Adaptive Multi-Criteria Model for Selecting Lightweight Cryptographic Components for Cyber-Physical Systems

Nataliya Maslova[1,2,*,†], Orest Polotai[1,†], Yevhen Siedin[1,†] and Andriy Ivanusa[1,†]

[1]*Lviv State University of Life Safety, 35 Kleparivska St., Lviv, 79007, Ukraine*
[2]*Donetsk National Technical University, 76 Sambirska St., Drohobych, Lviv region, 82100, Ukraine*

Abstract

Cyber-Physical Systems (CPS) integrate heterogeneous embedded devices that differ in computational capabilities, resource constraints, timing requirements, and information security demands. Under such conditions, selecting lightweight cryptographic components solely on the basis of cryptographic strength or performance does not ensure their effective use across all CPS segments. This study aims to improve the reliability of selecting lightweight cryptographic components for Cyber-Physical Systems by developing an adaptive multi-criteria evaluation model. The proposed approach formalizes typical information interaction scenarios, defines a system of evaluation criteria with scenario-dependent weighting coefficients, and introduces an algorithm for the integrated evaluation and ranking of cryptographic components. The model was experimentally validated using ASCON-128, GIFT-COFB, TinyJambu-128, and Xoodyak based on official NIST Lightweight Cryptography benchmarking results, the FELICS, FELICS-AEAD, and eBACS evaluation frameworks, and published implementation studies. The results demonstrate that the optimal cryptographic component depends on the information interaction scenario and the functional role of the corresponding CPS segment. TinyJambu-128 achieved the best performance for resource-constrained sensor nodes, whereas ASCON-128 obtained the highest integrated scores in scenarios with stringent performance, security, and implementation security requirements. The scientific contribution of this work is a scenario-oriented adaptive multi-criteria evaluation model that integrates information security requirements with resource, timing, and implementation characteristics into a unified decision-making framework. The proposed approach can be applied to the design and modernization of Cyber-Physical Systems, industrial automation systems, Internet of Things (IoT) infrastructures, and critical infrastructure facilities.

Keywords

Cyber-Physical Systems, lightweight cryptography, cryptographic components, authenticated encryption, multi-criteria evaluation, adaptive selection, information security

1. Introduction

Cyber-Physical Systems (CPS) integrate computational and communication components with physical processes through sensors, gateways, controllers, and actuators. They are widely deployed in industrial automation, energy systems, transportation, healthcare, robotics, and civil protection applications. Since the outcomes of digital data processing directly affect the state of physical objects, security breaches in CPS may result not only in information compromise but also in incorrect execution of control commands, disruption of technological processes, and threats to human safety.

Cryptographic components provide confidentiality, integrity, and authenticity of information exchange between CPS nodes while protecting communications against message forgery and replay attacks. However, their deployment introduces additional computational, memory, and energy overhead and may increase data processing latency. In Cyber-Physical Systems, these characteristics are of critical importance because delayed message delivery or authentication may adversely affect the execution of physical processes.

UkrCrypto2026: International Conference on Cryptographic Information Security, September 23–25, 2026, Kyiv, Ukraine
*Corresponding author.
†These authors contributed equally.
masgpp@gmail.com (Nataliya Maslova); orest.polotaj@gmail.com (Orest Polotai); ye.sedin@ldubgd.edu.ua (Yevhen Siedin); ivaaanusa@gmail.com (Andriy Ivanusa)
0000-0002-9078-0973 (Nataliya Maslova); 0000-0003-4593-8601 (Orest Polotai); 0009-0004-9654-0577 (Yevhen Siedin); 0000-0001-9141-8039 (Andriy Ivanusa)
© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

A considerable proportion of CPS nodes is implemented on resource-constrained microcontrollers and embedded platforms. This necessitates the use of lightweight cryptographic algorithms optimized with respect to program code size, memory consumption, computational complexity, energy efficiency, and hardware implementation cost. Nevertheless, improvements in resource efficiency should not come at the expense of an unacceptable reduction in the security level of the cryptographic component.

The requirements imposed on cryptographic components depend on their functional role within the CPS architecture. Different information interaction channels prioritize confidentiality, integrity, and authenticity differently and are characterized by distinct latency constraints, available computational resources, and potential consequences of security compromise. Consequently, a cryptographic algorithm or implementation that is suitable for one segment of a system may not satisfy the requirements of another.

Traditional assessments of cryptographic strength are primarily based on key length, cryptographic design characteristics, and the computational complexity of the best-known attacks. However, these metrics do not fully characterize the suitability of a particular cryptographic component for CPS, as they fail to simultaneously account for implementation security, resource consumption, timing characteristics, and deployment conditions. Likewise, evaluation based solely on performance or resource efficiency cannot guarantee an adequate level of security.

These considerations highlight the need for a comprehensive evaluation of lightweight cryptographic components that jointly considers their theoretical cryptographic strength, implementation security, resource efficiency, and compliance with the functional and timing requirements of Cyber-Physical Systems. Since the relative importance of individual characteristics depends on the application scenario, an adaptive approach is required in which evaluation criteria and their corresponding weights are determined according to the functional role of the device, available resources, the threat model, and the criticality of the underlying physical process.

The objective of this study is to improve the reliability of selecting lightweight cryptographic components for Cyber-Physical Systems by developing a system of evaluation criteria and an adaptive algorithm for their comprehensive assessment that considers the information interaction scenario, security requirements, resource constraints, and acceptable latency.

To achieve this objective, the following tasks are addressed: to determine the role of cryptographic components within the CPS architecture; to characterize typical information interaction scenarios; to define requirements for confidentiality, integrity, authenticity, and latency; to develop a system of evaluation criteria; to demonstrate the limitations of relying solely on cryptanalytic complexity as an evaluation metric; and to develop an adaptive integrated evaluation algorithm.

The following section reviews existing approaches to the evaluation of lightweight cryptographic algorithms and components and identifies the unresolved issues that motivate this research.

2. Related Work and Problem Statement

Contemporary research on the cryptographic protection of Cyber-Physical Systems (CPS) encompasses the theoretical cryptanalysis of lightweight algorithms, the evaluation of software and hardware implementations, investigations of side-channel attacks, the development of secure protocols for resource-constrained devices, and the comparative assessment of cryptographic components in terms of performance. An analysis of these research directions is essential for determining the extent to which existing approaches take into account the deployment context of cryptographic components within different CPS segments.

Cyber-Physical Systems belong to the class of distributed intelligent systems in which computational and communication components are tightly integrated with physical processes, sensors, and actuators. According to the NIST conceptual framework, CPS analysis should simultaneously consider functional properties, trustworthiness, security, timing characteristics, data, system boundaries, and lifecycle aspects [1]. This interdependence implies that cryptographic protection in CPS cannot be evaluated solely as an isolated property of an algorithm, since its implementation directly affects sensor data

transmission, control decision-making, and the execution of physical actions.

One of the key characteristics of CPS is the presence of strict or constrained timing requirements. NIST SP 1500-203 emphasizes that time, synchronization, latency, and the resilience of timing mechanisms constitute independent CPS characteristics that must be considered during requirements specification and system design [2]. Violations of timing consistency, communication delays, or message processing latency may alter the behavior of the control loop even when data confidentiality is preserved. Therefore, cryptographic processing in CPS must not only ensure information security but also operate within the acceptable response time of the corresponding physical process.

