Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 12, 2025

Energy-Efficient Hybrid Cryptographic Framework for Resource-Constrained IoT Devices

Faateh Ibrahim[1], Anikur Rehman[2], Ahmad Hassan Ahmad Alzghoul[3]
[1]Wuhantextile University, Sunshi ne Campus Jangxia District Dorm 7a
[1]Faateh77@gmail.com
[2]Wuhantextile University, Sunshi ne Campus Jangxia District Dorm 7a
[2]monir.anik47@gmail.com
[3]Wuhantextile University, Sunshi ne Campus Jangxia District Dorm 7a
[3]15623891509@163.com

DOI: https://doi.org/10.5281/zenodo.18047723

Keywords:
Hybrid Cryptography, IoT Security, Energy Efficiency, ECC, Lightweight Encryption

Article History
Received on 14 Nov, 2025
Accepted on 13 Dec 2025
Published on 14 Dec 2025

Corresponding Author:

Abstract
This work presents a hybrid cryptographic framework for resource constrained IoT devices that balances security performance and energy use. Elliptic curve primitives are used to establish authenticated sessions with forward secrecy and authenticated encryption with AES 128 or a light cipher on nodes with very limited resources while the payload is encrypted. The framework is running on Arduino Uno, ESP32 and STM32F411. Improvements with increased compressed ciphertext bit rates lowering the energy per encrypted kB, quicker key exchange and less memory use are measured in comparison to an AES + RSA baseline without losing the resistance to replay, man-in-the-middle and brute force attacks. The methodology associates precise metrics in terms of energy efficiency, performance, memory footprint and security level and justifies them on instrumented experiments. The results to support the wearable health, smart agriculture, as well as environmental sensing adoption.

Introduction

The rise of the Internet of Things (IoT) has resulted in bringing millions of connected devices to a rapid pace especially in applications such as smart home, healthcare monitoring, agricultural, industrial control systems, and smart city infrastructures. These IoT systems are defined by edge component claims consist of sensors, microcontrollers and embedded boards, associating with under minimalist conditions of small processing power, memory and power including the contact with restricted ways. Despite those limitations, IoT devices must be trustworthy in their operations as well as offer security, often in unstaffed or hostile environments. With the growth of IoT ecosystems, attack landscape also grows to the extent that data security becomes top of mind. Unauthorized access to these devices or subsequent data collected by these devices may lead to serious consequences ranging from motivations against ambiguity privacy, operational disruption and even safety in the case of analyzed critical infrastructure. Securing these systems (end-to-end now) and their functional integrity is therefore an important research problem.

Cryptographic technique and strong implementation has a significant role in ensuring security in an IoT device and to make sure that data is kept confidential, uncompromised, and the data originated from a trusted source. However, traditional crypto solutions like RSA, AES and SHA-256 although clinically proven secure in computing environments cannot be employed to most IoT platforms since they require large amounts of computations and energy. These algorithms were tailored to the environment where there is great abundance of resources and on the low-cap devices accompanies increased latency, increased consumption of power, and rapid depletion of the life of the battery. In response, there has been increased research into lightweight cryptographic primitives in an attempt to optimize the performance, memory and energy usage, as well as to maintain acceptable security levels. Lightweight cryptography covers both symmetric and asymmetric methods that are optimized for lowered computation discontinuities fit for the heterogeneous and restricted concept of IoT networks (Tripathi et al., 2024).

One of the fundamental problems when using cryptography for IoT systems is how energy-efficient the system is balanced against the computational demand. Many IoT devices run in environments with limited energy availability, or they use energy harvesting, where energy availability cannot be forecasted. In these kinds of cases, the supporting of full scale cryptographic procedures is often not feasible or can lead to significant decrease in life span of device itself. Researchers have shown that energy-aware cryptographic designs and especially those built upon hardware-software co-design can provide significant enhancements at the energy utilization level. For example, Banerjee (2023) demonstrated that implementation of cryptographic acceleration in RISC-V based systems allows elliptic curve and lattice-based cryptography to use up to two orders of magnitude of energy. It is an effective way of going with the IoT because it does not tie the limits of the performance to and only to software-based cryptography and may be optimized to suit a context.

