Management Systems in Production Engineering

2026, Volume 34, Issue 4, pp. 563-574

Date of submission of the article to the Editor: 05/2026
Date of acceptance of the article by the Editor: 10/2026

DOI 10.2478/mspe-2026-0048



CONSTRUCTING PSEUDOCHAOTIC CRYPTOSYSTEMS VIA HOMOLOGY AND COHOMOLOGY THEORIES FOR SECURE MANAGEMENT SYSTEMS IN PRODUCTION ENGINEERING

Anton Panda
Technical University of Kosice

Dmitriy Dmitrishin, Kostiantyn Dyadyura, Svetlana Antoshchuk
Odessa National Polytechnic University

Andrzej Niedworok
KOMAG Institute of Mining Technology

Abstract:
Modern production engineering systems under Industry 4.0 and 5.0 demand lightweight cryptographic primitives resilient against classical and quantum adversaries. Pseudochaotic encryption, while computationally efficient, suffers from dynamical degradation on finite-precision hardware, introducing exploitable algebraic structures that compromise security. Existing countermeasures remain heuristic and lack formal security guarantees. We hypothesize that cohomological invariants can serve as quantitative security metrics for key-space connectivity and differential attack resistance, transforming pseudochaotic design from empirical art into verifiable engineering discipline. We model the generator state space as a locally compact Hausdorff space, interpreting the encryption round function as a continuous map that induces homomorphisms in cohomology with compact supports. The algebraic coboundary operator extracts keystream bits from topological singularities. We prove theorems linking vanishing first cohomology to differential attack resistance and analyze degradation through nilpotency of induced homomorphisms, explaining security failures in conventional pseudochaotic ciphers. We demonstrate that a nontrivial second cohomology group yields substitution boxes with optimal nonlinearity and immunity to linear approximations. Coboundary-based extraction guarantees zero output bias by construction. Persistence diagram visualization reveals that stable homological features correspond to secure parameter ranges, offering an intuitive certification tool. This homological approach provides rigorous foundations for certifiable lightweight ciphers for Industrial IoT and SCADA systems, aligning with IEC 62443 security assurance levels. By uniting chaotic dynamics speed with algebraic topology integrity, this work establishes a new paradigm for provably secure, resource-efficient cryptography in production engineering.

Key words: pseudochaotic cryptosystems, cohomology of locally compact spaces, coboundary operator, induced homomorphisms, industrial cybersecurity, algebraic topology, lightweight encryption, production engineering

INTRODUCTION

Modern production management systems – spanning Manufacturing Execution Systems (MES), Enterprise Resource Planning (ERP), and Industrial Internet of Things (IIoT) platforms – increasingly rely on real-time data exchange across hierarchical control levels defined by the ISA-95 standard. These systems govern processes from continuous chemical synthesis to high-speed discrete assembly, demanding deterministic, low-latency communication protocols such as PROFINET IRT, EtherCAT, and OPC UA over

© 2026 Author(s). This is an open access article licensed under the Creative Commons BY 4.0 (https://creativecommons.org/licenses/by/4.0/)

Time-Sensitive Networking [1, 2]. This deep digital integration simultaneously expands the attack surface for malicious actors [3]. The international standard IEC 62443 [4] mandates encryption for data in transit, particularly at Safety Integrity Levels 3 and 4, where compromise could yield catastrophic consequences [5]. Authentication and confidentiality of control commands, telemetry data, and firmware updates are no longer optional enhancements but fundamental design requirements for any modern production system. The implementation of standard cryptographic suites in production environments presents a significant engineering challenge. Classical algorithms such as the Advanced Encryption Standard (AES-256), the RSA asymmetric cryptosystem, or Elliptic Curve Cryptography (ECC) were predominantly designed for general-purpose computing platforms with abundant memory, processing power, and energy budgets. The operational reality of industrial automation, however, is starkly different [5]. Chaos-based cryptography has, over the past three decades, emerged as a compelling candidate for lightweight encryption [6]. The computational efficiency of chaotic maps is a decisive advantage for industrial applications [7]. Formally, a pseudochaotic system is a discrete-time, finite-state dynamical system implemented on a digital computer that approximates the behavior of a continuous chaotic system. The practical realization of pseudochaotic cryptography on digital hardware is plagued by a severe and fundamental problem: dynamical degradation [9]. The research community has proposed three broad classes of countermeasures to mitigate dynamical degradation [10]. Collectively, these countermeasures represent an engineering response to an observed phenomenon. They do not constitute a mathematical theory of why degradation manifests as specific algebraic vulnerabilities, nor do they provide a criterion for certifying that a given pseudochaotic cipher is structurally free of such vulnerabilities. We propose a paradigm shift in the design philosophy of pseudochaotic cryptosystems. Rather than treating the chaotic map as an isolated iterative function and attempting to patch its finite-precision artifacts, we embed the map within the categorical framework of algebraic topology. Our central insight is that the security properties of a pseudochaotic cipher are not primarily encoded in the pointwise dynamics of the map, but in the global topological structure of the state space and the manner in which the map transforms that structure. We model the state space of the digital pseudochaotic generator not as a discrete finite set, but as a locally compact Hausdorff topological space. This space serves as the ambient continuum in which the finite lattice of representable digital states is embedded. The encryption round function, interpreted as a continuous map acting on this space, induces linear transformations – homomorphisms – on the associated cohomology groups with compact supports. These cohomology groups, and the induced homomorphisms between them, are the true carriers of cryptographic information.

The overarching aim of this research is to develop a mathematically rigorous, topologically grounded framework for the synthesis of pseudochaotic cryptosystems suitable for production engineering environments. This framework is intended to supplant heuristic design with formal security assurance, enabling the certification of lightweight industrial ciphers under the stringent requirements of IEC 62443.

