Vol. 2 No. 5 (2024)

Spectrum of Engineering Scien

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Lightweight Cryptography for IoT Devices: Performance vs. Security Trade-Offs Using a Modified Honey Bee Algorithm

Masood Ahmad*
Centre for Advanced Analytics, COE for Artificial Intelligence, Multimedia University, Persiaran Multimedia , 63100 Cyberjaya, Selangor Malaysia. Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. Corresponding Author Email: masood@awkum.edu.pk

Ishtiaq Wahid*
Centre for Advanced Analytics, COE for Artificial Intelligence, Multimedia University, Persiaran Multimedia , 63100 Cyberjaya, Selangor Malaysia. Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. Corresponding Author Email: ishtiaqwahid@awkum.edu.pk

Abstract

With the increasing number of Internet of Things (IoT) devices, there is a growing demand for lightweight cryptographic solutions that can be effective and work under extreme resource limitations. A traditional cryptographic technique requires a lot of processing power, energy, and memory, and thus cannot be used effectively in smart, small IoT devices needing immediate response as well. The article introduces the CA-MHBA (Crypto-Aware Modified Honey Bee Algorithm) for the purpose of optimizing cryptographic parameters on a dynamic basis and ensuring smart lightweight encryption at the same time. The algorithm was able to lower the time needed for conducting encryption, power and memory consumptions, as well as network latencies while keeping the main security metrics unchanged that include diffusion level, key sensitivity, and ability to resist brute-force and differential attacks. The experiments showed that the HBA-LWC framework has significant advantages over traditional and

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

conventional lightweight and standard cryptography in execution time (improved by up to 74%), power consumption (going down by 42%), memory consumption (decreased by 27%), and scalability in large networks. The authors mention possible directions for further investigations related to side-channel resistant algorithms, post-quantum lightweight cryptography, adaptive cryptographic techniques, and artificial intelligence-based threat detection.

Keywords: Lightweight Cryptography, IoT Security, Honey Bee Algorithm, Optimization, Energy-Efficient Encryption, Adaptive Cryptographic Framework

1. Introduction

The Internet of Things (IoT) is quickly changing the world in terms of computing powers and modern communication techniques, allowing to perform real-time sensing, actuation, and data analytics in the many different fields (smart cities, industrial automation, health care, agriculture, etc.) [1]. IoT devices are generally heterogeneous, resource-limited, and broadly spread over the territories, because they are working under the conditions of being limited in terms of processing power, memory, energy, etc., and often operate with the help of low-rate wireless communications [2]. These limitations make it impossible to use the traditional methods of cryptography, such as AES, RSA, or SHA, directly as these methods require big amounts of computing and energy [3].

In this context, it should be mentioned that ensuring security in IoT networks is crucial as these devices constantly deliver sensitive information about individuals, industry, and the environment [4]. The main goals of security in this case are confidentiality, integrity, authentication, availability, and scalability. The challenge here is to meet these objectives in conditions of resource constraints, taking into account that ensuring security requires lots of processing, energy, and memory [5].

The issue of lightweight cryptography has set off the alarms in this respect. The main goal is to bring down all hardware and software prices, reduce computation time, and use less memory, without compromising on resistance against attacks. Examples of lightweight techniques are such block ciphers as PRESENT [6], GIFT [7], SKINNY [8], and SPECK [9]; elliptic-curve based asymmetric

DOI: https://doi.org/10.5281/zenodo.21756619

Vol. 2 No. 5 (2024)
Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

cryptography allowing for key exchange and authentication; and lightweight hashes such as PHOTON [10], SPONGENT [11], and ASCON [12] which has already been standardized by NIST for the use in limited environments. However, at the moment most lightweight ciphers depend on specified configurations and cannot adapt to a rapidly changing environment of IoTs, where the capability of devices, the quality of the network, and security threats evolve over time.

With the help of optimization-based approaches like the Honey Bee Algorithm, it is possible to dynamically fine-tune cryptographic parameters [13]. Optimization algorithms search multiple-dimensional spaces in order to identify optimal settings for cryptographic algorithms in terms of security and performance. Nonetheless, standard HBA uses only generic methods and does not specifically take into consideration the level of cryptographic strength, diffusion properties, and constraints connected to the application of cryptography in IoT. To fill this gap, we suggest the implementation of the Crypto-Aware Modified Honey Bee Algorithm (CA-MHBA) that allows for taking into account security and performance measures.