The architecture of a typical CPS involves information exchange among heterogeneous nodes that differ significantly in computational capabilities, memory capacity, power supply, functional roles, and levels of physical protection. Sensor nodes primarily perform measurements and transmit relatively small amounts of telemetry data; gateways aggregate information and perform protocol translation; controllers generate control decisions; and actuators directly influence the state of the physical system. This provides a basis for distinguishing three typical information interaction scenarios—sensor–gateway, gateway–controller, and controller–actuator—each of which imposes different requirements on cryptographic protection.

The sensor–gateway channel is characterized by limited computational resources, short messages, battery-powered operation, and periodic or event-driven data transmission. In this scenario, source authentication, measurement integrity, energy consumption, and memory requirements are of primary importance. The gateway–controller channel involves larger data volumes, concurrent servicing of multiple devices, and communication across different network segments. Accordingly, throughput, scalability, node authentication, and protection of aggregated data become the dominant requirements. In the controller–actuator channel, message integrity, source authentication, command freshness, and predictable low latency are of highest priority, since message forgery or delayed delivery may directly result in hazardous physical actions.

IETF documents addressing constrained-node networks emphasize that such devices possess severe limitations in processing power, memory, and energy resources. At the same time, they are often deployed in physically unprotected environments, increasing the risk of direct attacker access to the device, cryptographic keys, and hardware implementations of cryptographic mechanisms [3]. Consequently, selecting an efficient yet cryptographically secure algorithm should be complemented by evaluating credential protection, support for cryptographic updates, and resilience against physical attacks.

These limitations have driven the development of lightweight cryptography, intended for devices in which conventional cryptographic mechanisms may be impractical because of insufficient computational performance, limited memory, or energy constraints. Lightweight algorithms optimize transformation structures, internal state size, the number of operations, program code size, and hardware implementation complexity. Importantly, lightweight design does not imply reduced cryptographic strength but rather seeks an appropriate balance between security and resource efficiency.

A systematic review of lightweight symmetric algorithms conducted by V. Thakor, M. Razzaque, and M. Khandaker examined 41 cryptographic algorithms and compared them in terms of block and key length, memory usage, throughput, energy consumption, and other operational characteristics [4]. Their study demonstrated that the suitability of an algorithm for resource-constrained devices cannot be determined solely by key length or the type of cryptographic primitive. Instead, performance depends on the hardware platform, software implementation, message size, and operating mode.

In studies of software implementations of lightweight ciphers, the primary evaluation metrics typically include processor cycle count, execution time, throughput, program code size, RAM consumption, and energy usage. In particular, studies based on the FELICS framework evaluate implementations using RAM size, ROM size, and cryptographic execution time [5, 6]. Other studies complement these metrics with the number of processed blocks or frames, encryption time for messages of different lengths, and microcontroller energy consumption [7].

For hardware implementations, commonly used evaluation metrics include circuit area measured in logic elements or gate equivalents (GE), maximum operating frequency, throughput, latency, power

consumption, and the throughput-to-area ratio. However, hardware evaluation results strongly depend on the manufacturing technology, target platform, implementation architecture, and applied countermeasures. Therefore, direct comparison of results obtained on different FPGA, ASIC, or microcontroller platforms is not always meaningful without appropriate normalization.

The NIST Lightweight Cryptography competition marked an important stage in the development of lightweight cryptography. During the final round, ten authenticated encryption and hashing algorithms were evaluated, with the selection criteria including not only theoretical cryptographic strength but also the efficiency of software and hardware implementations, flexibility, ease of use, and suitability for protecting information in constrained environments [8]. In 2023, NIST selected the ASCON family for standardization, and in August 2025, NIST SP 800-232 was published, specifying Ascon-AEAD128, Ascon-Hash256, Ascon-XOF128, and Ascon-CXOF128 [9]. The design principles of the ASCON family, its authenticated encryption and hashing modes, and the rationale behind the balance between cryptographic strength and implementation efficiency are examined in detail in the foundational work of its developers [10].

The selection of ASCON confirmed the relevance of a comprehensive analysis of lightweight cryptographic components. In NIST IR 8454, security was considered together with performance across different platforms, memory requirements, hardware efficiency, ease of secure implementation, and the available security margin [8]. At the same time, the standardization of an algorithm does not automatically guarantee the security of every implementation, since the security of a specific cryptographic component depends on implementation decisions and the countermeasures applied against physical attacks.

This conclusion is supported by studies of secure ASCON implementations. A. Kandi et al. proposed hardware implementations incorporating countermeasures against side-channel attacks and fault injection and demonstrated that the introduction of such countermeasures affects the circuit area, performance, and resource characteristics of the component [11]. B. Gigerl et al. investigated masked software implementations of ASCON designed to protect against second-order power analysis [12]. Thus, the cryptographic strength of an algorithm and the security of its implementation are related but not identical characteristics.

Comparative experimental studies of AES, SPECK, ASCON, and other lightweight algorithms also demonstrate that the relative advantage of a particular algorithm depends on the selected criterion. An algorithm may require less execution time but consume more energy, use less memory but provide lower throughput, or demonstrate better software performance while requiring a more complex secure hardware implementation. Therefore, one-dimensional ranking does not provide a sufficiently justified basis for selecting a cryptographic component across all device types and CPS scenarios.

A separate research direction focuses on evaluating cryptographic strength on the basis of the complexity of specialized attacks that exploit the structural properties of cryptographic transformations. In [13], a linear-algebraic analysis of a Rijndael-like cipher using round differentials was proposed. The obtained results demonstrate that an assessment based solely on the size of the key space may be overestimated if the differential, linear, and algebraic properties of the algorithm are not taken into account.

Studies [14, 15] investigated the acceleration of exponentiation in Galois fields on multicore processor and microcontroller platforms. The proposed methods demonstrate the possibility of reducing the execution time of cryptographic operations through computational decomposition, parallelization, and precomputation. These results confirm the need to include latency, scalability, and compatibility with the architecture of the target device among the evaluation criteria.

The efficiency of a cryptographic component also depends on the complexity of the basic algebraic operations used in its structure. In [16], a fast algorithm for factoring a polynomial over a finite Galois field without constructing the entire field was proposed, together with its sequential and parallel implementations. Comparison with the standard linear method demonstrated the possibility of substantially reducing computational complexity. This indicates that the evaluation of a cryptographic component should take into account not only the general structure of the algorithm but also the implementation efficiency of its basic operations on the target platform.

The reviewed studies advance methods for assessing cryptanalytic complexity and accelerating the basic operations of cryptographic algorithms. However, theoretical security and computational efficiency are generally analyzed separately and without considering the functional role of the component within the CPS architecture.

Another group of studies concerns secure network protocols for IoT and constrained environments. RFC 7925 defines TLS/DTLS profiles for devices that collect sensor data or control actuators. The use of such protocols enables confidentiality, integrity, and protection against message forgery [17]. However, the protocol layer does not eliminate the need to select cryptographic primitives in accordance with the resource and timing constraints of individual nodes. Moreover, the overhead associated with session establishment, transmission of service data, and authentication verification may be significant for short messages and time-critical control commands.

The conducted review makes it possible to identify several major directions of contemporary research: investigation of the theoretical resistance of lightweight algorithms to differential, linear, algebraic, and other forms of cryptanalysis; experimental evaluation of the performance, memory usage, energy consumption, and throughput of software implementations; evaluation of the circuit area, operating frequency, latency, and energy efficiency of hardware implementations; analysis of resistance to side-channel attacks and fault injection; development of authentication and secure communication protocols for resource-constrained devices; and comparison of lightweight algorithms according to individual technical characteristics.

At the same time, existing approaches have several limitations.

