

УДК 004.421.2

Ya. Yu. Dorogyy, Doctor of Sciences, Professor

I. A. Nazarova, PhD, Associate Professor

N. O. Maslova, PhD, Associate Professor

T. V. Altukhova, PhD, Associate Professor

^{1,2,4}Donetsk National Technical University, Drohobych, Ukraine³Lviv State University of Life Safety, Lviv, Ukraine¹yaroslav.dorohyi@donntu.edu.ua²iryna.nazarova@donntu.edu.ua³masgpp2@gmail.com⁴tetiana.altukhova@donntu.edu.ua

INTEGRATION OF STIFF CHAOTIC MODELS AND NUMERICAL SOLVERS INTO CRYPTOGRAPHIC FRAMEWORKS

This article addresses the actual scientific-technical problem of enhancing the efficiency of chaotic cryptographic frameworks by integrating stiff dynamical systems and their numerical solvers. A chaos-based cryptosystem has been developed and investigated, comprising a mathematical chaotic core, a numerical solver, and a keystream extraction module. Detailed design and analysis were conducted regarding the cryptographic and mathematical properties of chaotic cores based on non-autonomous oscillators: the Van der Pol, the nonlinear Van der Pol–Duffing, and the hybrid Rayleigh–Van der Pol–Duffing oscillators. Specialized solvers were created and tested, including a block k -point predictor-corrector method, a stabilized Skvortsov method, and a semi-implicit Rosenbrock method. Unlike classical explicit and implicit numerical schemes, these methods ensure the accurate numerical reproduction of chaotic dynamics and stability against external perturbations. The computational methods were parallelized, significantly boosting performance and ensuring the cryptosystem's scalability on multiprocessor architectures. It was demonstrated that block multi-point methods exhibit superior parallelism characteristics, featuring near-linear speedup and high scalability. An analysis of the key domain for each crypto-core was performed, covering the assessment of theoretical and effective capacity, the impact of correlation parameters, and stable regions of the phase space. Additionally, the statistical properties of the LSB-based step modification and its suitability for generating cryptographically secure sequences were investigated.

Keywords: cryptographic frameworks, stiff chaotic systems, crypto core, numerical solvers, block-multipoint method, predictor-corrector schemes, key space.

DOI: 10.31474/1996-1588-2026-2-43-97-110

Introduction

At the current stage of information security technology development, traditional cryptographic algorithms are approaching the limits of their computational complexity and efficiency. This forces researchers to seek fundamentally new approaches to solving such problems. One of the most promising areas of development is chaotic cryptography.

Dynamic systems with stiff chaos possess unique properties: sensitivity to initial conditions (the butterfly effect), pseudo-random behavior, and topologically transitive mixing. These characteristics satisfy Shannon's fundamental cryptographic principles, such as diffusion and confusion. Despite their high potential, the practical implementation of chaotic cryptosystems faces significant challenges. The dynamics of hard chaotic systems are described by complex systems of nonlinear differential equations. Their software and hardware implementation in digital

processors inevitably introduces discretization and rounding effects. Finite-precision errors can cause numerical deterioration of chaotic properties, leading to the appearance of short periodic orbits and a subsequent decrease in cryptographic security. Therefore, there is an urgent need to select and adapt modern high-precision numerical methods capable of accurately reproducing chaotic trajectories without losing their inherent entropic properties.

Object of study: the processes of generating pseudorandom sequences and data encryption based on stiff chaotic nonlinear dynamic systems.

Subject of study: modified cryptographic algorithms and numerical methods specialized numerical methods, (Rosenbrock schemes, stabilized Skvortsov integrators, block-parallel predictor-corrector algorithms) ensuring the stability of chaotic characteristics within a finite digital word length.

Purpose of study. The aim of this research is to develop, design and implement a secure

cryptographic algorithm based on complex chaotic systems using optimized numerical methods, ensuring high encryption speed and resistance to known cryptanalytic attacks.

To achieve this goal, this paper addresses the following objectives:

- 1) analysis of existing chaotic systems in terms of their complexity and suitability for cryptographic applications;
- 2) comparative analysis of the impact of various numerical methods on the preservation of chaotic properties during discretization;
- 3) development of a cryptosystem architecture (either a pseudorandom number generator, a stream cipher, or a block cipher);
- 4) evaluation of the cryptographic security of the developed algorithm using NIST statistical test suites and differential analysis.

1. Theoretical Background and Related Work

The use of stiff Cauchy problems in cryptographic algorithms is a specialized interdisciplinary research field that lies at the intersection of chaotic cryptography, dynamical systems theory, and numerical methods. The basic idea is to integrate nonlinear chaotic systems to generate pseudorandom sequences that are sensitive to the underlying information (the set of keys) and resistant to cryptanalysis. Below is a review of the literature and scientific approaches on this topic.

First, the basic works (on dynamic systems, numerical methods, cryptography) are presented, which lay the theoretical foundations for the authors' research. The basic monograph by S. H. Strogatz [1] on nonlinear dynamics contains mathematically rigorous formulations of chaos, bifurcations, Lyapunov exponents, phase portraits, etc. In addition, descriptions of real chaotic dynamic systems are provided. The monograph [2] systematizes the theoretical foundations of using stiff dynamic systems to build robust cryptographic frameworks. This publication demonstrates the practical application of chaotic models in information security. The fundamental work of E. Hairer and G. Wanner [3] serves for the integration of stiff nonlinear models. It contains descriptions of advanced numerical methods and technologies for the efficient modeling of chaotic behavior. The final section of this block presents a fundamental mathematical work that laid the foundations for the analysis of nonlinear systems [4]. It formulates Takens's famous theorem on reconstructing the phase space of a dynamical system from a one-dimensional time series. In the context of cryptography, Takens's work is critically important: it describes methods by which a cryptanalyst can recover a secret key or the structure of a chaotic attractor by intercepting an encrypted data stream.

The next group of articles is devoted to the

basic requirements and problems of digital degradation of chaos [5-7]. This section forms the theoretical basis for research, describing the vulnerabilities of chaotic systems in a digital environment (a finite-bit computer grid) and the requirements for secure encryption. In article [5], the author mathematically proves that standard computational methods destroy the properties of chaos and thus justifies the need to develop specialized numerical solvers. The article [6] examines scrambling algorithms and cryptanalysis methods. The authors propose a combined approach: dynamic scrambling combined with zigzag scanning. The method effectively breaks the strong correlation between adjacent pixels. The scheme is a classic example of the implementation of the diffusion stage. The work [7] is also fundamental, laying out the rules for constructing chaotic cryptosystems. The authors systematized the basic requirements for ciphers: key space size, key sensitivity, high entropy, absence of periodicity, and resistance to known types of cryptanalyses. The article substantiates the need for a transition to complex, multidimensional stiff systems.

Descriptions of modern models of stiff nonlinear chaotic systems in cryptography are provided in many sources [7-11]. Particular attention is given to Van der Pol oscillators and their modifications, as well as multidimensional Lorenz-type problems.

The paper [7] also belongs to this class, as it proposes a modification of the classical Van der Pol oscillator for generating stable chaos. The authors demonstrated a solution to the problem of oscillation damping and the narrowing of chaotic zones in this model. In the next article [8], the authors present a new four-dimensional chaotic system whose stability and dynamics are enhanced by introducing quadratic terms. Based on this system, they designed an encryption algorithm using a two-level mixing method and symmetric bidirectional diffusion. Paper [9] describes a classical Van der Pol oscillator with an additional sinusoidal nonlinearity containing an absolute value function. This modification eliminates hidden periodic parameter windows. Its use makes the system an efficient pseudorandom number generator (PRNG), completely secure against linear cryptanalysis. In article 10, the authors propose a new extended class of hybrid Van der Pol–Duffing systems, adding new nonlinear dynamic factors. This modification makes the system's behavior sensitive not only to the initial coordinates but also to parameter combinations, allowing for a significant expansion of the encryption key space. The following article [11] examines an even more complex modification of the Van der Pol problem. The complex Rayleigh–Van der Pol–Duffing oscillator is introduced and studied. This is one of the stiffest and most chaotic structures. Combining the three models generates multidimensional hyperchaos with multiple positive Lyapunov exponents. The authors demonstrate the

application of this complex system to cryptographic security algorithms.

The following several scientific works [12-17] are devoted to high-precision numerical methods for integrating stiff systems. Since purely explicit/implicit one-step methods were described previously, this section presents studies corresponding to three new approaches to solver design. The first group of methods consists of semi-implicit Rosenbrock schemes, which effectively solve multidimensional stiff problems [12]. They preserve the A - or L -stability of implicit methods but have lower computational complexity.