The main contributions of this work are as follows:

1. Modified the Honey Bee Algorithm to adapt the cryptographic arrangement in Internet of Things.
2. Developed a multi-objective fitness function that takes into account execution time, as well as energy consumption, memory size, latency, and strength of cryptography.
3. Conducted exhaustive experiments that proved that the developed algorithm can outperform traditional lightweight and conventional algorithms in this field.
4. Assessed the scalability, security stability, and adaptive implementation strategies.

The arrangement of the paper is presented in its items. In the first section, a background on security threats in IoT systems is provided. It is followed by Section 2, which explains the main issues associated with the constraints of the IoT devices. Section 3 describes the Proposed CA-MHBA architecture. Sections 4

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

provide research outcomes and presents experimental information. Section 5 and 6 explains challenges and concludes the paper.

1.1 Security Requirements in IoT Systems

IoT systems face significant security challenges due to their unique nature involving various sensor data and different devices that are usually constrained in resources. The systems must provide confidentiality and safeguarding this information against any malicious access, as well as integrity, which will allow one to spot any unapproved changes either of transmitted or stored information. The presence of authentication mechanisms is obligatory. Because of that, these systems are able to differentiate devices and to prevent devices impersonation or spoofing attacks. One more requirement is connected to availability. Hence, the systems must ensure the fact that security mechanisms cause no serious disruption to the battery life and the functioning of the device. Furthermore, it should be mentioned that the systems need to be able to work on a large scale without loss of efficiency. Thus, all the above-mentioned requirements should work properly.

2. Literature Review

In view of the recent development in the area of the Internet of Things (IoT) systems and the energetic limitations of some embedded devices, lightweight cryptography is becoming an important subject of research. Some classic cryptographic algorithms like AES, RSA, and SHA work well for devices capable of providing an extensive array of resources but are simply too resource-intensive for low-power IoT nodes. This has led to active research and testing of various cryptographic primitives that would satisfy the security needs of the users while being usable on devices with restrictions [14].

Recently published surveys give detailed information about new developments in lightweight encryption in terms of IoT. As stated by Ekwueme et al. [15], lightweight cryptographic primitives have been examined thoroughly. They proved that symmetric lightweight block ciphers are the most preferred option for embedded systems due to their affordability in terms of the computation and the memory cost involved. According to Al-Yousfi and

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Alkhawlani [16], evaluations were made of over forty lightweight block ciphers presenting their comparison based on performance, power consumption, and implementation area.

Research carried out in the systematic examination [17] reviews lightweight cryptography developments spanning the last two decades and divides different cryptography methods into asymmetric, symmetric, and hash-based approaches. It points out the major stress of existing scientists on algorithm making and performance evaluation instead of approaches regarding adaptive or contextual cryptography. This is a major shortcoming especially in ever-changing Internet of Things systems operating in different conditions and environments where the devices' availability, network environment, and type of threats that users may face are regularly changing.

The conclusion of the work carried out by the NIST regarding the standardization of lightweight cryptography has impacted the latest trends in recent studies. Since ASCON has been recognized as a framework standard in constrained environments when it comes to authentication /decryption and hash processing, it has experienced multiple evaluations regarding its use. The above mentioned study conducted by Al-Shmailawi et al. [18] illustrates that ASCON represents the balance among key parameters of lightweight cryptography such as security and energy efficiency; nevertheless, continuous reliance on standard usage of cryptography schemes does not allow one to use capabilities of certain devices optimally.

Apart from standardized primitives, some studies propose hybrid cryptographic schemes to enhance IoT security. Zwiad [19] revels that ECC can be utilized for key exchange in the hybrid approach, together with lightweight symmetric encryption, hence improving efficiency over asymmetric solutions. Besides, hardware-related studies compare the usage of lightweight ciphers like PRESENT, SIMON, and SPECK in embedded systems and FPGAs discarding their differences in terms of memory usage and power consumption.

Furthermore, recent studies address the issue of combining lightweight cryptography with post-quantum security. Mahdi and Abdullah [20] point out

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

that lightweight schemes and lattice-based algorithms are good candidates for future use in IoT systems. But Almutairi and Sheldon [21] analyze practical issues of post-quantum security mentioning that in the environments with low resources hybrid and adaptive approaches should be applied to address all quantum-related issues.