First, a significant proportion of studies focuses on comparing algorithms or implementations without considering their functional role within the CPS architecture. The obtained results generally do not distinguish between the requirements of the sensor–gateway, gateway–controller, and controller–actuator channels.

Second, confidentiality, integrity, authenticity, replay protection, and acceptable latency are often analyzed separately. Their relative importance is not considered to vary depending on the purpose of the message. For telemetry data, energy consumption and integrity may be decisive, whereas for a control command, authenticity, message freshness, and guaranteed processing time are of greater importance.

Third, the theoretical complexity of the best-known cryptanalytic attack does not fully characterize the actual security of a cryptographic component. It does not account for information leakage through side channels, the possibility of fault injection, protection of cryptographic key material, implementation flaws, physical accessibility of the device, or the availability of hardware protection mechanisms.

Fourth, the use of performance metrics alone is also insufficient. Minimum execution time or low memory consumption does not guarantee the required level of security, while the introduction of additional countermeasures against physical attacks may significantly alter the original characteristics of the implementation.

Fifth, most comparative studies employ a static system of criteria. Criterion weights are either not defined or remain identical for all platforms and scenarios. As a result, an algorithm that achieves the highest overall score may prove unsuitable for a particular CPS segment because of excessive latency, high energy consumption, or insufficient resistance to physical attacks.

Therefore, the problem of context-dependent evaluation of lightweight cryptographic components remains unresolved. Such an evaluation should consider not only their theoretical cryptographic strength and resource efficiency but also the functional role of the component, the type of protected message, device characteristics, the threat model, and the requirements for authenticity, integrity, confidentiality, and acceptable latency.

This problem necessitates the development of an interconnected system of evaluation metrics covering at least four groups of characteristics:

- theoretical cryptographic strength;
- implementation and physical security;
- resource efficiency;

- contextual characteristics related to the CPS architecture and timing requirements.

Since the significance of individual characteristics varies depending on the application scenario, integrated evaluation should be performed using an adaptive algorithm. Such an algorithm should adjust the criterion weights according to the channel type, the functional role of the device, the criticality of the physical process, the available resources, and the adversary model. Unlike a universal static ranking, adaptive evaluation should identify not an abstractly "best" cryptographic algorithm, but the component that most closely satisfies the requirements of a specific segment of a Cyber-Physical System.

Thus, the scientific problem lies in the mismatch between the complex, context-dependent nature of the cryptographic protection requirements of CPS and the predominantly static approaches used to evaluate lightweight cryptographic components. These approaches do not provide simultaneous consideration of theoretical cryptographic strength, implementation security, resource consumption, acceptable latency, and the functional criticality of the protected channel.

3. Typical Information Interaction Scenarios and uirements for CPS Cryptographic Components

3.1. Formal Model of Cyber-Physical System Architecture

Cyber-Physical System is a set of interconnected software, communication, and physical components that continuously exchange information in real time. Unlike traditional information systems, the results of data processing in CPS directly affect physical processes through the control system, which imposes increased requirements on the reliability, timeliness, and security of information interaction.

In the general case, the CPS architecture can be represented as a directed graph

$$F = (V, Q)\,, \tag{1}$$

where

$V = \{v_1, v_2, \ldots, v_n\}$ denotes the set of system nodes;

Q denotes the set of directed information communication channels between the nodes.

According to their functional roles, the set of nodes V is partitioned into four pairwise disjoint subsets: sensor nodes (S), gateways (G), controllers (C), and actuators (A), such that $V = S \cup G \cup C \cup A$, $S \cap G = S \cap C = S \cap A = G \cap C = G \cap A = C \cap A = \varnothing$.

Each group of nodes performs a specific function within the overall control cycle. Sensor nodes measure physical parameters of the environment, such as temperature, pressure, speed, or substance concentration, and generate primary information messages. Gateways provide data aggregation, protocol conversion, and information routing between local networks and external information systems. Controllers process the received information, perform computational algorithms, and make decisions concerning the generation of control commands. Actuators implement physical actions on the controlled object by changing its state.

Within the generalized architecture adopted in this work, the typical CPS control cycle is represented by the sequence $S \to G \to C \to A$.

Each information communication channel is characterized by specific cryptographic protection requirements determined not only by the type of transmitted messages but also by its functional purpose, the resources available at the communicating nodes, and the permissible timing constraints.

The adopted CPS architecture and the corresponding information interaction channels are illustrated in Fig. 1.

As shown in Fig. 1, information interaction in a CPS takes place sequentially among sensor nodes, gateways, controllers, and actuators. Each channel (q_i) is characterized by the message type, resource constraints, timing characteristics, and threat model, which determine the requirements for the corresponding cryptographic component.

To formalize these differences, each channel is described by a set of parameters

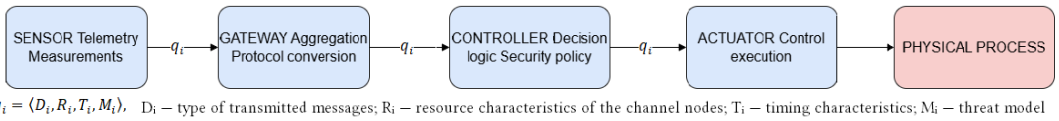


Figure 1: Formal Model of Information Interaction and Cryptographic Components in CPS

$$q_i = (D_i, R_i, T_i, M_i), \qquad q_i \in Q, \tag{2}$$

where
D_i denotes the type of transmitted messages;
R_i denotes the resource characteristics of the channel nodes;
T_i denotes the timing characteristics;
M_i denotes the model of potential threats.
The message type is defined as

$$D_i = (D_t, D_c, D_s), \tag{3}$$

where
D_t denotes telemetry data;
D_c denotes control commands;
D_s denotes service messages, including authentication, synchronization, and other service information.

The resource characteristics of the nodes describe the available computational resources:

$$R_i = (CPU_i, RAM_i, ROM_i, E_i), \tag{4}$$

where
CPU_i denotes processor performance;
RAM_i denotes available random-access memory;
ROM_i denotes available non-volatile memory;
E_i denotes available energy resources.
The timing characteristics are defined by the maximum allowable delay:

$$T_i \leq T_i^{\max}, \tag{5}$$

the violation of which may disrupt the operation of the control system or result in the loss of information relevance.

The threat model

$$M_i = \{m_1, m_2, \ldots, m_k\}, \tag{6}$$

defines the set of potential attacks relevant to a particular information interaction channel. This set may include attacks against information confidentiality, message modification, packet replay attacks, side-channel attacks, fault injection, compromise of cryptographic key material, and physical access to the device.

The proposed model differs fundamentally from the traditional representation of a cryptographic algorithm as an isolated mathematical transformation. In this study, a cryptographic component is considered an element of a specific information channel whose characteristics determine the uirements for cryptographic strength, resource efficiency, and acceptable latency.

Therefore, further evaluation is performed not for an algorithm in general, but for its use within a specific information interaction scenario. This approach provides a basis for developing an adaptive system of evaluation criteria in which the significance of individual criteria is determined by the functional purpose of the channel, the characteristics of the nodes, and the criticality of the physical process.

3.2. Typical Information Interaction Scenarios

The operation of most Cyber-Physical Systems is based on a cyclic process of acquiring information about the state of the physical environment, transmitting the collected data, analyzing it, and generating appropriate control actions. Despite the diversity of CPS architectures, information flows can be generalized into three fundamental interaction scenarios between system components: sensor–gateway, gateway–controller, and controller–actuator. Each of these scenarios is characterized by its own functional purpose, message types, resource constraints, timing requirements, and threat model. These differences determine the requirements imposed on the corresponding cryptographic component and should therefore be taken into account during its evaluation.