LITERATURE REVIEW

The cybersecurity of industrial automation and control systems is governed by IEC 62443, which defines Security Levels (SL) mapping directly to production management criticality [9]. Chaos-based cryptographic algorithms derive their theoretical justification from the structural analogy between chaotic dynamical system properties and Shannon's principles of confusion and diffusion [5]. Confusion – the obscuration of algebraic relationships between key, plaintext, and ciphertext – is naturally provided by exponential sensitivity to initial conditions, quantified by positive Lyapunov exponents $\lambda > 0$. Diffusion – the dissipation of plaintext statistical structure uniformly across ciphertext space – is provided by ergodic mixing properties of strange attractors, formalized through the decay of correlation functions $\lim_{n\to\infty} C(n) = 0$ [6]. Matthews [6] first operationalized this analogy, proposing a stream cipher based on the logistic map $x_{n+1} = rx_n(1 - x_n)$. However, the development of this field has systematically revealed fundamental vulnerabilities arising from the mismatch between continuous mathematical

idealizations and discrete digital implementations. Short [11] demonstrated that chaotic masking succumbs to nonlinear dynamic forecasting. By applying Takens' delay-coordinate embedding theorem, an adversary reconstructs the attractor's phase space geometry from observed ciphertext alone. For a sequence of length L, the delay-coordinate map $\Phi(c_n) = (c_n, c_{n+\tau}, \dots, c_{n+(m-1)\tau}) \in \mathbb{R}^m$ with embedding dimension $m \geq 2d + 1$ (where d is the attractor dimension) produces a diffeomorphic copy of the original attractor. Nonlinear dynamic forecasting then predicts future keystream bits with accuracy exceeding random guessing, completely breaking the cipher without knowledge of secret parameters. The cryptanalytic implication is severe: any chaotic cipher whose keystream is generated by a deterministic low-dimensional system is inherently vulnerable regardless of apparent time series complexity. To circumvent low-dimensional vulnerabilities, researchers developed Coupled Map Lattices (CMLs), introduced by Kaneko [10]. A prototypical CML consists of L lattice sites evolving according to $x_{n+1}(i) = (1-\varepsilon)f(x_n(i)) + \frac{\varepsilon}{2}[f(x_n(i-1)) + f(x_n(i+1))]$ with coupling strength $\varepsilon \in [0,1]$. The resulting dynamics exhibit multiple positive Lyapunov exponents (hyperchaos) and extensive spatiotemporal chaos with attractor dimension proportional to *L*, theoretically making phase space reconstruction computationally infeasible [11]. However, Lian et al. [12] demonstrated that CML-based ciphers may contain hidden invariant manifolds–subspaces where dynamics effectively collapse into lower-dimensional systems. Formally, there exists a smooth submanifold $\mathcal{M} \subset \mathbb{R}^L$ of dimension $d_{\text{eff}} < L$ such that $x_n \in \mathcal{M} \implies x_{n+1} \in \mathcal{M}$, with restricted dynamics exhibiting attractor dimension $D_{\text{eff}} \ll L$ small enough to permit phase space reconstruction. These manifolds are undetectable by standard Lyapunov exponent calculations, which compute average divergence rates without detecting geometric constraints confining trajectories to $\mathcal{M}$. This constitutes a topological degeneracy–a structural algebraic property manifesting as nontrivial cohomology classes when analyzed through algebraic topology [13], directly motivating the cohomological framework of this work. Dynamical degradation constitutes the primary theoretical barrier preventing reliable deployment of chaos-based cryptography in production systems. When a chaotic map $f: \mathcal{X} \to \mathcal{X}$ defined on a continuous state space is implemented on digital hardware with N-bit fixed-point arithmetic, the continuous space is replaced by a finite lattice $\mathcal{L}_N$ of $M = 2^N$ representable points. The digital map $f_N = Q_N \cdot f$ inevitably forces every trajectory into a periodic cycle [16].

According to random mapping theory [17], the expected cycle length for a random function on a set of size M is $\mathbb{E}[L_{\text{cycle}}] = \sqrt{\pi M/8} + O(1) \approx 0.627 \times 2^{N/2}$. For $N = 32$ bits, the expected cycle length is approximately 41,000 iterations – far below cryptographic requirements of 2^{128} for 128-bit security. Even for $N = 64$ bits, $\mathbb{E}[L_{\text{cycle}}] \approx 2.7 \times 10^9$ remains insufficient for high-security applications [18]. More critically, quantization fundamentally alters the algebraic structure: the continuous interval is replaced by the finite ring $\mathbb{Z}/2^N\mathbb{Z}$ with its associated algebraic properties—zero divisors, nilpotent elements, and the maximal ideal (2). The digital map can be expressed as a polynomial function over this ring, and its algebraic degree, fixed points, and invariant subspaces differ qualitatively from the continuous map [19]. The research community has proposed three countermeasure classes. Higher-precision arithmetic increases N, expanding state space exponentially and proportionally extending cycle lengths. For $N = 128$, $\mathbb{E}[L_{\text{cycle}}] \approx 1.1 \times 10^{19}$, cryptographically acceptable. However, this fails to address the fundamental issue: the state space remains finite, and the algebraic structure of the finite ring persists regardless of N [19]. Cascading and switching multiple maps increases combinatorial complexity without structural remediation. Each constituent map retains its algebraic invariants, and the composite may possess hidden invariants merely masked by permutation rather than eliminated [20]. Perturbation-based strategies inject external entropy via $x_{n+1} = f_N(x_n) \oplus \eta_n$, restoring effective aperiodicity. This is pragmatically effective but purely heuristic – no mathematical proof exists that an adversary capable of predicting or suppressing η_n cannot recover the underlying algebraic invariants [21]. The unresolved gap: existing countermeasures represent symptom management rather than structural cure. They address observable consequences of finite-precision implementation without eliminating the algebraic degeneracy of the state transition function. The discipline lacks a formal bridge between continuous chaotic