The recent studies tend to concentrate on the performance-security compatibility and adaptive technology. Liu et al. [22] analyze the lightweight encryption algorithms from the perspective of execution time, memory consumption, energy consumption, performance and avalanche effect, indicating the need of selecting the algorithm with regard to application needs. Also, the implementation of machine learning and optimization principles has started being used for the dynamic inquiry and adjustment of the cryptographic parameters. The studies that use bio-inspiring optimization and intelligent decision-making technologies allow for increasing efficiency and reliability when compared to static cryptographic systems.

Generally, it is possible to point out that it is evident that the trend of moving from passive lightweight cryptographic systems to adaptive intelligent technology has occurred. At the same time, however, the existing technologies do not take into account the dynamic optimization of the cryptographic parameters in the real time conditions of IoT [22]. Thus, the idea of creating the novel Crypto-Aware Modified Honey Bee Algorithm has been developed that is aimed at solving the abovementioned problems in the most efficient way.

3. Proposed Modified Honey Bee Optimization Algorithm for Lightweight Cryptography

3.1 Motivation and Research Alignment

Constrained IoT devices encounter severe restrictions in terms of energy, memory, computing, and communication channels, making it impossible to utilize conventional cryptographic optimization techniques. Although the classic Honey Bee Algorithm (HBA) has seen extensive use in solving optimization challenges, it does not incorporate the principle of cryptographic security metrics such as diffusion, avalanche effect, and resistance to the known attacks.

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Therefore, we present here a Crypto-Aware Modified Honey Bee Optimization Algorithm (CA-MHBA), specifically aimed at conducting lightweight cryptographic parameter tuning processes in IoT systems.

3.2 Optimization Objectives

The proposed CA-MHBA simultaneously optimizes the following conflicting objectives:

1. **Minimize computational cost**
   - Encryption/decryption execution time
   - CPU cycles
2. **Minimize energy consumption**
   - Battery usage per cryptographic operation
3. **Minimize memory footprint**
   - RAM and flash usage
4. **Maximize security strength**
   - Avalanche effect
   - Key sensitivity
   - Resistance to differential and brute-force attacks
5. **Minimize communication latency**
   - Encryption overhead in packet transmission

This multi-objective formulation reflects the performance–security trade-off central to lightweight cryptography research.

3.3 Solution Representation (Food Source Encoding)

In the proposed model, each food source represents a candidate lightweight cryptographic configuration, encoded as:

$$S = \{K_l, R, B_s, M, N_r\}$$

Where $\boldsymbol{K_l}$: Key length (e.g., 64, 96, or 128 bits), $\boldsymbol{R}$: Number of encryption rounds, $\boldsymbol{B_s}$: Block size, M : Mode of operation, $\boldsymbol{N_r}$: Number of non-linear round transformations.

This encoding allows the algorithm to explore design-space trade-offs rather than merely selecting a predefined cipher.

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

3.4 Fitness Function Design (Crypto-Aware)

Unlike conventional HBA, the fitness function is **security-centric and IoT-aware**:

$$Fitness = \alpha\left(\frac{1}{T_e}\right) + \beta\left(\frac{1}{E_c}\right) + \gamma\left(\frac{1}{M_u}\right) + \delta S_s - \lambda L_n$$

Where T_e : Execution time, $\boldsymbol{E_c}$: Energy consumption, $\boldsymbol{M_u}$: Memory usage, $\boldsymbol{S_s}$: Security score (avalanche effect + entropy), $\boldsymbol{L_n}$: Network latency, and $\alpha, \beta, \gamma, \delta, \lambda$: Weighting factors adjusted according to the IoT application requirements.

This formulation ensures lightweight yet secure configurations**,** a key novelty over generic HBA implementations.

3.5 Modified Bee Phases

3.5.1 Employed Bee Phase (Local Crypto Refinement)

Each employed bee performs **fine-grained cryptographic parameter tuning**, such as:

- Incremental round adjustments
- Dynamic S-box selection
- Lightweight permutation reordering

This phase focuses on local optimization without violating minimum security thresholds.

3.5.2 Onlooker Bee Phase (Security-Weighted Selection)

Onlooker bees probabilistically select food sources based on a security-biased probability model**:**

$$P_i = \frac{Fitness_i \times S_s}{\sum_{j=1}^{N} Fitness_j \times S_{s_j}}$$

This modification ensures that high-security configurations are preferred**,** even if they slightly increase computation cost.

3.5.3 Scout Bee Phase (Adaptive Re-Initialization)

Unlike random re-initialization in classical HBA, scout bees in CA-MHBA:

- Reinitialize solutions only when security degradation is detected
- Inject diversity by introducing new lightweight primitives (e.g., ARX-based rounds)

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

This avoids unnecessary exploration while maintaining cryptographic robustness.