The next group of methods [13-15] are Skvortsov's stabilized explicit one-step methods with an extended stability domain. In his basic work, Skvortsov laid the foundation for his one-step stabilization theory, described a mathematical algorithm for calculating stability polynomials, and proposed various numerical methods for automatically constructing one-step schemes for given polynomials. The author proposes a mathematical framework for calculating stability polynomials that extends the stability domain of a scheme along the real axis. Skvortsov's paper [14] is crucial for chaotic cryptography because it addresses a hidden problem: the loss of precision and order reduction of numerical methods when faced with stiffness. This study utilizes specialized explicit, stabilized one-step methods designed to preserve theoretical order of precision even in extremely complex dynamic domains. Article [15] describes the design and analysis of highly accurate foreign methods with a dynamically expanding stability domain, as well as their modern stabilized modifications. The next group of methods considered that can be used to solve stiff systems are block or multipoint schemes. Among the many design options, the predictor-corrector computational configuration has the best stability characteristics for use in chaotic cryptography [16-17].

Fundamental requirements for chaos-based cryptosystems are presented and analyzed in [18]. These include sensitivity to initial conditions, key space size, statistical properties, and other. The study applied some of these basic standards to demonstrate the robustness of the resulting systems. The paper [19] presents a set of statistical tests. The publication serves as a foundational source for validating cryptographic random number generators, ensuring that they meet security requirements and are resilient to statistical vulnerabilities. The last group of articles [20-22] is a small part of the authors' work devoted to the development and research of modern numerical methods for solving stiff initial value problems, including for parallel architectures.

Based on the presented materials and conducted research, the following conclusions can be drawn. Constructing an effective cryptographic algorithm and its software equivalent is a complex, multi-step task.

This requires developing and selecting not only a dynamic nonlinear chaotic system, but also an appropriate numerical solver for it.

Clearly, classical multi-stage and multi-point explicit integration methods have a very limited scope of application due to their inability to integrate stiff problems. Implicit one-step Runge-Kutta methods, like implicit block methods, allow solving nonlinear systems of virtually any stiffness. At the same time, they are computationally very complex due to the need to solve systems of nonlinear algebraic equations (SNAE) at each step. Therefore, the main objective of this research will be to develop new and modify existing computational schemes for cryptographic frameworks based on chaotic nonlinear systems of varying stiffness and complexity.

2. General approaches to developing a cryptographic framework

The development of a chaotic crypto architecture consists of several consecutive stages: from the selection of a mathematical core and set of keys to the final generation of the encryption gamma. The encryption process can be generally described as follows. The sender selects the information to be encrypted and a set of secret keys (initial values, core parameters, etc.) to generate chaotic pseudo-random sequences. Then, it performs chaotic scrambling and chaotic XOR encryption on the original information. The encrypted information is transmitted to the recipient via a public channel, and the keys are transmitted via a secret channel for security. On the other side, the recipient recovers the information using the reverse operation of chaotic encryption with the correct keys.

General scheme of the cryptographic algorithm for chaotic cipher is shown in Figure 1. We will provide a more detailed description of each step and the features of its implementation in the developed framework.

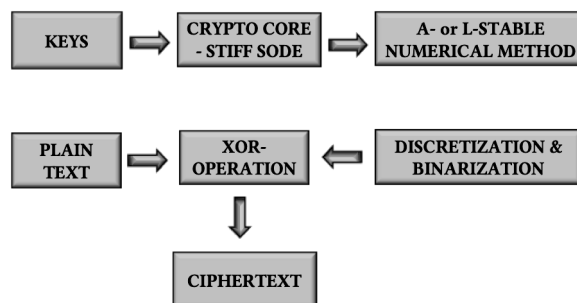


Figure 1 – General scheme of the cryptographic algorithm for chaotic cipher

Step 1: choosing a stiff chaotic core (discussed in detail in section 2). To develop a new stream cipher taking into account dynamic chaos, it is optimal to use stiff Cauchy systems (for example, VdP-modifications,

Lorentz, or Rössler attractors). Their main advantage is the extreme avalanche effect and computational asymmetry: it is easy to encrypt (knowing the key), but practically impossible to break (without knowing the exact initial conditions).

Step 2: key generation. The key space is the secret parameters that the legitimate user knows and the attacker tries to guess. For almost all systems, the starting point is the master key, the main element of secrecy. Changing the initial value even by 10^{-15} due to the butterfly effect (chaos) after a hundred steps will lead to a completely different, uncorrelated gamma. Core parameters are also often used but are considered partial keys. In nonlinear systems, chaos exists only in certain combinations of these parameters. It is possible to allow the user to choose them randomly, but a situation is likely where the system will enter a stable cycle, for example.

Step 3: iterative entropy extraction cycle.

Previously, a numerical solver is selected for a specific stiff crypto core (section 3) and, accordingly, a method for controlling the integration step is chosen (section 4). Next, several steps are performed cyclically. Numerical integration: the system performs a one step or series of integration steps until a data acquisition condition is met (e.g., a step along the period of an external force or a zero crossing). Then, every N steps, a microperturbation is introduced to prevent the digital trajectory from degenerating into periodic cycles. Finally, nonlinear coordinate mixing: the current real variables are multiplied using a nonlinear formula, transforming the physical dynamics of the oscillator into a single value. This stage of cryptographic architecture development in chaotic encryption is the most complex and requires careful consideration. Each dynamic system selected as a crypto core requires not only consideration of its parameters but also the choice of a specific, efficient numerical solution method.

Step 4: gamma generation or discretization of chaos (transformation of a continuous solution of a SODE at a step into binary code). A crypto core is a continuous chaotic system. For use in digital cryptography, it is necessary to perform time discretization, i.e., convert double-precision floating-point numbers (Figure 2) to a bit stream. Continuous chaotic time signal $X_n(t) = (x_{n,1}, x_{n,2}, \dots, x_{n,m})^T$ is discretized and converted into a binary sequence K_n , where m – dimension of the system of equations, n – integration step number.

In the proposed encryption schemes, this step includes several different ways of processing the data obtained at each integration step. First, the non-random part is truncated (skipping bits). The most significant digits of the number (the integer part and the first decimal places after the decimal point) change slowly and predictably, without exhibiting chaotic properties. All randomness is concentrated in the fractional part of the number. Each variable of the solution vector is

processed at a step: it is multiplied by a large coefficient to shift the mantissa, and the integer part is discarded (only the fractional remainder is taken using the *mod 1* operation).

Next, we convert the resulting value into a bit sequence. This can be done by comparing it to a threshold value (the attractor median) or by bit extraction. The computer takes the binary representation of the Float64 number and extracts the last 8 or 16 bits of the mantissa (the least significant digits), which, due to chaos, change completely randomly from step to step.

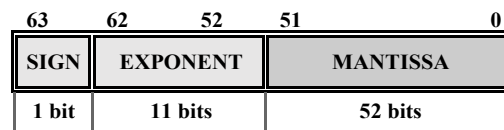


Figure 2 – Format of IEEE 754 double precision floating point number

And the final step is protection against cryptanalysis (post-processing). The direct bit stream from one coordinate may not be completely random, so an XOR operation is applied between the bits obtained from different coordinates of the system:

$$K_n = \bigoplus_{i=1}^m \text{Bit}(x_{n,i}).$$

The resulting bit sequence is a cryptographic gamma function. It is XORed with the secret plain text or file, converting it into ciphertext. Using only one coordinate allows a cryptanalyst to reconstruct the entire spatial structure of the attractor using Takens' theorem [4] and fully predict future bits.

Step 5: gamma overlay (encryption / garming). XOR- operation is performed bitwise on the current block of Plaintext and the resulting portion of the cryptographically secure chaotic gamma. Ciphertext generation: the result of the operation is stored as an encrypted file or data stream. The process is repeated until the entire volume of information is encrypted.

Additionally, the cryptosystem's operating algorithm may include the following stages. For example, a system warm-up phase (transient reset). The chaotic system is run idle for a fixed number of integration steps (e.g., 10^4 iterations of RK4). This is necessary for the trajectory to leave the starting point and enter a complex chaotic attractor. In conclusion, we note that the structure of the cryptographic algorithm and the mechanisms used in it, given the general approach, differ significantly with mathematically different cores and numerical solvers.