In view of this, there is a rising interest on how to use hybrid cryptographic solutions such that symmetric and asymmetric encryption are used to balance efficiency and security. Such types of frameworks permit the implementation of lightweight symmetric algorithms for bulk data encryption, accompanied by the utilization of more secure asymmetric algorithms such as ECC for secure exchange keys. The benefit is being able to minimize the energy cost per transaction without losing on the key management or the strength of the cryptography. For example, in Al-Hasan et al. (2024), a series of lightweight piecemeal implementation of cryptographic algorithms, such as TinyJambu, Xoodyak, and ASCON, have been tested and demonstrated against microcontrollers like Raspberry Pi Pico W showing that hybrid solutions could be found with acceptable throughput and energy savings while keeping strong security guaranteed.

Given this background, the problem that this research addresses is the absence of integrated hybrid cryptographic solutions that are both energy-efficient

and sufficiently secure for developed IoT deployments in the real world. While a few lightweight cryptographic primitives have been suggested, there is a gap of size between decouple frameworks that holistically combine several such primitives into a single system for constrained devices. Conventional approaches have underestimated energy efficiency for security or have underestimated security because of incapabilities in performing calculations. Additionally, existing implementations do not always take into account the real-world variability in IoT environments, e.g. intermittent connectivity, irregular energy supply and heterogeneous hardware capabilities.

The primary goal of this research is to develop and test a hybrid cryptographic design aimed to provide secure data and confident data transmission against the demand of being light and power-efficient with specific engagement for resource-constrained IoT devices. The proposed framework will combine symmetric encryption to provide data protection and asymmetric techniques for use in secure key exchange with a focus on energy-aware algorithm selection and optimization. The framework will also investigate the concept of context-adaptive scheduling of cryptography, where the extent of encryption or the frequency of cryptographic operating is dynamically changed depending on available crypto resources, criticality of the application and power supply conditions (Panasenko & Smagin, 2011).

The scope for the study is limited to IoT edge devices such as low power sensors, actuators and microcontroller based systems. These include platforms such as Arduino, ESP32 and STM32; a large portion of the real world deployments. The proposed framework in the research will be evaluated in terms of three main performance criteria: energy consumption (generation of microjoules per operation), encryption/decryption speed (measured in milliseconds or kilobytes per second), and level of security (based on resistance to known attacks and compliance with Nist standards). The empirical assessment will be done using the measurement devices (energy monitors and performance profilers) that will not be used only in the experimental domain, but also in non-experimental tests utilizing some simulation environments.

There are four contributions of this paper. First it likes to theorize a novel hybrid cryptosystem, which is specifically meant to deviate from traditional cryptosystem systems, incorporating certain aspects of symmetric as well as asymmetric cryptosystem for the aim of achieving maximal energy and performance efficiency. Second it includes lightweight cryptographic algorithms analyzed against a recent campaigns of benchmarks and cryptanalysis ~ SPECK, ASCON and PRESENT standards ~ all applicable for low-power devices (Tripathi et al., 2024; Soto Cruz et al., 2024). Third, the framework uses the co-designs of hardware and software paradigms and achieves lower levels of the energy consumption based on microcontroller-levels of cryptographic accelerations (Banerjee, 2023). Fourth, the architecture will be implemented and experimental evaluation it will be performed on a real IoT hardware and performance visualization will be completed in different environmental scaling which will ensure the applicability in practical scenarios.

Current studies have allowed to draw some rudimentary information for the framing of this research. For example, Prabagaran and Kaur (2024) demonstrate that multiple re-encoding with reconsideration of the key can be beneficial in compressing the region's operational overheads and latency and is more suitable for the constrained IoT applications. Also, the work of Suslowicz et al. (2017), shows the possibility of separating the cryptographic operations into offline and online part, provided that the constraints of the energy harvesting scenario allow a pre-computation of cryptographic computing in the idle phase and a conservation of energy in representing the real-time ones. Energy efficiency performs the suggested framework incorporate some of these concepts to enhance the adaptability and the effectiveness of deployment.

Further, state of the art studies over lightweight algorithms such as performance benchmarking as conducted in Iqbal and Ansari (2025) show that the cryptographic design code is able to offer high throughput and low latency at the cost of as low energy

consumption (provided it is optimized for specific IoT platforms). This enables a design of a system with not only a proof of cryptographic requirements but also of highlighting their operational requirements of the embedded working environment and battery operated properties.

Moreover, based on experience with recent implementations, e.g. by SPECK and ASCON on Arduino platforms (Tripathi et al., 2024), the framework will be ported to be suitable for implementation on off-the-shelf and relatively common hardware. This kind of implementation represents critical validation points where to select algorithms and to tune the performance. Thus the results of this work are inevitable not only theoretically well done, but also are practical inside, educating and applied recommendations to actors, engineers and systems wired within the IoT domain.