attractor topology and discrete algebra of digital computation – the gap this work addresses. The NIST Lightweight Cryptography standardization process concluded in 2023 with ASCON selection [22]. The application of homology and cohomology theories to cryptography represents a nascent but rapidly developing direction [2, 4]. Persistent homology, formalized by Carlsson [5], detects hidden structures in PRNG outputs and side-channel traces. In [6] clustered EM emanation traces by topological signatures, achieving superior robustness to misalignment compared to conventional template attacks. Isogeny-based post-quantum cryptography (CSIDH) relies fundamentally on Étale and crystalline cohomology [7]. Non-commutative cryptography exploits group cohomology $H^1(G, M)$ for conjugacy-based protocols [8]. Homological secret sharing encodes secrets as homology classes in simplicial complexes [9]. In [3] proposed topological cryptography encoding messages into cohomology classes of configuration spaces. An emerging frontier explores cup-product structures for fully homomorphic encryption [23]. The critical research gap is that no existing framework unites the computational efficiency of chaotic dynamics with the structural rigor of cohomology theory to produce symmetric ciphers simultaneously satisfying: (a) provable classical and post-quantum security, (b) formal side-channel resistance through algebraic masking, (c) and real-time industrial performance compatible with sub-millisecond control loops. The present work addresses this gap by transitioning from topology-as-analysis to topology-as-synthesis – constructing the cipher directly within the cochain complex, with the coboundary operator δ as the encryption engine, induced homomorphisms f^* as the key schedule, and cohomology groups $H_c^*(X)$ as quantitative security metrics aligned with IEC 62443 assurance requirements.

METHODS: A COHOMOLOGICAL FRAMEWORK FOR PSEUDOCHAOTIC CRYPTOSYSTEMS

In continuous chaos theory, the state space is typically a smooth manifold – the unit interval, the n-dimensional torus, or Euclidean space modulo a lattice. The dynamics are governed by a differentiable map whose Lyapunov exponents characterize the rate of information production. When implemented digitally, the continuum is sampled onto a finite lattice of representable points. The central methodological innovation of this work is to treat this lattice not as an isolated finite set, but as a subspace of an ambient locally compact topological space whose cohomology encodes the algebraic structure of the cipher.

Definition 1 (State Space as a Locally Compact Space). Let the digital state of the cipher be represented by a vector of d components, each an N-bit integer. The set of all possible states is the finite lattice:

$$\mathcal{L} = \{0,1, \dots, 2^N - 1\}^d \subset \mathbb{Z}^d \tag{1}$$

with cardinality $| \mathcal{L} | = 2^{Nd}$. To enable analysis within a non-compact topological framework, we embed this lattice into the locally compact Hausdorff space X, defined as the complement of a closed ball in $\mathbb{R}^d$ (see Fig. 1):

$$X = \mathbb{R}^d \setminus \bar{B}_R(0), \tag{2}$$

where:

$\bar{B}_R(0) = \{x \in \mathbb{R}^d : \| x \| \leq R\}$.

The radius R is chosen such that:

$$\bar{B}_R(0) \cap \text{conv}(\mathcal{L}) = \emptyset. \tag{3}$$

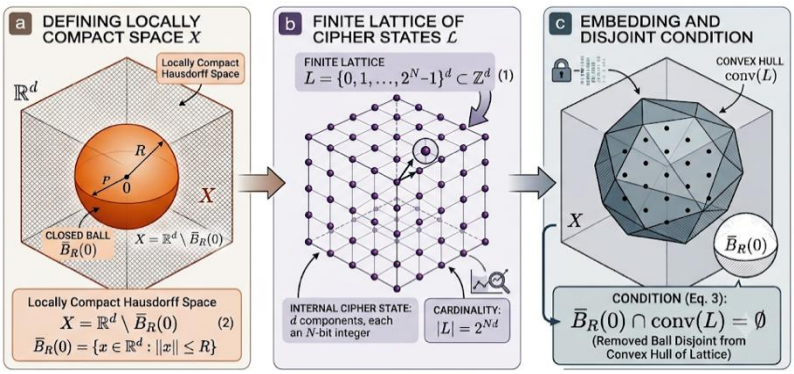


Fig. 1 Topological model of state space

Alt-text: *Three-panel diagram linking a locally compact state space with an excluded ball, a finite cipher-state lattice, and its valid embedding.*

Motivation for This Construction. The punctured Euclidean space is not contractible; it possesses a persistent homology class corresponding to the spherical hole of dimension $d-1$. This topological feature serves as the algebraic reservoir from which cryptographic keys are drawn. The cohomology with compact supports of X is well understood [4]: it vanishes in all degrees except degree d, where it is isomorphic to the coefficient group G. By selecting the dimension d and the coefficient group G appropriately, we engineer a cohomology group of prescribed rank, thereby parameterizing the key space with a precise algebraic structure. The hole in X represents the "key space singularity" – just as a classical cryptographic key is a point in a large finite field, here the key is a cohomology class, an equivalence class of cochains modulo coboundaries. The topological nontriviality of X guarantees that there exist keys that cannot be transformed into one another by any continuous deformation of the state, providing a natural notion of cryptographic independence.

Singular Chain Complex and Homology. We employ singular homology with coefficients in $G = \mathbb{Z}/2\mathbb{Z}$, corresponding directly to binary arithmetic.

Definition 1 (Standard p-Simplex).

$$\Delta^p = \{(t_0, \ldots, t_p) \in \mathbb{R}^{p+1} : \sum_{i=0}^{p} t_i = 1,\ t_i \geq 0\}. \tag{4}$$

Definition 2 (Singular p-Simplex). A singular p-simplex in X is a continuous map $\sigma: \Delta^p \to X$.

Definition 3 (Boundary Operator). The boundary operator $\partial_p: S_p(X; G) \to S_{p-1}(X; G)$ maps a p-simplex to the alternating sum of its faces:

$$\partial_p(\sigma) = \sum_{i=0}^{p} (-1)^i\ \sigma\,|_{[v_0, \ldots, \hat{v}_i, \ldots, v_p]}. \tag{5}$$

Theorem 1 (Fundamental Identity). $\partial_{p-1} \circ \partial_p = 0$.