3. Modeling of stiff chaotic systems for cryptographic core

This section presents three progressively more complex continuous non-autonomous systems used in the study: the classical Van der Pol (VdP) oscillator,

the hybrid Van der Pol–Duffing (VdPD) system, and the new 9-parameter Rayleigh–Van der Pol–Duffing (RVD) model. The application of modified and hybrid Van der Pol dynamic systems in cryptography and chaotic encryption is a challenging but very popular area of modern research. This paper presents a detailed analysis of the advantages and disadvantages of these systems when used as pseudorandom number generators, mixing algorithms, and chaotic ciphers.

The chaotic core is a fundamental component of modern cryptographic systems, determining their security, pseudo randomness, and resistance to nonlinear attacks. Studying the dynamics of chaotic systems, particularly the analysis of phase portraits and the domains of influence of initial conditions, enables the rational selection of optimal parameters for encryption algorithms. Understanding the limits of deterministic chaos leads to the creation of robust cryptographic mechanisms capable of resisting both statistical analysis and phase space reconstruction methods.

The simplest stiff Van der Pol problem models the behavior of an autonomous oscillator [1-2], and is given by an equation having the following two classical forms:

$$\begin{aligned} \frac{d^2x}{dt^2} - \mu(1 - x^2) \frac{dx}{dt} + x &= 0 \text{ or} \\ \ddot{x} - \mu(1 - x^2)\dot{x} + x &= 0, \end{aligned} \quad (1)$$

where parameter μ , $\mu > 0$ determines the degree of nonlinearity and stiffness.

The classical VdP system is not widely used as the basis for chaotic encryption for several fundamental reasons. Firstly, due to the practical absence of chaos in the autonomous mode. Under these conditions, the Van der Pol oscillator can converge only to fixed points or limiting, strictly periodic cycles. In fact, it is sufficient to intercept a minimal segment of the ciphertext to completely predict all subsequent values. Secondly, the system has too small a phase space dimension and, as a consequence, there are known fairly easy methods for reconstructing the attractor. Finally, the autonomous oscillator has low sensitivity to initial conditions in some phases. The cryptographic core must exhibit an "avalanche effect", meaning that a microscopic change in the key should result in a completely different ciphertext.

In real research in chaotic cryptography, a mathematical model described by a system of non-autonomous Van der Pol oscillators with variable parameters is often used. To transition the system to a state of deterministic chaos, an external periodic force is added, which is usually written using a harmonic function $F(t)$ – sine or cosine:

$$\begin{aligned} \frac{d^2x}{dt^2} - \mu(1 - x^2) \frac{dx}{dt} + x &= F(t), \\ F(t) &= A \cdot \sin(\omega t) \text{ or } F(t) = A \cdot \cos(\omega t), \end{aligned}$$

where A – the amplitude of the external force, ω – angular frequency.

For numerical modeling, the equations are often reduced to a system of two first-order equations:

$$\begin{cases} \frac{dx}{dt} = y \\ \frac{dy}{dt} = \mu(1 - x^2)y - x + A\cos(\omega t) \end{cases}. \quad (2)$$

When constructing cryptographic algorithms (PRNGs or stream ciphers) based on the Van der Pol non-autonomous system, the cosine variant is almost always used: $A \cdot \cos(\omega t)$. The choice of cosine is due to applied reasons and is primarily associated with the exclusion of the degenerate state at $t = 0$ (zero phase step). In cryptography, the initial state of the system ($t = 0$) is entirely specified by the secret key or initialization vector. When using the sine $\sin(\omega t)$ at $t = 0$, the external influence is zero ($\sin(0) = 0$).

At this moment, the first step of the generated pseudo-random sequence depends only on internal system variables and does not take into account the external amplitude parameter A . When using $\cos(\omega t)$, the external influence at the moment $t = 0$ immediately has a maximum amplitude $A \cdot \cos(0) = A$. This ensures that the nonlinear interaction between the internal dynamic chaos and the external forcing signal is instantaneously enabled from the very first byte of the gamma (prevents a weak initial state attack).

In a non-autonomous classical Van der Pol system, chaotic behavior is highly localized. For cryptography, this means the emergence of statistical patterns and temporal predictability. However, for certain values of the parameters $\{\mu, A, \omega\}$, the system's phase trajectory forms a strange attractor, generating a non-periodic and unpredictable signal (Figure 3).

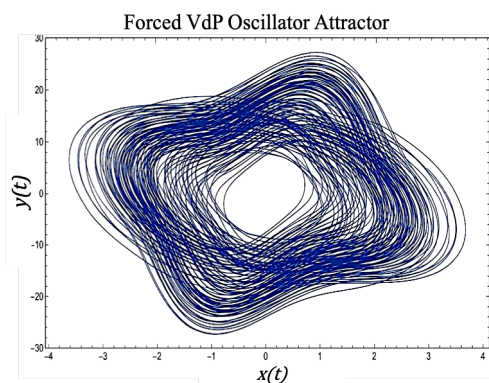


Figure 3 – Forced Van der Pol Oscillator Attractor,
 $\mu = 8.5, A = 17.5, \omega = 1.02$

Thus, the scope of application of such a Van der Pol oscillator is limited to problems requiring the software implementation of chaotic states with a high degree of determinism, but without strict

cryptographic security requirements (lightweight masking systems, analog covert communication).

Note that the classical model has relatively small parameter domains with a positive Lyapunov exponent, which limits the effective key space. In modern cryptosystems, the classical van der Pol oscillator often serves as the base model and is typically supplemented with Duffing and Rayleigh nonlinearities to increase entropy.

The general form of the non-autonomous Van der Pol-Duffing equation is written as a second-order differential equation:

$$\ddot{x} - \mu(1 - x^2)\dot{x} + \alpha x + \beta x^3 = F(t), \quad (3)$$

where $\ddot{x}$ – acceleration, $\mu(1 - x^2)\dot{x}$ – the Van der Pol term (nonlinear damping).

At small amplitudes ($|x| < 1$), the coefficient is negative, the system pumps energy (self-oscillation). At large amplitudes ($|x| > 1$), the coefficient is positive, the system dissipates energy (absorbs oscillations). $F(t)$ is an external harmonic excitation, similar to VdP-model $F(t) = A \cdot \cos(\omega t)$ or $A \cdot \sin(\omega t)$. Duffing term, nonlinear cubic stiffness, $\alpha x + \beta x^3$ – restoring force: αx is linear elasticity (as in an ordinary pendulum) and βx^3 is a cubic nonlinearity ($\beta > 0$ is a stiff spring, $\beta < 0$ is a soft spring).

Although the classical form of the van der Pol oscillator does not exhibit fully chaotic dynamics, its modifications do lead to chaos. The most famous example is the Van der Pol–Duffing oscillator, which adds cubic nonlinearity and an external periodic forcing to the equation. In such a system, bifurcations, transitions to chaos through period doubling, strange attractors and intermittency regimes are possible. This makes the model universal for studying nonlinear processes in chaotic cryptography.

The non-autonomous VdPD model is a fully-fledged chaotic system with two wells. The nonlinear Van der Pol term prevents trajectory decay, and the cubic Duffing part generates complex two-center chaos. This combination of models is practically the standard for constructing chaotic ciphers.

The hybrid Rayleigh – Van der Pol – Duffing (RVD) model combines three key mechanisms of nonlinear dynamics:

- 1) Rayleigh damping: nonlinear friction dependent on the velocity $\dot{x}$;
- 2) Van der Pol damping: nonlinear friction dependent on the x -coordinate;
- 3) Duffing nonlinearity: cubic stiffness determining the potential profile of the system.

The classical general RVD equation of motion, taking into account the external periodic forcing $F(t) = A \cdot \cos \omega t$, has the form:

$$\ddot{x} - \underbrace{\mu_1(1 - \gamma_1 x^2)\dot{x}}_{\text{VdP therm}} + \underbrace{\mu_2 \left(1 - \frac{1}{3}\gamma_2 \dot{x}^2\right)\dot{x}}_{\text{Rayleigh therm}} + \alpha x + \beta x^3 = A \cdot \cos \omega t. \quad (4)$$

$$+ \underbrace{\alpha x + \beta x^3}_{\text{Duffing therm}} = A \cdot \cos \omega t.$$

For modeling and cryptographic applications, the system is reduced to phase variables:

$$\frac{dx}{dt} = y,$$

$$\frac{dy}{dt} = \left[\mu_1(1 - \gamma_1 x^2) + \mu_2 \left(1 - \frac{1}{3}\gamma_2 y^2\right) \right] y - \alpha x - \beta x^3 + A \cos \omega t. \quad (5)$$

Due to the combination of two self-oscillating mechanisms and cubic nonlinearity, the RVD system exhibits complex hyperchaotic behavior. The large key space (at least nine parameters) is continuous and multidimensional, making brute-force key search virtually impossible.

