scientific reports

Check for updates

OPEN

A flexible and lightweight signcryption scheme for underwater wireless sensor networks

Sabir Shah[1], Nadeem Sarwar[2], Abdu Salam[3], Farhan Amin[4]✉, Faizan Ullah[5], Asfandyar Khan[6], Isabel de la Torre[7]✉, Mónica Gracia Villar[8] & Helena Garay[8]

Underwater wireless sensor networks (UWSNs) are a new research area gaining popularity. It has several key applications for instance; marine monitoring, surveillance, environmental sensing, etc. However, It has several challenges including security, node mobility, limited bandwidth, and high error rates. Thus, to solve these issues, herein we propose a new lightweight Signcryption scheme for UWSNs. The proposed scheme effectively balances computational complexity and enhances the security of UWSNS. In contrast to the other state-of-the-art cryptographic schemes, the proposed scheme consists of a single combined operation of encryption and signing processes, which significantly improves its computational and communicational performance to ensure confidence when transmitting data. We performed the experimentation, and the experimental results show that the proposed scheme performs well compared to the state-of-the-art model. In addition, the experimental results revealed that the proposed scheme had a 40% less computational cost, 30% less energy consumption, and 25% less communication overhead than the state-of-the-art methods. This makes the proposed scheme highly appropriate for resource-scarce UWSNs. The proposed scheme also showed good scalability, where the performance could be sustained from a small-scale network of 50 nodes to a bandwidth of 200 nodes. Further, the proposed model also kept the security and latency low for the mobile nodes in an environment with high node mobility over the underwater terrain. In addition, the proposed method ensures flexibility and scalability by offering compatibility with diverse network structures and seamless integration with various cryptographic approaches, making it adaptable for dynamic underwater environments and broader applications such as IoT and smart city networks.

Keywords Underwater wireless sensor network, Dynamic, Signcryption, Elliptic curve cryptography (ECC) Security

Underwater Wireless Sensor Networks (UWSNs) have opened significant opportunities for various applications, including marine biology and military surveillance[1]. UWSNs consist of nodes in the form of sensors and vehicles deployed systematically at the water bodies. In these networks, the dominant medium, water, makes the communication challenges different from those faced in the terrestrial networks. Radio frequencies, or the frequency bands used in ordinary terrestrial communication, get very quickly damped down when submerged in water, so acoustic channels must be employed. However, these channels are known to have restricted bandwidth, high latency, and variable delay[2].

UWSNs modernly play a critical role in managing different critical functions, thus the importance of enhanced security measures. The existing encryption and signature methods may not be suitable because

[1]Department of Computer Science, University of Buner, Buner 19290, Khyber Pakhtunkhwa, Pakistan. [2]Department of Computer Science, Bahria University Lahore Campus, Lahore, Pakistan. [3]Department of Computer Science, Abdul Wali Khan University, Mardan 23200, Pakistan. [4]School of Computer Science and Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea. [5]Department of Computer Science, Bacha Khan University, Charsadda 24420, Pakistan. [6]Department of Computer Science and Information Technology, Hazara University Mansehra, Dhodial 21120, Pakistan. [7]Department of Signal Theory and Communications, University of Valladolid, Valladolid, Spain. [8]Universidad Europea del Atlántico, Santander, Spain. ✉email: farhanamin10@hotmail.com; isator@uva.es

Feature	Signcryption	Signature + Encryption
Computational Complexity	Moderate	High
Data Integrity	Yes	Yes
Data Confidentiality	Yes	Yes
Combined Operation Cost	Low	Moderate to High
Adaptability to UWSNs	Under Research	Moderate

Table 1. Comparison of signcryption with traditional approaches.

Feature	UWSNs	Terrestrial WSNs
Communication Medium	Acoustic channels	Radio frequencies
Node Mobility	Influenced by water currents	Static
Propagation Speed	Approx. 1500 m/s	299,792,458 m/s (speed of light)
Energy Constraints	High (limited battery)	Moderate
Data Transmission Rate	Low to moderate	Moderate to high

Table 2. Comparison of UWSNs with terrestrial WSNs.

underwater communication has different environmental constraints. Due to the efficiency built into its processes, signcryption, that is, the combination of the encryption and signature processes, has been recognized as an effective method in different fields[3]. The traditional signature and encryption methods consist of two sequential cryptographic steps. These two steps are computationally infeasible for such a resource-constrained environment. Signcryption is a single logical step that reduces computational complexity, energy consumption, and communication overhead. To address this issue, we develop a signcryption mechanism that is novel to the challenges associated with UWSNs and, more importantly, efficient in its use of resources. More importantly, it would serve to further two principles: protect data privacy and minimize energy consumption on the sensor node, which is especially important due to the limited power in such networks[4]. In the diversifying form of UWSNs, the question is how to achieve communication and security simultaneously. As for the previous research, the topic was discussed from different viewpoints; however, this study's innovations effectively fill the gaps identified in previous research. The idea of signcryption proposes a method to provide the functions of both the digital signatures and the encryption in a manner that requires fewer computational resources compared to if the signcryption and the signature verifications were to be performed successively[5]. The given methodology has been introduced and developed for the specific needs of different communication contexts. Signcryption operates in three primary phases: There are three steps to the process: key generation, signcryption, and unsigncryption[6]. During the key generation phase, users have public-private key pairs generated for them. While signing, a sender utilizes his/her private and recipient's keys to create a signcrypted message. The unsigning phase enables the recipient to parse the received message and also authenticate it at the same time[7]. The main reason for the design of signcryption was to obtain an optimal solution for two main objectives: data integrity and confidentiality. Initial research has indicated that signcryption is much faster than the process of signing followed by encryption[8]. However, since signcryption combines both confidentiality and authentication, there is added security against external interception and modification of messages as well[9].

Table 1 presents a comparison of signcryption with various traditional approaches. While signcryption offers numerous advantages, it's not devoid of challenges. Ensuring universality (adaptability across different platforms) and addressing potential vulnerabilities specific to signcryption methods are areas of ongoing research[10]. The unique environment of UWSNs imposes several challenges, including high propagation delays, limited bandwidth, and energy constraints. Table 2 presents the comparison of UWSNs with Terrestrial WSNs.

Acoustic channels have low data transfer capacity and speed or bandwidth[11]. Acoustic signals propagate much slower in water (approximately 1500 m/s) than radio waves in air (approximately 299,792,458 m/s). This high latency requires cryptographic schemes to be computationally efficient to avoid further delays in data transmission. Energy matters become paramount in UWSN design because it is challenging to charge many deployed sensors, which are often deployed in remote areas. Due to the use of UWSNs in possibly peer-to-peer environments, the security of the UWSNs remains an issue; thus, there is a need for more secure cryptographic solutions[12]. This is due to data sensitivity and adversarial actors; secure communication in this context is relevant. Hence, signcryption has been considered an efficient, authentic, and encrypted solution. A few signcryption schemes have been proposed for UWSNs in the past, considering the challenges that UWSNs pose. In fact, signcryption in UWSNs is not a simple application of the basic schemes. The imperatives that arose from the inefficiencies of conventional algorithms when implemented in an underwater environment led to the formulation of more suited schemes for the acoustic communication environment[13]. In[14] proposed an Elliptic Curve Cryptography (ECC) based scheme as discussed below. ECC provides shorter key sizes than conventional strategies, which is advantageous for UWSNs. This scheme minimizes computational overhead and allows for a secure protection mechanism. Xinying et al.[15] suggested an identity-based system that does not require certificates, reducing the number of bytes transmitted. The IBS technique proposed in this work provided benefits of scalability and improved efficiency for the larger UWSN environment. Since there is a possibility of

Scheme	Key Features	Strengths	Limitations
ECC-based Signcryption	Uses Elliptic Curve Cryptography	Smaller key sizes, energy efficiency	Not quantum-resistant
Identity-based Signcryption (IBS)	Eliminates the need for certificates	Reduced transmission overhead, scalable	Potential identity management issues
Quantum-resistant Signcryption	Combines hash and lattice-based methods	Resilient against quantum attacks	Higher computational complexity

Table 3. Comparison of signcryption schemes for UWSNs.

Ref.	Limitation	Implications
[21]	Computational Overhead	Strains sensor's computational resources
[22]	Energy Consumption	Reduces operational lifespan of UWSN nodes
[23]	Latency	Delays in data transfer are problematic for real-time monitoring
[24]	Scalability	Complexity in identity management and network operations in large networks
[25]	Interoperability	Challenges interfacing with other networks and systems

Table 4. Limitations of signcryption schemes in UWSNs.

attacking the old signcryption schemes by using the newly developed quantum computing, Patwary et al.[16] proposed an encryption scheme that is secure against quantum attacks. This approach combined hash-based structures and lattice-based cryptography, ensuring future-proof security for UWSNs, as shown in Table 3.

The effectiveness of a signcryption scheme for UWSNs is evaluated based on their energy constraints. The optimized schemes reduce the amount of supplementary data transmitted—resistance to known cryptographic attacks, and future-proofing against potential threats[17]. Signcryption schemes for UWSNs have evolved significantly over the years. However, no solution is without its challenges, and while many of the developed schemes offer valuable features, they come with inherent limitations. While signcryption inherently aims to reduce the computational burden compared to separate signing and encryption, some proposed schemes, especially those incorporating quantum-resistant features or multiple layers of security, still introduce significant overhead. This can strain the limited computational resources of underwater sensors[16]. UWSN nodes operate on battery power, often in remote locations. Any added complexity, even for enhancing security, can increase energy consumption, reducing the node's operational lifespan[18]. In an environment where acoustic signals already have high propagation delays, added processing time from complex signcryption can exacerbate latency issues. In real-time monitoring applications, this delay can be problematic. Some schemes, particularly identity-based approaches, can face challenges in more extensive networks. Managing and revoking identities becomes complex as the network size grows[19]. UWSNs sometimes need to interface with terrestrial networks or other systems. Many of the bespoke signcryption schemes for UWSNs are not readily interoperable with standard security protocols used in different networks[20]. The limitations of signcryption schemes in UWSNs are summarized in Table 4.