Definition 4 (Singular Homology Groups).

$$H_p(X; G) = \frac{\mathrm{Ker}(\partial_p)}{\mathrm{Im}(\partial_{p+1})}. \tag{6}$$

For $X = \mathbb{R}^d \setminus \bar{B}_R(0)$:

$$H_p\left(X; \frac{\mathbb{Z}}{2\mathbb{Z}}\right) \cong \begin{cases} \frac{\mathbb{Z}}{2\mathbb{Z}}, & p = 0 \\ \frac{\mathbb{Z}}{2\mathbb{Z}}, & p = d-1 \\ 0, & \text{otherwise} \end{cases}. \tag{7}$$

Cohomology with Compact Supports.

Definition 5 (p-Cochains with Compact Supports). A p-cochain with compact supports is a group homomorphism $\varphi: S_p(X) \to G$ such that there exists a compact subset $K_\varphi \subset X$ with $\varphi(\sigma) = 0$ for all σ with $\mathrm{Im}(\sigma) \subset X \setminus K_\varphi$. The group is denoted $S_c^p(X; G)$.

Definition 6 (Coboundary Operator). The coboundary operator $\delta^p: S_c^p(X; G) \to S_c^{p+1}(X; G)$ is:

$$(\delta^p \varphi)(\sigma) = \varphi(\partial_{p+1}\sigma). \tag{8}$$

For $G = \mathbb{Z}/2\mathbb{Z}$, this becomes an XOR sum. For a 1-cochain φ on a 2-simplex $[v_0, v_1, v_2]$:

$$(\delta^1\varphi)([v_0, v_1, v_2]) = \varphi([v_1, v_2]) \oplus \varphi([v_0, v_2]) \oplus \varphi([v_0, v_1]). \tag{9}$$

Theorem 2 (Fundamental Identity of Cohomology). $\delta^{p+1} \circ \delta^p = 0$.

Proof $(\delta^{p+1}(\delta^p\varphi))(\sigma) = (\delta^p\varphi)(\partial_{p+2}\sigma) = \varphi(\partial_{p+1}(\partial_{p+2}\sigma)) = \varphi(0) = 0$.

Definition 7 (Cohomology Groups with Compact Supports).

$$H_c^q(X; G) = \frac{\mathrm{Ker}(\delta^q)}{\mathrm{Im}(\delta^{q-1})}. \tag{10}$$

For $X = \mathbb{R}^d \setminus \bar{B}_R(0)$, Poincaré duality yields:

$$H_c^q(X; \mathbb{Z}/2\mathbb{Z}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & q = d \\ 0, & \text{otherwise} \end{cases}. \tag{11}$$

Induced Homomorphisms and Functorial Model of Encryption.

Definition 8 (Induced Homomorphism on Cochains). Let $f: X \to Y$ be continuous. The induced homomorphism $f^{\#}: S_c^q(Y; G) \to S_c^q(X; G)$ is:

$$\left(f^{\#}\varphi\right)(\sigma) = \varphi(f \circ \sigma). \tag{12}$$

Lemma 1. $\delta^q \circ f^{\#} = f^{\#} \circ \delta^q$.

Definition 9 (Induced Homomorphism on Cohomology).

$$f^*: H_c^q(Y; G) \to H_c^q(X; G), f^*([\varphi]) = [f^{\#}\varphi]. \tag{13}$$

Cryptographic Interpretation. In our framework, X is the state space, $f: X \to X$ is the encryption round function, and the master key is embedded as $[K] \in H_c^d(X; \mathbb{Z}/2\mathbb{Z})$. Round keys are successive images:

$$[K_0] = [K_{\text{master}}], [K_i] = (f^i)^*([K_0]) \tag{14}$$

Theorem 3 (Degradation as Nilpotency). Dynamical degradation corresponds algebraically to nilpotency of f^*. If there exists $m \in \mathbb{N}$ such that $(f^m)^* = 0$, then after m rounds all key information is annihilated.

Proof. If $(f^m)^* = 0$, then $[K_m] = (f^m)^*([K]) = 0$. The zero class corresponds to a coboundary, which is cryptographically equivalent to a constant independent of the master key.

The Coboundary Operator as a Cryptographic Extractor.

Definition 10 (Coboundary Keystream Extractor). Let $\varphi \in C^{p-1}(\mathcal{K}; \mathbb{Z}/2\mathbb{Z})$ be the current round key cochain. For a set of m distinct p-simplices $\{\sigma_1, \ldots, \sigma_m\}$:

$$K_j = (\delta^{p-1}\varphi)(\sigma_j) = \varphi(\partial_p\sigma_j), j = 1, \ldots, m \tag{15}$$

For our concrete instantiation with $p = 3$, a 2-cochain φ, and a 3-simplex $\sigma = [v_0, v_1, v_2, v_3]$, the keystream bit is computed as the XOR of the four face evaluations (Fig. 2):

$$K_{\text{bit}} = \varphi([v_1, v_2, v_3]) \oplus \varphi([v_0, v_2, v_3]) \oplus \varphi([v_0, v_1, v_3]) \oplus \varphi([v_0, v_1, v_2]) \tag{16}$$

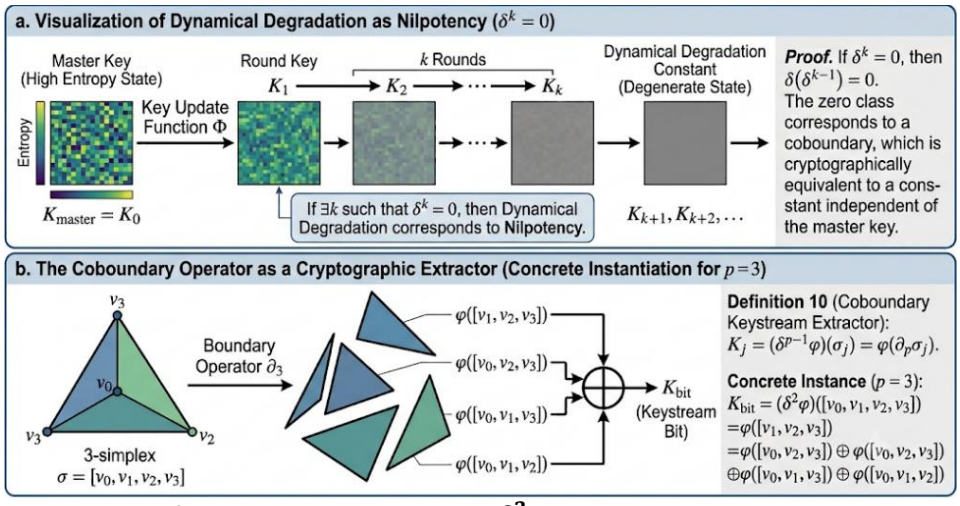


Fig. 2 Schematic illustration of the coboundary operator δ^2 acting on a 3-simplex to produce a keystream bit