3.2.1. Sensor–Gateway Scenario

The first scenario describes the transmission of primary information from a sensor node to a gateway:

$$S \rightarrow G.$$

The primary purpose of this communication channel is to deliver telemetry data, measurement results, and event notifications from distributed sensor nodes to the gateway, where preliminary data processing is performed. Typical messages include measurements of temperature, pressure, humidity, position, liquid level, gas concentration, equipment status, and other monitoring data.

A distinguishing characteristic of sensor nodes is the use of microcontrollers with limited computational capability, restricted RAM and ROM capacities, and autonomous power supplies. In most cases, a sensor node is responsible only for data acquisition, preliminary signal processing, and the generation of short information messages. Consequently, cryptographic operations must incur minimal processor time, memory, and energy overhead.

The principal threats associated with this scenario include telemetry data forgery, replay attacks, compromise of authentication keys, and physical access to the sensor node. At the same time, the confidentiality of transmitted information is not always critical, particularly in open environmental or industrial monitoring systems.

Therefore, the primary requirements for the sensor–gateway scenario are source authentication, data integrity, low energy consumption, and minimal memory requirements.

3.2.2. Gateway–Controller Scenario

The second scenario describes the interaction between a gateway and a controller:

$$G \rightarrow C.$$

At this stage, aggregated information received from multiple sensor nodes is transmitted. In addition to telemetry data, the transmitted information may include event logs, service information, authentication messages, configuration parameters, and the results of local analysis.

A gateway generally has significantly greater computational resources than a sensor node, supports multiple network protocols, and performs routing, message format conversion, buffering, and preliminary data filtering. In this scenario, energy constraints become less significant, whereas the performance and throughput requirements imposed on the cryptographic component increase.

The main threats include information interception, unauthorized packet modification, man-in-the-middle attacks, compromise of the gateway node, and disruption of communication channel availability.

Therefore, the cryptographic component should ensure the confidentiality of aggregated data, integrity protection, mutual authentication of the nodes, and sufficient performance under conditions of intensive information exchange.

3.2.3. Controller–Actuator Scenario

The third scenario involves the transmission of control commands from a controller to an actuator:

$$C \rightarrow A.$$

Unlike the previous scenarios, this channel directly affects the physical state of the controlled object. The transmitted messages contain commands to switch equipment on or off, change operating modes, move mechanisms, regulate process parameters, or initiate an emergency shutdown.

Compromise of this channel may lead not only to information security violations but also to physical consequences, including equipment damage, accidents, disruption of technological processes, or threats to human life. Therefore, command source authenticity, command integrity, and timely delivery become the most critical requirements.

This scenario is characterized by strict timing constraints. Even an algorithm with a high level of cryptographic strength cannot be used if the latency introduced by encryption, authentication, or message verification exceeds the acceptable response time of the control system.

Another important characteristic is the high likelihood of physical access to or interference with the equipment, which increases the relevance of side-channel attacks, fault injection, and compromise of cryptographic key material. Accordingly, the cryptographic component should provide not only the cryptographic strength of the algorithm but also the security of its software or hardware implementation.

3.2.4. Comparative Analysis of the Scenarios

The analysis shows that the same cryptographic algorithm may be used in all three scenarios; however, the requirements imposed on its characteristics differ considerably. For sensor nodes, the decisive factors are minimal energy consumption and memory usage. For gateways, performance and scalability are of primary importance, whereas for the control channel, guaranteed latency, command authenticity, and resistance to physical attacks become critical.

These differences are summarized in Table 1.

Table 1
Comparative Characteristics of Typical Information Interaction Scenarios in CPS

Characteristic	S→G	G→C	C→A
Primary message type	Telemetry data	Aggregated data	Control commands
Node computational capability	Low	Medium/High	Medium
Memory constraints	High	Moderate	Moderate
Energy constraints	High	Low	Medium
Acceptable latency	Moderate	Low	Very Low
Criticality of physical consequences	Low	Medium	High
Priority requirements	Integrity, authenticity, energy efficiency	Confidentiality, integrity, performance	Authenticity, integrity, timeliness

Therefore, the selection of a cryptographic component cannot be performed independently of its functional role within the CPS architecture. The same cryptographic algorithm may be optimal for a sensor node but unsuitable for a control channel because of excessive latency or insufficient implementation security. This highlights the need to move beyond the universal evaluation of cryptographic algorithms toward a context-aware approach that takes into account the specific characteristics of each information interaction scenario. Accordingly, the following subsection defines a set of requirements for cryptographic components, which serves as the foundation for the development of the evaluation criteria and the adaptive algorithm for integrated evaluation.

3.3. Formalized Set of Requirements for Cryptographic Components

The selection of a cryptographic component for a Cyber-Physical System is determined not only by the cryptographic strength of the underlying algorithm but also by its ability to provide the required level of information security under the given resource constraints and timing requirements. The analysis of the typical information interaction scenarios presented in Section 3.2 demonstrates that the relative importance of individual requirements depends significantly on the functional role of the information interaction channel. For example, energy efficiency and memory usage are the primary concerns for sensor nodes, whereas processing latency, authenticity, and resistance to physical attacks become critical for the control channel.

To formalize the evaluation process, we define the set of requirements for a cryptographic component associated with an information interaction scenario S_i as

$$Req_i = (Sec_i, Res_i, Tim_i, Phy_i)\,, \tag{7}$$

where
$i = 1, \ldots, l$ is the scenario number, and
Sec_i denotes the information security requirements;
Res_i denotes the computational resource requirements;
Tim_i denotes the timing requirements;
Phy_i denotes the implementation security requirements.

Thus, the requirement set describes not the cryptographic algorithm itself but the criteria that its implementation must satisfy within a specific CPS operating scenario.

The individual groups of requirements are considered below.

Information Security Requirements. The first group comprises the classical information security properties provided by cryptographic mechanisms. Formally, it is defined as

$$Sec_i = \{C, I, At, Fr\}, \tag{8}$$

where
C denotes confidentiality;
I denotes integrity;
At denotes authenticity;
Fr denotes protection against replay attacks (freshness).

Confidentiality prevents unauthorized disclosure of transmitted information. Integrity ensures that any modification of a message can be detected. Authenticity confirms that the message originates from a legitimate node, whereas freshness protects against the reuse of previously transmitted packets.

Resource Requirements. Since most CPS components operate on embedded platforms, the resource characteristics of cryptographic implementations are of particular importance.

The set of resource requirements is defined as

$$Res_i = \{CPU, RAM, ROM, EE\}, \tag{9}$$

where
CPU denotes processor performance, the requirements for which are determined by the computational complexity of the algorithm;
RAM denotes the amount of random-access memory required for the operation of the cryptographic implementation;
ROM denotes the amount of non-volatile memory required to store the program code;
EE denotes energy efficiency of the cryptographic implementation.

For sensor nodes, this group of indicators is often decisive: under otherwise equal conditions, the feasibility of practical application of a cryptographic algorithm is lower for nodes with more limited computational capabilities.