The RVD model has many other advantages, but is also the most difficult to integrate numerically. It is used to create transmitter-receiver circuits for secure communications and for digital image encryption. Comparison of the phase portraits and main parameters (Table 1) demonstrates how the increasing complexity of the systems changes the geometric structure of the attractors and critical cryptographic properties. The key difference of the RVD-model for cryptography is the phase space filling. A secure stream cipher requires that the generated gamma be free of statistical regularities.

In the RVD model, the combination of nonlinear friction from velocity (Rayleigh) and coordinates (Van der Pol) completely destroys the regularity of the trajectory, transforming the phase portrait into a dense "pseudo-random grid" resistant to attacks using the phase space reconstruction method (Takens' Embedding Theorem) [1].

Departing from the single standard constant of $1/3$ obviously expands the secret key vector. This allows for finer control of the Lyapunov exponent and the creation of domains with even higher chaotic complexity. Chaotic cryptographic algorithms most often employ the hybrid RVD model with a polynomial generalization.

The use of a hybrid Rayleigh system is effective in specialized generators, such as those for multimedia protection. Clearly, the RVD model is the most effective of those considered.

The proposed models, VdP, VdPD, and RVD, exhibit fundamentally different forms of chaos. The key criterion here is the presence of topological mixing or strong chaos. For VdP-type systems, mixing ensures a key requirement of cryptography – the avalanche effect (diffusion). Changing just one bit in the plaintext completely alters the trajectory within a few steps. As a result, the ciphertext will be radically altered and cannot be recovered, since chaos has mixed up all the original data.

Table 1 – Comparison of three stiff chaotic models based on the Van der Pol system

MODEL and SET OF PARAMETERS	PHASE PORTRAIT	CRYPTOGRAPHIC PROPERTIES
Non-autonomous Van der Pol: $\{\mu, A, \omega, x(0), y(0)\}$	Single limit cycle, slightly blurred by chaotic oscillations under the external force.	Weak for cryptography. Limited region of phase space; low entropy; trajectories are easily predicted by phase reconstruction.
Van der Pol – Duffing: $\{\mu, \alpha, \beta, A, \omega, x(0), y(0)\}$	Double-scroll strange attractor with a classic "effect butterfly."	Moderate security. Jumps between two potential wells provide good pseudo randomness, but the attractor structure has clear geometric boundaries.
Rayleigh – Van der Pol – Duffing: $\{\mu_1, \mu_2, \gamma_1, \gamma_2, \alpha, \beta, A, \omega, x(0), y(0)\}$	Dense, hyperchaotic trajectory uniformly filling large regions of phase space.	High security. Maximum entropy, absence of pronounced geometries ("holes"), highest sensitivity to keys.

The non-autonomous Van der Pol system exhibits weak chaos. The system has only one center (one potential well). An external force somewhat distorts the stability of change. Topological mixing is either completely absent or extremely weakly expressed within very narrow parameter ranges.

The Van der Pol-Duffing model exhibits chaos with mixing. The presence of cubic elasticity transforms the system into a double-well. A full-fledged strange attractor emerges. The trajectory constantly flies from one well to the other, twisting along a complex spiral. This gives rise to a global stretching/folding of the phase space (avalanche effect) – classical topological mixing.

The RVD hybrid model exhibits developed chaos with extremely strong mixing. The combination of the nonlinear damping of Van der Pol and Rayleigh with the elasticity of Duffing creates a complex dynamic. Under certain parameters, this system exhibits not one, but several positive Lyapunov exponents (hyperchaos). The phase space mixes at maximum speed, making the system even more unpredictable than the modernized van der Pol-Duffing model.

4 Development and performance study of numerical solvers for cryptographic frameworks

The use of the stiff chaotic crypto core based on the Van der Pol oscillator developed in Section 2 requires the development of new robust computational frameworks. The choice of the underlying numerical integration method determines not only the encryption throughput, but also the cryptosystem's resistance to cryptanalysis. This section presents studies of the feasibility and effectiveness of various modern classes of adaptive numerical solvers.

The developed numerical algorithms represent fundamentally different computational approaches:

1) classical explicit and implicit integration based on embedded forms;

2) semi-implicit L -stable Rosenbrock's methods;

3) improved explicit integration with extended stability regions;

4) parallel block multipoint methods.

For stiff nonlinear oscillators such as Van der Pol, Rayleigh, and Duffing, the choice of numerical integration method is critical. These systems often fall into the category of stiff differential equations (ODEs), where standard explicit methods (such as the classical RK4) either require a sufficiently small integration step or lead to numerical instability. Implicit methods are specially developed for stiff systems and have the property of A -stability (for example, Radau IIA). This approach is well suited for cryptographic purposes but obviously has high computational complexity due to the stage system solution.

Rosenbrock's methods belong to the class of semi-implicit Runge–Kutta methods. Their fundamental advantage over implicit methods is that they do not require iteratively solving systems of nonlinear algebraic equations. Instead, stiffness is handled by explicitly embedding the Jacobian matrix into the stage system, reducing the problem to solving linear systems (SLAEs) at each step.

A rigorous mathematical description of the Rosenbrock method with accuracy of order $O(h^p)$ is presented below. The internal stage vectors $k_j, j = \overline{1, s}$ are resolved sequentially by solving a sequence of SLAE rather than executing non-linear Newton loops. The general formulation for the j -th stage is defined as:

$$(I - \gamma h \cdot J(X_n)) \cdot k_j = F \left(X_n + h \sum_{i=1}^{j-1} \alpha_{ji} k_i \right) + h \cdot J(X_n) \cdot \sum_{i=1}^{j-1} \beta_{ji} k_i, \quad (6)$$

where I is the identity matrix, γ is a fixed real stability parameter, and α_{ji}, β_{ji} are the structural design coefficients of the method. Upon resolving all s

sequential linear stages, the final forward state vector X_{n+1} is evaluated via a weighted linear quadrature:

$$X_{n+1} = X_n + \sum_{j=1}^s b_j k_j, \quad (7)$$

where b_j represent the integration weights of the solver. To achieve fourth-order global accuracy $O(h^4)$ and ensure L -stability under the stringent constraints imposed by the eigenvalues, a minimum of $s = 4$ stages is required. The numerical experiments employed one of the most computationally efficient and widely used 4-order/4-stage Rosenbrock schemes [12].

In formula (6), the left-hand side contains the same matrix for all four stages. This means that for each step h , the LU -decomposition of this matrix only needs to be performed once, followed by four back-substitutions. In classical applications, this is an advantage, but in cryptography, computing determinants and inverses of matrices in real time significantly reduces encryption throughput.

The next class of integration methods with stability characteristics suitable for solving stiff problems are explicit stabilized methods. These include specially designed explicit methods whose coefficients are calculated using Chebyshev polynomials [13-15]. On the other hand, they are called Skvortsov methods with extended stability regions (stability region is infinitely extended along the negative real axis). The length of the stability interval increases proportionally to the square of the number of stages in the method, s^2 . This allows for the efficient solution of stiff systems with a real spectrum.

A general s -stage explicit stabilized solver based on the Skvortsov method is described by the following mathematical recurrence formula:

$$g_1 = X_n,$$

$$g_j = X_n + h \sum_{i=1}^{j-1} a_{ji} F(g_i), j = 2, 3, \dots, s. \quad (8)$$

After calculating all the stage coefficients, the solution vector is determined using a weighted linear combination of the derivatives:

$$X_{n+1} = X_n + h \sum_{j=1}^s b_j F(g_j), \quad (9)$$

where b_j denote the final integration quadrature weights.

To guarantee a strict $O(h^4)$ global accuracy while maximizing the real stability interval up to $Re(z) \sim -18$, the Butcher coefficient matrices (a_{ji}, c_j, b_j) are analytically derived from the roots of the 4th-degree stabilization polynomial. The exact numerical parameters for the 5-stage cryptographically secure Skvortsov algorithm are given in [13-14].

Comparative estimates of the stability convergence and computational complexity of the proposed methods allow us to identify areas of their priority use for crypto cores of varying degrees of stiffness.

A distinctive feature of this research is the development of cryptographic algorithms based on parallel integration methods. Moreover, we are not talking about parallelization of traditional numerical solvers used in cryptography. The approach used is based on methods with an inherently parallel structure, namely block or multipoint methods [16-17]. It should be noted that these methods not only accelerate computations, but also increase encryption throughput.