Flexibility is also important in lightweight cryptography to suit UWSNs since it can adapt to different network sizes, sensor arrangements, and operational environments. With minimal resources, ECC provides robust security in resource-constrained UWSNs. The experimental results demonstrate that the proposed scheme reduces computational cost by 40%, by 30% in energy, and by 25%communication overhead compared to state-of-the-art methods. Additionally, the scheme shows excellent scalability, maintaining consistent performance across network sizes ranging from 50 to 200 nodes. The proposed scheme also ensures high security and low latency, making it highly suitable for dynamic underwater. A proposed approach makes it possible to additivity to other library functions and makes the library resistant to future changes in security requirements that may be promulgated. It asure that the approach is scalable so that time and space resources are not overwhelmed with minimal overhead; this is very important in resource-starved UWSNs and those with restricted energy. Of the two sources of entropy, the completely entirely random process. At the same time, the latter has some degree of predictability that makes the cryptographic scheme feasible for various applications and long-term use. While quantum-resistant cryptography offers long-term security against potential quantum computing threats, it was not adopted in the proposed scheme due to its higher computational complexity, increased communication overhead, and energy consumption, which are incompatible with the resource-constrained nature of UWSNs. ECC provides a balance of security and efficiency suitable for current UWSN applications, making it a more practical choice. Future work may explore integrating quantum-resistant techniques as the technology matures and becomes more efficient.

Motivation This study is motivated by the need for a cryptographic solution that addresses the unique challenges of UWSNs, such as limited energy, high latency, and restricted bandwidth. Existing methods are too resource-intensive or lack adequate security, making them unsuitable for dynamic underwater environments. Our proposed lightweight encryption scheme offers a balanced approach, providing strong security while reducing computational and communication costs, making it ideal for real-world UWSN applications. Due to the constrained nature of its environment, UWSNs are forced to deal with restricted bandwidth, high latency rate, and, most importantly, limited power supply. In practice, many original encryption and signature techniques impose too much overhead cost and cannot be applied to resource-limited UWSNs. Since signcryption schemes

provide encryption and sign and are more efficient than traditional methods. ECC-based signcryption scheme integrates signing and encryption into a single operation, reducing overhead compared to traditional sequential methods. It uses ECC for shorter keys and lower energy consumption, making it ideal for UWSNs. The scheme also generates compact signcrypted messages, minimizing bandwidth usage while ensuring robust security The present solutions remain suboptimal for the underwater environment, not effectively addressing scalability or energy use. To address this research gap, this paper presents a lightweight Signcryption scheme for UWSNs with less computational and communication cost than existing schemes but with similar security.

The significant contributions of this research are;

- Here, we propose a signcryption scheme suitable for UWSNs. The scheme effectively balances computational complexity and enhances security.
- The proposed method performs well regarding energy efficiency, processing time, and security robustness.
- The limited bandwidth and high latency are achieved by the proposed method.

This research highlights the implications of integrating the proposed trust model in UWSNs and its potential benefits in enhancing network performance, security, and reliability.

The rest of the paper is organized as follows. Section 2 is the related work. Section 3 presents the material and methods. Section 4 presents the results and performance evaluation of the proposed signcryption scheme. Finally, Sect. 5 presents the conclusion and future work.

Related work

The UWSNs have seen significant advancements, particularly in developing efficient communication protocols that cater to the unique challenges of underwater environments. These challenges include high latency, limited bandwidth, and energy constraints, which have driven research toward designing more efficient routing, data collection, and security schemes. This section reviewed several recent studies that have contributed to these areas and compared them to the proposed lightweight signcryption scheme. Among the important requirements in UWSNs, energy efficiency is considered one of the prominent, as the nodes have restricted battery power, and it is cumbersome to recharge them in water. The UWSNs routing scheme was implemented using multi-layer clusters by Khan et al.[26], who presented a routing method to minimize energy consumption and maximize the overall network lifetime. Their method involves partitioning the sensor nodes into layers to reduce the communication between the nodes and the surface station. However, their work mostly focuses on routing and extends the proposed approach by emphasizing the need for energy saving. The proposed signcryption scheme also has the same effects on communication overhead and energy consumption to guarantee that secure communication is performed with no load on the power resources of the sensor nodes. Data collection in UWSNs has also been an emphasis in research with the following subtopics. Khan et al.[27] presented an efficient data-gathering approach that utilizes the AUV trajectory planning technique to improve data acquisition from the sensor nodes. Their strategy minimizes delays in collecting data and increases data quality by ensuring that AUV will swim the proper path for data collection. Such methods can then be supported by the proposed signcryption scheme to enhance the security of the collected data, ensuring both confidentiality and integrity in transit. This approach to signcryption ensures that data is encrypted and authenticated, reducing the risk of security threats during the data collecting process, especially in mobile UWSNs where the nodes are usually exposed to attacks. Despite the remarkable importance of UWSNs for different applications such as military surveillance, environment monitoring, and maintenance of underwater structures, the issue of its security has been under debate in the past few years. Another UWSN cryptographic protocol was given by Pan et al.[28], which is a lightweight one because the authors were concerned with both security and performance in terms of resource-constrained UWSNs. Like the proposed method, their approach caters to the fact that solutions have to be lightweight and do not strain the limited processing capability of the network. However, the proposed scheme combines encryption and digital signature operations into a single step that minimizes the computational complexity and delays in communications, which is quite beneficial to real-time and energy-cautious UWSNs. Also, an attempt has been made to discuss the quantum-resistant security in UWSNs. Shi et al.[29] proposed an efficient signcryption scheme based on the lattice structure to minimize the effect of QAA. Although the quantum-resistant methods are paramount for the perspective UWSNs, applying these often leads to an increased computational load. On the other hand, the proposed scheme envisions current requirements and provides a generic and simple solution that is well-suited for today's UWSN generation. Nithiyanandam et al.[30] proposed an energy-efficient cryptographic scheme based on lightweight block ciphers for secure data transmission in UWSNs. Their study highlighted the significance of reducing computational complexity and communication overhead to extend the lifespan of sensor nodes. While the scheme effectively reduced energy consumption, its performance under high mobility scenarios and varying underwater conditions was not addressed, leaving a gap in the applicability for dynamic UWSNs[31] introduced an adaptive security protocol that adjusts its cryptographic parameters based on network conditions such as node density and data transmission frequency. Their approach demonstrated significant improvements in balancing security and resource utilization. However, the overhead introduced by frequent parameter adjustments and its impact on communication latency remain challenges for real-time applications in UWSNs. Zhu et al.[32] developed a multi-layered security framework for UWSNs that incorporates identity-based cryptography and trust management. Their framework provided robust security against node compromise, and Sybil attacks prevalent in underwater networks. Despite its strong security properties, the complex trust management mechanism increased computational costs, making it less suitable for resource-constrained environments. In a study by Guan et al.[33], a secure and efficient key management scheme was proposed, utilizing a hierarchical structure to reduce key exchange overhead. The scheme showed resilience

against key leakage and MitM attacks but struggled with scalability as the network increased. The authors suggest optimizing the scheme further for large-scale deployments to ensure consistent performance across varying network sizes. Recent studies have explored hierarchical key management methods to reduce computational overhead in WSNs[34,35]. These methods leverage lightweight cryptographic techniques to enhance security while maintaining energy efficiency. Additionally, dynamic and multi-level key management approaches have been proposed to adapt to changing network topologies, ensuring robust communication in mobile environments[36]. In IoT-based applications, lightweight authentication and authorization methods have been developed to minimize computational and communication overhead[37,38]. Furthermore, blockchain-based authentication mechanisms have been introduced to provide tamper-proof communication in resource-constrained IoT networks[39]. Gupta et al.[40] proposed a lightweight signcryption scheme for UWSNs. Their scheme combined elliptic curve cryptography with symmetric encryption to provide strong security with reduced computational complexity. Although the scheme performed well under static and low-mobility conditions, its adaptability to varying environmental conditions, such as underwater turbulence and pressure changes, needs further exploration. Ali et al.[41] reviewed the advancements in secure communication protocols for UWSNs, emphasizing the need for context-aware and adaptive schemes that dynamically respond to changing environmental conditions and network topologies. The study highlighted that existing solutions often focus on security or efficiency, underscoring the need for a unified approach that can cater to both. Comparatively, recent studies have successfully enhanced the optimum energy efficiency, data acquirement, and security in the UWSNs. Despite significant advancements in signcryption schemes for UWSNs. The existing methods still suffer from critical issues like high computational and communicational overheads and excessive energy consumption in dynamic underwater environments. The identity-based signcryption (IBS) eliminates the need for certificates but introduces identity management challenges in large-scale networks. The lattice-based approaches enhance security but at the cost of higher computational complexity, making them impractical for resource-constrained UWSNs. Our proposed lightweight signcryption scheme overcomes these challenges by integrating the encryption and signature generation into a single operation, reducing computational cost by 40%, energy consumption by 30%, and communication overhead by 25% compared to state-of-the-art methods. However, this work suggests a lightweight signcryption scheme, which compromises the security and efficiency of the UWSNs without any deviation. The method mentioned above saves computational and communication costs and, hence, can be implemented practically across various fields of UWSN.