For cyber-physical systems, one of the critical parameters is the timeliness of information processing. The timing requirements can be defined by the set

$$Tim_i = \{Tim_e, Tim_d, Tim_v\}, \tag{10}$$

where
Tim_e denotes encryption time;
Tim_d denotes decryption time;
Tim_v denotes authentication verification time.
For each information interaction scenario, there is a maximum allowable delay

$$Tim_e + Tim_d + Tim_v \leq T_i^{\max}, \tag{11}$$

where
$T_i^{\max}$ denotes the maximum acceptable latency for scenario S_i.
Consequently, even a cryptographically strong algorithm may be unsuitable for practical deployment if the total execution time of the cryptographic operations exceeds the acceptable response time of the control system.
Implementation Security Requirements
A distinctive feature of Cyber-Physical Systems is that many devices are physically accessible, which significantly increases the relevance of attacks targeting cryptographic implementations.
The corresponding set of requirements is defined as

$$Phy_i = \{SCA, FI, KM\}, \tag{12}$$

where
SCA denotes resistance to side-channel attacks;
FI denotes resistance to fault injection;
KM denotes security of cryptographic key storage mechanisms.
For sensor nodes and actuators, this group of requirements is particularly important because an attacker may gain physical access to the equipment.
By combining all groups of characteristics, the integrated requirement set is obtained as

$$Req_i = (C, I, At, Fr, CPU, RAM, ROM, EE, Tim_e, Tim_d, Tim_v, SCA, FI, KM). \tag{13}$$

The proposed requirement set encompasses both the cryptographic properties of the algorithm and the characteristics of its software or hardware implementation (Table 2).
Unlike traditional approaches, in which all requirements are treated as equally important, the proposed model assigns their priorities according to the corresponding information interaction scenario. To this end, a dedicated weighting vector is defined for each requirement set Req_i and, consequently, for each information interaction scenario S_i

$$W_i = (w_{i1}, w_{i2}, \ldots, w_{in}), i \in \{1, \ldots, l\}, \quad l = 3. \tag{14}$$

Each weighting coefficient w_{ik} represents the relative importance of the k-th requirement (evaluation criterion), where $k \in \{1, \ldots, n\}$ and i denotes the scenario index. For use in the mathematical model, the weighting coefficients are normalized as follows:

$$w_{ik} = \frac{p_{ik}}{\sum_{j=1}^{n} p_{ij}}, \tag{15}$$

$$\sum_{k=1}^{n} w_{ik} = 1, \qquad 0 \leq w_{ik} \leq 1, \tag{16}$$

where p_{ik} is the expert-assigned priority level of the k-th requirement for scenario S_i.

Table 2
Formalized Set of Requirements for Cryptographic Components

Group	Requirement	Notation	Evaluation Criterion
Information Security	Confidentiality	C	Cryptographic strength of the algorithm
	Integrity	I	Availability of an integrity verification mechanism
	Authenticity	At	Availability of an authentication mechanism
	Message freshness	Fr	Protection against replay attack
Resource Characteristics	Computational cost	CPU	Number of operations or processor cycles
	RAM usage	RAM	Random-access memory usage (bytes)
	ROM usage	ROM	Program code size (bytes)
	Energy efficiency	EE	Evaluation of the energy efficiency of the cryptographic implementation
Timing Characteristics	Encryption time	$Time$	Average encryption time per message (μs)
	Decryption time	$Timd$	Average decryption time (μs)
	Authentication verification time	$Timv$	Average authentication verification time (μs)
Implementation Security	Resistance to side-channel attacks	SCA	Level of resistance to side-channel attacks
	Resistance to fault injection	FI	Level of resistance to fault injection
	Cryptographic key protection	KM	Security of cryptographic key storage mechanisms

Table 3
Expert-Assigned Priority Levels and Normalized Weighting Coefficients for Different Information Interaction Scenarios

Requirement	$S \to G\, p_{1k}$	$S \to G\, w_{1k}$	$G \to C\, p_{2k}$	$G \to C\, w_{2k}$	$C \to A\, p_{3k}$	$C \to A\, w_{3k}$
Confidentiality	2	0.063	3	0.111	2	0.069
Integrity	3	0.094	3	0.111	3	0.103
Authenticity	3	0.094	3	0.111	3	0.103
Message Freshness	3	0.094	3	0.111	3	0.103
Computational Complexity (CPU)	3	0.094	2	0.074	2	0.069
RAM Usage (RAM)	3	0.094	1	0.037	1	0.034
ROM Usage (ROM)	3	0.094	1	0.037	1	0.034
Energy efficiency (EE)	3	0.094	1	0.037	2	0.069
Timing Characteristics ($Time$,$Timd$,$Timv$)	2	0.063	3	0.111	3	0.103
Resistance to Side-Channel Attacks (SCA)	2	0.063	2	0.074	3	0.103
Resistance to Fault Injection (FI)	2	0.063	2	0.074	3	0.103
Cryptographic Key Protection (KM)	3	0.094	3	0.111	3	0.103
Σ	32	1.000	27	1.000	29	1.000

The expert-assigned priority levels and the corresponding normalized weighting coefficients for each scenario are presented in Table 3.

The expert priorities of the requirements and their corresponding normalized weighting coefficients presented in Table 3 reflect the functional characteristics of the three typical CPS information interaction scenarios. The first scenario prioritizes resource characteristics, the second prioritizes throughput and data protection, and the third prioritizes timing constraints, authenticity, integrity, and implementation security.

3.4. Adaptive Multi-Criteria Evaluation Model and Algorithm

The requirement set Req_i established in Section 3.3 defines the criteria that a cryptographic component must satisfy within a particular information interaction scenario. However, individual component characteristics are measured in different units, have different relative importance, and may conflict with one another. For example, increasing cryptographic strength is often accompanied by longer cryptographic processing time or higher computational resource consumption. Therefore, the evaluation of cryptographic components should be based on an adaptive multi-criteria model that takes into account the characteristics of a specific CPS operating scenario.

Let the set of cryptographic components to be evaluated be defined as

$$K = \{K_r\}, \qquad r \in \{1, 2, \ldots, m\}, \tag{17}$$

where r denotes the index of the cryptographic component.

The characteristics of a cryptographic component corresponding to the defined evaluation criteria may depend not only on the algorithm Alg_r, but also on its implementation $Impl_r$ and the platform $Plat_r$. Therefore, in the general case,

$$K_r = \langle Alg_r,\ Impl_r,\ Plat_r \rangle. \tag{18}$$

Each component K_r is characterized by the vector

$$X_r = (x_{rj}), \qquad j \in \{1, 2, \ldots, n\}, \tag{19}$$

where j denotes the evaluation criterion and x_{rj} is the value of the j-th criterion for the r-th cryptographic component.

Quantitative and qualitative criteria are first represented in numerical form, after which their values are normalized to the interval $[0, 1]$. For qualitative criteria, an ordinal scale from 0 to 3 is used (0 — the property is absent, 1 — basic level, 2 — enhanced level, and 3 — high level).

The normalized scores are relative and are determined within the given set of candidate components. For criteria whose values are to be maximized, the following expression is used:

$$z_{rj} = \frac{x_{rj} - x_j^{\min}}{x_j^{\max} - x_j^{\min}}, \tag{20}$$

whereas for criteria to be minimized,

$$z_{rj} = \frac{x_j^{\max} - x_{rj}}{x_j^{\max} - x_j^{\min}}, \tag{21}$$

and

$$z_{rj} = 1, \qquad \text{if } x_j^{\max} = x_j^{\min}. \tag{22}$$

As a result, all characteristics are represented on the same evaluation scale:

$$0 \le z_{rj} \le 1. \tag{23}$$

The weighting coefficients of the evaluation criteria are determined according to the information interaction scenario. For each scenario S_i the corresponding weighting vector

$$W_i = (w_{i1}, w_{i2}, \ldots, w_{in}), \tag{24}$$

is used, with its values given in Table 3. This approach enables the model to adapt to the specific characteristics of different segments of a Cyber-Physical System.

