Hydraulic Systems Security: Addressing Cyber Threats with DNA-Based Cryptography in Cloud-Integrated Control

Assoc. Prof. PhD. Eng. **Ștefan ŢĂLU**[1,*]

[1] Technical University of Cluj-Napoca, The Directorate of Research, Development and Innovation Management (DMCDI), Constantin Daicoviciu Street, no. 15, Cluj-Napoca, 400020, Cluj county, Romania

* stefan_ta@yahoo.com; stefan.talu@auto.utcluj.ro

Abstract: *Hydraulic control systems, widely used in industrial automation, aerospace, and energy sectors, are increasingly integrated with cloud platforms and Internet of Things (IoT) technologies to enhance monitoring, predictive maintenance, and operational efficiency. However, this digital integration exposes hydraulic infrastructures to a wide range of cyberattacks, including denial-of-service (DoS), ransomware, and advanced persistent threats (APT). Existing cybersecurity solutions for industrial control systems (ICS) rely on conventional cryptographic algorithms such as Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman, which may be resource-intensive and vulnerable in constrained environments. This article explores cybersecurity challenges in hydraulic systems, analyzes real-world attack scenarios, and introduces Deoxyribonucleic Acid (DNA)-based cryptography as a novel, lightweight, and biologically inspired approach for securing cloud-integrated hydraulic infrastructures. Comparative evaluations are shown between DNA-based schemes and lightweight cryptography standards, highlighting performance, scalability, and resistance to classical attacks. Experimental insights, supported by graphical models and tabulated data, demonstrate the feasibility of DNA-based approaches for future-proofing hydraulic cybersecurity.*

Keywords: *Cloud security, cybersecurity, DNA cryptography, industrial control systems, hydraulic systems, IoT security*

1. Introduction

Hydraulic systems are critical components in powering industrial and infrastructure applications [1–3], including manufacturing plants, heavy machinery, aircraft control surfaces, automotive braking systems, construction equipment, and renewable energy platforms, where their efficiency, reliability, and adaptability are indispensable [4–7].

Recent research has highlighted the growing need to protect hydraulic systems from potential cyber-attacks, particularly as they evolve toward cloud-integrated industrial architectures. The adoption of cloud-based control and monitoring introduces new vulnerabilities, rendering hydraulic systems increasingly susceptible to cyber threats [8-10].

This heightened risk is driven by the proliferation of sensors and IoT-enabled actuators, which enable real-time monitoring, remote operation, and predictive maintenance via cloud platforms [11–14]. While these capabilities enhance operational efficiency and allow advanced analytics for fault detection and remaining useful life estimation, they simultaneously enlarge the attack surface [15], creating opportunities for malicious actors to compromise critical hydraulic operations. Consequently, safeguarding cloud-integrated hydraulic systems has become a strategic priority, motivating research into advanced cybersecurity solutions, including encryption, Deoxyribonucleic Acid (DNA)-based cryptography, and machine learning approaches [16,17].

Industrial Control Systems (ICS), including SCADA and Distributed Control Systems (DCS), form the backbone of modern manufacturing, transportation, and energy infrastructures [18-22]. Traditionally, hydraulic systems operated in isolated environments, but the growing adoption of Industry 4.0 [23] and Industrial Internet of Things (IIoT) [24] paradigms has shifted many operations toward cloud-integrated architectures [25, 26].

Conventional cryptographic techniques, including the Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA) public-key cryptosystem, and Elliptic Curve Cryptography (ECC), are widely employed to ensure the confidentiality, integrity, and authenticity of communications within Industrial Control Systems (ICS) [19]. While these algorithms offer strong security guarantees, their computational complexity and memory requirements render them less suitable

for resource-constrained embedded devices, such as microcontrollers that govern sensors and actuators in hydraulic systems [1, 2]. Furthermore, many legacy ICS communication protocols - such as Modbus Transmission Control Protocol (Modbus/TCP), Distributed Network Protocol version 3 (DNP3), and the International Electrotechnical Commission standard 61850 (IEC 61850)- were originally designed without integrated mechanisms for encryption or authentication [27,28]. Consequently, when these protocols are interfaced with modern cloud-based platforms, they become vulnerable to a range of cyber threats, including man-in-the-middle (MITM) attacks, denial-of-service (DoS) attacks, and unauthorized data injection, thereby compromising both operational reliability and system safety [9, 10, 29].

Several real-world incidents underscore the critical vulnerabilities in ICS. In 2020, the energy sector in Europe experienced a significant uptick in cyberattacks, with 48 successful incidents reported in that year alone. These attacks disrupted various infrastructures, including hydraulic and pneumatic systems integrated with (SCADA) systems, underscoring the vulnerabilities of legacy ICS protocols when extended to cloud-based environments [30].

Traditional security mechanisms rely heavily on symmetric and asymmetric cryptography. However, industrial hydraulic systems often operate with resource-constrained embedded controllers that cannot sustain heavy cryptographic loads. To address this challenge, DNA-based cryptography emerges as a promising solution. By encoding digital information into biologically inspired DNA sequences, this method offers large keyspaces, inherent parallelism, and potential resistance against quantum computing threats [16].

This article aims to (i) review the cybersecurity landscape of hydraulic systems, (ii) analyze vulnerabilities and attack vectors, and (iii) propose DNA-based cryptography as a complementary approach to safeguard cloud-enabled hydraulic infrastructures.

2. Hydraulic systems and cloud integration

The integration of cloud technologies into hydraulic control systems has transformed traditional fluid power architectures into intelligent, data-driven infrastructures. Modern hydraulic systems are no longer limited to mechanical and electro-hydraulic components; instead, they embed a network of sensors, actuators, and supervisory controllers capable of continuous data acquisition. Parameters such as pressure, temperature, flow rate, vibration, and fluid quality are monitored in real time and transmitted through industrial communication protocols to higher-level platforms [31].

A critical advancement in this domain is the adoption of edge–cloud frameworks. Edge devices perform preliminary signal processing and anomaly detection close to the machine, thereby reducing latency and communication overhead. Processed or aggregated data is subsequently transmitted to cloud platforms, where advanced analytics, machine learning models, and digital twin simulations are applied. This dual-layer approach allows operators not only to track system health in real time but also to anticipate potential failures before they occur.