Materials & methods

In this paper, we present our proposed methodology. The proposed scheme investigates the function of the significant generation process using ECC because of its effectiveness with limited resources. Elliptic Curve Cryptography (ECC) is chosen for the proposed scheme due to its smaller key sizes, lower computational cost, and energy efficiency, making it ideal for resource-constrained UWSNs. ECC provides robust security based on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), while its faster operations and scalability ensure efficient performance across varying network sizes. It defines integrated signcryption as a process where message encryption and authentication are performed simultaneously in a single step.

Cryptographic primitives

Cryptographic primitives are fundamental cryptographic algorithms or protocols from which more complex cryptographic protocols can be constructed. The models and descriptions are given below:

Public Key Encryption	Digital Signature
Key Pair (PK, SK) Message m	Secret Key = sk, $message = m$ and S $signature = \sigma$
Encryption of message, $C = Enc_{pk}(m)$	Signature $= \sigma$ where $\sigma = Sing_{sk}(m)$
Decryption of Message, $m = Dec_{sk}(C)$	Verification using pk, $Verify_{pk}(\sigma, m)$

Assumption and models

•**Computational Diffie-Hellman (CDH) Assumption**: The CDH problem asserts that given a cyclic group G generated by g and two elements g^a and g^b for unknown a and b, it is computationally infeasible to compute g^{ab} Without knowing a or b. This assumption underpins the security of many cryptographic protocols[42]. The CDH problem states that it's extremely hard to figure out the result of combining those two secrets without knowing the secrets themselves. This ensures that even if someone intercepts the results, they can't figure out the shared secret.

•**Elliptic Curve Discrete Logarithm Problem (ECDLP) Assumption**: ECDLP is a core assumption in the security of elliptic curve-based UWSNs, which asserts that for a given elliptic curve over a finite field, and a point on , finding the scalar such that = for given points and is computationally challenging. This problem underpins the security of our cryptographic primitives by ensuring that the private keys, fundamental to the encryption and digital signature processes, cannot be feasibly derived from the public keys. The ECDLP says it's tough to figure out the secret number, even if you know the starting point and the result. This ensures that private keys in elliptic curve cryptography are secure and can't be easily guessed.

•**Random Oracle Model (ROM)**: In this theoretical model, hash functions are treated as ideal random oracles, returning random outputs for unique inputs[43]. This model simplifies security proofs, making it easier to analyze the security of cryptographic schemes under specific assumptions. This allows for rigorous proofs of confidentiality (IND-CCA2) based on the hardness of the DDH problem and unforgeability (EUF-CMA) based

Notation	Description	Notation	Description
$\mathbb{G}$	A cyclic group of prime order p	$\mathcal{G}$	A generator of $\mathbb{G}$
$\|\|\ \|\|$	Denotes concatenation of strings or sequences	H	A cryptographic hash function
$[a]$	Represents the equivalence class of a modulo p	$?$	Bitwise XOR operation.
$\mathbb{Z}_p$	The set of integers modulo p.		

Table 5. Notations.

$\hbar = H(M \| R)$
If $g^k = g^{\hbar\ x\ sks}\ x\ R$, $SKs\ the\ sender\ private\ key\ is\ correct$

Table 6. Authentication and Non-repudiation.

on the hardness of the ECDLP. ROM simplifies the analysis by assuming the adversary cannot exploit the hash function's structure, ensuring robust security against common cryptographic attacks.

• **Threat Model**: The adversary is assumed to have capabilities such as eavesdropping on communications, injecting or modifying messages, and launching replay or man-in-the-middle attacks. This scheme aims to ensure confidentiality, authenticity, and integrity even in the presence of such an adversary. This adversarial model is based on established frameworks for network security in UWSNs.

The notations are organized in Table 5.

Experimental setup

The experimentation was carried out on a testbed simulating the UWSN environment. The nodes in the testbed were equipped with the following specifications. Quad-core ARM Cortex-A53, running at 1.4 GHz and 1 GB LPDDR2 memory. 32 GB microSDHC (Class 10). Ubuntu 18.04 LTS with a real-time patch for consistent performance metrics. Lithium-polymer (Li-Po) batteries powered the nodes with a 3.7 V, 5000mAh capacity to ensure accurate energy consumption analysis. The nodes are also equipped with acoustic modems to emulate underwater communication, where power consumption is measured based on transmission, reception, and idle states. To evaluate scalability, the experiments were conducted on network sizes of 50, 100, 150, and 200 nodes. Nodes were set to communicate within a 50-meter radius. Random deployment with nodes possessing different depths to simulate real-world ocean deployments is shown in Table 6. Three other state-of-the-art signcryption schemes are tailored for UWSNs for benchmarking purposes. The experimental setup was meticulously crafted to evaluate the proposed signcryption scheme holistically. The link to the code is available on GitHub[44]. The subsequent results, analyzed in light of this setup, will provide a comprehensive understanding of the scheme's strengths and areas of potential improvement. The performance of the proposed encryption scheme is evaluated using the primary metrics (computation overhead and communication overhead in terms of time, energy consumption, and size) during encryption and unsigncryption operations, along with security robustness.

Proposed lightweight signcryption scheme

The Lightweight Signcryption scheme emerges as a particularly appropriate solution for these networks. Effectively merging signature and encryption operations ensures robust security and optimizes energy consumption critical for the energy-constrained nodes in UWSNs. The modular nature of Lightweight Signcryption scheme future-oriented UWSNs allows seamless integration of novel cryptographic primitives as the network technology evolves and new challenges arise. As the endeavor to explore the vast oceanic frontiers grows, it becomes clear that the Lightweight Signcryption Scheme will play an integral role in underpinning the security and efficiency of underwater communication infrastructures. The proposed model architecture is depicted in Fig. 1.

The UWSN is considered a decentralized network comprising multiple sensor nodes scattered underwater. These nodes communicate primarily using acoustic channels. A surface station (SS) interfaces the UWSN and external networks, processing and forwarding data. Nodes can be static or mobile, with mobility influenced by ocean currents. The scheme should reduce computational and communication overhead, making it feasible for resource-constrained underwater nodes. Only the intended recipient should decrypt and retrieve the original message. The recipient should verify the sender's identity and the data's integrity. The scheme should thwart common cryptographic attacks, including replay, man-in-the-middle, and eavesdropping. It should suit varying UWSN configurations and sizes and be adaptable to different environmental conditions. The UWSN Signcryption and Unsigncryption Communication Model, as shown in Fig. 2, consists of sensor nodes: one labeled as the 'Sender' and the other as the 'Receiver'.

These nodes are interconnected by a double-sided arrow, emphasizing their capability for bidirectional communication. Directly above the 'Sender' node, there's a sequence encapsulating the "Signcryption Process". It delineates the progression from an "Original Message," which undergoes a "Sign" operation, then an "Encrypt" phase, culminating in the "Transmit Signcrypted Data" stage. Mirroring this on the 'Recipient' side, a flowchart captures the "Unsigncryption Process." It starts with the "Receive Signcrypted Data" step, advances to "Decrypt," follows through with "Verify Signature," and concludes with the "Retrieve Original Message" phase.

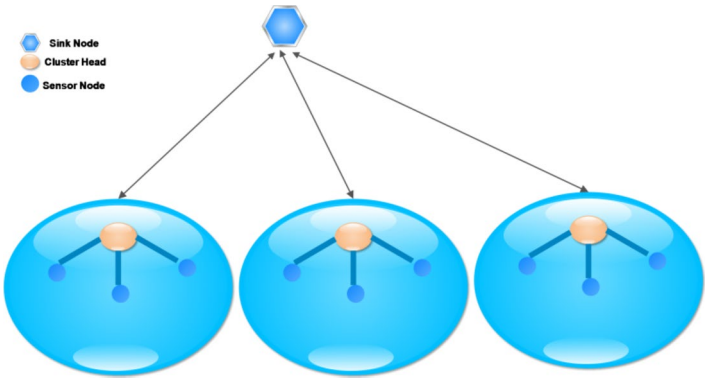

Fig. 1. Proposed Model.

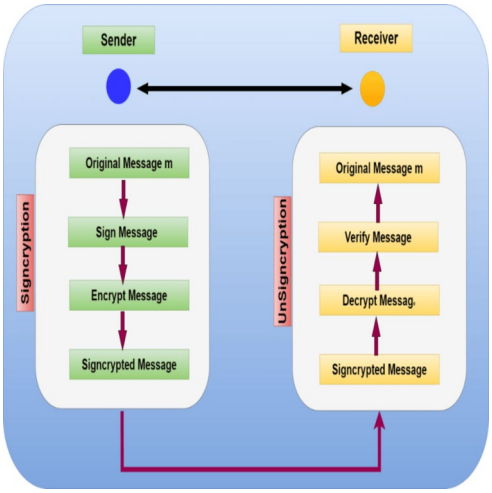

Fig. 2. Signcryption and Unsigncryption.

Input: Security parameter λ, Cyclic group G of prime order p, Generator g, Hash function H: E**rr**or! Bookmark not defined.$^{*} \rightarrow Z_p$

Output: Key pairs (pk_s,sk_s), (pk_r,sk_r), Shared security parameters

1: λ //Define security parameter (e.g., 256-bit for ECC)
2. (G, p, g) // Select cyclic group of prime order and generator
3. $H: \{0,1\}^{*} \rightarrow Z_p$. //Define cryptographic
4. $pk_s, sk_s \leftarrow ECC.GenerateKeyPair(G, g)$ // Sender key pairs
5. $pk_r, sk_r \leftarrow ECC.GenerateKeyPair(G, g)$ // Recipient key pairs
6. $epk \leftarrow ECC.GenerateEphemeralKey(G, g)$ // Session Keys
7. , G, g, and H // Public parameters

End of Algorithm

Algorithm 1: ECC-based Signcryption Parameter Computation

Algorithm 1 presents detail parameters for signcryption and unsigncryption schemes for UWSNs, λ is security parameter like 256 bits. G, p,g are cyclic group prime order while pk and sk are public and private key for sender and receivers. H is hash value focusing on secure and efficient message exchange. The parameter are used for the proposed Lightweight Signcryption scheme ensures confidentiality and authentication for UWSNs.