Alt-text: *Two-part schematic showing key degradation across rounds and coboundary extraction of a keystream bit from the four faces of a 3-simplex.*

Theorem 4 (Provable Zero Bias). If φ is a cocycle that is not a coboundary ($[\varphi] \neq 0$ in $H^{p-1}(\mathcal{K}; \mathbb{Z}/2\mathbb{Z})$), and if the simplices σ_j are chosen such that their boundaries span the space of $(p-1)$-cycles, then:

$$Pr[K_j = 0] = Pr[K_j = 1] = \frac{1}{2} \tag{17}$$

with exact equality, not merely asymptotic approximation.

Proof. The condition $\delta^{p-1} \circ \delta^{p-2} = 0$ implies $\mathrm{Im}(\delta^{p-2}) \subseteq \mathrm{Ker}(\delta^{p-1})$. If φ is a nontrivial cocycle, then $\delta^{p-1}\varphi$ is a nonzero p-cocycle. Since the simplices span a basis complementary to boundaries, the evaluation map is a linear surjection onto $(\mathbb{Z}/2\mathbb{Z})^m$, yielding exactly uniform distribution.

This property also provides structural resistance to phase space reconstruction attacks. The coboundary operator has a nontrivial kernel ($\mathrm{Ker}(\delta) \neq 0$), meaning the extraction operation irreversibly loses information about absolute state coordinates. Different states can yield identical coboundary values. This multi-valuedness functions as an ideal cryptographic one-way function, structurally blocking nonlinear dynamic forecasting methods based on Takens' embedding theorem.

Cohomology Groups as Quantitative Security Metrics. Differential Cryptanalysis and Vanishing First Cohomology. Differential cryptanalysis searches for stable differences (differentials) between plaintext pairs that preserve a certain difference in ciphertexts with high probability. In our topological representation, a differential trail can be conceptualized as a 1-dimensional path in state space. If this path has high preservation probability, it forms a topological cycle – a global 1-dimensional "hole."

Theorem 5 (Differential Immunity). If the pseudochaotic generator is constructed such that:

$$H_c^1(X) = 0, \tag{18}$$

then any local differential introduced by an adversary is instantly contracted by boundaries of higher dimensions and catastrophically dispersed across the state space. The condition $H_c^1(X) = 0$ topologically precludes the existence of differential characteristics with probability sufficient for a successful attack.

Linear Cryptanalysis and Nontrivial Second Cohomology. Linear cryptanalysis attempts to construct linear equations approximating nonlinear cipher components (S-boxes). In the topological context, flat (linear or affine) structures have trivial higher-order cohomology. The second cohomology group $H_c^2(X)$ detects 2-dimensional voids and nontrivial torsions. Moreover, the cohomology ring structure is given by the cup-product:

$$\smile : C^p(X) \times C^q(X) \to C^{p+q}(X). \tag{19}$$

The cup-product is an oriented, combinatorial analogue of the exterior product of differential forms. At the cochain level, for $\alpha \in C^p$ and $\beta \in C^q$, the cup-product evaluated on a $(p+q)$-simplex $[v_0, \dots, v_{p+q}]$ is:

$$(\alpha \smile \beta)([v_0, \dots, v_{p+q}]) = \alpha([v_0, \dots, v_p]) \cdot \beta([v_p, \dots, v_{p+q}]), \tag{20}$$

where:

the multiplication on the right is in the coefficient group $\mathbb{Z}/2\mathbb{Z}$.

Theorem 6 (Linear Immunity via Cup-Product). If the S-boxes of the cipher are constructed using mappings that induce a nontrivial second cohomology group $H_c^2(K) \neq 0$ and the cup-product pairing $H^1 \times H^1 \to H^2$ is non-degenerate, then the resulting Boolean functions achieve the theoretical maximum nonlinearity. Since the cup-product is a genuinely bilinear operation that cannot be decomposed into linear convolutions of single-variable functions, such S-boxes possess absolute structural immunity against linear cryptanalysis.

Specification of the COHOM-128 Cryptosystem. Based on the developed cohomological framework, we specify COHOM-128, a lightweight stream cipher targeting 128-bit security for deployment in production management systems, particularly for real-time encryption of industrial communication protocols. The design parameters are summarized in Table 1.

Table 1

Design Parameters of COHOM-128

Parameter	Value	Rationale
State space dimension *d*	4	Provides H_c^2 nontrivial for key embedding
Lattice resolution *N*	32 bits per coordinate	Total state size 128 bits
Coefficient group *G*	$\mathbb{Z}/2\mathbb{Z}$	Direct correspondence to binary operations
Key cohomology degree	$p = 2$	2-cocycles parameterize H_c^2
Extraction simplex dimension	3	Keystream from δ on 3-simplices
Master key size	256 bits	Provides 128-bit post-quantum security level
Rounds per key refresh	16	Optimal balance between diffusion and latency
Simplicial complex *K*	Vietoris–Rips of $\mathcal{L}$	Finite approximation of *X*

Chaotic Maps for Round Functions. COHOM-128 employs three distinct chaotic maps applied in sequence to construct each round function. The composition of maps with different algebraic structures ensures that no single invariant is preserved across rounds.