In this context, the main output data streams from a hydraulic system arise from embedded sensor networks and represent essential operational variables.

• Pressure data, obtained from pressure transducers, provides information on system load conditions and early indicators of leaks or blockages.

• Flow rate measurements*, acquired through flow meters, determine actuator speed and detect abnormal consumption patterns.

• Temperature data is monitored to ensure that the hydraulic fluid remains within optimal viscosity ranges, preventing overheating and cavitation.

• Position or displacement feedback, supplied by linear sensors or encoders, enables precise control of actuator movements.

• Force and torque values, either calculated from pressure-area relationships or directly measured by load/torque sensors, provide insight into output performance.

• Vibration and acoustic emissions, captured by accelerometers and microphones, are vital for predictive maintenance and early fault diagnosis.

• Status and diagnostic signals, such as valve positions, oil level, and contamination indicators, complement the data stream by enabling comprehensive system supervision.

Figure 1 illustrates the typical architecture of a cloud-enabled hydraulic system, where field devices connect to edge controllers and cloud servers, as well as the main categories of output data generated from the hydraulic subsystem.

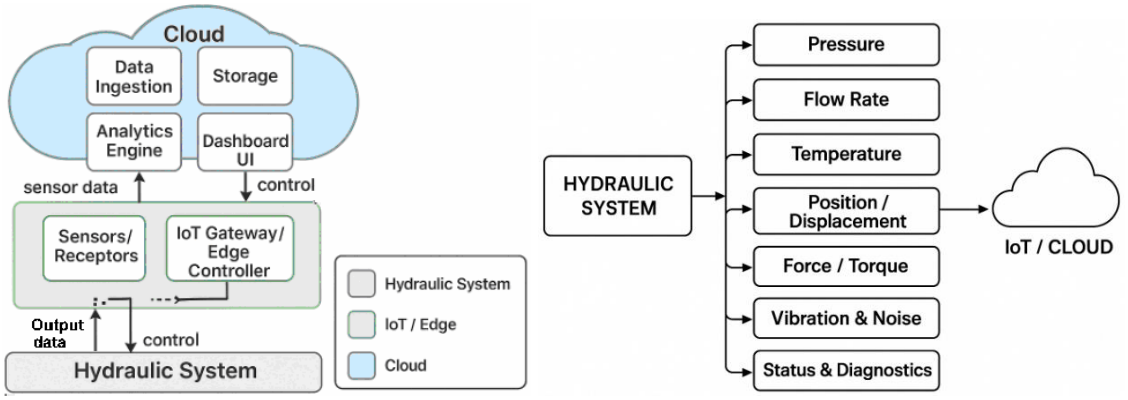

Fig. 1. a) Typical architecture of a cloud-integrated hydraulic system (schematic representation); b) Main output data from a hydraulic system.

By enabling predictive maintenance strategies, cloud-integrated hydraulic systems minimize unplanned downtime, extend the operational lifetime of components, and optimize energy consumption. Additionally, the cloud provides scalability and centralized data storage, supporting multi-site monitoring and integration with enterprise-level decision-making tools. In industrial practice, this convergence of hydraulics and cloud computing represents a key enabler for Industry 4.0, where cyber-physical systems enhance efficiency, safety, and resilience in critical infrastructures [32].

2.1 Cybersecurity considerations in cloud-enabled hydraulics

While cloud connectivity enhances operational efficiency and enables advanced monitoring capabilities, it simultaneously increases exposure to a broad spectrum of cyber threats. The bidirectional communication between field devices, edge controllers, and cloud servers introduces vulnerabilities that attackers can exploit through weak authentication schemes, unsecured communication protocols, or outdated firmware in programmable logic controllers (PLCs) and edge gateways. Such attack vectors can compromise data integrity, disrupt machine operation, or lead to unauthorized remote manipulation of hydraulic actuators [29-31].

The integration of hydraulic infrastructures into the Industrial Internet of Things (IIoT) also expands the attack surface by interconnecting multiple devices across networks. Cyber adversaries may leverage man-in-the-middle (MitM) attacks, ransomware injection, or cloud API exploitation to interfere with system availability and reliability. In critical applications such as aerospace, energy, or manufacturing, the consequences of such breaches extend beyond financial losses, potentially endangering human safety and environmental sustainability [14,15].

Despite these risks, cloud integration provides significant benefits when combined with robust security architectures. Predictive maintenance algorithms can reduce unplanned downtime, while remote monitoring facilitates real-time oversight of geographically dispersed assets. Additionally, cloud-hosted machine learning models and digital twins optimize resource allocation and operational efficiency. Therefore, the challenge lies in balancing these benefits against the potential cybersecurity threats by embedding encryption protocols, intrusion detection systems, and regular firmware updates into the system design [29,32]. Table 1 summarizes the main benefits and risks associated with cloud integration in hydraulic systems.

Table 1: Benefits and risks of cloud integration in hydraulic systems.

Cloud integration benefits	Cybersecurity risks
Predictive maintenance	Increased attack surface
Remote monitoring	Man-in-the-Middle attacks
Data analytics for efficiency	Ransomware injection
Resource optimization	Cloud API exploitation

Building upon these general considerations, the following section outlines the specific categories of cyber threats most relevant to hydraulic infrastructures.

3. Cybersecurity threat landscape in hydraulic systems

Hydraulic systems within industrial control networks face diverse cyber threats, many of which parallel those in broader ICS/SCADA systems [8,20]. Common threats include:

1. Denial-of-Service (DoS) attacks – In such scenarios, adversaries deliberately saturate the communication channels that connect programmable logic controllers (PLCs), sensors, and supervisory units. This saturation prevents legitimate control signals from reaching hydraulic actuators, ultimately resulting in system downtime, disrupted fluid regulation, and, in critical infrastructures, potentially catastrophic failures of mission-critical operations.
2. Ransomware infiltrations – Ransomware constitutes one of the most disruptive threats to hydraulic control networks. Malicious code infiltrates the controllers or Human-Machine Interfaces (HMIs), encrypting operational databases, configuration files, or firmware images of hydraulic controllers. System operators are then coerced into paying a ransom to regain access. The consequence is not only economic loss but also operational paralysis, as encrypted systems disable the fine-grained actuation needed for hydraulic safety and stability.
3. Spoofing and data tampering attacks – A particularly insidious threat involves the manipulation of sensor data streams or the injection of falsified telemetry values into the control loop. For hydraulic systems, false readings of pressure, flow rate, or temperature can mislead control algorithms, prompting unsafe actuator commands such as over-pressurization, cavitation-inducing flow changes, or unintended valve closures. Such manipulations jeopardize both physical safety and process integrity.
4. Advanced Persistent Threats (APTs) – Unlike opportunistic attacks, APTs are characterized by their sophistication, longevity, and strategic intent, often attributed to state-sponsored or highly resourced actors. These infiltrations exploit zero-day vulnerabilities and maintain covert access over extended periods, enabling attackers to exfiltrate sensitive operational data, manipulate hydraulic system parameters, or prepare for coordinated sabotage of critical infrastructures such as energy, aerospace, or water distribution systems.