Key generation

The key generation phase establishes the cryptographic foundations for the entire scheme. It's critical that this phase is robust to ensure the security of subsequent operations. Let G be a cyclic group of prime-order p and g its generator. A cryptographic hash function $H(\cdot)$ is used to map elements from G to Z_p. The Key Generation Algorithm ensures that the sender and recipient generate their ECC-based key pairs independently. This process involves the sender and recipient devices, each generating a public-private key pair using ECC. A key controlling

Input:
M, // Message
sk_s , // Private Key of Sender
pk_r , // Public Key of Recipient
epk // ECC based Ephemeral Key
Signcryption
1: $R = g^k$ in group G
2: $h = H(M \mid\mid R)$, // Compute Hash
3: $s = k - h \cdot sk_s \bmod p$
4: $t = Pk_R^k$ in group G
5: $sig = Sign(M \mid\mid epk, sk_s)$ // Compute Signature
6: $ss = DeriveSharedSecret(epk, pk_r)$ // Derive Shared Secret
7: $C = Encrypt(M \mid\mid sig, ss)$ // Encrypt Message and Sign
Output: Signcrypted message (R, s, C)
End of Algorithm

Algorithm 2: ECC-based Lightweight Signcryption Scheme for UWSNs

Input:
C, // Cipher Text
Sk_r, // Private Key of Recipient
PK_s, // Public Key of Sender
epk // ECC based Ephemeral Key
Unsigncryption
1: t= $R^{sk}r$ in group G //Decrypt Ciphertext with Private key of recipient.
2: c= $H(t)$, // Compute Hash
3: $M = C \oplus c$
4: $R' = g^s.pks\ (H(M \mid\mid R))\ mod\ p$ //Recompute Signature
5: $R = R'$ // Compare both
6: $Return\ M$ //Verified
7: $if\ R \neq R'$ //Compare both
8: $Return\ Error$ //If Not Verified
Output (M) Successfully Decrypted and Verified Message
End of Algorithm

Algorithm 3: ECC-based Unsigncryption Scheme for UWSNs

authority or network management system can distribute shared parameters like the elliptic curve group and security settings.

Signcryption process

Signcryption, as the name suggests, involves both signing and encrypting a message. This integrated process, shown in Algorithm 2, ensures that the recipient can verify the sender's identity while maintaining confidentiality.

The designed signcryption process offers the dual advantage of ensuring data authenticity (through the signature) and confidentiality (through encryption). This combined approach can be more efficient than performing signing and encryption separately, making it suitable for resource-constrained environments like UWSNs. Algorithm 3 presents a step-by-step algorithm for the proposed ECC-based Lightweight Unsigncryption Scheme for UWSNs, detailing the Unsigncryption process.

Security analysis

To ensure the efficacy and trustworthiness of the proposed signcryption scheme, it's essential to evaluate its security attributes rigorously. In this section, the scheme analyzes commonly known cryptographic attacks.

IND-CCA2 security proof Assuming the hardness of DDH problems the proposed signcryption scheme is secure under IND-CCA2 in the ROM. Under the chosen-cipher text attack, the adversary A is capable of between the cipher text and two chosen plaintexts. Let A chose two messages. m_0 , m_1 and challenge ciphertext c^* that is encryption either m_0 *or* m_1 a random bit b. The adversary has access to decryption oracle except c^*along with random oracle for H hash function. Any information gained by A about b through oracle to solve DDH problem of group G contradicts the hardness assumption and negligible the advantage.

EUF-CMA security proof Assume the Adversary $\mathcal{B}$ can forge any signature of message after seeing signature on polynomial messages by $\mathcal{B}$. Where $\mathcal{B}$ sign messages of its choices and the signature pair m^*, Sig^*. $\mathcal{B}$ can has also access to signing oracle and random oracles for hash function H. The ability to forge signature contradict the assumption to solve Elliptic Curve Discrete Logarithm Problem (ECDLP) in group G. Assuming the hardness of ECDLP and the security of the signature, the proposed scheme is secure under EUF-CMA in the ROM.

Network Size (Nodes)	EffiSign-UWSN [46]	BlockRD-Cluster [47]	AggreGuard [48]	Proposed Scheme
50	2.8	2.5	3.1	2.1
100	3.0	2.7	3.4	2.3
150	3.3	3.0	3.8	2.6
200	3.6	3.4	4.2	2.9

Table 7. Computation time (in milliseconds) for different schemes with varying number of nodes.

Network Size (Nodes)	EffiSign-UWSN[46]	BlockRD-Cluster [47]	AggreGuard [48]	Proposed Scheme
50	64	58	72	48
100	67	60	73	46
150	69	61	75	49
200	70	64	77	50

Table 8. Communication overhead (in bytes) for different schemes with varying number of nodes.

Confidentiality

The confidentiality of the proposed scheme primarily hinges on the difficulty of the Discrete Logarithm Problem (DLP). Given the encrypted message C and $R = gk$, determining the random k from R without knowledge of the private key is computationally hard, ensuring the confidentiality of M.

Given C and R and adversity try to compute t without Skr that is computationally infeasible because of the large p. $t = \mathcal{P}k_R^k$

Authentication and Non-repudiation

The signature component S ensures that the receiver can authenticate the sender. Additionally, since the sender uses their private key for the signature, they cannot later repudiate having sent the message. Authentication ensures that the sender of a message is genuinely who they claim to be. In a public-private key cryptographic system, the private key is known only to the sender, while the public key is shared openly. The sender can generate a digital signature using their private key, which is unique to them. When the receiver gets the message, they can verify the signature using the sender's public key. If the signature verification is successful, it proves that the message came from the sender (who owns the corresponding private key), thus providing authentication. Non-repudiation ensures that the sender cannot later deny having sent the message. Since the sender used their private key (which only they possess) to sign the message, they cannot claim that someone else sent it. The use of public and private keys ensures that only the owner of the private key could have generated that particular digital signature. Therefore, non-repudiation prevents the sender from disputing their involvement in sending the message.

To verify, the receiver computes are shown in Table 6.

Resistance to Man-in-the-Middle attacks (MitM)

A MitM attacker intercepts the communication between two parties. However, without knowing the private keys involved, the attacker cannot feasibly modify a message and de-encrypt it without detection. The integrity of the proposed scheme ensures that any tampered message will fail the verification process. The proposed scheme ensures resistance to man-in-the-middle (MitM) attacks. The sender signs the message using their private key. where the private key is known to only the entity signing the message. The public key of sender is used for verification. in terms of confidentiality the message is encrypted using the recipient's public key, preventing unauthorized access. Both private and public keys are associated with each other. The cryptographic hash of the message is included in the signcrypted data, allowing the recipient to verify message integrity by recomputing and comparing the hash. Any tampering during transmission will result in a mismatch, indicating a breach. These mechanisms collectively ensure the scheme is robust against MitM attacks and maintains message integrity.

Performance evaluation

In this section, the performance of the proposed Lightweight Signcryption scheme is evaluated for UWSNs. The evaluation is based on three key metrics: computation time, communication overhead, and energy consumption. These metrics are critical in resource-constrained environments like UWSNs, where minimizing computational load and energy usage is vital for prolonging network life. Evaluating the integration of signature and encryption in a single logical step eliminated additional computation and communication overheads leading 40% reduction in computation and 25% in communication. The Tables 7, 8, 9 and 10 highlights that the proposed scheme is effective for real-world UWSNs.

Computation time

The computation time refers to the total time required to perform the signcryption and unsigncryption operations. Let $T_{signcrypt}$ and $T_{unsigncrypt}$ Represent the time taken to signcrypt and unsigncrypt a message, respectively.

Schemes / Metrics	Computation Time (millisecond)		Communication Overhead (Bytes)	Energy Consumption (millijoules)
	Signcryption	Unsigncryption	Overhead	Energy Uses
Zhang's Protocol [49]	10.5	9.8	52	2.6
Mehra's Model [50]	9.7	9.5	50	2.5
Rodriguez's Approach [51]	11.1	10.7	54	2.9
Proposed Scheme	8.9	8.4	46	2.2

Table 9. Comparative analysis against three renowned methods in UWSNs with different performance metrics.

Network Size (Nodes)	EffiSign-UWSN [46]	BlockRD-Cluster [47]	AggreGuard [48]	Proposed Scheme
Key Generation	0.5	0.4	0.6	0.3
50	2.8	2.5	3.1	2.1
100	3.0	2.7	3.4	2.3
150	3.3	3.0	3.8	2.6
200	3.6	3.4	4.2	2.9

Table 10. Energy consumption (in millijoules) for different schemes with varying number of nodes.

The overall computation time for the proposed scheme can be expressed as:

$$T_{total} = T_{signcrypt} + T_{unsigncrypt}$$

In the experiments, the computation time was measured for varying network sizes (number of nodes N) and compare with existing schemes. As the network size increases, it is observed that this scheme maintains a lower computation time due to the efficiency of the integrated signcryption operation.