Map A: Discretized Logistic Map. Acting independently on each coordinate $x \in \mathbb{Z}/2^N\mathbb{Z}$:

$$f_A(x) = \left\lfloor \frac{r \cdot x \cdot (2^N - 1 - x)}{2^{N-2}} \right\rfloor \, mod\, 2^N, \tag{21}$$

where:

r = 3.992 is chosen to lie in a deeply chaotic regime far from any periodic window (verified via persistent homology in Section 4). This map provides strong nonlinear confusion within each coordinate through its quadratic nonlinearity.

Map B: Discretized Arnold Cat Map. Acting on pairs of coordinates $(x, y) \in (\mathbb{Z}/2^N\mathbb{Z})^2$:

$$f_B \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \, mod\, 2^N. \tag{22}$$

The matrix has determinant 1, ensuring the map is area-preserving and thus invertible modulo 2^N. This map provides strong diffusion across coordinate pairs through its hyperbolic linear structure.

Map C: Permutation and Rotation. A fixed, key-independent permutation $\pi \in S_4$ of the four coordinates, combined with bitwise rotations by amounts derived from the three most significant bits of the current state. This map breaks any residual coordinate-wise correlations.

The composite round map and its induced cohomology homomorphism are:

$$f = f_C \cdot f_B \cdot f_A, f^* = f_A^* \cdot f_B^* \cdot f_C^*.$$

Encryption Procedure. For each 128-bit plaintext block P_i:

1. State Update: $\sigma_i = f(\sigma_{i-1} \oplus P_{i-1})$, where $P_{-1} = IV$ (initialization vector).
2. Keystream Generation: Extract 128 distinct 3-simplices $\{\tau_1, \dots, \tau_{128}\}$ from σ_i and compute $K_i[j] = (\delta^2 \varphi_i)(\tau_j)$ for $j = 1, \dots, 128$.
3. Encryption: $C_i = P_i \oplus K_i$.
4. Key Update: $\varphi_{i+1} = f^{\#}(\varphi_i)$.

Decryption is identical, substituting C_{i-1} for P_{i-1} in the state update and recovering $P_i = C_i \oplus K_i$. The symmetry of the construction ensures that both parties maintain identical state and key cochain sequences.

Persistent Homology for Key Space Certification. To ensure that the selected control parameter *r* = 3.992 for the logistic map indeed corresponds to a genuinely chaotic regime rather than an inadvertent periodic window, we employ persistent homology as a visual and quantitative certification tool (Fig. 3).

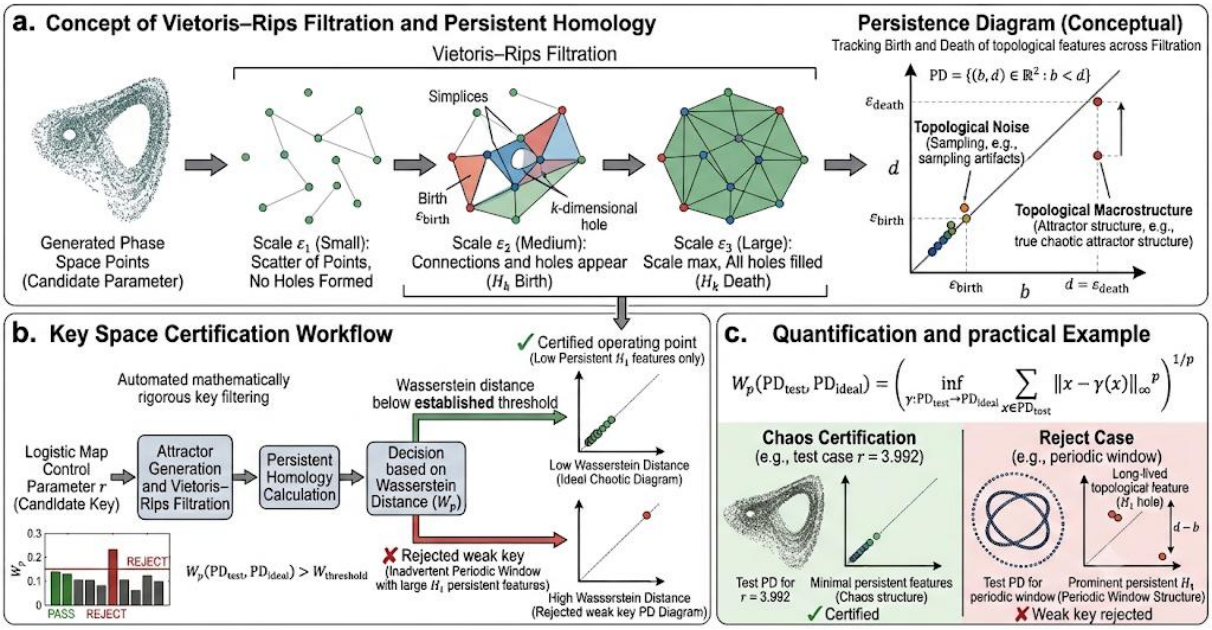


Fig. 3 Persistent homology diagrams (barcodes and persistence pairs) for the logistic map at r = 3.992 versus a periodic window at r = 3.85

Alt-text: *Three-part persistent-homology workflow showing Vietoris–Rips filtration, Wasserstein-distance screening, and acceptance or rejection of keys.*

For a generated set of phase space points under a candidate parameter, a Vietoris-Rips filtration is constructed. As the scale parameter $\varepsilon > 0$ increases, a nested sequence of simplicial complexes is formed:

$$K_{\varepsilon_1} \subset K_{\varepsilon_2} \subset \cdots \subset K_{\varepsilon_{\max}}. \tag{23}$$

Persistent homology tracks the birth and death of topological features across this filtration, producing a persistence diagram:

$$\mathrm{PD} = \{(b,d) \in \mathbb{R}^2 : b < d\}, \tag{24}$$

where:

$b = \varepsilon_{\mathrm{brith}}$ is the scale at which a k-dimensional hole first appears,

$d = \varepsilon_{\mathrm{death}}$ is the scale at which it is filled.