The basic idea behind block methods is as follows: in a single step of integrating the initial problem, not one but k new values of the desired functions are calculated. Thus, the entire integration grid is divided into N_{bl} blocks, each of which contains k points (Figure 4).

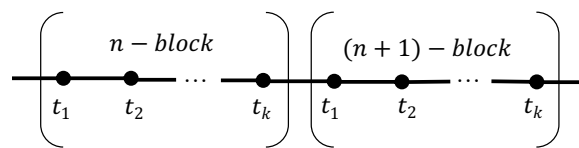


Figure 4 – Integration grid structure for the block k -point method

Parallel block methods, like sequential integration schemes, are divided into multi-step and one-step, explicit and implicit. Multi-step block methods do not meet cryptographic requirements, purely explicit methods do not solve stiff problems. Some of the previous works of the authors [20-23] are devoted to implicit block one-step methods and their implementation. These methods, due to their stability characteristics, can be applied to stiff core, but have high computational complexity (solving the SNAE at each step). Next, we will consider explicit one-step block methods of the predictor-corrector (PC) type and show that they are best suited for cryptographic solvers.

The basic matrix form of a k -point explicit block predictor-corrector method:

1) explicit one-step predictor:

$$X_{n+1}^{[0]} = eX_n + h d F_n,$$

where $e = (1, 1, \dots, 1)^T$ is a unit column vector of dimension k , $d = (d_1, d_2, \dots, d_k)^T$ is the common vector of predictor coefficients, in the simplest case of a uniform grid: $d = (1, 2, \dots, k)^T$, $X_{n+1}^{[0]} = (X_{n+1}^{[0]}, X_{n+2}^{[0]}, \dots, X_{n+k}^{[0]})^T$;

2) block parallel corrector, iterative correction process (Picard iteration) at step $(l + 1)$:

$$X_{n+1}^{[l+1]} = eX_n + h d F_n + h A F(X_{n+1}^{[l]}),$$

$$\begin{pmatrix} X_{n+1} \\ X_{n+2} \\ \vdots \\ X_{n+k} \end{pmatrix}^{[l+1]} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} F_n + h \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_k \end{pmatrix} F_n +$$

$$+h \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} \end{pmatrix} \begin{pmatrix} F_{n+1} \\ F_{n+2} \\ \vdots \\ F_{n+k} \end{pmatrix}^{[l]}.$$

A – the main square matrix of corrector coefficients of size $k \times k$. Since the method is a single-step, implicit method within the block, matrix A is dense (not triangular).

The proposed k -point parallel block method with a predictor-corrector structure is classified as explicit. Traditionally, in numerical analysis, almost all explicit schemes are unable to solve stiff problems because they have a limited stability region. However, the developed parallel algorithm based on the PC scheme has demonstrated effectiveness in integrating chaotic cryptographic core, including the 9-parameter Rayleigh-van der Pol-Duffing system.

This study used a $2 \div 8$ -point predictor-corrector block method. As an example, we will provide calculation schemes and specific numerical coefficients of the 4-point block method of the predictor-corrector type:

$$X_{n+i}^{[0]} = X_n + ihF_n, i = \overline{1,4},$$

$$F_{n+i}^{[0]} = F(X_{n+i}^{[0]}), i = \overline{1,4},$$

$$X_{n+1}^{(l+1)} = X_n + \frac{h}{24} (9F_n + 19F_{n+1}^{[l]} - 5F_{n+2}^{[l]} + F_{n+3}^{[l]}),$$

$$X_{n+2}^{(l+1)} = X_n + \frac{h}{3} (F_n + 4F_{n+1}^{[l]} + F_{n+2}^{[l]}),$$

$$X_{n+3}^{(l+1)} = X_n + \frac{3h}{8} (F_n + 3F_{n+1}^{[l]} + 3F_{n+2}^{[l]} + F_{n+3}^{[l]}),$$

$$X_{n+4}^{(l+1)} = X_n + \frac{2h}{3} (F_n + 4F_{n+2}^{[l]} + F_{n+4}^{[l]}).$$

The calculation algorithm for the described computational scheme consists of the following steps. Using explicit formulas, a rough initial approximation of the solution is calculated at all points in the block. The resulting solution vector is substituted into the right-hand side of the Van der Pol or RVD system to calculate intermediate derivatives. Based on the calculated derivatives, the implicit corrector matrix recalculates the solution vector, producing a refined approximation. The new refined solution is again substituted into the equations to update the derivative vectors: A final, second pass of the implicit corrector matrix is performed. The output is the final solution for the current step, which is declared the base point for the next block. Thus, for each 4-point block, one prediction and exactly two consecutive corrections are performed.

Each iteration of the block corrector expands the region of absolute stability of the method. Typically, two iterations are sufficient for the block method to be stable when integrating a stiff oscillator. During the solution process, the convergence condition

is not checked (as in Newton's method), and exactly two iterations are performed on both smooth and stiff regions of the attractor. The computational complexity and time required for the cryptographic core remain constant throughout the entire encryption process.

To compare the numerical solvers described, the following computational experiments were conducted in addition to theoretical analyses. For three fourth-order methods applied to a hybrid RVD oscillator model, the encryption time (in seconds) was recorded relative to the volume of encoded information (Figure 5).

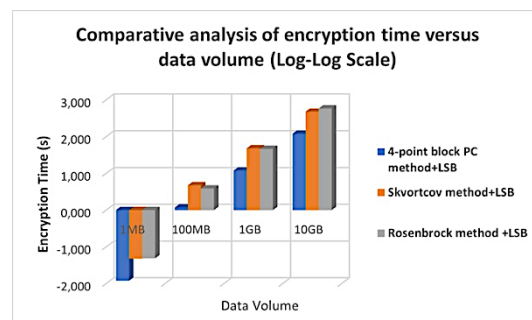


Figure 5 – Comparative analysis 3 numerical solvers: block 4-point predictor-corrector methods, stabilized explicit Skvortsov method and semi-implicit Rosenbrock method $O(h^4)$

Regardless of data size, the developed block method requires less time than the Skvortsov-Rosenbrock method, demonstrating the method's linear scalability.

The Rosenbrock method exhibits an anomalous timing spike: for small data volumes (1 MB, 100 MB), it operates faster than the Skvortsov method because its adaptive step size allows it to proceed using a coarser grid. However, with 1 GB and 10 GB datasets, the encryption time increases sharply and non-linearly. This clearly indicates non-linear delays associated with Jacobian calculations and Newton iterations, thereby creating a timing side-channel that could be exploited to compromise the key.

In parallel, results from key tests within the NIST STS suite [19] are presented for each experimental point (Table 2). These data make it possible to trace the relationship between the computational scheme, its execution time, and cryptographic strength.

With data volumes of 10 GB, the Rosenbrock method completely fails NIST tests ($P_{value} \rightarrow 0$). This is due to the property of strong numerical L -stability. Over extremely long-time intervals, the Rosenbrock method transforms the cryptographic stream into a deterministic sequence that is rejected by NIST tests ($P_{value} < T, T = 0.01$). The Skvortsov and block methods with LSB -modification maintain high, uniform P_{value} levels (approximately 0.6–0.7), demonstrating an infinite pseudo randomness period.

Table 2 – Basic NIST SP 800 22 Statistical Testing Results on RVD-core

Data Volume	NIST Test	4-Point Block PC method	Skvortsov method (Stabilized Explicit)	Rosenbrock Method (Semi-Implicit)
1 MB	Block Frequency	Pass (0.6421)	Pass (0.5891)	Pass (0.4102)
	Serial Test	Pass (0.7104)	Pass (0.6122)	Pass (0.4915)
	Runs Test	Pass (0.5519)	Pass (0.5224)	Pass (0.3984)
100 MB	Block Frequency	Pass (0.6811)	Pass (0.5914)	Pass (0.4251)
	Serial Test	Pass (0.6933)	Pass (0.6341)	Pass (0.4119)
	Runs Test	Pass (0.5822)	Pass (0.5401)	Pass (0.3542)
1 GB	Block Frequency	Pass (0.7024)	Pass (0.6115)	Pass (0.3104)
	Serial Test	Pass (0.7241)	Pass (0.6482)	Pass (0.2981)
	Runs Test	Pass (0.6105)	Pass (0.5593)	Pass (0.3015)
10 GB	Block Frequency	Pass (0.7185)	Pass (0.6234)	Fail (0.0000)
	Serial Test	Pass (0.7310)	Pass (0.6512)	Fail (0.0000)
	Runs Test	Pass (0.6244)	Pass (0.5711)	Fail (0.0002)

5. LSB-modification

All methods used in this study are adaptive. In the classical, generally accepted case, this means a built-in mechanism for controlling the integration step, the so-called PI-regulation [3, 20-21]. The formula for calculating the new step in this case is as follows:

$$h_{n+1} = h_n \min(fac_{max}, \delta),$$

$$\delta = \max \left(fac_{min}, fac \cdot \sqrt[r+1]{\frac{tol}{\varepsilon_n}} \right),$$

where fac , fac_{max} , fac_{min} – guaranteeing multipliers, r – order of the method, ε_n – current local error. Mathematically, this approach is effective for arbitrary stiff systems and solvers. However, when simulation systems selected as the crypto core, it is completely unsuitable for such critical reasons. First, PI-regulation makes the cryptosystem completely vulnerable to timing attacks. The described approach continuously adapts the step size, smoothing its changes over the error history $(\varepsilon_n, \varepsilon_{n-1})$. The processor's time spent simulating a single time interval becomes a complex continuous function of the chaotic attractor trajectory. An attacker, having intercepted the data packet encryption timing graph, can use reverse engineering techniques to reverse engineer the trajectories. Secondly, due to the complex step control logic ($\min, \max$ operations, raising to a fractional power), the crypto core loses encryption speed.