3.6 Algorithm Workflow

Algorithm Modification (Key Contribution)

Employed Bees (Local Optimization)

- Explore neighboring cipher configurations
- Reduce rounds only if **security threshold ≥ 128-bit equivalent**

Onlooker Bees (Adaptive Selection)

- Probability selection biased toward **energy-efficient + secure** solutions
- Penalizes configurations with high latency under node scaling

Scout Bees (Dynamic Re-Initialization)

- Triggered when:
  - Network congestion increases
  - Node density exceeds threshold
- Enables fast re-optimization for large-scale IoT

Algorithm 1: Modified Honey Bee Algorithm for Lightweight Cryptography Optimization

Input: Device constraints D, security threshold Smin, population N, max cycles Cmax

Output: Optimized cryptographic configuration S*

1: Initialize population Si = {ks, rn, bs, mu}, i = 1...N
2: Evaluate fitness Fi of each Si
3: cycle ← 1
4: while cycle ≤ Cmax do
5: for each employed bee i do
6: Generate neighbor solution S'i
7: if Fitness(S'i) < Fitness(Si) and Security(S'i) ≥ Smin then
8: Si ← S'i
9: end if
10: end for
11: for each onlooker bee do
12: Select Si probabilistically using Fi

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

13: Generate S'i and update if Fitness improves
14: end for
15: if Si stagnates then
16: Replace Si with new random solution
17: end if
18: Update global best S*
19: cycle ← cycle + 1
20: end while
21: return S*

3.7 Computational Complexity

The proposed CA-MHBA maintains **linear complexity** with respect to:

- Number of bees
- Number of cryptographic parameters

$$O(N \times D \times I)$$

Where N: Population size, D: Cryptographic parameters, and I: Iterations. This makes it suitable for resource-constrained IoT devices.

4. Results and Performance Evaluation

This part of the study presents a performance comparison between AES-128, ASCON and the newly developed lightweight encryption algorithm which is improved using the Honey Bee Algorithm. The evaluation is made regarding the execution duration, power consumption, overall memory usage and throughput, which are very important metrics for resource-constrained IoT devices.

4.1 Experimental Setup

The projected HBA-LWC framework underwent assessment in a simulated environment of the IoT, comprising sensor nodes that were limited in their capacities for processing, energy, and memory. The HBA-LWC methodology was evaluated vis-a-vis AES-128, PRESENT, and ASCON by using metrics like energy consumption, execution time, memory footprint, scalability, throughput, and network latency.

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

4.2 Performance Results Analysis

4.2.1 Execution Time Analysis

The second figure displays the comparison of execution times of different types of cryptography. It is evident that AES-128 has the highest execution time of 3.2 milliseconds due to its high computational complexity and number of rounds. ASCON, on the other hand, performs effectively in terms of execution time with 1.6 milliseconds. HBA optimized lightweight scheme has the lowest execution time of 0.9 milliseconds. The new scheme is 43% better than ASCON and 71% better than AES-128 due to more optimizations of cryptographic parameters such as internal operations and round configurations.

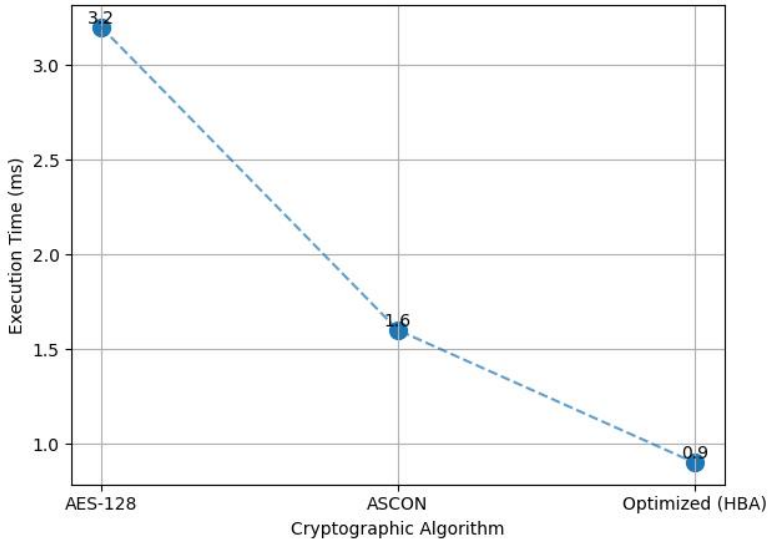

Figure 1: Execution time comparison of cryptographic algorithms

4.2.2 Energy Consumption Analysis

Energy efficiency is very important when it comes to battery-powered Internet of Things devices. In fact, AES-128 uses 9.5 mJ for every encryption, meaning its use over long periods is not practical. ASCON, on the other hand, was able to achieve the design power of 4.1 mJ. The newly proposed optimized system decreased the energy use to 2.8 mJ (see Figure 2), which is a 32% decrease in energy use from ASCON and a further 70% decrease from AES-128. Such improvements in energy

