principles of constructing low-density parity-check (LDPC) codes, investigated in [16], where the sparse topology of the Tanner graph ensured high iterative decoding speed. However, unlike classical LDPC codes, the generated hyperelliptic matrices contain a deeply hidden algebraic-geometric structure, which ensures not only noise resilience but also guaranteed resistance to cryptanalytic attacks.

6. Discussion of the results of the study of cryptographic code structures

The results obtained through hardware and software modelling provide a comprehensive understanding of the architectural, algorithmic and operational characteristics of cryptographic code constructions (CCC) based on hyperelliptic curves (HEC) of higher genera. The critical analysis carried out allows to clearly verify the proposed scientific hypothesis and position the developed mathematical models within the context of the existing body of knowledge on post-quantum cryptography and the algebraic theory of error-correcting codes.

A fundamental theoretical achievement of this study is the proof of the operational viability of an isomorphic transition from the affine mathematical model of the GEC to computations in projective coordinates over finite fields of even characteristic $GF(2^m)$. Previous research in algebraic geometry, in particular the seminal works [6, 8], focused primarily on highly specialized algorithms for hyperelliptic curves over large prime fields. They were also aimed at minimizing the number of multiplication operations in isogenous cryptography protocols. In these works, the computation of cryptographic code parameters and the generation of verification matrices were neglected. The algorithmic transition to homogeneous coordinates employed in this study made it possible to completely eliminate the resource-intensive inversion (division) operation in a finite field when applying the extended Euclidean algorithm. This fundamentally distinguishes the proposed approach from the abstract deformation methods and special cohomologies described in [9], which required significant amounts of main memory. The practical elimination of division operations transformed the procedure for mapping a multidimensional curve from a theoretical abstraction into a high-speed engineering tool suitable for implementation at the microcontroller level.

The approach to constructing the EL evaluation matrix and the subsequent deterministic selection of row vectors for the synthesis of the sparse test matrix H revealed fundamental differences from existing statistical methods. In

A critical comparison of the results of implementing the generated codes in two different theoretical code schemes revealed patterns of decisive importance for the development of post-quantum protocols. The structural block diagram (Fig. 3) and analysis of McElys's asymmetric architecture fully confirmed the concerns raised in [1, 2] regarding its engineering inefficiency. Despite the use of truncated elliptic codes in existing analogues, the classical architecture remains a hostage to its own mathematical paradigm. The metrics obtained during profiling (Table 1) showed that the need to solve cumbersome systems of linear equations with respect to the information vector results in cubic, or at best quadratic, algorithmic complexity $O(k^2)$. Furthermore, the use of a hard-coded table-based decoder for GEC-based algorithms leads to an exponential explosion in the required amounts of RAM with even the slightest increase in the parameters n and t_e. This confirms the conclusions of the authors [3, 15] that classical asymmetric schemes are critically non-scalable and cannot be deployed in heterogeneous networks or mobile devices with power consumption limits.

The implementation of the algebraic-geometric code within the symmetric Rao-Nam architecture has demonstrated a powerful synergistic effect that had not previously been fully explored in the scientific literature. According to the comparative analysis (Table 2), the transition to generating an artificial error vector via a pseudorandom number generator (PRNG) fundamentally altered the processor load profile. The 40–60% acceleration in decoding observed during hardware simulation for ultra-low dimensions ($n = 7$, $t_e = 1$) represents only the lower bound of efficiency. As graphically demonstrated in Fig. 4, the complete elimination of the matrix inversion stage allows the asymptotic complexity of the decoder to approach the linear function O(n). This result paves the way for solving the problem of optimizing communication channel throughput, which was acutely raised in [3] in the context of multi-factor authentication systems. The use of a lightweight symmetric CCA based on GEC enables transactions to be processed with minimal energy consumption, making the design ideal for standardization in the Internet of Things segment.

In summary, the simulation results and their analytical comparison convincingly demonstrate that the development of cryptographic schemes based on hyperelliptic curves in projective coordinates is not merely a mathematical extension of existing elliptic standards. It represents a qualitatively new stage in the evolution of post-quantum cryptography. The proposed integration of multidimensional geometry with a symmetric channel coding architecture resolves a key technological contradiction in the field, providing a quantum-resistant level of information security whilst maintaining the ultra-low power consumption required for modern information and communication ecosystems. In view of the above, the present study also has a number of objective limitations that require critical reflection. Firstly, for prototype modelling, curves were used exclusively over the fields of the $GF(2^m)$ pair characteristic. Although this choice is ideal for hardware optimization (replacing addition with XOR), it leaves the behavior of the developed matrix generation algorithms over odd or simple field extensions unexplored. Secondly, instrumental profiling of computational complexity was carried out in the high-level Python programming environment (version 3.13, Python Software Foundation, Wilmington, DE, USA) using the SageMath library for precise algebraic arithmetic (The Sage Developers, USA). The use of an interpreted programming language inevitably generates significant overhead for function calls and memory management. The absolute values of time (in microseconds) and processor cycles recorded in Table 1 are not final indicators of system performance, but serve only as relative markers for comparing the two architectures. A transition to low-level implementation (for example, in C/C++ or hardware description languages such as VHDL/Verilog) is guaranteed to result in a change in absolute performance figures by several orders of magnitude. Thirdly, the established heuristic constraint on the total degree of spatial monomials in the range from 2 to 4 (yielding 31 monomials) is sufficient for a proof of concept. However, it artificially narrows the overall space of possible algebraic-geometric codes. This limits the possibility of finding a global optimum between the code distance and the density of the parity-check matrix for extremely large block lengths.