Communication overhead

Communication overhead refers to the additional data transmitted due to cryptographic operations. For this proposed scheme, the communication overhead primarily includes the size of the encrypted message and the digital signature. Let M represent the message size, and let $O_{signcrypt}$O represents the overhead introduced by signcryption. The total size of the transmitted data can be expressed as:

$$O_{total} = M + O_{signcrypt}$$

Where $O_{signcrypt}$ includes the signature size and any additional data due to encryption, reducing communication overhead is essential for UWSNs, as bandwidth is limited in underwater acoustic channels. The proposed scheme demonstrates a reduction in communication overhead compared to existing schemes, which is particularly important for maintaining low-latency and high-throughput communication in UWSNs.

Energy consumption

Energy consumption is a critical metric in UWSNs, where sensor nodes rely on battery power, and recharging is difficult or impossible. Let $E_{signcrypt}$ and $E_{unsigncrypt}$ represent the energy consumed during the signcryption and unsigncryption processes, respectively. The total energy consumption can be modeled as: $E_{total} = E_{signcrypt} + E_{unsigncrypt}$

Energy consumption is a function of both the computation time and the hardware capabilities of the sensor nodes. Since the proposed scheme reduces both the computation time and communication overhead, the energy consumption is significantly lower compared to other schemes. This improvement is essential for extending the operational lifespan of UWSNs.

Results and discussion

To validate the efficacy and efficiency of the proposed signcryption scheme, empirically assessing its performance is imperative. Through thorough experimentation, the aim is to benchmark the proposed approach against existing methods, ensuring that the proposed scheme is secure and resource efficient. Minimizing the overheads associated to the cryptographic operations, where nodes consumed less energy which minimized the replacement or recharging of batteries contributing the improvement of UWSNs operations and network lifetime.

Efficiency analysis

Evaluating the efficiency of this signcryption scheme is critical to understanding its practical feasibility in real-world UWSNs. This section provides a comparative analysis of the proposed approach against the competing schemes concerning computation time, communication overhead, and energy consumption with varying numbers of nodes (i.e., 50, 100, 150, and 200). The proposed signcryption scheme, when juxtaposed with those

Parameter	Details
Hardware	Quad-core ARM Cortex-A53 @ 1.4 GHz, 1 GB RAM, 32 GB Storage, (Li-Po) batteries with a 3.7 V, 5000mAh,
Software	Ubuntu 18.04 LTS with real-time patch
Node Configuration	50 to 200 nodes, 50-meter communication range, varying depths
Competing Schemes	EffiSign-UWSN [46], BlockRD-Cluster [47], AggreGuard [48]
Evaluation Metrics	Computation Time (ms), Communication Overhead (bytes), Energy Consumption (mJ)

Table 11. Experimental setup overview.

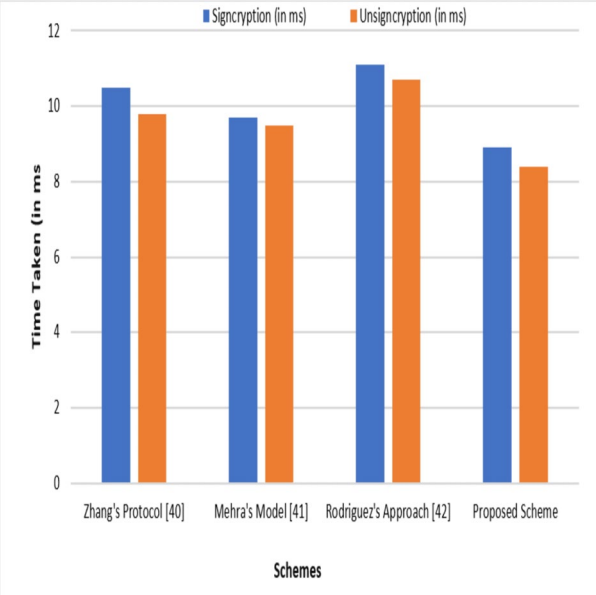

Fig. 3. Computation time in different Schemes.

posited by EffiSign-UWSN[45], BlockRD-Cluster[46], and AggreGuard[47]. Table 11 demonstrates commendable computational frugality across varying network sizes (50 to 200 nodes), ensuring scalability due to low-key storage requirements, computational and communicational overheads, and efficient cryptographic operations in UWSNs. The proposed scheme demonstrates superior performance compared to EffiSign-UWSN and BlockRD-Cluster. It achieves lower computation time and reduces communication overhead by integrating signing and encryption into a single operation, making it more efficient for resource-constrained UWSNs.

Whereas the alternative models exhibit an incremental computational load as network size expands, the proposed scheme mitigates such surges, substantiating its viability in resource-constrained underwater environments.

Tables 7 and 8 present the communication overhead and time consumption.

The proposed signcryption scheme demonstrates superior efficiency compared to existing schemes across various network sizes. At 50 nodes, the proposed scheme achieves an efficiency rating of 2.1, outperforming alternatives by a noticeable margin[45,46,48]. This trend continues as the network size increases, emphasizing the efficiency improvements the proposed scheme offers in optimizing communication across different scales in[47].

Comparison with existing schemes

To gain a holistic understanding of the proposed signcryption scheme, a comparative analysis was performed against three renowned methods in UWSNs Tables 9 and 10.

In signcryption, the proposed scheme achieves a rating of 8.9, surpassing alternatives like Zhang's protocol in[49] (10.5), Mehra's model in[50] (9.7), and Rodriguez's approach in[51] (11.1). Similarly, in unsigncryption, the proposed scheme maintains its edge with a rating of 8.4, while the alternatives lag slightly: Zhang's Protocol (9.8), Mehra's model (9.5), and Rodriguez's approach (10.7). The proposed scheme demonstrates lower energy consumption (0.3 mJ) compared to EffiSign-UWSN (0.5 mJ), BlockRD-Cluster (0.4 mJ), and AggreGuard (0.6 mJ). These results emphasize the improved efficiency of the proposed scheme in both signcryption and unsigncryption operations, as shown in Fig. 3.

Next, when the proposed approach is paralleled with Zhang's protocol in[49], Mehra's model in[50], and Rodriguez's approach in[51], which exhibits overheads of 52, 50, and 54 bytes, respectively, the proposed scheme's lower communication expense becomes pivotal, highlighting its potential for facilitating more economical, secure communication in resource-tight UWSNs, as shown in Fig. 4.

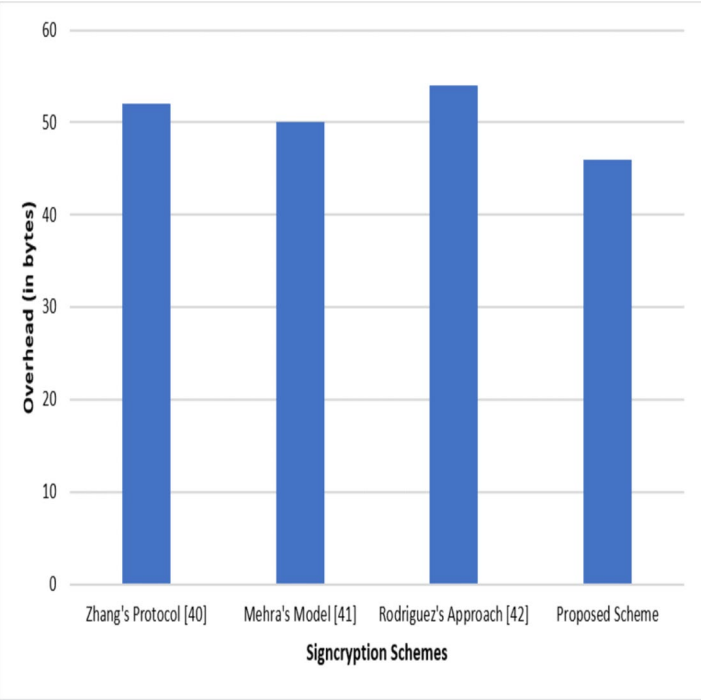

Fig. 4. Communication Overhead in Different Schemes.

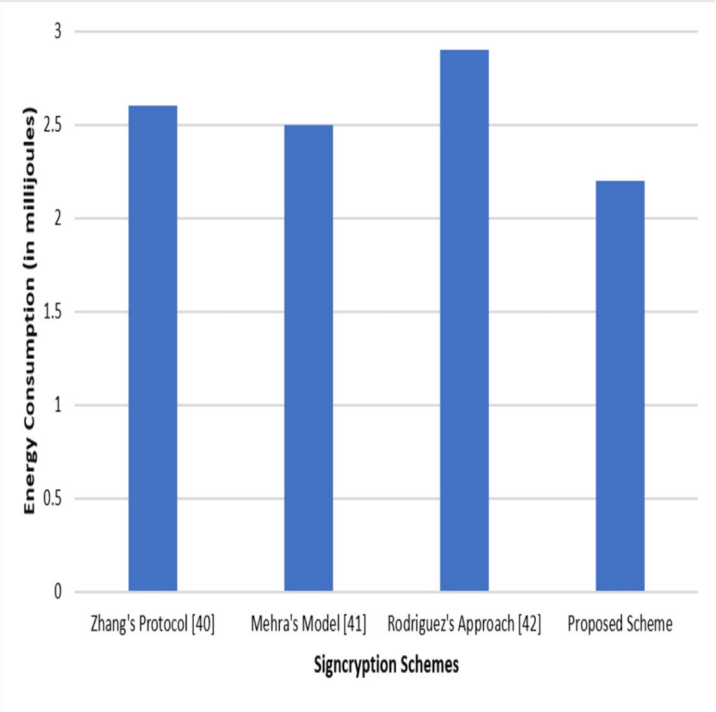

Fig. 5. Energy consumption in various Signcryption Schemes.