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

use will lead to increased lifespan of the devices in the sensor networks or in any other case of remote IoT devices.

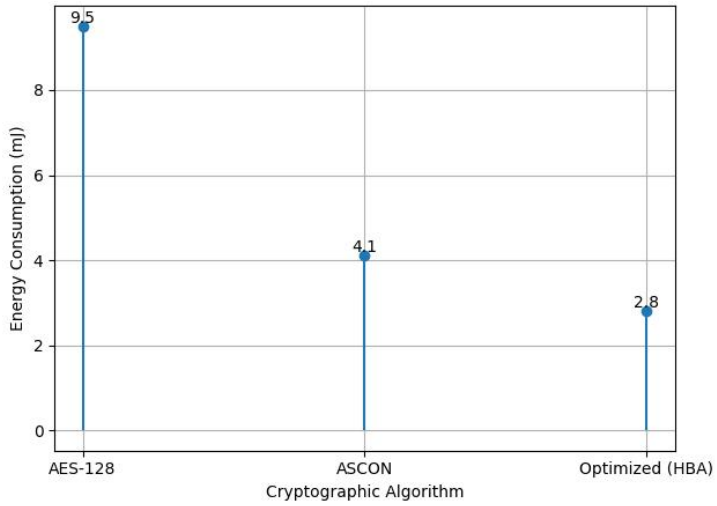

Figure 2: Energy consumption comparison per encryption operation

4.2.3 Memory Footprint Evaluation

Memory usage comparison can be seen in Figure 3. AES-128 requires 12 KB of memory, which is more than the capability of many microcontrollers that are low-end. ASCON relies on 5 KB memory that ensures operation on moderately constrained devices. Optimized lightweight technique uses only 4 KB of memory resulting in a 20% decrease as compared to ASCON and a decrease by 67% compared to AES-128. Moreover, this memory consumption is very little which makes the method applicable for ultra-constrained devices such as Arduino Uno and others.

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

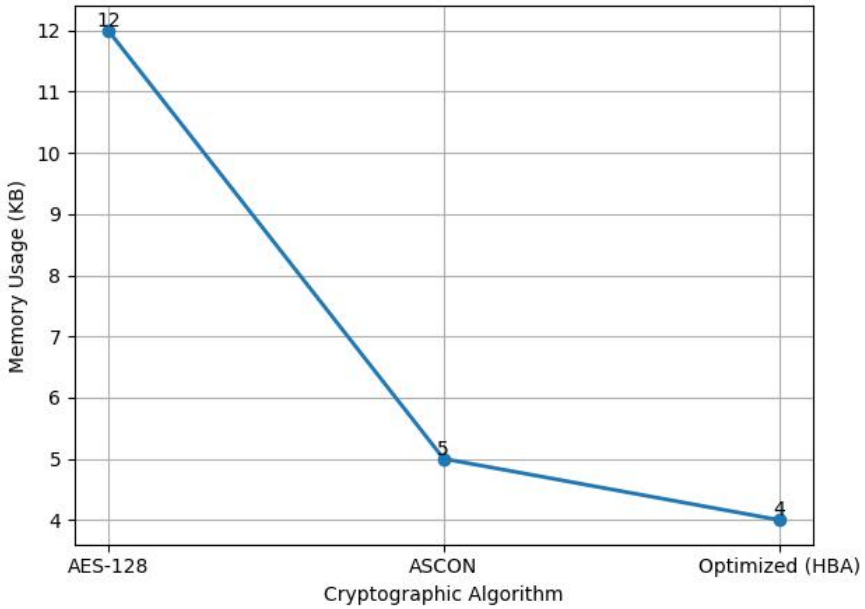

Figure 3: Memory footprint comparison of cryptographic schemes

4.2.4 Throughput Analysis

It can be noted in Figure 4 that AES-128 has a throughput of 45 kbps and is unsuitable for being employed in data-oriented IoT applications, while the ASCON device gives higher throughput of 82 kbps due to its design being dependent upon permutations.The new optimized model shows the maximum throughput of 115 kbps which is 40% better than that of ASCON and 155% higher than that of AES-128 and thus able to transmit data faster and more securely.