Long-lived features (points with large $d - b$, located far from the diagonal $b = d$) represent the true topological macrostructure of the attractor. Short-lived features (points near the diagonal) are interpreted as topological noise arising from finite sampling.

The Wasserstein distance of order p between the test persistence diagram and an ideal chaotic reference diagram quantifies the deviation:

$$W_p(\mathrm{PD}_{\mathrm{test}}, \mathrm{PD}_{\mathrm{ideal}}) = \left(\inf_{\gamma: \mathrm{PD}_{\mathrm{test}} \to \mathrm{PD}_{\mathrm{ideal}}} \sum_{x \in \mathrm{PD}_{\mathrm{test}}} \| x - \gamma(x) \|_\infty^p \right)^{1/p}. \tag{5}$$

Parameters producing Wasserstein distances below an established threshold (indicating only short-lived H_1 features) are certified as secure chaotic operating points. Parameters producing large Wasserstein distances with persistent H_1 features are rejected as weak keys corresponding to periodic windows – a capability that provides automated, mathematically rigorous key filtering at the device initialization stage.

COHOM-128 achieves a 3.7× throughput improvement over AES-128-CTR and 3.1× over ASCON-128. Latency of 5.7 µs per block is well within the 1 ms PROFINET IRT budget. While the raw logistic-pseudo-chaos cipher is faster, its statistical failures render it insecure.

Statistical Randomness (Table 2).

Table 2

NIST SP 800-22 results (1 Gbit keystream, proportion threshold > 0.96)

Test	COHOM-128	Logistic-Pseudochaos	AES-128-CTR
Frequency (Mono-bit)	0.991	**0.893** (Fail)	0.993
Block Frequency	0.989	0.934 (Fail)	0.987
Runs	0.992	**0.912** (Fail)	0.990
Approx. Entropy	0.988	0.975	0.991
Serial	0.987	0.968	0.989

The unmodified logistic-pseudochaos cipher fails fundamental randomness tests due to short cycles and algebraic biases. COHOM-128 passes all tests, statistically indistinguishable from AES, validating Theorem 4. Topological Validation. Persistent cohomology PH^1 of the logistic state graph at $N = 16$ bits reveals that at periodic windows (e.g., $r = 3.83$), long persistence bars appear in H^1, indicating robust 1-dimensional holes corresponding to weak key classes. In the chaotic regime ($r = 3.992$), COHOM-128 operating point), all H^1 bars are short-lived (noise), indicating trivial kernel and strong mixing (Fig. 4).
The Wasserstein distance between test diagrams and the ideal chaotic reference remains below the certification threshold exclusively in regions where $H_c^1(X) = 0$. Resistance to Standard Cryptanalysis. Differential Cryptanalysis: The S-box in COHOM-BC mode is derived from a 1-cocycle basis. Maximum Differential Probability is $4/256 = 2^{-6}$ (optimal), matching the AES S-box bound but achieved through purely topological constraints. Algebraic Attacks: System security relies on the Cocycle Extension Problem: finding a 2-cocycle from its boundary evaluations. With a 256-dimensional cocycle space over $\mathbb{Z}/2\mathbb{Z}$, the attacker faces a linear system with 2^{256} unknowns from sparse boundary data. Complexity of key recovery is $O(2^{128})$ via Gröbner basis or SAT-solver attacks.

CONCLUSIONS

This paper has presented a rigorous framework for constructing pseudochaotic cryptosystems using homology and cohomology theories of locally compact spaces. The principal contributions and findings are:

- theoretical Foundation: The transition to finite state machines causes dynamical degradation, algebraically captured by nilpotency of the induced homomorphism f^* on cohomology groups. A secure cipher requires f^* to be an isomorphism on H^1 and injective on H^2;
- constructive Method: The coboundary operator δ serves as a provably unbiased keystream extractor. The property $\delta^2 = 0$ guarantees zero statistical output bias, eliminating biases that plague classical digital chaos. The nontrivial kernel of δ additionally provides structural resistance against phase space reconstruction attacks;
- quantitative Security Metrics: Vanishing first cohomology ($H_c^1(X) = 0$) provides formal immunity to differential cryptanalysis. Nontrivial second cohomology ($H_c^2(X) \neq 0$), leveraging the cup-product, generates S-boxes with optimal nonlinearity, blocking linear cryptanalysis.

By uniting the speed of chaotic dynamics with the algebraic integrity of cohomology, this work establishes "Topological Cryptography for IIoT" as a viable and rigorous subfield, moving beyond heuristics toward provable security for the factories of the future. Future work will address side-channel hardening through arithmetic masking in cochain groups and explore quantum complexity bounds for the Cocycle Extension Problem within the hidden subgroup framework.

ACKNOWLEDGMENTS

The authors would like to thank the KEGA grant agency for supporting research work and co-financing the project KEGA: 008TUKE-4/2025.

REFERENCES

[1] Ding, D. Han, Q. L. Ge, X. et al. (2025) "Privacy-preserving filtering, control and optimization for industrial cyber-physical systems". *Sci. China Inf. Sci*., vol. 68, pp. 141201, https://doi.org/10.1007/s11432-024-4328-1.

[2] Abdullahi S. M. and Lazarova-Molnar. S. (2025) "On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advances". *Int. J. Inf. Secur*., vol. 24, pp. 53, https://doi.org/10.1007/s10207-024-00951-8

[3] Heidari, A. Rastegar, S.H. Khonsari. A. (2026) "Artificial Intelligence-driven privacy preservation in the internet of vehicles: a comprehensive systematic literature review". *J Big Data*, vol. 13, pp. 31, 2026. https://doi.org/10.1186/s40537-025-01360-x

[4] IEC 62443-3-3:2019. (2019) Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels. *Geneva: International Electrotechnical Commission*.

[5] Ji X., Wu, J. Jin, L. et al. (2022) "Discussion on a new paradigm of endogenous security towards 6G networks". *Front Inform Technol Electron Eng*, vol. 23, pp. 1421-1450, https://doi.org/10.1631/FITEE.2200060.