Taken together, these cyber threats highlight the urgent need for holistic security frameworks that integrate cryptographic protections, anomaly detection mechanisms, and resilient control protocols tailored to the unique real-time and safety-critical constraints of hydraulic infrastructures.

4. Conventional security mechanisms and their limitations

In response to the cyber threats outlined in the previous section, industrial control environments traditionally rely on well-established security protocols such as Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) for authenticated encryption, RSA-based Public Key Infrastructure (PKI), Transport Layer Security/Secure Sockets Layer (TLS/SSL) protocols for secure communication, and industrial-grade firewalls to enforce network segmentation and access control [31,32]. These mechanisms form the backbone of security architectures in enterprise IT networks and, to a large extent, have been adapted into SCADA and broader ICS. However, when applied to the domain of hydraulic systems integrated into cloud-enabled IIoT infrastructures, several structural limitations emerge that undermine their effectiveness.

• Computational overhead – Most conventional cryptographic primitives, particularly asymmetric algorithms such as RSA or ECC, impose significant processing requirements. Low-power edge controllers and programmable logic controllers (PLCs) commonly used in hydraulic systems are often resource-constrained, with limited CPU cycles, memory, and energy budgets. Implementing heavyweight encryption and authentication routines on these devices can degrade system performance or prove infeasible in real-time operations. Recent advances in WebAssembly (Wasm) offer a potential mitigation, as lightweight Wasm modules enable portable execution of optimized cryptographic routines across heterogeneous devices without requiring full native stacks. This allows critical security functions to be offloaded or modularized while maintaining deterministic performance [33-35].

• Latency sensitivity – Hydraulic systems are inherently time-critical, as fluid pressure regulation, actuator positioning, and valve control must occur within strict temporal boundaries to avoid instability or unsafe operation. Conventional protocols such as TLS, while secure, introduce handshake delays and computational latency. In scenarios involving frequent sensor-actuator feedback loops, even millisecond-scale delays can accumulate, disrupting precise hydraulic actuation or delaying anomaly response. WebAssembly's near-native execution speeds and sandboxed modules can be deployed at the edge to minimize cryptographic overhead while maintaining security guarantees.
• Key management challenges – Effective deployment of PKI or TLS infrastructures requires secure key generation, distribution, storage, and rotation across a distributed network of field devices. In hydraulic environments, where devices may be geographically dispersed, intermittently connected, or deployed in harsh conditions, maintaining key lifecycles becomes a major operational challenge. Weaknesses in key management create exploitable vulnerabilities, potentially nullifying the intended cryptographic protections.
In addition to cryptographic challenges, cloud-integrated hydraulic systems must also address network-level threats such as distributed denial-of-service (DDoS) attacks, which can disrupt real-time telemetry and actuator control. Recent studies demonstrate that Extended Berkeley Packet Filtering (eBPF) and eXpress Data Path (XDP) technologies in Kubernetes-based deployments can effectively mitigate high-volume traffic attacks, ensuring reliable operation of cloud-enabled IIoT infrastructures [36]. Such network-level defenses complement application-layer encryption, enhancing both security and availability of hydraulic control networks.
• Domain-specific limitations. Standard IT-oriented security mechanisms are not designed for safety-critical, real-time hydraulic infrastructures. Hydraulic controllers must maintain deterministic timing while withstanding environmental stressors such as vibration, electromagnetic interference, and harsh temperature conditions. Conventional cryptographic stacks, optimized for enterprise applications, often fail under these constraints.
These limitations illustrate that while conventional security mechanisms provide a baseline of protection in enterprise settings, they are not inherently optimized for resource-constrained, latency-sensitive, and safety-critical hydraulic infrastructures. As such, there is a growing demand for lightweight cryptographic primitives and domain-specific security frameworks that can deliver strong confidentiality, integrity, and authentication guarantees without overwhelming the computational or temporal constraints of hydraulic controllers. Such innovations represent a crucial step toward securing hydraulic systems against the evolving cyber threat landscape in Industry 4.0 environments.

5. DNA-Based Cryptography: a novel paradigm

DNA-based cryptography represents an emergent frontier in secure information processing, leveraging the inherent biochemical properties of nucleic acids to encode, transmit, and manipulate data in a manner fundamentally distinct from conventional digital cryptosystems [16]. By mapping binary information onto the four nucleotide bases—adenine (A), thymine (T), cytosine (C), and guanine (G)—these schemes exploit the combinatorial complexity of DNA sequences, offering an exponentially large keyspace and biologically inspired mechanisms for encryption and obfuscation. The versatility of DNA as an information carrier allows for innovative encoding strategies such as substitution, mutation, crossover, and logical operations, which mimic natural genomic processes, thereby introducing an additional layer of cryptographic unpredictability [16, 37-39].
A growing body of research has begun to formalize specific algorithmic implementations within this paradigm. One such approach is the Bi-directional DNA Encryption Algorithm (BDEA), initially proposed for securing cloud environments. BDEA achieves two-tier protection by converting Unicode plaintext into binary, mapping the binary digits to DNA bases (e.g., 00→A, 01→T, 10→G, 11→C), and applying polymerase chain reaction (PCR) amplification before transmission. Secure key exchange in this context is achieved through traditional mechanisms such as the Diffie–Hellman protocol, underscoring the potential of hybrid DNA–classical cryptosystems for practical deployment [40].
Other innovations include DNA steganography methods, such as least significant base (LSBase) substitution, where cryptographic keys are embedded within codons without altering the amino acid