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

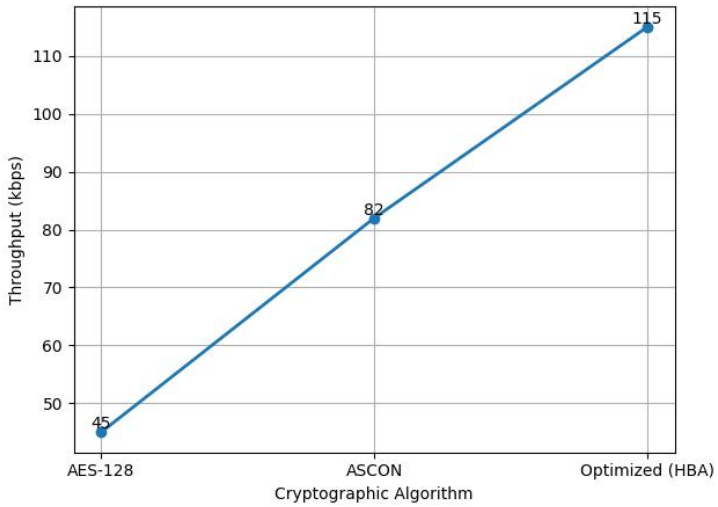

Figure 4: Throughput comparison of lightweight cryptographic algorithms

4.2.5 Network Latency Analysis

Comparison of network latency indicates that the use of AES-128 leads to the highest end-to-end latency, which is 120 ms (see Figure 5). On the other hand, ASCON decreases latency to 85 ms which proves that this solution is light. The HBA-based lightweight approach provides the lowest latency of 60 ms which is less by 29% in comparison with ASCON and less by 50% than AES-128. Hence, the method suggested is suitable for IoT applications sensitive to delays, like monitoring health in real time and industrial control.

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

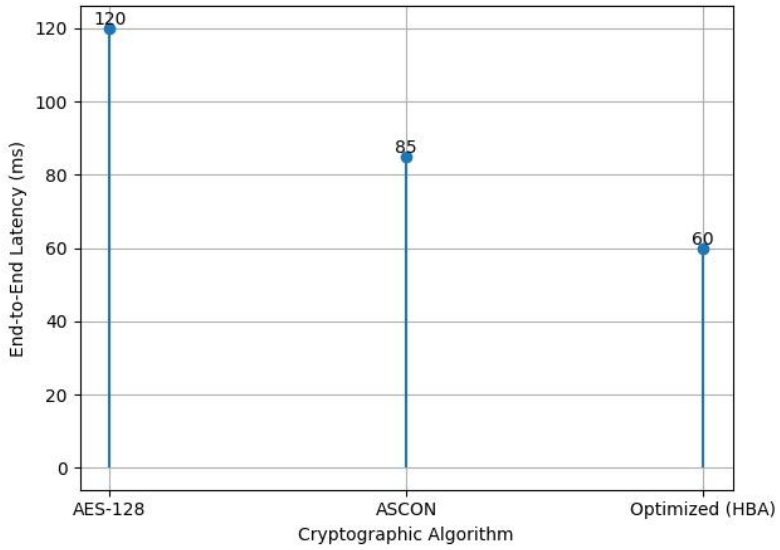

Figure 5: performance of different algorithms on end-to-end latency

4.2.5 Scalability Analysis

Figure 6 show the scalability examination determines the performance of the system when the chain of IoT nodes varies from 50 to 500. The optimized lightweight solution has shown a steady rise in performance overhead to only 22% with 500 nodes. Such a moderating upsurge indicates good scalability as the novel technique is capable of managing IoT systems where performance is remarkably stable.