The integrated score of a cryptographic component is calculated as

$$Score\,(K_r, S_i) = \sum_{j=1}^{n} w_{ij} z_{rj}. \tag{25}$$

However, in cyber-physical systems, some characteristics constitute mandatory constraints. For example, exceeding the maximum allowable delay, insufficient RAM capacity, or non-compliance with key information protection requirements makes the use of a cryptographic component impossible regardless of its integrated score.

To account for such requirements, the admissibility function is introduced:

$$\delta(K_r, S_i) = \begin{cases} 1, & \text{if all mandatory requirements are satisfied,} \\ 0, & \text{otherwise.} \end{cases} \tag{26}$$

The admissible set is defined as

$$K_i^{adm} = \{K_r \in K : \delta(K_r, S_i) = 1\}. \tag{27}$$

Thus, the set K_i^{adm} includes only those cryptographic components that satisfy all mandatory requirements of scenario S_i. If $K_i^{adm} = \varnothing$, no suitable cryptographic component for scenario S_i exists within the given set of candidates.

The optimal cryptographic component for an information interaction scenario is determined according to the criterion

$$K_i^* = \arg \max_{K_r \in K_i^{adm}} Score(K_r, S_i). \tag{28}$$

Thus, the same cryptographic component may obtain different integrated scores depending on its functional role within the architecture of a Cyber-Physical System.

Based on the proposed adaptive multi-criteria model, an algorithm for evaluating cryptographic components was developed. The algorithm implements a sequence of procedures for selecting the optimal alternative for a given information interaction scenario. It includes the formation of a set of requirements, the selection of criterion weighting coefficients, the evaluation of cryptographic components, verification of mandatory requirements, calculation of the integrated score, and ranking of admissible alternatives.

The flowchart of the proposed algorithm is presented in Fig. 2.

The proposed algorithm implements a sequence of adaptive evaluation procedures for cryptographic components depending on the information interaction scenario in a cyber-physical system. At the first stage, the initial parameters of the model are specified: the number of scenarios l, the number of cryptographic components m, and the number of evaluation criteria n. For each scenario S_i, the corresponding set of requirements Req_i is formed, after which the vector of weighting coefficients W_i is selected according to expert-defined priorities. Next, the set of candidate cryptographic components K to be evaluated is formed.

The main loop of the algorithm is performed for each cryptographic component K_r. At this stage, the values of the evaluation criteria x_{rj} are determined and normalized to obtain the dimensionless characteristics z_{rj}. Compliance with the mandatory requirements is then verified using the admissibility function $\delta(K_r, S_i)$. For each admissible component, the integrated score $Score(K_r, S_i)$ is calculated. The obtained results are accumulated for all components. After completion of the loop, the admissible

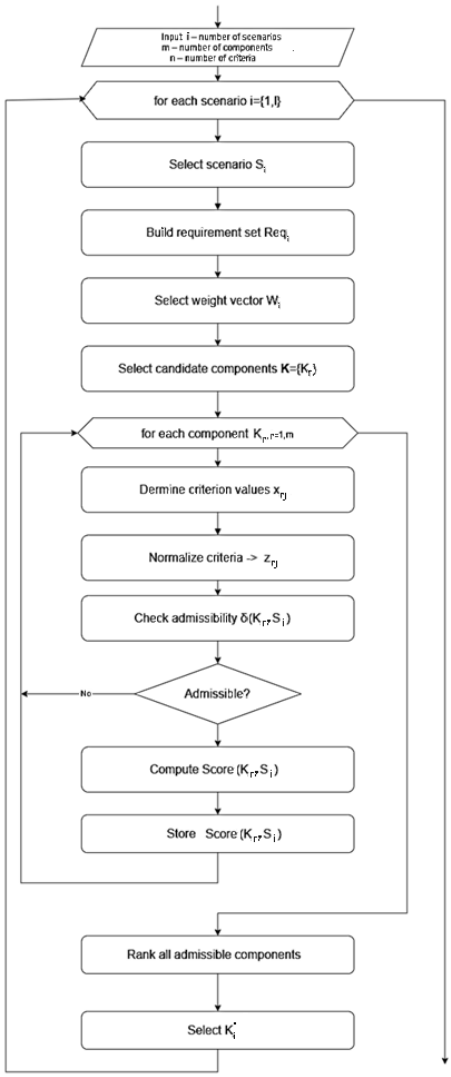


Figure 2: Flowchart of the Adaptive Multi-Criteria Evaluation Algorithm for CPS Cryptographic Components

components belonging to K_i^{adm} are ranked according to their integrated scores, and the optimal cryptographic component K_i^* is selected for the corresponding information interaction scenario.

The proposed adaptive multi-criteria model provides a comprehensive evaluation of cryptographic components by taking into account the characteristics of the information interaction scenario, information security requirements, resource constraints, and timing characteristics. Unlike conventional approaches, which primarily rely on individual indicators of cryptographic strength or performance, the proposed model employs a system of normalized weighting coefficients, enabling the selection procedure to be adapted to the operating conditions of different segments of a Cyber-Physical System. The experimental validation of the proposed model is presented in the following section.

4. Results

To validate the proposed adaptive multi-criteria model, a comparative evaluation of four lightweight cryptographic components—ASCON-128, GIFT-COFB, TinyJambu-128, and Xoodyak—was conducted. These algorithms were selected because they were finalists in the NIST Lightweight Cryptography competition, support Authenticated Encryption with Associated Data (AEAD), and have publicly available specifications and software benchmarking results for microcontroller platforms [18, 19, 20, 21]. The comparison of resource and timing characteristics was additionally based on the methodologies of

FELICS, FELICS-AEAD, and eBACS, which are designed to evaluate cryptographic implementations under identical or closely comparable execution conditions [5, 6, 22].

The PRESENT-80 algorithm was not included in the primary set of alternatives despite its widespread use in resource-constrained embedded devices. PRESENT is a lightweight block cipher standardized in ISO/IEC 29192-2, whereas the cryptographic components considered in this study implement complete AEAD schemes [23, 24]. When used as a standalone algorithm, PRESENT-80 does not provide message authenticity, integrity protection, or protection against replay attacks. To satisfy these requirements, it must be combined with an appropriate mode of operation, a message authentication code (MAC), and a nonce or counter management mechanism. Therefore, a direct comparison between PRESENT-80 and AEAD components would be methodologically inappropriate. The evaluation of composite cryptographic constructions consisting of a block cipher, mode of operation, MAC, and nonce management mechanism is identified as a direction for future development of the proposed model.

The evaluation was performed for the three information interaction scenarios formalized in Section 3: S_1 — sensor $\rightarrow$ gateway, S_2 — gateway $\rightarrow$ controller, and S_3 — controller $\rightarrow$ actuator. A dedicated vector of normalized weighting coefficients, W_i, presented in Table 3, was used for each scenario. This approach increased the importance of RAM usage, ROM usage, computational complexity, and energy consumption in the first scenario, while assigning greater weight to timing characteristics, authenticity, integrity, and implementation security in scenarios S_2 and S_3.

The initial characteristics of the evaluated components were compiled by synthesizing the results of the official NIST Lightweight Cryptography benchmarking, the implementation repository, and the corresponding experimental datasets [18, 19, 20]. Information regarding the finalist status, design characteristics, and evaluation results of the algorithms was verified using NIST publications [20, 21]. Resource and timing characteristics were compared in accordance with the methodological principles of FELICS, FELICS-AEAD, and eBACS [5, 6, 22]. Since resistance to side-channel attacks and fault injection depends not only on the cryptographic algorithm but also on the specific software or hardware implementation, the corresponding evaluations were derived separately from specialized studies [11, 12, 25].