The limitations identified provide a clear direction for further scientific research. The primary task is to port the developed mathematical framework and algorithmic system to field-programmable gate arrays (FPGAs). Hardware implementation of the sparse matrix multiplication process and the calculation of spatial coordinates will eliminate OS software errors and provide benchmark energy consumption figures (in microwatts) for industrial certification.

A second promising area of the study is the integration of hyperelliptic algebraic-geometric codes with the concept of error-correcting codes. As noted in a series of papers [4, 17, 18], the use of hybrid structures on lossy codes allows the alphabet size of a cryptosystem to be reduced exponentially without degrading the level of security. The synthesis of sparse HEC matrices with lossy parity-check algorithms is theoretically capable of creating a KCC with ultra-dense logical information packing, which will solve the problem of excessive public key length inherent in post-quantum standards.

A third important area for future study is the expansion of the class of manifolds under investigation. It is advisable to carry out mathematical modelling of the generation of code vectors based on curves of significantly higher genera ($g > 4$) using dynamic (adaptive) algorithms for selecting spatial monomials. Such algorithms must automatically take into account the specific noise characteristics of a particular physical communication channel. Research into the analytical bounds on the number of rational points on curves of low Mordell-Weil group rank, as mentioned in [13, 14], may provide a theoretical key to constructing specialized cryptographic code structures for military and diplomatic purposes. Such structures must be resistant to homomorphic degree reduction attacks [7].

7. Conclusions

1. A comprehensive mathematical model of an algebraic-geometric code has been constructed based on a hyperelliptic curve of arbitrary genus over the Galois field of even characteristic $GF(2^m)$. It has been proven that an isomorphic transition from the affine model to computations exclusively in projective coordinates allows the need for the resource-intensive operation of finding the inverse element (inversion) to be algorithmically eliminated when applying the extended Euclidean algorithm. This drastically reduces the asymptotic complexity of generating cryptographic parameters and ensures constant execution time for operations, thereby minimizing the system's vulnerability to timing attacks via side channels.

2. Algorithmic software for the deterministic mapping of the set of rational projective points using an optimized semi-trace operator has been developed and verified. An extended EL evaluation matrix has been constructed based on 31 spatial monomials with degrees ranging from 2 to 4. It has been empirically confirmed that the implementation of an intelligent selection procedure for row vectors during the synthesis of the check matrix H allows for effective control of the Hamming weight spectrum of the target code. The resulting sparse matrices exponentially reduce the number of multiplication operations required when calculating syndromes in the decoder.

3. The generated hyperelliptic codes have been implemented in two fundamental coding theory architectures: the asymmetric McEliece scheme and the symmetric Rao-Nam scheme. It has been established that the classical asymmetric paradigm with a hard-coded decoder requires $O(k^2)$ operations to solve linear systems relative to the plaintext and leads to an exponential increase in RAM requirements. In contrast, the integration of an algebraic-geometric code into a symmetric channel architecture, utilising a cryptographic pseudorandom number generator to generate an artificial error mask, has made it possible to completely bypass the stage of inverting dense matrices.

4. The operational efficiency of solutions based on instrumental profiling of computational complexity over the field $GF(4)$ has been demonstrated. The use of a symmetric cryptographic code construction is guaranteed to reduce the number of processor cycles by 20–60% for the base dimensions ($n = 7$, $t_e = 1$). The results obtained are objectively limited by the overhead of the Python interpreter (version 3.13, Python Software Foundation, Wilmington, DE, USA) and the constraint on the total degree of spatial monomials. Despite these modelling limitations, mathematical extrapolation demonstrates that the symmetric architecture approaches linear decoding complexity O(n).

Conflict of interest

The authors declare that they have no conflicts of interest regarding this study, including financial, personal, author-

ship or other conflicts that could influence the study and its results as presented in this article.

Funding

The study was conducted without financial support.

Data availability

The manuscript has no associated data.