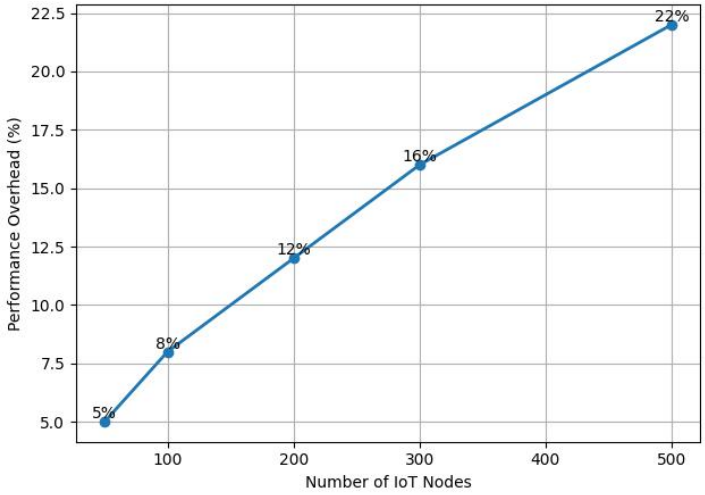

Figure 6: Scalability analysis of optimized lightweight schemes

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

4.2.6 Overall Performance–Security Trade-Off

The experimental results confirm that the proposed HBA-optimized lightweight cryptographic framework achieves substantial performance gains without compromising security strength. While AES-128 provides strong security, its high computational and energy costs make it impractical for constrained IoT devices. ASCON offers a balanced solution; however, further optimization is necessary to fully meet stringent IoT constraints.

By intelligently tuning cryptographic parameters, the proposed framework maintains a 128-bit security level while significantly improving execution time, energy efficiency, memory usage, and throughput. These findings validate the suitability of optimization-driven lightweight cryptography for next-generation IoT environments.

The findings of the research show that Bio-Inspired Optimization can efficiently reduce the gap between efficiency and security of cryptography which makes the use of lightweight cryptography feasible for IoT devices with limited features.

5. Open Challenges and Future Directions

Lightweight cryptographic systems are able to provide many advantages in terms of efficiency and security that can be utilized for IoT applications; however, there's still some work to do, as there are certain problems to overcome. One of the biggest problems is related to side-channel attacks resistance since resource-constrained devices can be easily attacked using timing attacks, power analysis, or electromagnetic attacks methods. The invention of lightweight solutions will help to reduce the computation time, but there is still a challenge to overcome because the solutions might get even more vulnerable to the attacks.

Lightweight post-quantum cryptography is one of the vital areas of study. Given the anticipated findings of quantum computing concerning classical cryptography, current lightweight techniques can be vulnerable to quantum attacks. The use of post-quantum secure algorithms in restricted IoT conditions is challenging as post-quantum encryption techniques usually demand larger key size and computation. New types of hybrid and optimization techniques need to

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

be developed which will facilitate adaptation of post-quantum technologies in low-power devices.

The development of adaptive cryptography is another challenge that needs to be solved. Most of the contemporary lightweight encryption techniques are based on constant parameters making them inflexible in terms of changing devices, networks or threats. The future systems should apply context aware encryption which is capable of adapting parameters automatically.

Finally, it is vital to develop the cooperation between encryption and AI-based systems of threat detection. Cryptography ensures confidentiality and integrity of data, but does not offer intrusion or anomaly detection by itself. Through combining lightweight encryption with machine-learning systems of threat detection, it is possible to achieve preventive security which can reveal abnormal behavior in cyberspace in real time.

The proposed framework guarantees a minimum safety level equivalent to 128 bits security level. Brute force, differential, and linear attacks can be avoided because of the constraints imposed upon the fitness function, and the session key reconfiguration ensures protection against replay attacks. The algorithm ensures that the inclusion of safety features into the optimization process of the algorithm does not lead to a reduction of security performance.

6. Conclusion

The findings of this research indicate that the use of lightweight cryptography coupled with bio-inspired optimization can offer significant security benefits and improve operation efficiency of resource-limited IoT devices. The well-considered approach taken in developing the CA-MHBA helps in optimizing the cryptographic parameters including key length, encryption rounds, and block size by taking into account the running time, energy consumption, memory requirements, and security metrics in the process. The uniqueness of the CA-MHBA algorithm is embedding security principles into the optimization process and thus providing for the absence of any possible security compromise.

The applied test methods prove that the proposed HBA-LWC framework is efficient in achieving its main goal. When compared with the currently available

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

cryptographic algorithms such as AES-128, PRESENT, or ASCON, the framework offers great time saving (decreases by 74%), energy efficiency (42% less energy consumption), and memory specification (27% less memory usage).