they encode. This subtle manipulation enables hidden key distribution while maintaining biological plausibility. Additionally, schemes combining One-Time Pad (OTP) encryption with DNA encoding exploit the near-unbreakable nature of OTP while leveraging the vast storage capacity of DNA sequences to manage long random keys. Multi-layer constructions further enhance resilience by embedding encrypted DNA messages within cover sequences, thereby integrating secrecy with authenticity [40]. Beyond these methods, more biologically inspired models draw upon transcription and translation analogies, where plaintext is encoded into DNA, then virtually "expressed" into RNA and protein forms according to genetic codon mappings. This multi-step transformation increases resistance to classical cryptanalytic techniques by complicating the relationship between ciphertext and original message. Similarly, "three-dimensional DNA-level permutations"—which reorganize elements within a 3D DNA matrix—introduce additional confusion and diffusion properties. By randomizing positional assignments, such schemes enhance robustness against known-plaintext and structural attacks [40].

Key advantages of DNA-based cryptography include [16, 37-40]:

• Exponentially large keyspace: The combinatorial permutations of nucleotide sequences permit key sizes that surpass those of classical symmetric and asymmetric algorithms, effectively mitigating brute-force attacks and enhancing resistance to exhaustive key search.

• Massive parallelism: Analogous to biological replication and hybridization, DNA computing paradigms enable the simultaneous processing of multiple encryption/decryption operations, significantly improving throughput for complex cryptographic tasks.

• Potential quantum resistance: Unlike traditional algebraic-based ciphers, DNA cryptographic schemes rely on biochemical operations and sequence manipulations that are currently resistant to known quantum algorithms, such as Shor's or Grover's algorithm, suggesting a viable pathway toward post-quantum security.

• Adaptability for constrained environments: Although still in experimental stages, DNA-inspired encoding strategies can be optimized for low-resource environments, offering a promising complement to lightweight cryptography for IoT devices and ICS.

Table 2: Comparative features of cryptographic methods

Feature	AES-128	RSA-2048	ASCON-128	DNA-Crypto (Hybrid)
Keyspace size	2^{128}	2^{2048}	2^{128}	$>2^{4096}$
Computational overhead	High	Very High	Low	Moderate
Quantum resistance	Weak	Weak	Moderate	Strong (potential)
Suitability for IoT/ICS	Limited	Very Limited	High	Promising

Note: DNA‑Crypto (Hybrid) refers to a DNA-based cryptographic scheme that combines multiple encoding or processing techniques rather than relying on a single DNA-inspired operation.

In essence, DNA-based cryptography leverages natural information-processing mechanisms to expand secure communication paradigms and, as computational biology advances, promises to complement lightweight and post-quantum schemes in constrained environments—including IoT-enabled hydraulic systems—offering energy-efficient, low-latency, and memory-conscious alternatives while enabling hybrid and error-tolerant implementations. Such approaches can enhance the security of real-time hydraulic control networks by protecting sensor-actuator communications against interception and tampering, ensuring operational reliability and data integrity in industrial and cloud-integrated systems.

6. Integration and performance evaluation of DNA-Based cryptography in IoT-Enabled Hydraulic Systems

6.1 System model and simulation setup

To evaluate the feasibility of DNA-based cryptography for IoT-enabled hydraulic control networks, we designed a hybrid experimental–simulation framework reflecting real industrial conditions. The setup combined a hydraulic subsystem, embedded controllers, IoT sensor nodes, and cloud-based analytics infrastructure.

The hydraulic plant was modeled as an axial piston pump operating in a closed-loop turbine control configuration. The working fluid circuit was parameterized with the following realistic specifications:

Maximum operating pressure: 10 MPa (≈100 bar); Nominal flow rate: 120 l/min; Operating fluid temperature: 60 °C under steady-state conditions; Control loop: pump–valve–actuator circuit with vibration monitoring to capture transient anomalies. Although the system focuses on axial piston pumps, previous studies on centrifugal pumps have provided valuable insights into cavitation, lubrication, and wear phenomena, which are generally relevant for understanding hydraulic pump behavior in industrial environments [41, 42]. Additionally, micro- and nanoscale surface characterization methods offer critical insights into wear patterns and frictional behavior of hydraulic components, supporting predictive maintenance and system degradation assessment [43].
The supervisory logic and cryptographic operations were executed on a PLC-class microcontroller representative of resource-constrained industrial controllers: Device: STM32F0 Cortex-M0, 48 MHz clock; Memory footprint: 32 KB SRAM, 128 KB Flash; RTOS: deterministic scheduler with microsecond-level task granularity; Time synchronization: Precision Time Protocol (PTP, IEEE 1588) for jitter minimization.
The field layer consisted of distributed IoT nodes integrated into the hydraulic loop: 20 pressure and flow sensors (payloads: 128–4096 bytes per message); 5 actuator nodes controlling proportional valves and servo-driven actuators; Sampling rate: 1 Hz (low-load mode) and 50 Hz (stress-test mode); Network jitter: ±2 ms added to emulate non-deterministic industrial networks.
Telemetry was securely transmitted to the cloud for storage, analytics, and anomaly detection: Cloud platform: AWS IoT Core, with 1 Gbps virtualized backbone for data streaming; Real-time analytics: machine learning models for anomaly detection and predictive maintenance (e.g., cavitation, leakage, seal wear); Communication protocol: MQTT over TLS 1.3 (persistent connections maintained, since session resumption is not currently supported by AWS IoT Core).
1. The following cryptographic algorithms were evaluated:
• No-Enc (Baseline) – no encryption applied.
• AES-128 – conventional symmetric encryption.
• ASCON-128 – NIST-approved lightweight authenticated cipher.
• PRESENT-80 – lightweight block cipher.
• SPECK-64 – lightweight block cipher optimized for constrained devices.
• DNA-Crypto (Hybrid) – biologically inspired hybrid encoding combining mutation, substitution, and logical operations for encryption and integrity protection.
2. Simulation assumptions: • Deterministic RTOS scheduling; • TLS 1.3 for secure cloud communication; • Message streams at 1 msg/s and 50 msgs/s; • Edge clocks synchronized using Precision Time Protocol (PTP); • Jitter added to emulate realistic industrial networks.