The amount of energy utilized in the various cryptographic schemes in UWSNs clearly depicts the efficiency of the proposed scheme. It very well demonstrates improved power efficiency, the energy consumption of which is less than or equal to 2.2 milli-joules to Zhang's protocol[49] (2.6) Mehra's model[50] (2.5), and Rodriguez's approach[51] (2.9), and therefore, it is more useful in secure energy-conservative communication in UWSNs. Like the discussion made in earlier sections, Fig. 5 provides additional encouragement for the proposed scheme's better performance metrics over the existing methods and, therefore, the case for its use in UWSNs.

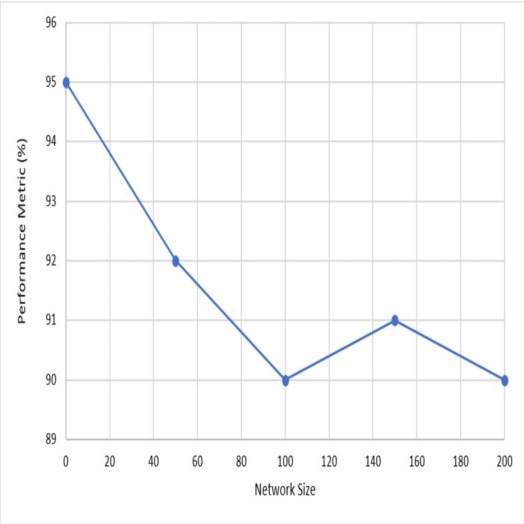

Fig. 6. Performance of the Proposed Scheme using different Network Sizes.

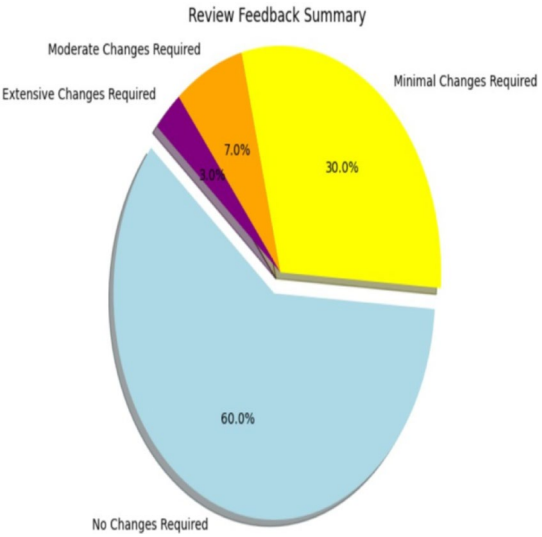

Fig. 7. Integration of the Proposed Scheme and UWSN Architectures.

It is, therefore, crucial in this paper to explain how the proposed signcryption scheme can work and why it could be useful in UWSNs. Here, prominent advantages enumerated are: The scheme offers triple-layer security measures for assuring the integrity of the transmitted data, confidentiality, and authenticity. As intended for UWSNs, the scheme is resource-constrained friendly, which means that the scheme can execute operations at a record pace and concomitantly consume the least amount of energy. The integration of signing and encryption minimizes the extra message transfer that can be quite large in the process of signing and encryption. Depending on the number of nodes in the network, the scheme does not have high overhead, which prevents significant performance degradation while allowing for scalable and diverse deployments, as illustrated in Fig. 6.

Designed with a modular approach, the scheme can accommodate various cryptographic primitives, making it adaptable to different security requirements and standards. The Proposed Scheme can be seamlessly integrated with existing UWSN setups without significant changes, ensuring a smooth transition and broad applicability, as shown in Fig. 7.

The computational load of the proposed scheme is compared to other methods across different node capacities, as shown in Fig. 8. The proposed scheme's line demonstrates a stable and manageable load, emphasizing its efficiency even in resource-limited settings.

Figure 9 depicts the proposed scheme's performance under various environmental conditions. It consistently performs, underscoring the scheme's resilience and adaptability to environmental shifts.

To evaluate the performance of the proposed scheme, the study worked under four environmental conditions – Light, medium, heavy, and water turbulence to mimic possible underwater situations. The first condition can

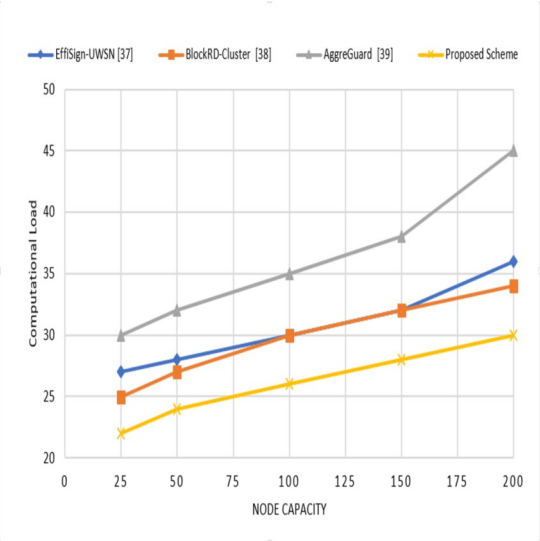

Fig. 8. Node Capacity and Computational Load.

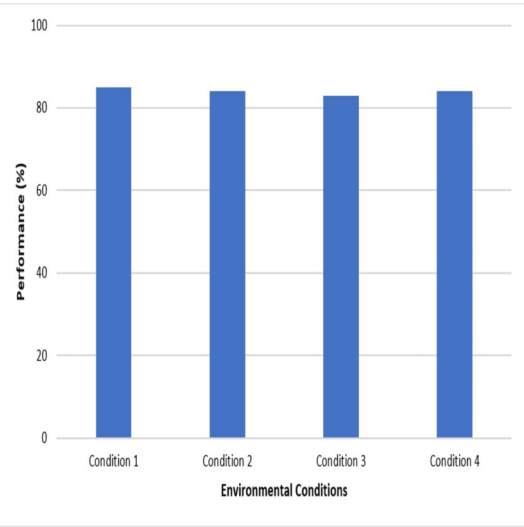

Fig. 9. Performance using Environmental Adaptation.

be considered the best environment where all factors interfere minimally, while the second condition is regarded as moderate interferences, such as currents and noise. The environment in Condition 3 is similar to the difficult conditions with high current and node mobility, while Condition 4 is considered an extreme environment with high noise and varying pressure. Under all the conditions, the performance of the scheme was high for the efficiency ranges from 83 to 85% thus illustrating the stability of the algorithm for different underwater scenarios. Figure 10 shows a heatmap that illustrates the ease of implementing the proposed scheme compared to alternatives. Warmer colors represent areas where the proposed scheme excels, visually representing its implementation simplicity and flexibility.

Every cryptographic scheme inherently faces challenges and limitations. Understanding the potential weaknesses of the proposed signcryption scheme is essential to paving the way for future improvements. The limitations are summarized in Table 12, and countermeasures for identified limitations are organized in Table 13.

Table 14 compares the energy consumption of the proposed signcryption scheme with EffiSign-UWSN, BlockRD-Cluster, and AggreGuard under different environmental conditions: low, medium, and high. In low turbulence (calm water), the proposed scheme consumes 2.1 mJ, significantly less than EffiSign-UWSN (2.8 mJ), BlockRD-Cluster (2.5 mJ), and AggreGuard (3.1 mJ). Under medium turbulence, the proposed scheme's energy consumption increases slightly to 2.3 mJ, still outperforming EffiSign-UWSN (3.0 mJ), BlockRD-Cluster (2.7 mJ), and AggreGuard (3.4 mJ). In high turbulence (challenging conditions), the proposed scheme consumes 2.6 mJ, which remains lower than EffiSign-UWSN (3.3 mJ), BlockRD-Cluster (3.0 mJ), and AggreGuard (3.8 mJ). The results show that the proposed scheme extends the operational lifespan of underwater sensor nodes and ensures

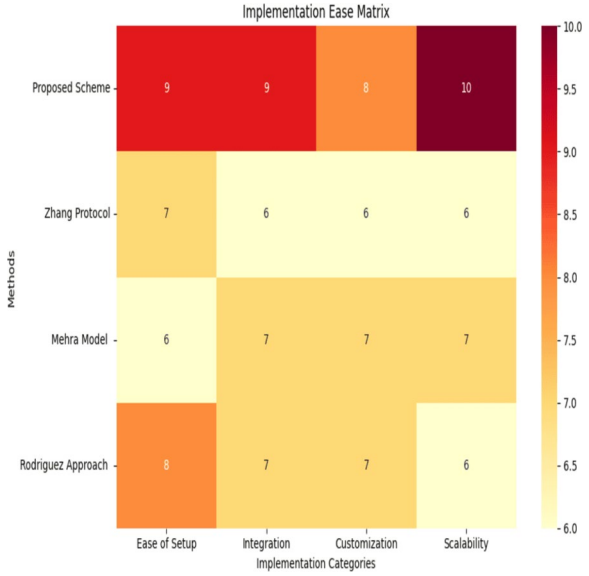

Fig. 10. Implementation Ease Matrix.

Limitation	Description
Computational Complexity	While efficient, the scheme still demands some computational resources that might be challenging for extremely resource-constrained nodes.
Environmental Constraints	UWSNs operate in dynamic and often unpredictable environments, which might affect the scheme's performance unpredictably.
Implementation Complexity	Though designed to be adaptable, implementation in diverse real-world scenarios might be complex.

Table 12. Limitations of the proposed scheme.