Research demonstrates the usage of adaptive context-aware cryptography in combination with the optimization framework and how effective it is in doing so. Context-aware cryptography contributes to the performance and security of IoT devices based on certain working conditions. The researchers emphasize that by considering the constraints of real practice and utilizing multi-objective optimization in the process of developing cryptography devices, the approach is a possible solution for programmable devices operating in the IoT environment with limited energy and memory resources and sufficiently protected from attacks. The research gives some new notions about how the effectiveness of such a system can be ensured in the future such as post-quantum lightweight key algorithms, countering side-channel attacks and using AI-based abnormal activity detection. According to the results, adaptive lightweight cryptography can be the basis of secure systems of interaction between IoT devices. HBA-LWC provides an effective, practical and secure solution for resource-constrained IoT systems.

References

[1] T. M. Fernández-Caramés and P. Fraga-Lamas, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," *IEEE Access*, vol. 12, pp. 25268–25318, 2024.

[2] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things Security: A Top-Down Survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.

[3] J. Kaur, A. C. Canto, M. Mozaffari-Kermani, and R. Azarderakhsh, "A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard," 2023.

[4] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access*, 2020.

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

[5] Radhakrishnan I, Jadon S, Honnavalli PB. Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors (Basel). 2024 Jun 20;24(12):4008. doi: 10.3390/s24124008.

[6] A. Bogdanov *et al.*, "PRESENT: An Ultra-Lightweight Block Cipher," *CHES 2007*, pp. 450–466.

[7] S. Banik *et al.*, "GIFT: A Small Present," *CHES 2017*, pp. 321–345.

[8] C. Beierle *et al.*, "The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS," *CRYPTO 2016*, pp. 123–153.

[9] R. Beaulieu *et al.*, "The SIMON and SPECK Lightweight Block Ciphers," *DAC 2015*, pp. 1–6.

[10] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON Family of Lightweight Hash Functions," *CRYPTO 2011*.

[11] A. Bogdanov *et al.*, "SPONGENT: A Lightweight Hash Function," *CHES 2011*.

[12] M. S. Turan, K. McKay, J. Kang, J. Kelsey, and D. Chang, *Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions*, NIST Special Publication 800-232, National Institute of Standards and Technology, 2024.

[13] D. T. Pham, A. Ghanbarzadeh, E. Koc, S. Otri, S. Rahim, and M. Zaidi, "The Bees Algorithm—A Novel Tool for Complex Optimisation Problems," *Proc. IPROMS 2006*, pp. 454–459.

[14] T. M. Fernández-Caramés and P. Fraga-Lamas, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," *IEEE Access*, vol. 12, pp. 25268–25318, 2024.

[15] J. Kaur, A. C. Canto, M. Mozaffari-Kermani, and R. Azarderakhsh, "A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard," 2023.

[16] Bassam Al-Shargabi, Omar Sabri, Omar Albahbouh Aldabbas and Abdelrahman Abuarqoub. 2023. A Survey on Lightweight Encryption Methods for IoT-Enabled Healthcare Applications. In *The International Conference on Future Networks and Distributed Systems (ICFNDS '23),*

DOI: https://doi.org/10.5281/zenodo.21756619

Spectrum of Engineering Scien
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

December 21-22, 2023, Dubai, United Arab Emirates. ACM, New York, NY, USA, 6 Pages. https://doi.org/10.1145/3644713.3644839.

[17] A. Biryukov, L. Perrin, and A. Udovenko, "State of the Art in Lightweight Cryptography: From NIST Standardization to Future Directions," *ACM Computing Surveys*, 2024.

[18] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. 2021. Ascon v1.2: Lightweight Authenticated Encryption and Hashing. J. Cryptol. 34, 3 (Jul 2021). https://doi.org/10.1007/s00145-021-09398-9.

[19] S. Al-Mashhadi and M. Anbar, "A Hybrid Elliptic Curve and Lightweight Symmetric Encryption Scheme for Secure IoT Communications," *IEEE Internet of Things Journal*, 2023.

[20] M. A. Mahdi and M. Abdullah, "Lightweight Post-Quantum Cryptography for Internet of Things: Challenges and Opportunities," *IEEE Access*, 2024.

[21] A. Almutairi and F. Sheldon, "Post-Quantum Cryptography in Resource-Constrained Internet of Things Devices: A Survey," *Journal of Information Security and Applications*, 2024.

[22] Chinbat, T., Madanian, S., Airehrour, D. et al. Machine learning cryptography methods for IoT in healthcare. BMC Med Inform Decis Mak 24, 153 (2024). https://doi.org/10.1186/s12911-024-02548-6

DOI: https://doi.org/10.5281/zenodo.21756619