Third, PI control leads to dynamic degeneration of final states, since its goal is error minimization, not entropy generation. On a finite computer grid (double

precision, IEEE 754), the adaptive step, while following deterministic formulas, still has finite memory. After a finite number of steps, rounding errors cause the system to enter a periodic cycle, and the cryptographic pseudorandom number generator begins producing identical bytes. On the other hand, simulating chaotic systems with a fixed step size also fails to solve the fundamental problem of digital chaos: attractor degradation and cycling. Due to the finite precision of data representation, the trajectory eventually reaches a point it has previously visited. At that moment, the PRNG begins to endlessly repeat the same sequence (cycle). To control the integration step in cryptosystems, the following simple and effective dynamic loop destructor is used in the work:

$$h_n = h_0 + \Delta \cdot LSB(x_n),$$

where LSB – least significant bit.

In practice, at each step the algorithm takes the least significant bit of the current coordinate $LSB(x_n)$, which takes the value either 0 or 1. The integration step h_n becomes dynamic: it is either equal to the basic step h_0 or increases slightly by a microscopic amount $h_n + \Delta$. This microscopic step change completely destroys the fixed discrete time grid. As a result, computer rounding can never trap the system in a period trap. The generator acquires a large (practically infinite) repetition period, which is critical for cryptographic security. The method using LSB does not determine the system's stiffness zone, since the computational complexity of the step h_0 and $h_0 + \Delta$ for the processor is exactly the same, preserving resistance to timing attacks. Thus, the stochastic least

significant bit (LSB) integration step control method offers several advantages over standard adaptive step controllers.

6. Determination and analysis of the key space size

The main criterion for determining a cryptosystem's resistance to brute-force attacks is the key space and its dimension [18]. For chaotic cryptosystems based on the Van der Pol oscillator, the key consists of three parts: the parameters of the chaotic core, the initial values, and the parameters of the numerical method. Strictly mathematically, the key space can be described using a Cartesian: $K = K_{core} \times K_{IV} \times K_{solver}$. The size of the key space is understood as the total number of all possible unique combinations each part of key and is defined as:

$$Key_Space = |K| = |K_{core}| \cdot |K_{IV}| \cdot |K_{solver}|.$$

In cryptography, this characteristic is measured in binary form: $|K| = 2^k$, where k is the equivalent key length in bits ($k = \log_2(Key_Space)$). General calculation formula: if a key K consists of n independent parameters $K = \{p_1, p_2, \dots, p_n\}$, then: $|K| = \prod_{i=1}^n k_i$, $k_i = |p_i|$, the key length in bits k is calculated using the binary logarithm:

$$k = \log_2(Key_Space) = \sum_{i=1}^n \log_2 k_i.$$

According to modern cryptographic standards [19] established by the National Institute of Standards and Technology (NIST USA), the theoretical upper bound on the size of the key space should be $> 2^{128}$. Next, this constraint is verified for continuous chaotic systems (such as VdP, VdPD, and RVD oscillators), chosen as cores in the developed cryptographic algorithms. The key space is limited by the initial values and parameters of the systems, which are, by definition, real floating-point numbers. The calculation procedure includes three main steps. Firstly, determining the representation accuracy Δ . On a digital computer, a floating-point number is represented with a certain precision. If the IEEE 754 Double Precision standard (64 bits) is used, the mantissa contains 52 bits (Figure 2). With a precision of $\Delta = 10^{-14}$, each unit interval of the parameter $[0,1]$ contains $k_i = 1/\Delta = 10^{14}$ discrete values. Secondly, the chaotic behavior of the system is generally bounded. Key parameters vary only within specific intervals $[p_{min}, p_{max}]$ rather than ranging from negative to positive infinity. Therefore, the number of permissible values for a single parameter is calculated as follows: $k_i = (p_{i,max} - p_{i,min})/\Delta_i$. The third step is the actual calculation of the key space size for the selected crypto core. The value 10^{-14} corresponds exactly 47 bits in a discrete representation: $k_i = \log_2(10^{14}) = 46.51 \approx 47$ bits. Thus, choosing a precision of 10^{-14} allows us

to produce the maximum possible entropy from the IEEE 754 Double Precision standard, but at the same time not to cross the boundary beyond which chaotic processor rounding errors begin during numerical calculations. First, define the key space size for the Van der Pol oscillator. The key vector for VdP includes next parameters: initial conditions (x_0, y_0) and system parameters (μ, A, ω) . Key vector: $K_{VdP} = \{x_0, y_0, \mu_{vdp}, A, \omega\}$, number of parameters $n = 5$.

Key space size:

$$k_{VdP} = \log_2(10^{14})^5 = \log_2(10^{70}) \approx 232 \Rightarrow$$

$$Key_Space (VdP) \approx 2^{232}.$$

For the following model, the Van der Pol – Duffing oscillator, the cubic nonlinearity parameters of the potential (α, β) are summed, defining a double-well structure. Key vector: $K_{VdPD} = \{x_0, y_0, \mu, \alpha, \beta, A, \omega\}$, number of parameters $n = 7$. Key space size: $k_{VdPD} = \log_2(10^{98}) = 98 \cdot \log_2 10 \approx 325$ bits: $Key_Space (VdPD) \approx 2^{325}$.

The third model, the hybrid RVD (oscillator, adds the Rayleigh parameter (μ_R) and the nonlinearity coefficient (γ) . Key vector: $K_{RVD} = \{x_0, y_0, \mu_{vdp}, \mu_R, \alpha, \beta, \gamma, A, \omega\}$, number of parameters $n = 9$. $k_{RVD} = (10^{14})^9 = 10^{126}$. Key space size: $k_{RVD} = \log_2(10^{126}) = 126 \cdot \log_2 10 \approx 418$ bits:

$$Key_Space (RVD) \approx 2^{418}.$$

Note, due to existence of correlated parameters and stable regions in the phase portrait, the actual key space is approximately 60-70% of the theoretical estimate. For example, for RVD, this yields a value of $2^{260} - 2^{290}$ bits, exceeding the cryptographic strength requirements.

Conclusion

The research presented in the article describes the solution to a complex multidisciplinary problem situated at the intersection of cryptographic theory, the theory of dynamical systems, and modern numerical methods. Overall, the research results demonstrate that a cryptosystem based on hybrid nonlinear Van der Pol models forms a scalable, mathematically sound, and computationally efficient structure. It combines chaotic dynamics, adaptive numerical methods, and parallel execution into a coherent design capable of supporting modern cryptographic requirements.

As a result of the research conducted, the following scientific results were obtained:

- 1) generalized cryptosystem based on chaotic nonlinear models has been developed, incorporating parameter-controlled modifications of Van der Pol, Duffing, and Rayleigh oscillators;
- 2) specialized numerical methods for chaotic cryptosystems have been proposed, including Rosenbrock schemes, a stabilized Skvortsov method, and block predictor-corrector algorithms, ensuring

stable integration under conditions of stiffness;

3) an expanded key domain for the cryptosystem has been proposed, encompassing parameters of the chaotic core, the numerical method, and the sampling and quantization schemes, thereby significantly increasing the effective size of the key space;

4) formulas for nonlinear mixing in LSB-extraction have been derived and validated, ensuring the suppression of correlations and an increase in the entropy of the output bitstream.