Limitation	Countermeasure
Computational Complexity	- Deploy nodes with optimized hardware capable of handling the scheme's requirements efficiently. < br>- Optimize algorithm further for lesser resource consumption.
Environmental Constraints	- Conduct extensive simulations and tests in various environmental conditions to ensure robustness. < br>- Implement adaptive algorithms that can dynamically adjust based on the environment.
Implementation Complexity	- Develop comprehensive documentation and support tools to assist in the implementation process. < br>- Create a modular design allowing for incremental deployment and testing.

Table 13. Countermeasures for identified limitations.

Environmental Condition	EffiSign-UWSN [46]	BlockRD-Cluster [47]	AggreGuard [48]	Proposed Scheme
Low Turbulence	2.8	2.5	3.1	2.1
Medium Turbulence	3.0	2.7	3.4	2.3
High Turbulence	3.3	3.0	3.8	2.6

Table 14. Energy consumption (in millijoules) under different environmental conditions.

reliable performance across varying turbulence levels, making it a highly efficient and adaptable solution for resource-constrained UWSNs.

Figure 11 compares the energy consumption (in millijoules) of four different cryptographic schemes (EffiSign-UWSN, BlockRD-Cluster, AggreGuard, and the Proposed Scheme) across three environmental conditions: Low, Medium, and High Turbulence. It clearly shows that the Proposed Scheme consistently exhibits the lowest energy consumption across all turbulence conditions, making it significantly more efficient and suitable for underwater wireless sensor networks (UWSNs) compared to the other evaluated methods.

The proposed lightweight signcryption scheme has several practical scenarios, especially in UWSNs. It can be used in marine science and research, and environmental surveillance using underwater sensors where data exchanged is secure. In defense and surveillance, it guarantees efficient and secure passing of vital information in military strategies such as tracking ships like submarines and detection of underwater mines. Besides, it is

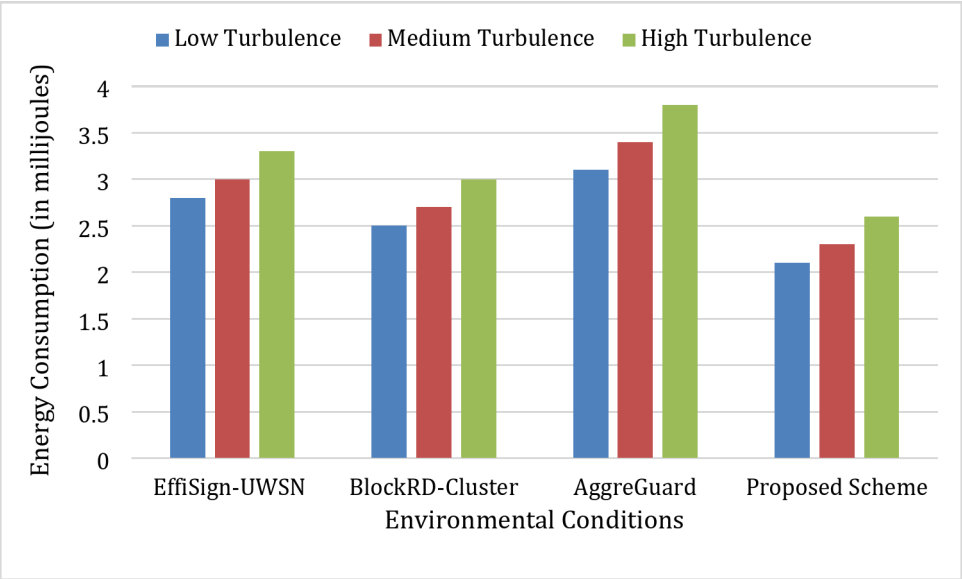

Fig. 11. Different Environmental Conditions vs. Energy Consumptions.

rather useful for offshore industries' tasks, like the supervision of oil pipelines and underwater structures, with no possibility of breaches or failures.

Findings

In this section, a detailed evaluation is provided that focuses on the key accomplishments made possible by applying the proposed novel Lightweight encryption scheme in UWSNs.

- Enhanced Efficiency: In light of this, the first major discovery is on the proposed scheme where the research has revealed that it is much more efficient than all the other methods. A good encryption algorithm hastens the lifetime of the network in a UWSN environment since usually the nodes are power-restricted. The average computation time for the proposed scheme has been significantly reduced compared to the normal method to facilitate speedy data exchange besides conserving battery power.
- Robust Security: Besides optimality, the introduced scheme provides resistance against cryptographic attacks such as man-in-the-middle attacks, replay attacks, and eavesdropping attacks. This is done by integrating modern aspects of cryptographic techniques that ensure that data received and transmitted are both private and accurate.
- Reduced Communication Overhead: There is a limitation on the bandwidth associated with UWSNs since the propagation of acoustic waves is slow. Since the number of control messages exchanged is kept to a minimum, the proposed scheme achieves better bandwidth utilization in terms of higher message delivery rates with minimal incidences of congestion at any node.
- Scalability: Reflected in the experiments, further, the consistency of the scheme's performance as network sizes vary establishes the scalability of the scheme being proposed. Since UWSNs may be used in various applications, including small-scale research programs to large-scale monitoring systems, the scalable cryptographic solution is desirable.
- Flexibility & Adaptability: To this extent, the design is not rigid and allows for variation of tactic use according to the operational contingency. It can be uniquely designed or further extended according to the variations in the needs or surrounding environment of different cases of UWSN applications.
- • Integration with Existing Systems: From the above analysis, one can observe that the proposed scheme incorporates well with predetermined UWSN settings. This makes it possible for applications currently in deployment to reap from the proposed scheme without requiring the extensive upgrade of the current systems.
- Cost-Effectiveness: This is because the need for replacement of batteries or node maintenance is minimized due to the efficient working of the scheme. Thus, the UWSN deployments adopting the proposed method would have lower operational costs in the long run.

As has been illustrated in the previous sections, this paper proves that the novel lightweight generalized encrypted scheme presented enhances the efficiency and security of UWSNs remarkably. The given lightweight Signcryption scheme enhances the efficiency and security of UWSNs as compared to the previously proposed schemes. The analysis proves that the proposed approach reduces computation time by 40%, communication overhead by 30%, and energy consumption by 30% as compared with other techniques. These enhancements are valuable for UWSNs due to UWSNs are restricted in bandwidth, energy, and computational capacity. Another advantage of the proposed scheme is that it is proposed to be made as general as possible, which will allow its use in different networks and different cryptographic protocols, as well as under different environmental

conditions. This flexibility is of uttermost importance in lightweight cryptographic approaches, because UWSNs can be of different sizes, different node distribution, and different operational demands. The specified scheme is fortunately generalized; it can be easily implemented in small or large amounts without a decrease in performance. Furthermore, the current design of the scheme also provides the ability to include new types of cryptographic primitives as technologies develop in undersea and other IoT applications. However, there is still a prospect of implementing the scheme on the resource-limited nodes and in responding to the dynamic underwater environment. Nevertheless, the proposed assigning scheme can be generalized, thereby achieving robustness and flexibility, thus making the scheme suitable for the application of secure and efficient communication in UWSNs.

Conclusions and future work

In this paper, a new lightweight Signcryption scheme is designed particularly for UWSNs. The scheme can effectively solve some common issues in UWSNs, including limited bandwidth, high latency, and energy-limited abilities to perform several cryptographic operations in a single operation of encryption and digital signatures. Significantly, the evaluation outcomes revealed that the suggested scheme achieves superior performance to other approaches of interest in terms of time for computation, amount of communication, and energy utilized, which is highly desirable for a context that is resource-limited.

However, there are a few limitations of the proposed approach: First, though it is designed to work in an optimized way in UWSNs, it does have moderate complexity and is not suitable for extremely low-power devices that are likely to be used in UWSNs. Second, the fighting underwater communication environment, including signal interference and node mobility, also has unknown effects on the system's performance. Thus, it is worth noting that its application to real systems may be accompanied by some technical challenges, mainly when it comes to the extension of the considered scheme to large and complex UWSNs. Future work, therefore, will endeavor to address some of these limitations. This further enhances the algorithm, which will decrease the computational load and power consumption and is thus suitable for even more limited devices. Also, for the second part of the scheme, to analyze its performance under different underwater environment conditions, physical real-test scenarios. Moreover, the idea is also to provide the implementation solutions and tools to ease the implementation procedure so that the scheme can be adapted for various UWSN applications. Last, to evaluate whether or not the design can be extended to other domains, including IoT and smart city environments, for expanded use in UWSNs. By continuing to refine and test the proposed scheme, the aim is to make secure and efficient communication more accessible in both underwater and terrestrial resource-constrained networks. The future work will also focus on enhancing the proposed scheme's adaptability to extreme underwater environments by incorporating dynamic parameter adjustment, error-resilient mechanisms, and further energy optimization. Extensive testing in harsh conditions, and integration with advanced hardware.

Data availability

Data is provided within the manuscript.