The summarized characteristics of the evaluated cryptographic components are presented in Table 4.

Table 4
Summarized Characteristics of the Evaluated Cryptographic Components

Criterion	ASCON-128	GIFT-COFB	TinyJambu-128	Xoodyak
Cryptographic Strength Level	High	High	High	High
AEAD Support	Yes	Yes	Yes	Yes
RAM Usage	Low	Low	Very Low	Low
ROM Usage	Low	Medium	Low	Medium
Performance	High	High	Medium – High	High
Energy Efficiency	High	High	Very High	High
Implementation-Level Resistance to SCA/FI(based on published studies)	High	High	Medium	High

Note. The values presented in Table 4 are generalized qualitative estimates. They were derived from the results of NIST LWC Benchmarking [18, 19, 20, 21], the FELICS and FELICS-AEAD methodologies [5, 6], the eBACS system [22], and specialized studies of implementation security [11, 12, 25]. For subsequent calculations, the qualitative levels were converted into normalized values z_{rj} in accordance with the rules defined in Section 3.4.

Table 4 shows that all four components satisfy the basic requirements for confidentiality, integrity, and authenticity; however, they differ in their resource and implementation characteristics. TinyJambu-128 has the lowest RAM and ROM requirements and high energy efficiency, making it suitable for

autonomous sensor nodes. ASCON-128 and Xoodyak demonstrate a more balanced trade-off between performance, cryptographic strength, and the feasibility of developing secure implementations. GIFT-COFB also provides a high level of security; however, in terms of the combined resource and timing characteristics considered in the proposed model, it performs slightly below the leading alternatives.

The integrated scores were obtained using the adaptive multi-criteria model described in Section 3.4. For each component K_r, the initial characteristics x_{rj} were normalized, after which compliance with the mandatory requirements was verified using the admissibility function $\delta(K_r, S_i)$. All four AEAD components satisfied the admissibility conditions for the specified scenarios. The final values of $Score(K_r, S_i)$ were calculated using the scenario-dependent weights presented in Table 3.

Table 5
Results of the Adaptive Multi-Criteria Evaluation of Cryptographic Components for Different Information Interaction Scenarios

Cryptographic component	S1	S2	S3	Recommended Application Scenario
ASCON-128	0.94	0.97	0.98	General-purpose applications and critical CPS nodes
GIFT-COFB	0.90	0.92	0.93	Embedded devices with moderate resource constraints
TinyJambu-128	0.96	0.88	0.85	Autonomous sensor nodes and resource-constrained IoT devices
Xoodyak	0.93	0.95	0.96	Gateways, controllers, and general-purpose IoT devices

The values presented in Table 5 are the result of applying the proposed evaluation model to the normalized characteristics of the investigated cryptographic components. Unlike the initial characteristics obtained from published sources, the integrated scores represent the authors' original results, calculated by taking into account the criterion weighting coefficients and the specific characteristics of each information interaction scenario.

For the sensor–gateway scenario, TinyJambu-128 achieved the highest score (0.96). This result is explained by the high weighting assigned to resource-related criteria in this scenario, together with the algorithm's very low memory requirements and high energy efficiency. ASCON-128 and Xoodyak also demonstrated high scores; however, their advantages in performance and implementation security did not fully compensate for their somewhat higher resource requirements.

In the gateway–controller and controller–actuator scenarios, ASCON-128 ranked first, with integrated scores of 0.97 and 0.98, respectively. This result is attributable to its well-balanced combination of performance, cryptographic strength, and the availability of well-studied implementation countermeasures against side-channel attacks (SCA) and fault injection (FI) [9–11, 25]. Xoodyak achieved comparable scores (0.95 and 0.96) and may therefore be considered a competitive alternative for gateways and controllers. GIFT-COFB maintained consistently high scores across all scenarios; however, it did not rank first under any weighting configuration.

These results demonstrate that the selection of a cryptographic component for Cyber-Physical Systems should not be based solely on its nominal level of cryptographic strength. Resource characteristics, timing characteristics, and implementation security are equally important, and their relative significance varies depending on the specific system segment. This dependence justifies the use of the proposed adaptive multi-criteria evaluation model instead of selecting a single universal cryptographic algorithm for all nodes of a Cyber-Physical System.

5. Discussion

The obtained results confirm the effectiveness of applying an adaptive multi-criteria approach to the selection of cryptographic components for Cyber-Physical Systems. Unlike conventional approaches, which are primarily based on evaluating the cryptographic strength of algorithms or individual performance metrics [4, 7], the proposed model simultaneously considers security requirements, resource constraints, timing characteristics, and implementation security according to the specific information interaction scenario.

The evaluation demonstrated that no cryptographic component is optimal for all CPS segments. For resource-constrained sensor nodes, TinyJambu-128 achieved the highest integrated score owing to its minimal memory requirements and high energy efficiency. In contrast, ASCON-128 delivered the best results for the gateway–controller and controller–actuator scenarios, which is consistent with the outcomes of the NIST standardization process and recent studies of its software and hardware implementations [9–11, 21]. Xoodyak exhibits characteristics comparable to those of ASCON and may therefore be regarded as an effective alternative for general-purpose CPS platforms, whereas GIFT-COFB remains a competitive solution for systems with moderate resource constraints [17–22].

The proposed model is general in nature and can be applied not only to the finalists of the NIST Lightweight Cryptography competition but also to other cryptographic components, provided that their experimental characteristics are available. By adjusting the criterion weighting coefficients, the evaluation procedure can be adapted to the requirements of a particular application domain or the architecture of a specific Cyber-Physical System.

The limitations of this study include the use of generalized data from the literature on the resource and timing characteristics of cryptographic components obtained on different hardware platforms. Future research should include the experimental evaluation of all candidate components on a common hardware testbed, which would improve the accuracy of the integrated scores. In addition, the proposed approach can be extended to composite cryptographic solutions based on lightweight block ciphers, particularly PRESENT [23, 24], combined with appropriate modes of operation and message authentication mechanisms.

6. Conclusions

This study proposed an adaptive multi-criteria model for selecting lightweight cryptographic components for Cyber-Physical Systems. The model provides a comprehensive evaluation of cryptographic components by taking into account the information interaction scenario, information security requirements, resource constraints, and timing characteristics. Unlike existing approaches, the proposed model enables the integrated evaluation of cryptographic components according to their intended operating conditions.

The research identified the role of cryptographic components within the architecture of Cyber-Physical Systems, formalized typical information interaction scenarios, developed a system of evaluation criteria and a formalized set of requirements for cryptographic components, and proposed an adaptive algorithm for integrated multi-criteria evaluation. The results demonstrate that relying solely on cryptographic strength or the complexity of cryptanalytic attacks does not provide a sufficiently justified basis for selecting a cryptographic component without considering resource, timing, and implementation characteristics.

The scientific contribution of this work lies in the development of a scenario-oriented adaptive evaluation model that integrates a system of evaluation criteria, scenario-dependent weighting coefficients, and an integrated ranking algorithm for cryptographic components. The experimental evaluation of ASCON-128, GIFT-COFB, TinyJambu-128, and Xoodyak confirmed the applicability of the proposed approach and demonstrated that the optimal choice of a cryptographic component is determined by the functional role of the corresponding segment of a Cyber-Physical System.