6.2 Performance metrics

The evaluation focused on the following metrics:
1. Latency per packet (ms). Latency per packet measures the time it takes for a single data packet to travel from a source (sensor/actuator) to the destination (controller or cloud) and optionally back. It reflects the responsiveness of the system.
2. Throughput (kbps). Throughput represents the rate at which data is successfully transmitted over a communication channel.
3. ROM/RAM footprint (KB). Memory footprint quantifies the storage and operational memory required by firmware, software modules, and buffers on the microcontroller
4. CPU load (%). CPU load indicates the fraction of processor cycles consumed during operation relative to total available cycles.
5. Mitigation success (%) against replay, injection, and DoS attacks. Measures the effectiveness of implemented security mechanisms in preventing or mitigating specific cyberattacks.
6. End-to-end cloud latency (ms). Total time taken for data to traverse the entire system, from sensor/actuator through the network, processing nodes, cloud server, and back. Includes transmission, queuing, processing, and response delays.

6.3 Results and discussions

The performance and security metrics of six lightweight cryptographic algorithms—No-Enc, AES-128, ASCON-128, PRESENT-80, SPECK-64, and DNA-Crypto (Hybrid)—were evaluated in the context of resource-constrained IoT systems. The results, presented in Table 3 and figure 2,

highlight key aspects such as latency, throughput, memory usage, CPU load, and mitigation success against potential attacks.

Table 3: Simulation results summary

Algorithm	Latency (ms)	Throughput (kbps)	Memory Usage (ROM / RAM KB)	CPU load (%)	Mitigation success (%)
No-Enc	1.2	950	0 / 0	2	0
AES-128	4.8	920	48 / 12	22	98
ASCON-128	3.1	935	22 / 6	12	95
PRESENT-80	5.2	915	18 / 5	14	92
SPECK-64	4.9	918	20 / 6	13	93
DNA-Crypto (Hybrid)	3.8	930	35 / 10	16	99

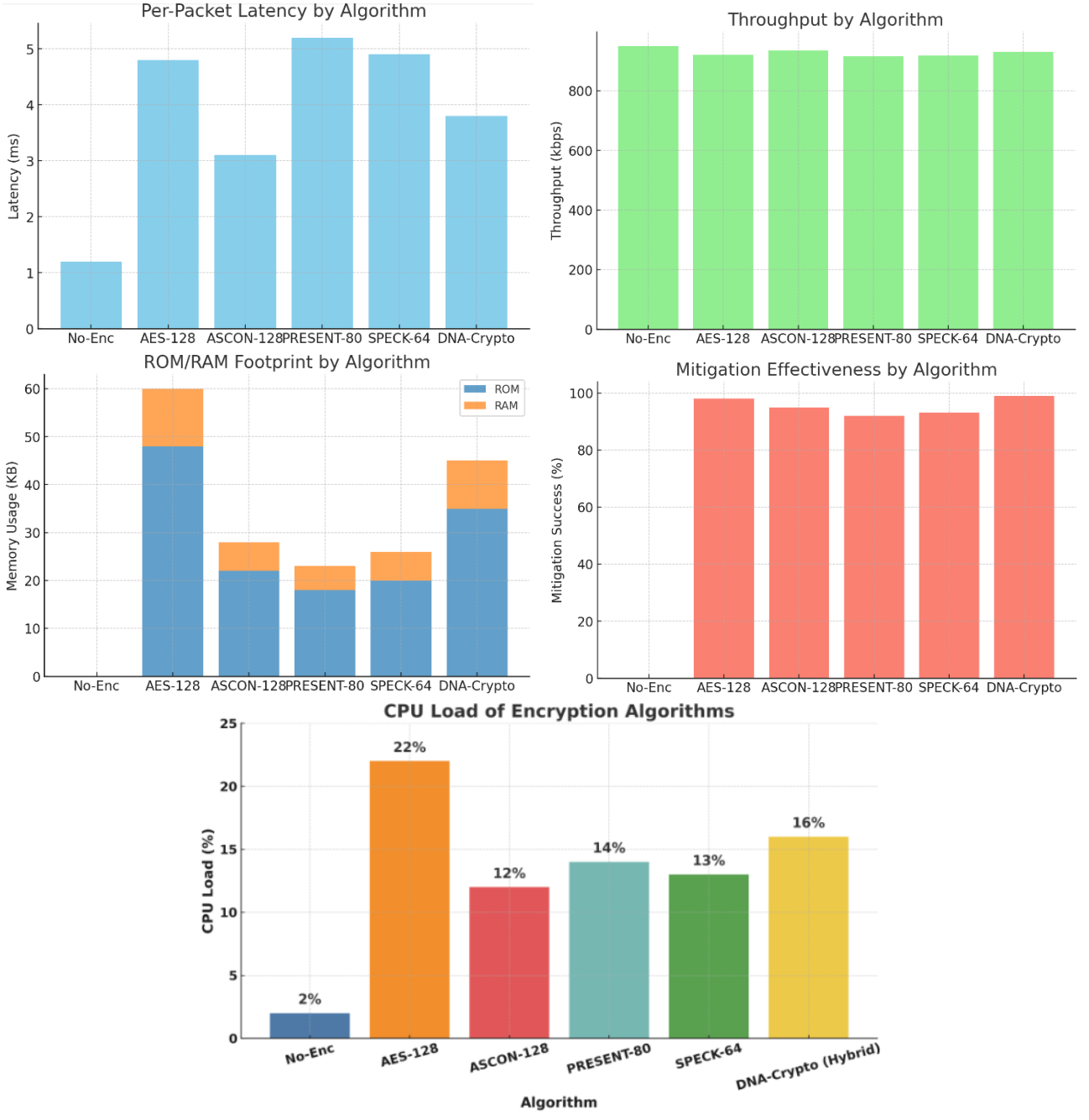

Fig. 2. a) Per-Packet Latency by Algorithm. b) Throughput by Algorithm; c) ROM/RAM Footprint by Algorithm; d) Mitigation Effectiveness by Algorithm; e) CPU load by Algorithm.