Further research will focus on several key areas. First, it is planned to increase the complexity of the crypto core models under consideration by incorporating the chaotic dynamics of systems of coupled nonautonomous van der Pol oscillators. Furthermore, more complex nonlinear multivariate

systems will be integrated as chaotic cores into cryptographic algorithms. Preliminary mathematical analysis of the Lorenz, Rössler, Chua, and Dmitriev–Kislov systems has been conducted.

Use of Artificial Intelligence and AI-based Technologies

During the preparation of the manuscript, the artificial intelligence tool Gemini was used for grammar and stylistic checks, as well as for the rapid structuring of raw data. AI was not involved in the interpretation of scientific data, the formulation of conclusions, or the development of the study's theoretical framework. The authors bear full responsibility for the final text of the article, the results obtained, and their scientific interpretation.

Bibliography

1. Strogatz S. H. *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. 3rd ed. New York: Chapman and Hall/CRC, 2024. 616 p. DOI: <https://doi.org/10.1201/9780429398490>.
2. *Chaos-Based Cryptography: Theory, Algorithms and Applications* / ed. by L. Kocarev, S. Lian. Berlin; Heidelberg: Springer, 2011. 398 p. DOI: <https://doi.org/10.1007/978-3-642-20542-2>.
3. Hairer E., Wanner G. *Solving Ordinary Differential Equations II: Stiff and Differential-Algebraic Problems*. 2nd ed. Berlin: Springer-Verlag, 1996. 614 p. DOI: <https://doi.org/10.1007/978-3-642-05221-7>.
4. Takens F. Detecting Strange Attractors in Turbulence. *Dynamical Systems and Turbulence, Warwick 1980: Proceedings of a Symposium held at the University of Warwick 1979/80* / eds. D. A. Rand, L.-S. Young. Berlin: Springer, 1981. (Lecture Notes in Mathematics; Vol. 898). P. 366–381. DOI: <https://doi.org/10.1007/BFb0091924>.
5. Lozi R. Can We Trust Numerical Simulations of Chaotic Systems for Cryptographic Applications? *Discontinuity, Nonlinearity, and Complexity*. 2013. Vol. 2, No. 3. P. 293–302. DOI: <https://doi.org/10.1142/S225118571350022X>.
6. Wang X., Chen X. An Image Encryption Algorithm Based on Dynamic Row Scrambling and Zigzag Transformation. *Chaos, Solitons & Fractals*. 2021. Vol. 147. Art. 110962. DOI: <https://doi.org/10.1016/j.chaos.2021.110962>.
7. He J., Cai J. Design of a New Chaotic System Based on Van Der Pol Oscillator and Its Encryption Application. *Mathematics*. 2019. Vol. 7, No. 8. Art. 743. DOI: <https://doi.org/10.3390/math7080743>.
8. Gao P., Lu T., Dong J. Color Image Encryption Based on a Square-Term Enhanced 4D Chaotic System. *Electronic Research Archive*. 2026. Vol. 34, No. 7. P. 4577–4610. DOI: <https://doi.org/10.3934/era.2026202>.
9. Sambas A. et al. Exploring Chaotic Dynamics with Absolute-Embedded Sinusoidal Nonlinearity in a Sinusoidal-Enhanced Van der Pol Oscillator. *Mathematical Modeling and Computing*. 2025. Vol. 12, No. 1. P. 109–121. DOI: <https://doi.org/10.23939/mmc2025.01.109>.
10. Kyurkchiev N., Zaeviski T., Vasileva M., Kyurkchiev V., Iliev A., Rahnev A. Dynamics of a Class of Extended Duffing–Van Der Pol Oscillators: Melnikov's Approach, Simulations, Control over Oscillations. *Mathematics*. 2025. Vol. 13, No. 14. Art. 2240. DOI: <https://doi.org/10.3390/math13142240>.
11. Al Themairi A., Mahmoud G. M., Farghaly A. A., Abed-Elhameed T. M. Complex Rayleigh–Van-der-Pol–Duffing Oscillators: Dynamics, Phase, Antiphase Synchronization, and Image Encryption. *Fractal and Fractional*. 2023. Vol. 7, No. 12. Art. 886. DOI: <https://doi.org/10.3390/fractalfract7120886>.
12. Sadek L., Aldawish I. The Symmetry Preserving Rosenbrock Approach: Application to Solve the Chaotic Lorenz System. *Symmetry*. 2025. Vol. 17, No. 11. Art. 1844. DOI: <https://doi.org/10.3390/sym17111844>.
13. Skvortsov L. M. Explicit Stabilized Runge-Kutta Methods. *Computational Mathematics and Mathematical Physics*. 2011. Vol. 51, No. 7. P. 1153–1166. DOI: <https://doi.org/10.1134/S0965542511070165>.
14. Skvortsov L. M. How to Avoid Accuracy and Order Reduction in Runge-Kutta Methods as Applied to Stiff Problems. *Computational Mathematics and Mathematical Physics*. 2017. Vol. 57, No. 7. P. 1126–1141. DOI: <https://doi.org/10.1134/S0965542517070119>.
15. Abdulle A. Fourth-Order Chebyshev-Runge-Kutta Methods. *SIAM Journal on Scientific Computing*. 2002. Vol. 23, No. 6. P. 2041–2054. DOI: <https://doi.org/10.1137/S106482750037619X>.

16. Nwaigwe C., Atangana A. Fourth-Order Predictor-Corrector Method for Initial Value Ordinary Differential Equation Problems. *Numerical Algorithms*. 2025. Vol. 101, No. 2. P. 1303–1336. DOI: <https://doi.org/10.1007/s11075-025-02043-7>.
17. Wang X., He W., Feng H., Atluri S. N. Fast and Accurate Predictor-Corrector Methods Using Feedback-Accelerated Picard Iteration for Strongly Nonlinear Problems. *Computer Modeling in Engineering & Sciences*. 2024. Vol. 138, No. 3. P. 2897–2918. DOI: <https://doi.org/10.32604/cmes.2024.049975>.
18. Alvarez G., Li S. J. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *International Journal of Bifurcation and Chaos*. 2006. Vol. 16, No. 8. P. 2129–2151. DOI: <https://doi.org/10.1142/S0218127406015970>.
19. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert N., Dray J., Vo S., Bassham L. E. NIST Special Publication 800-22 rev. 1a: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Gaithersburg, MD: National Institute of Standards and Technology, 2010. 131 p. DOI: <https://doi.org/10.6028/NIST.SP.800-22r1a>.
20. Nazarova I.A., Altukhova T.V., Kunda M.S. Efficiency Analysis of Parallel Implementations of One-Step Embedded Methods for Solving Large-Scale Cauchy Problems with Adaptive Step Size. *Scientific Works of Donetsk National Technical University. Series: Informatics, Cybernetics and Computer Engineering*. 2026. № 1 (42). C. 5–18. DOI: <https://doi.org/10.31474/1996-1588-2026-1-42-5-18>.
21. Nazarova I., Popova A. Numerical Modeling of Multidimensional Cauchy Problems with Adaptive Step Size. *Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference*. Drohobych: DonNTU, 2025. P. 165–170. DOI: <https://doi.org/10.5281/zenodo.15775240>.
22. Nazarova I., Dorohyi I., Altukhova T., Kunda M. Efficient Parallel Hybrid DIRK Solvers for Stiff Complex Critical Infrastructure Models. *CEUR Workshop Proceedings (Proceedings of the International Scientific and Practical Workshop "Resilient Systems: Secure Digital Technologies and Critical Infrastructure 2026" (RS-2026), Drohobych, Ukraine, June 30, 2026)*. Vol. 4225. P. 142–156. ISSN 1613-0073. URL: <https://ceur-ws.org/Vol-4225/> (дата звернення: 05.09.2026).