The practical significance of the proposed model lies in its potential use as a decision-support tool

for the design and modernization of Cyber-Physical Systems. Future research should focus on the experimental evaluation of cryptographic components on a common hardware testbed, the extension of the evaluation criteria system, and the adaptation of the proposed model to composite cryptographic solutions based on lightweight block ciphers combined with appropriate modes of operation and message authentication mechanisms.

Acknowledgments

The authors express their sincere gratitude to the members of the research group and the staff of the Department of Information Security Management for their constructive discussions, valuable scientific recommendations, and support throughout this research.

The authors also thank the University administration for providing favorable conditions for conducting scientific research and for supporting research initiatives.

Declaration on Generative AI

During the preparation of this manuscript, the authors used ChatGPT (OpenAI) exclusively for language editing, including grammar, spelling, and stylistic improvements. All scientific results, analyses, interpretation of the findings, conclusions, and the final content of the manuscript were developed by the authors, who assume full responsibility for its content.

References

[1] E. R. Griffor, C. Greer, D. A. Wollman, M. J. Burns, Framework for Cyber-Physical Systems: Volume 1, Overview, Technical Report NIST SP 1500-201, National Institute of Standards and Technology, 2017. doi:10.6028/NIST.SP.1500-201.

[2] D. A. Wollman, M. A. Weiss, Y.-S. Li-Baboud, E. R. Griffor, M. J. Burns, Framework for Cyber-Physical Systems: Volume 3, Timing Annex, Technical Report NIST SP 1500-203, National Institute of Standards and Technology, 2017. doi:10.6028/NIST.SP.1500-203.

[3] M. Ersue, D. Romascanu, J. Schoenwaelder, A. Sehgal, Management of Networks with Constrained Devices: Problem Statement and Requirements, Technical Report RFC 7547, Internet Engineering Task Force, 2015. doi:10.17487/RFC7547.

[4] V. A. Thakor, M. A. Razzaque, M. R. A. Khandaker, Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities, IEEE Access 9 (2021) 28177–28193. doi:10.1109/ACCESS.2021.3052867.

[5] L. C. Dos Santos, J. Grossschadl, A. Biryukov, FELICS-AEAD: Benchmarking of lightweight authenticated encryption algorithms, in: Smart Card Research and Advanced Applications (CARDIS 2019), volume 11833 of *Lecture Notes in Computer Science*, Springer, Cham, 2019, pp. 216–233. doi:10.1007/978-3-030-42068-0_11.

[6] D. Dinu, A. Biryukov, J. Grossschadl, D. Khovratovich, Y. Le Corre, L. Perrin, FELICS: Fair evaluation of lightweight cryptographic systems, NIST Workshop on Lightweight Cryptography, 2015. URL: https://www.cryptolux.org/images/8/80/Session7-dinu-paper.pdf.

[7] M. Khan, H. Dagenborg, D. Johansen, Performance evaluation of lightweight stream ciphers for real-time video feed encryption on ARM processor, Future Internet 16 (2024) 261. doi:10.3390/fi16080261.

[8] M. S. Turan, K. A. McKay, D. Chang, J. Kang, N. Waller, J. M. Kelsey, L. E. Bassham, D. Hong, Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process, Technical Report NIST IR 8454, National Institute of Standards and Technology, 2023. doi:10.6028/NIST.IR.8454.

[9] M. S. Turan, K. A. McKay, D. Chang, J. Kang, J. Kelsey, Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output

Functions, Technical Report NIST SP 800-232, National Institute of Standards and Technology, 2025. doi:10.6028/NIST.SP.800-232.

[10] C. Dobraunig, M. Eichlseder, F. Mendel, M. Schlaffer, Ascon v1.2, Journal of Cryptology 34 (2021) 33. doi:10.1007/s00145-021-09398-9.

[11] A. Kandi, A. Baksi, P. Gan, S. Guilley, T. Gerlich, J. Breier, A. Chattopadhyay, R. R. Shrivastwa, Z. Martinasek, S. Bhasin, Side-Channel and Fault Resistant ASCON Implementation: A Detailed Hardware Evaluation (Extended Version), Technical Report 2024/984, IACR Cryptology ePrint Archive, 2024. URL: https://eprint.iacr.org/2024/984.

[12] B. Gigerl, F. Mendel, M. Schlaffer, R. Primas, Efficient Second-Order Masked Software Implementations of Ascon in Theory and Practice, Technical Report 2024/755, IACR Cryptology ePrint Archive, 2024. URL: https://eprint.iacr.org/2024/755.

[13] S. Kovalov, N. Maslova, V. Psel, Cryptographic analysis of rijndael-like cipher, Scientific and Practical Cyber Security Journal 2 (2018) 42–46. URL: https://journal.scsa.ge/papers/cryptographic-analysis-of-rijndael-like-cipher/.

[14] O. P. Markovskyi, S. S. Nikolskyi, A method for distributed computation of exponentiation over galois fields on multicore processors for cryptographic applications, Problems of Informatization and Management 1 (2025) 59–71. doi:10.18372/2073-4751.81.20130.

[15] G. A. J. H. Al-Mrayt, O. Markovskyi, A. Stupak, Organization of fast exponentiation on galois fields for cryptographic data protection systems, Information, Computing and Intelligent Systems 3 (2022) 17–25. doi:10.20535/2708-4930.3.2022.265480.

[16] N. O. Maslova, V. O. Psol, Fast algorithm for polynomial factorization over galois fields, Scientific Papers of Donetsk National Technical University. Series: Informatics, Cybernetics and Computer Engineering 1 (2017) 95–99. URL: https://iktv.donntu.edu.ua/wp-content/uploads/2021/07/ikvt_1_24_2017.pdf.

[17] H. Tschofenig, T. Fossati, Transport Layer Security and Datagram Transport Layer Security Profiles for the Internet of Things, Technical Report RFC 7925, Internet Engineering Task Force, 2016. doi:10.17487/RFC7925.

[18] National Institute of Standards and Technology, Lightweight cryptography performance benchmarking, 2022. URL: https://csrc.nist.gov/projects/lightweight-cryptography/performance-benchmarking.

[19] National Institute of Standards and Technology, Lightweight-cryptography-benchmarking: Benchmarking of NIST LWC finalists on microcontrollers, 2021. URL: https://github.com/usnistgov/Lightweight-Cryptography-Benchmarking.

[20] National Institute of Standards and Technology, Benchmarking of NIST LWC finalists on microcontrollers, 2023. URL: https://data.nist.gov/od/id/mds2-2958. doi:10.18434/mds2-2958.

[21] National Institute of Standards and Technology, Lightweight cryptography finalists, 2021. URL: https://csrc.nist.gov/projects/lightweight-cryptography/finalists.

[22] D. J. Bernstein, T. Lange, eBACS: ECRYPT benchmarking of cryptographic systems, n.d. URL: https://bench.cr.yp.to.

[23] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe, PRESENT: An ultra-lightweight block cipher, in: Cryptographic Hardware and Embedded Systems – CHES 2007, volume 4727 of *Lecture Notes in Computer Science*, Springer, Heidelberg, 2007, pp. 450–466. doi:10.1007/978-3-540-74735-2_31.

[24] ISO/IEC, Information security — lightweight cryptography — part 2: Block ciphers, 2019. URL: https://www.iso.org/standard/78477.html.

[25] J.-P. Kaps, SCA evaluation and benchmarking of finalists in the NIST lightweight cryptography standardization process, NIST Lightweight Cryptography Workshop 2023, Virtual Event, 2023. URL: https://csrc.nist.gov/presentations/2023/sca-evaluation-and-benchmarking-for-lwc-finalists.