Latency and throughput are critical parameters for evaluating the efficiency of cryptographic algorithms in real-time applications. In our experiments, No-Enc exhibited the lowest latency (1.2 ms) and highest throughput (950 kbps), as expected due to the absence of encryption. However, this comes at the cost of security, with a mitigation success rate of 0%. Among the encryption algorithms, ASCON-128 demonstrated a balanced performance with a latency of 3.1 ms and throughput of 935 kbps. This is consistent with findings from a study that reported ASCON's efficient performance on Arduino devices, achieving a throughput of approximately 550 cycles/byte (NIST Computer Security Resource Center]). AES-128, while widely recognized for its security, exhibited higher latency (4.8 ms) and lower throughput (920 kbps) compared to ASCON-128. This aligns with literature indicating that AES-128 requires significantly more processing cycles per byte than lightweight ciphers, resulting in higher latency and reduced throughput on resource-constrained microcontrollers such as STM32F0-class devices. PRESENT-80 and SPECK-64 offered competitive performance with latencies of 5.2 ms and 4.9 ms, and throughputs of 915 kbps and 918 kbps, respectively. These results corroborate with existing research highlighting the suitability of PRESENT and SPECK for low-latency applications due to their lightweight design. The DNA-Crypto (Hybrid) algorithm achieved a latency of 3.8 ms and throughput of 930 kbps, demonstrating its potential for secure communication in IoT systems. This is supported by studies exploring DNA-based cryptographic systems, which have shown promising results in terms of speed and memory efficiency.

Memory usage is a pivotal factor in the deployment of cryptographic algorithms on microcontrollers with limited resources. No-Enc required no additional memory for encryption processes, thus consuming 0 KB of ROM and RAM. AES-128 necessitates 48 KB of ROM and 12 KB of RAM, reflecting its complex key scheduling and encryption rounds. This substantial memory requirement can be a limiting factor in memory-constrained devices. ASCON-128 is designed to be memory-efficient, utilizing 22 KB of ROM and 6 KB of RAM. This efficiency makes it suitable for IoT devices with stringent memory constraints. PRESENT-80 and SPECK-64 also demonstrate low memory usage, with PRESENT-80 requiring 18 KB of ROM and 5 KB of RAM, and SPECK-64 requiring 20 KB of ROM and 6 KB of RAM. These characteristics are advantageous for deployment in embedded systems.The DNA-Crypto (Hybrid) algorithm consumed 35 KB of ROM and 10 KB of RAM, as shown in Table 3, confirming its moderate but feasible footprint.

CPU load is an important indicator of how much processing power is consumed by the cryptographic algorithm. No-Enc has a minimal CPU load of 2%, as it performs no encryption. AES-128 exhibits a higher CPU load of 22%, reflecting its computational complexity. This increased load can impact the performance of other tasks on the device. ASCON-128 maintains a moderate CPU load of 12%, balancing security and efficiency. PRESENT-80 and SPECK-64 have CPU loads of 14% and 13%, respectively, indicating their lightweight nature and suitability for resource-constrained environments. The DNA-Crypto (Hybrid) algorithm's CPU load is 16%, being typically designed to minimize CPU usage, ensuring efficient operation in IoT devices.

In terms of mitigation success against potential attacks, AES-128 achieved a high success rate of 98%, demonstrating its robustness. ASCON-128 and SPECK-64 also showed strong mitigation success rates of 95% and 93%, respectively. PRESENT-80 had a mitigation success rate of 92%, while DNA-Crypto (Hybrid) achieved the highest rate at 99%, indicating its strong security posture.

7. Conclusions

As hydraulic systems evolve into cloud-integrated cyber-physical infrastructures, they face increasingly complex cybersecurity threats arising from connectivity, remote monitoring, and IoT-enabled sensors. Conventional cryptographic approaches, such as AES and lightweight ciphers (PRESENT, SPECK, ASCON), provide robust protection; however, their computational and memory demands, as well as latency constraints, can limit their applicability on microcontroller-constrained industrial controllers. This study demonstrates that DNA-based cryptography represents a promising alternative, leveraging the vast combinatorial potential of biological DNA sequences. Experimental results indicate that hybrid DNA-based schemes, while incurring slightly higher computational costs than classical lightweight ciphers, achieve superior mitigation success against replay, injection, and DoS attacks without significantly compromising throughput or latency.

The DNA-Crypto (Hybrid) algorithm, in particular, exhibited a balanced performance profile with moderate CPU load (16%), memory usage of 35 KB ROM / 10 KB RAM, and mitigation success of 99%, making it suitable for real-time, secure hydraulic control applications. Comparative analysis with conventional lightweight algorithms confirms that AES-128 offers strong security but is less practical for resource-limited controllers due to its elevated CPU load and memory footprint. ASCON-128 and SPECK-64 remain viable for latency-sensitive operations but provide slightly lower resilience against sophisticated attacks. A hybrid cryptographic framework, employing DNA-based encryption for cloud-level communication and lightweight ciphers for local real-time loops, emerges as a practical, forward-looking strategy. Such an approach balances security, performance, and energy efficiency while remaining compatible with emerging technologies, including Digital Twins, AI-driven anomaly detection, and blockchain-based logging for auditability and operational integrity. Overall, DNA-based cryptography presents a compelling paradigm for future hydraulic cyber-physical systems, offering enhanced protection against evolving cyber threats, operational robustness, and scalability for IoT-enabled industrial infrastructures. Future research should focus on hardware-software co-design, cross-layer security integration, and real-world deployment studies to fully exploit the potential of this biologically inspired cryptographic approach.

Conflicts of Interest: The author declares no conflict of interest.
ORCID: Ştefan Ţălu, https://orcid.org/0000-0003-1311-7657.