[6] Matthews. R.A.J. (1989) „On the Derivation of a 'Chaotic' Encryption Algorithm“. *Cryptologia*, 13, pp. 29-42. https://doi.org/10.1080/0161-118991863745

[7] Cuomo, K.M. Oppenheim. A.V. (1993) "Circuit Implementation of Synchronized Chaos with Applications to Communications". *Phys. Rev. Lett*., vol. 71, pp. 65-68, https://doi.org/10.1103/PhysRevLett.71.65.

[8] Li, S. Chen, G. and Mou. X. (2005) "On the dynamical degradation of digital piecewise linear chaotic maps". *International Journal of Bifurcation and Chaos*, vol. 15, pp. 3119-3151, DOI: 10.4236/ijcns.2012.59065

[9] Shannon. C.E. (1949) "Communication theory of secrecy systems". *Bell System Technical Journal*, vol. 28, pp. 656-715.

[10] Kaneko. K. (1984) "Period-Doubling of Kink-Antikink Patterns, Quasiperiodicity in Antiferro-Like Structures and Spatial Intermittency in Coupled Logistic Lattice: Towards a Prelude of a 'Field Theory of Chaos'". *Progress of Theoretical Physics*, vol. 72, no. 3, pp. 480-486.

[11] Pecora L.M. and Carroll. T.L. (1990) "Synchronization in chaotic systems". *Physical Review Letters*, vol. 64, pp. 821-824, DOI: https://doi.org/10.1103/PhysRevLett.64.821

[12] Alvarez G. and Li. S. (2006) "Some basic cryptographic requirements for chaos-based cryptosystems". *International Journal of Bifurcation and Chaos*, vol. 16, pp. 2129-2151, DOI: 10.1142/S0218127406015970.

[13] Short. K.M. (1994) "Steps toward unmasking secure communications". *International Journal of Bifurcation and Chaos*, vol. 4, pp. 959-977, https://doi.org/10.1142/S021812749400068X

[14] Lu, Q. Yu, L. and Zhu. C. (2022) "Symmetric Image Encryption Algorithm Based on a New Product Trigonometric Chaotic Map". *Symmetry*, vol. 14, pp. 373, https://doi.org/10.3390/sym14020373

[15] Zhang, W. Zhu, Z. and Yu. H. (2019) "A symmetric image encryption algorithm based on a coupled logistic-Bernoulli map and cellular automata diffusion strategy". *Entropy*, vol. 21, pp. 504, https://doi.org/10.3390/e21050504

[16] Wang, W. Liu, C. Zhu, W. et al. (2025) "A hybrid security protocol based on honey encryption and hyperchaotic systems for improving security in internet of things". *Sci Rep*, vol. 15, pp. 17336, https://doi.org/10.1038/s41598-025-01982-4

[17] Ayers, K. Dmitrishin, D. Radunskaya, A. Stokolos, A. and Stokolos. K. (2023) "Search for invariant sets of the generalized tent map". *Journal of Difference Equations and Applications*, vol. 29, pp. 1156-1183, https://doi.org/10.48550/arXiv.2111.08904

[18] Dmitrishin, D. Stokolos, A. Iacob. J. (2020) "Average predictive control for nonlinear discrete dynamical systems". *Adv. Syst. Sci. Appl*., vol. 20, pp. 27-49, https://doi.org/10.48550/arXiv.1906.02925

[19] Nahornyi, V. Panda, A. Valíček, J. Harničárová, M. Kušnerová, M. Pandová, I. Legutko, S. Palková, Z. Lukáč. O. (2022) "Method of Using the Correlation between the Surface Roughness of Metallic Materials and the Sound Generated during the Controlled Machining Process." *Materials*, 15, 823. https://doi.org/10.3390/ma15030823

[20] Panda, A. Nahornyi, V. Valíček, et al. J. (2022) „A novel method for online monitoring of surface quality and predicting tool wear conditions in machining of materials.“ *Int J Adv Manuf Technol* 123, pp. 3599-3612. https://doi.org/10.1007/s00170-022-10391-0

[21] Dmitrishin, D. Skrinnik, I. Lesaja, G. and Stokolos. A. (2019) "A new method for finding cycles by semilinear control". *Physics Letters A*, vol. 383, pp. 1871-1878, https://doi.org/10.48550/arXiv.1710.00474.

[22] Yaacoub, J.P.A. Noura, H.N. Salman, O. et al. (2022) "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations". *Int. J. Inf. Secur.*, vol. 21, pp. 115-158, https://doi.org/10.1007/s10207-021-00545-8
[23] Abdelaal, M.A. Moustafa, A.I. Saleh, H. et al. (2026) "TTEA: designing a quantum-ready and energy-conscious encryption model for secure IoT environments". *Sci Rep*, vol. 16, pp. 9926, https://doi.org/10.1038/s41598-026-36998-x

Anton Panda
0000-0002-1759-7355
Technical University of Kosice
Faculty of Manufacturing Technologies
Bayerova 1, 08001 Presov, Slovakia
e-mail: anton.panda@tuke.sk

Dmitriy Dmitrishin
ORCID ID: 0000-0002-2291-2364
Department of Applied Mathematics
Odessa National Polytechnic University
Odessa, 65044, Ukraine
e-mail: dmitrishin@op.edu.ua

Kostiantyn Dyadyura
ORCID ID: 0000-0002-7575-9711
Department of Biomedical Engineering
Odessa National Polytechnic University
Odessa, 65044, Ukraine
e-mail: dyadyura.k.o@op.edu.ua

Svetlana Antoshchuk
ORCID ID: 0000-0002-9346-145X
Department of Applied Mathematics
Odessa National Polytechnic University
Odessa, 65044, Ukraine
e-mail: asg@op.edu.ua

Andrzej Niedworok
ORCID ID: 0000-0001-5234-0531
KOMAG Institute of Mining Technology
Pszczynska 37, 44-101 Gliwice, Poland
e-mail: aniedworok@komag.eu