The use of artificial intelligence

The authors used exclusively the online service SciSpace (scispace.com, as a web-based literature search tool; version not specified) to search for and pre-select potentially relevant scientific sources for the literature review. All suggested references were manually checked by the authors for availability, relevance to the topic and accuracy of bibliographic data, and only verified sources were included in the manuscript. All parts of the manuscript text were written and edited by the authors without the use of generative artificial intelligence tools, and the total amount of AI assistance did not exceed 25% of the research work.

Authors' contributions

Olena Akhiiezer: Conceptualization, Investigation, Writing - original draft, Project administration; **Oleksandr Kushnerov:** Conceptualization, Methodology, Formal analysis, Writing – original draft; **Hanna Nelasa:** Validation, Investigation, Writing – review & editing; **Olha Korol:** Methodology, Investigation, Writing – original draft; **Klym Yamkovyi:** Software, Data curation; **Oleksandr Voitko:** Software, Visualization; **Vladyslav Sokol:** Software, Data curation; **Olena Voloshchuk:** Validation, Resources, Writing – review & editing; **Oleksandr Novoseletskyi:** Resources, Visualization; **Oleh Nelasyi:** Formal analysis, Supervision, Writing – review & editing.

References

1. Yevseiev, S., Rzayev, K., Korol, O., Imanova, Z. (2016). Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (82)), 18. https://doi.org/10.15587/1729-4061.2016.75250
2. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et al. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. https://doi.org/10.15587/1729-4061.2018.150903
3. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. https://doi.org/10.15587/1729-4061.2016.86175
4. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. https://doi.org/10.15587/1729-4061.2017.108461
5. Alimoradi, R. (2016). A Study of Hyperelliptic Curves in Cryptography. International Journal of Computer Network and Information Security, 8 (8), 67–72. https://doi.org/10.5815/ijcnis.2016.08.08
6. Sato, K., Onuki, H., Takagi, T. (2024). Explicit addition formulae on hyperelliptic curves of genus 2 for isogeny-based cryptography. JSIAM Letters, 16, 65–68. https://doi.org/10.14495/jsiaml.16.65
7. Fan, J., Fan, X., Song, N., Wang, L. (2022). Hyperelliptic Covers of Different Degree for Elliptic Curves. Mathematical Problems in Engineering, 2022, 1–11. https://doi.org/10.1155/2022/9833393
8. Furukawa, E., Kawazoe, M., Takahashi, T. (2004). Counting Points for Hyperelliptic Curves of Type y 2=x 5+ax over Finite Prime Fields. Selected Areas in Cryptography, 26–41. https://doi.org/10.1007/978-3-540-24654-1_3
9. Hubrechts, H. (2011). Memory efficient hyperelliptic curve point counting. International Journal of Number Theory, 07 (01), 203–214. https://doi.org/10.1142/s1793042111004034
10. Xiong, M., Zaharescu, A. (2012). Statistics of the Jacobians of hyperelliptic curves over finite fields. Mathematical Research Letters, 19 (2), 255–272. https://doi.org/10.4310/mrl.2012.v19.n2.a1
11. Kurlberg, P., Rudnick, Z. (2009). The fluctuations in the number of points on a hyperelliptic curve over a finite field. Journal of Number Theory, 129 (3), 580–587. https://doi.org/10.1016/j.jnt.2008.09.004
12. Chinis, I. J. (2016). Traces of high powers of the Frobenius class in the moduli space of hyperelliptic curves. Research in Number Theory, 2 (1). https://doi.org/10.1007/s40993-016-0043-9
13. Conceição, R. (2020). On integral points on isotrivial elliptic curves over function fields. Bulletin of the Australian Mathematical Society, 102 (2), 177–185. https://doi.org/10.1017/s0004972720000155
14. Katz, E., Rabinoff, J., Zureick-Brown, D. (2016). Uniform bounds for the number of rational points on curves of small Mordell–Weil rank. Duke Mathematical Journal, 165 (16). https://doi.org/10.1215/00127094-3673558
15. Abbasi, M., Cardoso, F., Váz, P., Silva, J., Martins, P. (2025). A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments. Cryptography, 9 (2), 32. https://doi.org/10.3390/cryptography9020032
16. Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O. et al. (2022). Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies, 2 (9 (116)), 44–59. https://doi.org/10.15587/1729-4061.2022.254545
17. Yevseiev, S., Tsyhanenko, O., Gavrilova, A., Guzhva, V., Milov, O., Moskalenko, V. et al. (2019). Development of Niederreiter hybrid crypto-code structure on flawed codes. Eastern-European Journal of Enterprise Technologies, 1 (9 (97)), 27–38. https://doi.org/10.15587/1729-4061.2019.156620
18. Yevseiev, S., Gavrilova, A., Tomashevsky, B., Samadov, F. (2019). Research of crypto-code designs construction for using in post quantum cryptography. Development Management, 16 (4), 26–39. https://doi.org/10.21511/dm.4(4).2018.03