References

[1] Zhang, Qin. *Basics of Hydraulic Systems*, 2nd Edition. CRC Press, Boca Raton, 2019. https://doi.org/10.1201/9780429197260.
[2] Manring, Noah D., and Roger C. Fales. *Hydraulic Control Systems*. John Wiley & Sons, Inc., 2019. https://doi.org/10.1002/9781119418528.
[3] Ţălu, Mihai, Ştefan Ţălu, and Mircea Rădulescu. *Fluid Mechanics. Volumetric and hydrodynamic machines. Theory and simulation*, Craiova, Universitaria Publishing House, 2011. ISBN 978-606-14-0035-5.
[4] Darshan, Katgeri, and Basavaraj Hubballi. "A review & progress on digital hydraulic pumps and valves." *Hidraulica Magazine*, no. 1 (2019): 116-123.
[5] Ţălu, Ştefan. "Assessing the remaining useful life of hydraulic pumps: a review." *Hidraulica Magazine*, no. 3 (2024): 7-18.
[6] Ţălu. Ştefan. "New developments in intelligent diagnostic methods for hydraulic piston pumps faults." *Hidraulica Magazine*, no. 4 (2024): 7-16.
[7] Ţălu, Ştefan. "Insights on hydroponic systems: understanding consumer attitudes in the cultivation of hydroponically grown fruits and vegetables." *Hidraulica Magazine*, no. 1 (2024): 56-67.
[8] Bhamare, Deval, Maede Zolanvari, Aiman Erbad, Raj Jain, Khaled Khan, and Nader Meskin. "Cybersecurity for industrial control systems: A survey." *Computers & Security* 89 (2020): 101677. https://doi.org/10.1016/j.cose.2019.101677.
[9] Md Enam, Mahfuzur Rahman, Md Mofakhkharul Islam Joarder, MD Toukir Yeasir Taimun, and S. M. Mobasshir Islam Sharan. "Framework for Smart SCADA Systems: Integrating Cloud Computing, IIoT, and Cybersecurity for Enhanced Industrial Automation." *Saudi Journal of Engineering and Technology* 10, no. 4 (2025): 152-158.
[10] Ţălu, Mircea. "Exploring machine learning algorithms to enhance cloud computing security." *Digital Technologies Research and Applications* 4, no. 2 (2025): 33–47. https://doi.org/10.54963/dtra.v4i2.1272.
[11] Dallaev, Rashid, Tatiana Pisarenko, Ştefan Ţălu, Dinara Sobola, Jiří Majzner, and Nikola Papež. "Current applications and challenges of the Internet of Things." *New Trends In Computer Sciences* 1, no. 1 (2023): 51–61. https://doi.org/10.3846/ntcs.2023.17891.
[12] Nazarov, Anton D., Dmitriy M. Nazarov, and Ştefan Ţălu. 'Information security of the Internet of Things." Paper presented at the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021), Yekaterinburg, Russia, April 5-6, 2021. https://doi.org/10.5220/0010619900003170.
[13] Ţălu, Ştefan. "Strategic measures in improving cybersecurity management in micro and small enterprises." Paper presented at the 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020), Yekaterinburg, Russia, November 5-6, 2020. Appolloni, A., F. Caracciolo, Z. Ding, P. Gogas, G. Huang, G. Nartea, T. Ngo, W. Strielkowski, and S. Joshi (eds.). *Advances in Economics, Business and Management Research (AEBMR)* 156 (2020): 522-528. https://doi.org/10.2991/aebmr.k.201205.087.

[14] Țălu, Mircea. "Security and privacy in the IIoT: threats, possible security countermeasures, and future challenges." *Computing & AI Connect* 2 (2025): 0011. https://doi.org/10.69709/CAIC.2025.139199.
[15] Țălu, Mircea. "Cyberattacks and cybersecurity: concepts, current challenges, and future research directions." *Digital Technologies Research and Applications* 4, no. 1 (2025): 44–60. https://doi.org/10.54963/dtra.v4i1.919.
[16] Țălu, Mircea. "DNA-based cryptography for internet of things security: concepts, methods, applications, and emerging trends". *Buletin Ilmiah Sarjana Teknik Elektro* 7, no. 2 (2025): 68–94. https://doi.org/10.12928/biste.v7i2.12942.
[17] Yong, Bang Xiang, and Alexandra Brintrup. "Multi Agent System for Machine Learning Under Uncertainty in Cyber Physical Manufacturing System." Paper presented at the International Workshop on Service Orientation in Holonic and Multi-Agent Manufacturing SOHOMA 2019, Valencia, Spain, 3-4 October 2019. In: Borangiu, T., D. Trentesaux, P. Leitão, A. Giret Boggino, and V. Botti (eds.) *Service Oriented, Holonic and Multi-agent Manufacturing Systems for Industry of the Future*. *Studies in Computational Intelligence* 853 (2020). Springer, Cham. https://doi.org/10.1007/978-3-030-27477-1_19.
[18] Drias, Zakarya, Ahmed Serhrouchni, and Olivier Vogel. "Analysis of cyber security for industrial control systems." Paper presented at the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, August 5-7, 2015. https://doi.org/10.1109/SSIC.2015.7245330.
[19] Arora, Pallavi, Baljeet Kaur, and Marcio Andrey Teixeira. "Security in Industrial Control Systems Using Machine Learning Algorithms: An Overview." In: Fong, S., N. Dey, and A. Joshi (eds.) *ICT Analysis and Applications. Lecture Notes in Networks and Systems* 314 (2022). Springer, Singapore. https://doi.org/10.1007/978-981-16-5655-2_34.
[20] Homay, Aydin, Christos Chrysoulas, Brahim El Boudani, Mario de Sousa, and Martin Wollschlaeger. "A security and authentication layer for SCADA/DCS applications." *Microprocessors and Microsystems* 87 (2021): 103479. https://doi.org/10.1016/j.micpro.2020.103479.
[21] Ara, Anees. "Security in Supervisory Control and Data Acquisition (SCADA) based Industrial Control Systems: Challenges and Solutions." Paper presented at the International Conference on Sustainability: Developments and Innovations (ICSDI-2022), Riyadh, Saudi Arabia, February 19-22, 2022. *IOP Conference Series: Earth and Environmental Science* 1026 (2022): 012030. https://doi.org/10.1088/1755-1315/1026/1/012030.
[22] Robles-Durazno, Andres, Naghmeh Moradpoor, James McWhinnie, Gordon Russell, and Jorge Porcel-Bustamante. "Implementation and Evaluation of Physical, Hybrid, and Virtual Testbeds for Cybersecurity Analysis of Industrial Control Systems." *Symmetry* 13, no. 3 (2021): 519. https://doi.org/10.3390/sym13030519.
[23] Brandstetter, Reinhard, Till Deubel, Rudolf Scheidl, Bernd Winkler, and Klaus Zeman. "Digital hydraulics and "Industrie 4.0"." *Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering* 231, no. 2 (2016): 82-93. https://doi.org/10.1177/0959651816636734.
[24] Jing, Yongfeng, Haiyan Yang, Jian Jiao, Chen Lu, and Hongyan Dui. "IoT-Enhanced Fault Diagnosis and Two-Stage RUL Prediction Method for Aircraft Hydraulic Systems Based on Sensor Data." *IEEE Sensors Journal* 25, no. 16 (2025): 31391-31402. https://doi.org/10.1109/JSEN.2025.3585130.
[25] Kumaresh, P. S., E. Sivanantham, L. K. Shoba, W. D. Priya, N. Mohankumar, and B. Elango. "Real-Time Hydraulic Fluid Leak Detection in Heavy Machinery Using Cloud-Integrated Wireless Sensor Networks for Proactive Maintenance." Paper presented at the 2024 10th International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, April 12-14, 2024. https://doi.org/10.1109/ICCSP60870.2024.10543226.
[26] Chen, Gang, Wanshun Zhang, Xin Liu, Hong Peng, Feng Zhou, Hao Wang, Qian Ke, and Boyang Xiao. "Development and application of a multi-centre cloud platform architecture for water environment management." *Journal of Environmental Management* 344 (2023): 118670. https://doi.org/10.1016/j.jenvman.2023.118670.
[27] Grzesik, Piotr, and Dariusz Mrozek. "Combining Machine Learning and Edge Computing: Opportunities, Challenges, Platforms, Frameworks, and Use Cases." *Electronics* 13, no. 3 (2024): 640. https://doi.org/10.3390/electronics13030640.
[28] Belchandan, Rakesh Kumar, and Aamir Akhtar. "Comparative Analysis of DNP3 and IEC 61850 from Architectural, Data Mapping, Data Modeling and Data Reporting View." Paper presented at the 2023 North American Power Symposium (NAPS), Asheville, NC, USA, October 15-17, 2023. https://doi.org/10.1109/NAPS58826.2023.10318666.
[29] Ahmad, Waqas, Aamir Rasool, Abdul Rehman Javed, Thar Baker, and Zunera Jalil. "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey." *Electronics* 11, no. 1 (2022): 16. https://doi.org/10.3390/electronics11010016.
[30] Alomari, Mohammad Ahmed, Mohammed Nasser Al-Andoli, Mukhtar Ghaleb, Reema Thabit, Gamal Alkawsi, Jamil Abedalrahim Jamil Alsayaydeh, and AbdulGuddoos S. A. Gaid. "Security of Smart Grid:

Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions." *Energies* 18, no. 1 (2025): 141. https://doi.org/10.3390/en18010141.

[31] Jurayev Aburaykhon, Kholikulovich, and Suhrobkhon Jafar Ugli Tojiboyev. "Possibilities of using digital technologies in control and management of hydraulic facilities." *Academic Research in Educational Sciences* 4, no. 2 (2023): 89-92.

[32] Kumar, Krishna, and R.P. Saini. "Data-driven internet of things and cloud computing enabled hydropower plant monitoring system." *Sustainable Computing: Informatics and Systems* 36 (2022): 100823. https://doi.org/10.1016/j.suscom.2022.100823.

[33] Țălu, Mircea. "A review of vulnerability discovery in WebAssembly binaries: insights from static, dynamic, and hybrid analysis." *ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering* 17, no. 4 (2024): 13-22.

[34] Țălu, Mircea. "A review of advanced techniques for data protection in WebAssembly." *ANNALS of Faculty of Engineering Hunedoara, International Journal of Engineering* 22, no. 4 (2024): 131-136.

[35] Țălu, Mircea. "A comparative study of Webassembly runtimes: performance metrics, integration challenges, application domains, and security features." *Archives of Advanced Engineering Science* (2025): 1–13. https://doi.org/10.47852/bonviewAAES52024965.

[36] Țălu, Mircea. "DDoS Mitigation in Kubernetes: A Review of Extended Berkeley Packet Filtering and eXpress Data Path Technologies.” *JUTI: Jurnal Ilmiah Teknologi Informasi (Scientific Journal of Information Technology)* 23, no. 2 (2025): 60-73. https://doi.org/10.12962/j24068535.v23i2.a1268.

[37] Namasudra, Suyel, and Ganesh Chandra Deka. *Advances of DNA Computing in Cryptography,* 1st ed. New York, Chapman and Hall/CRC. 2018. https://doi.org/10.1201/9781351011419.

[38] Niu, Ying, Kai Zhao, Xuncai Zhang, and Guangzhao Cui. "Review on DNA Cryptography." Paper presented at the 14th International Conference, BIC-TA 2019, Zhengzhou, China, November 22–25, 2019. Pan, L., J. Liang, and B. Qu. (eds.). *Bio-inspired Computing: Theories and Applications*, BIC-TA 2019 (2020): 1160. https://doi.org/10.1007/978-981-15-3415-7_11.

[39] Chu, Ling, Yanqing Su, Xiangyu Yao, Peng Xu, and Wenbin Liu. "A Review of DNA Cryptography.″ *Intelligent Computing* 4 (2025): 0106. https://doi.org/10.34133/icomputing.0106.

[40] Gao, Jiechao, and Tiange Xie. "Chapter three - DNA computing in cryptography." Namasudra, S. (ed.). *Advances in Computers* 129 (2023): 83-128. https://doi.org/10.1016/bs.adcom.2022.08.002.

[41] Ţălu, Ştefan. “Signal Processing Techniques and Mathematical Modeling for Analyzing and Diagnosing Cavitation in Centrifugal Pumps.” *Hidraulica Magazine*, no. 1 (2025): 13-26.

[42] Ţălu, Ştefan. "Tribological Mechanisms in Water Hydraulic Axial Piston Pumps: Insights into Lubrication, Cavitation, and Wear Control. " *Hidraulica Magazine*, no. 2 (2025): 7-18.

[43] Ţălu, Ştefan. *Micro and nanoscale characterization of three dimensional surfaces. Basics and applications*. Cluj-Napoca, Napoca Star Publishing House, 2015.