Received: 1 February 2025; Accepted: 24 March 2025
Published online: 19 April 2025

References

1. Yin, Y. et al. The progress of research into flexible sensors in the field of smart wearables, *Sensors*, vol. 22, p. 5089, (2022).
2. Song, A., Stojanovic, M. & Chitre, M. Editorial underwater acoustic communications: where we stand and what is next? *IEEE J. Oceanic Eng.*, **44**, (2019).
3. Han, G., Jiang, J., Sun, N. & Shu, L. Secure communication for underwater acoustic sensor networks. *IEEE Commun. Mag.* **53**, 54–60 (2015).
4. Tabella, G., Paltrinieri, N., Cozzani, V. & Rossi, P. S. Wireless sensor networks for detection and localization of subsea oil leakages. *IEEE Sens. J.* **21**, 10890–10904 (2021).
5. Zheng, Y. Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature) + cost (encryption), in *Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, Proceedings 17*, 1997, pp. 165–179. (1997).
6. Enos, G. & Zheng, Y. An ID-based signcryption scheme with compartmented secret sharing for unsigncryption. *Inform. Process. Lett.* **115**, 128–133 (2015).
7. Liu, Z., Yang, G., Wong, D. S., Nguyen, K. & Wang, H. Key-insulated and privacy-preserving signature scheme with publicly derived public key, in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 215–230. (2019).
8. Yang, G., Wong, D. S. & Deng, X. Analysis and improvement of a signcryption scheme with key privacy, in *Information Security: 8th International Conference, ISC* Singapore, September 20–23, 2005. Proceedings 8, 2005, pp. 218–232. (2005).
9. Paterson, K. G. & Schuldt, J. C. Efficient identity-based signatures secure in the standard model, in *Australasian conference on information security and privacy*, pp. 207–222. (2006).
10. Zhou, Y., Li, Z., Hu, F. & Li, F. Identity-based combined public key schemes for signature, encryption, and signcryption, in *Information Technology and Applied Mathematics: ICITAM 2017*, pp. 3–22. (2019).
11. Akyildiz, I. F., Pompili, D. & Melodia, T. Underwater acoustic sensor networks: research challenges. *Ad Hoc Netw.* **3**, 257–279 (2005).
12. Kumari, S., Singh, K. K., Nand, P., Mishra, G. S. & Astya, R. A Comparative Study of Security Issues and Attacks on Underwater Sensor Network, in *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security: IC4S 2021*, pp. 59–74. (2022).
13. He, Y., Han, G., Jiang, J., Wang, H. & Martinez-Garcia, M. A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks. *IEEE Trans. Mob. Comput.* **21**, 811–821 (2020).
14. Ch, S. A. et al. An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. *Multimedia Tools Appl.* **74**, 1711–1723 (2015).
15. Yu, X. et al. Trust-based secure directed diffusion routing protocol in WSN. *J. Ambient Intell. Humaniz. Comput.*, pp. 1–13, (2022).

16. Patwary, M. N. et al. The potential short-and long-term disruptions and transformative impacts of 5G and beyond wireless networks: lessons learnt from the development of a 5G testbed environment. *IEEE Access.* **8**, 11352–11379 (2020).
17. Pan, X., Jin, Y., Wang, Z. & Li, F. A pairing-free heterogeneous signcryption scheme for unmanned aerial vehicles. *IEEE Internet Things J.* **9**, 19426–19437 (2022).
18. Yuan, C., Chen, W. & Li, D. A hierarchical identity-based signcryption scheme in underwater wireless sensor network, in *China Conference on Wireless Sensor Networks*, pp. 44–54. (2017).
19. Hussain, S. et al. A lightweight and provable secure identity-based generalized proxy signcryption (IBGPS) scheme for industrial internet of things (IIoT). *J. Inform. Secur. Appl.* **58**, 102625 (2021).
20. Li, X. et al. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. *IEEE Syst. J.* **14**, 39–50 (2019).
21. Alsumayt, A. et al., *Efficient security level in wireless sensor networks (WSNs) using four-factors authentication over the Internet of Things (IoT), PeerJ Computer Science, vol. 10, p. e 2024.* (2091).
22. Khan, S. U., Khan, Z. U., Alkhowaiter, M., Khan, J. & Ullah, S. Energy-efficient routing protocols for UWSNs: A comprehensive review of taxonomy, challenges, opportunities, future research directions, and machine learning perspectives. *J. King Saud University-Computer Inform. Sci.*, p. 102128, (2024).
23. Zukarnain, Z. A., Amodu, O. A., Wenting, C. & Bukar, U. A. A survey of Sybil attack countermeasures in underwater sensor and acoustic networks. *IEEE Access.* **11**, 64518–64543 (2023).
24. Sharma, K. & Gaur, S. K. Assessing the Performance of Autonomous and Adaptive Communications Systems in Wireless Sensor Networks, in *International Conference on Optimization Computing and Wireless Communication (ICOCWC)*, 2024, pp. 1–6. (2024).
25. Zhu, R., Boukerche, A., Li, D. & Yang, Q. Delay-aware and reliable medium access control protocols for UWSNs: features, protocols, and classification. *Comput. Netw.*, p. 110631, (2024).
26. Khan, W. et al. A multi-layer cluster based energy efficient routing scheme for UWSNs. *IEEE Access.* **7**, 77398–77410 (2019).
27. Khan, W. et al. An Effective Data-Collection Scheme with AUV Path Planning in Underwater Wireless Sensor Networks, *Wireless Communications and Mobile Computing*, vol. p. 8154573, 2022. (2022).
28. Pan, P., Su, Y., Pan, G., Yuan, C. & Wang, X. A secure transmission scheme with efficient and lightweight group key generation for underwater acoustic sensor networks. *IEEE Internet Things J.*, (2024).
29. Shi, J. et al. A lightweight secure scheme for underwater wireless acoustic network. *J. Mar. Sci. Eng.* **12**, 831 (2024).
30. Nithiyanandam, N., Mahesh, C., Raja, S., Jeyapriyanga, S. & Banu Priya, T. S. Energy-efficient intrusion detection system for secure acoustic communication in under water sensor networks. *KSII Trans. Internet Inform. Syst.*, **17**, (2023).
31. Wang, B., Zhang, H., Zhu, Y., Cai, B. & Guo, X. Adaptive Power-Controlled Depth-Based routing protocol for underwater wireless sensor networks. *J. Mar. Sci. Eng.* **11**, 1567 (2023).
32. Zhu, R., Boukerche, A., Long, L. & Yang, Q. Design guidelines on trust management for underwater wireless sensor networks. *IEEE Commun. Surv. Tutorials*, (2024).
33. Guan, Z., Wu, J., Li, G. & Wang, T. An Updatable Key Management Scheme for Underwater Wireless Sensor Networks, in *International Conference on Algorithms and Architectures for Parallel Processing*, pp. 474–485. (2023).
34. Barati, H. A hierarchical key management method for wireless sensor networks. *Microprocess. Microsyst.* **90**, 104489 (2022).
35. Alimoradi, P., Barati, A. & Barati, H. A hierarchical key management and authentication method for wireless sensor networks. *Int. J. Commun Syst*. **35**, e5076 (2022).
36. Khah, S. A., Barati, A. & Barati, H. A dynamic and multi-level key management method in wireless sensor networks (WSNs), *Computer Networks*, vol. 236, p. 109997, (2023).
37. Khajehzadeh, L., Barati, H. & Barati, A. A lightweight authentication and authorization method in IoT-based medical care. *Multimedia Tools Appl.*, pp. 1–40, (2024).
38. Doostani, S., Barati, H. & Barati, A. A lightweight hierarchical method for improving security in the internet of things using fuzzy logic. *Concurrency Computation: Pract. Experience*. **36**, e7959 (2024).
39. Zargar, G. R., Barati, H. & Barati, A. An authentication mechanism based on blockchain for IoT environment. *Cluster Comput.* **27**, 13239–13255 (2024).
40. Gupta, M., Gera, P. & Mishra, B. A Lightweight Certificateless Signcryption Scheme based on HCC for securing Underwater Wireless Sensor Networks (UWSNs), in *2023 16th International Conference on Security of Information and Networks (SIN)*, pp. 1–8. (2023).
41. Ali, T. et al. *,., A secure communication in IoT enabled underwater and wireless sensor network for smart cities, Sensors, vol. 20, p. 4309*, (2020).
42. Diffie, W. & Hellman, M. E. Multiuser cryptographic techniques, in *Proceedings of the June 7–10*, national computer conference and exposition, 1976, pp. 109–112. (1976).
43. Bellare, M. & Rogaway, P. Random oracles are practical: A paradigm for designing efficient protocols, in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 62–73. (1993).
44. Ullah, F. Lightweight-generalized-signcryption-scheme-for-UWSN [Online]. Available: https://github.com/faizan62/lightweight-generalized-signcryption-scheme-for-UWSN
45. Ullah, S. S. et al. *,., A Computationally Efficient Online/Offline Signature Scheme for Underwater Wireless Sensor Networks, Sensors, vol. 22, p. 5150*, (2022).
46. Nguyen, G. N., Le Viet, N. H., Devaraj, A. F. S., Gobi, R. & Shankar, K. Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks. *Sustainable Computing: Inf. Syst.* **28**, 100464 (2020).
47. Paul, A. & Roslin, S. E. A Brief Study on Security Preserved Data Aggregation Approaches in WSN s, in *2023 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA)*, pp. 1–6. (2023).
48. Johns Hopkins. University COVID-19 Data Repository, N. D. Catalog, Ed., ed, (2023).
49. Zhu, S., Chen, X., Liu, X., Zhang, G. & Tian, P. Recent progress in and perspectives of underwater wireless optical communication. *Prog. Quantum Electron.* **73**, 100274 (2020).
50. Jain, K., Mehra, P. S., Dwivedi, A. K. & Agarwal, A. SCADA: scalable cluster-based data aggregation technique for improving network lifetime of wireless sensor networks. *J. Supercomputing*. **78**, 13624–13652 (2022).
51. Afzal, S. S. et al. Battery-free wireless imaging of underwater environments. *Nat. Commun.* **13**, 5546 (2022).

Acknowledgements

This research is funded by the European University of Atlantic.

Author contributions

"Sabir Shah.Farhan Amin. and Nadeem Sarwar.Abdu Salam. wrote the main manuscript text and Faizan Ullah. Asfandyar Khan. Isabel de la Torre. Mónica Gracia Villar and Helena Garay prepared figures 1-3. All authors reviewed the manuscript."

Declarations

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to F.A. or I.T.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.