References

1. Strogatz, S.H. (2024), *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*, 3rd ed., Chapman and Hall/CRC, New York, 616 p. DOI: <https://doi.org/10.1201/9780429398490>.
2. Kocarev, L., Lian, S. (eds.) (2011), *Chaos-Based Cryptography: Theory, Algorithms and Applications*, Springer, Berlin, Heidelberg, 398 p. DOI: <https://doi.org/10.1007/978-3-642-20542-2>.
3. Hairer, E., Wanner, G. (1996), *Solving Ordinary Differential Equations II: Stiff and Differential-Algebraic Problems*, 2nd ed., Springer-Verlag, Berlin, 614 p. DOI: <https://doi.org/10.1007/978-3-642-05221-7>.
4. Takens, F. (1981), "Detecting Strange Attractors in Turbulence", in Rand, D.A., Young, L.-S. (eds.), *Dynamical Systems and Turbulence, Warwick 1980: Proceedings of a Symposium held at the University of Warwick 1979/80*, Lecture Notes in Mathematics, Vol. 898, Springer, Berlin, pp. 366–381. DOI: <https://doi.org/10.1007/BFb0091924>.
5. Lozi, R. (2013), "Can We Trust Numerical Simulations of Chaotic Systems for Cryptographic Applications?", *Discontinuity, Nonlinearity, and Complexity*, Vol. 2, No. 3, pp. 293–302. DOI: <https://doi.org/10.1142/S225118571350022X>.
6. Wang, X., Chen, X. (2021), "An Image Encryption Algorithm Based on Dynamic Row Scrambling and Zigzag Transformation", *Chaos, Solitons & Fractals*, Vol. 147, Art. 110962. DOI: <https://doi.org/10.1016/j.chaos.2021.110962>.
7. He, J., Cai, J. (2019), "Design of a New Chaotic System Based on Van Der Pol Oscillator and Its Encryption Application", *Mathematics*, Vol. 7, No. 8, Art. 743. DOI: <https://doi.org/10.3390/math7080743>.
8. Gao, P., Lu, T., Dong, J. (2026), "Color Image Encryption Based on a Square-Term Enhanced 4D Chaotic System", *Electronic Research Archive*, Vol. 34, No. 7, pp. 4577–4610. DOI: <https://doi.org/10.3934/era.2026202>.
9. Sambas, A. et al. (2025), "Exploring Chaotic Dynamics with Absolute-Embedded Sinusoidal Nonlinearity in a Sinusoidal-Enhanced Van der Pol Oscillator", *Mathematical Modeling and Computing*, Vol. 12, No. 1, pp. 109–121. DOI: <https://doi.org/10.23939/mmc2025.01.109>.
10. Kyurkchiev, N., Zaeviski, T., Vasileva, M., Kyurkchiev, V., Iliev, A., Rahnev, A. (2025), "Dynamics of a Class of Extended Duffing–Van Der Pol Oscillators: Melnikov's Approach, Simulations, Control over Oscillations", *Mathematics*, Vol. 13, No. 14, Art. 2240. DOI: <https://doi.org/10.3390/math13142240>.
11. Al Themairi, A., Mahmoud, G.M., Farghaly, A.A., Abed-Elhameed, T.M. (2023), "Complex Rayleigh–Van-der-Pol–Duffing Oscillators: Dynamics, Phase, Antiphase Synchronization, and Image Encryption", *Fractal and Fractional*, Vol. 7, No. 12, Art. 886. DOI: <https://doi.org/10.3390/fractalfract7120886>.

12. Sadek, L., Aldawish, I. (2025), "The Symmetry Preserving Rosenbrock Approach: Application to Solve the Chaotic Lorenz System", *Symmetry*, Vol. 17, No. 11, Art. 1844. DOI: <https://doi.org/10.3390/sym17111844>.
13. Skvortsov, L.M. (2011), "Explicit Stabilized Runge-Kutta Methods", *Computational Mathematics and Mathematical Physics*, Vol. 51, No. 7, pp. 1153–1166. DOI: <https://doi.org/10.1134/S0965542511070165>.
14. Skvortsov, L.M. (2017), "How to Avoid Accuracy and Order Reduction in Runge-Kutta Methods as Applied to Stiff Problems", *Computational Mathematics and Mathematical Physics*, Vol. 57, No. 7, pp. 1126–1141. DOI: <https://doi.org/10.1134/S0965542517070119>.
15. Abdulle, A. (2002), "Fourth-Order Chebyshev-Runge-Kutta Methods", *SIAM Journal on Scientific Computing*, Vol. 23, No. 6, pp. 2041–2054. DOI: <https://doi.org/10.1137/S106482750037619X>.
16. Nwaigwe, C., Atangana, A. (2025), "Fourth-Order Predictor-Corrector Method for Initial Value Ordinary Differential Equation Problems", *Numerical Algorithms*, Vol. 101, No. 2, pp. 1303–1336. DOI: <https://doi.org/10.1007/s11075-025-02043-7>.
17. Wang, X., He, W., Feng, H., Atluri, S.N. (2024), "Fast and Accurate Predictor-Corrector Methods Using Feedback-Accelerated Picard Iteration for Strongly Nonlinear Problems", *Computer Modeling in Engineering & Sciences*, Vol. 138, No. 3, pp. 2897–2918. DOI: <https://doi.org/10.32604/cmescs.2024.049975>.
18. Alvarez, G., Li, S.J. (2006), "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems", *International Journal of Bifurcation and Chaos*, Vol. 16, No. 8, pp. 2129–2151. DOI: <https://doi.org/10.1142/S0218127406015970>.
19. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, N., Dray, J., Vo, S., Bassham, L.E. (2010), *NIST Special Publication 800-22 rev. 1a: A Statistical Test Suite for Random and Pseudorandom*, 131 p. DOI: <https://doi.org/10.6028/NIST.SP.800-22r1a>.
20. Nazarova, I.A., Altukhova, T.V., Kunda, M.S. (2026), "Efficiency Analysis of Parallel Implementations of One-Step Embedded Methods for Solving Large-Scale Cauchy Problems with Adaptive Step Size", *Scientific Works of Donetsk National Technical University. Series: Informatics, Cybernetics and Computer Engineering*, No. 1 (42), pp. 5–18. DOI: <https://doi.org/10.31474/1996-1588-2026-1-42-5-18>.
21. Nazarova, I., Popova, A. (2025), "Numerical Modeling of Multidimensional Cauchy Problems with Adaptive Step Size", *Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference*, Donetsk National Technical University, Drohobych, pp. 165–170. DOI: <https://doi.org/10.5281/zenodo.15775240>.
22. Nazarova, I., Dorohyi, I., Altukhova, T., Kunda, M. (2026), "Efficient Parallel Hybrid DIRK Solvers for Stiff Complex Critical Infrastructure Models", *CEUR Workshop Proceedings (Proceedings of the International Scientific and Practical Workshop "Resilient Systems: Secure Digital Technologies and Critical Infrastructure 2026" (RS-2026), Drohobych, Ukraine, June 30, 2026)*, Vol. 4225, pp. 142–156, ISSN 1613-0073, available at: <https://ceur-ws.org/Vol-4225/> (accessed 5 September 2026).

Надійшла до редакції 31.08.2026

Я. Ю. ДОРОГИЙ, І. А. НАЗАРОВА, Н. О. МАСЛОВА, Т. В. АЛТУХОВА

^{1,2,4} Донецький національний технічний університет, Дрогобич, Україна

³ Львівський державний університет безпеки життєдіяльності, Львів, Україна

¹ yaroslav.dorohyi@donntu.edu.ua, ² iryna.nazarova@donntu.edu.ua, ³ masgpp2@gmail.com,

⁴ tetiana.altukhova@donntu.edu.ua

ІНТЕГРАЦІЯ ЖОРСТКИХ ХАОТИЧНИХ МОДЕЛЕЙ ТА ЧИСЕЛЬНИХ РОЗВ'ЯЗНИКІВ У КРИПТОГРАФІЧНІ ФРЕЙМВОРКИ

Стаття присвячена вирішенню актуального науково-технічного завдання підвищення ефективності хаотичних криптографічних фреймворків за рахунок інтеграції жорстких динамічних систем та їх чисельних вирішувачів. Розроблено та досліджено узагальнену криптосистему на основі хаотичної динаміки, що включає математичне жорстке ядро, чисельний вирішувач та модуль вилучення ключового потоку. Виконано детальну розробку та аналіз криптографічних властивостей хаотичних ядер, заснованих на неавтономних осциляторах: Ван дер Поля, нелінійного Ван дер Поля–Даффінга та гібридного Релея–Ван-дер Поля–Даффінга. Створено та протестовано спеціалізовані вирішувачі для хаотичних криптосистем: k -точкова предиктор–коректор схема, стабілізований метод Скворцова, напівнеявний алгоритм Розенброка. На відміну від класичних явних та неявних чисельних схем, дані методи забезпечують коректне чисельне відтворення хаотичної динаміки та стійкість при зовнішніх збуреннях. Виконано аналіз ключового домену для кожного крипто ядра, включаючи оцінку його теоретичної та ефективної потужності. Проведено дослідження статистичних властивостей *LSB*-модифікації кроку та її придатності для створення криптографічно стійких послідовностей.

Ключові слова: криптографічні фреймворки, жорсткі хаотичні системи, криптографічне ядро, чисельні розв'язувачі, блоковий багатоточковий метод, схеми «предиктор–коректор», простір ключів.