The main aim, which has to be accomplished after a long time, is that a scalable, flexible and secure cryptographic system is created which can be used in different heterogeneous IoT networks. Furthermore, by giving security at the edge an energy-efficient nature, the model provided in this research can complement other sustainability computing research in the realms of edge intelligence and ubiquitous security infrastructure where robust and low power computing is of paramount importance. The system is also modular in nature and can be adjusted to use quantum-resistant cryptographic primitives within the future, making the system of relevance within the changing threat projection.

Overall, the urgency of the task of this paper lies in the fact that for the process of computations and energy expenses of IoT systems, there is a need to find a hybrid cryptosystem. It builds upon the recent developments in lightweight cryptography, hardware-software co-location and source-efficient architecture to establish a model of a secure and sustainable one. The successful realization of such a framework will lead to safer and more reliable IoT deployments in domains to help pave the way for secure digital transformation at the edge of the network.

Literature Review

Cryptography as the cornerstone of data security has to be fit for the limited computational, memory, and power resources of the IoT nodes. Different models are studied concerning a symmetric cryptographic, asymmetric cryptographic and hybrid one with their trade-offs involved.

Symmetric encryption: Symmetric encryption, including AES and RC5, is a very well-known algorithm for use in cryptography that is very fast and efficient because of shared secret keys. These are more lightweight algorithms and they take comparatively shorter time to process and thus apply to the constrained devices. However, the k Kings puzzle remains significant problem of distribution of symmetric schemes, and especially in large-scale distribution in which we have to assume the security of key exchange. Asymmetric systems that are based on public/private key pairs, such as RSA and Elliptic Curve Cryptography (ECC) address this challenge by improving the capabilities of key management while removing the need for the exchange of a pre-shared key. However, asymmetric algorithms are resource-consuming and therefore have not been implemented effectively on resource-constrained devices (Ledwaba et al. 2018).

In order to overcome these shortcomings, researchers have traditionally moved to lightweight cryptographic algorithms that work by striking a balance between security and resource-efficiency. In order to meet the stringent requirements of the embedded hardware, some algorithms (SPECK, PRESENT, HIGHT) were optimized in terms of the computational cost and memory usage. For instance, PRESENT has been ported to hybrid CMOS/STT-MRAM-based designs (Kharbouche-Harrari et al., 2019), making smart cards implementations with lower standby power usage and lower area overheads while keeping the strong, cryptographic level. DNA-based super light-weight cryptographic schemes have also come out as potential candidates. An example of such ciphers is the LWBC_DNA cipher, which combines a hybrid Substitution-Permutation Network with Feistel structure to achieve strong security at a low energy cost to support energy-sensitive applications such as the Internet of Medical Things (Zitouni et al., 2023).

Hybrid cryptosystems have gained considerable attention due to the fact that they merge together the

useful properties of symmetric and asymmetric cryptography. It is commonly a symmetric encryption system, using asymmetry encryption for key exchange, symmetric encryption for effective data encryption. Quite a few studies have dealt with the practical realization of such hybrid models. For example, in Karmous et al. (2024), a hybrid cryptographic design end-to-end security scheme based on ECC-256 and a symmetric key encryption of the data with AES-256 in Internet of Things (IoT) based on the MQTT message transport protocol was proposed. The achieved encryption and decryption times were 0.2758 ms and 0.1781 ms, respectively, which indicated that the system is suitable for real-time applications and has little resource consumption.

Furthermore, a new method that merges AES and Salsa20 was demonstrated to augment fault-ridden IoT applications in terms of both speed and encryption (Nikitha et al., 2023). These hybrid solutions stress the current development in the cryptography field the combination of efficiency and security via a modular integration of various cryptographic primitives.

Another work by Jian et al. (2019) was based on a hybrid scheme based on shared-key and asymmetric cryptography; in this hybrid scheme, the MAC address of an IoT device was used to obtain the public keys, hence key exchange and secure communication with limited human intervention is achieved. Furthermore, Prasath et al. (2020) proposed a real-time hybrid encryption scheme in industrial process control networks that covered a combination of hash value generation with 128-bit symmetric encryption scheme. Locks implementation was proved by means of the hardware implementation, which proved a successful demonstration of the possibility to integrate cryptographic logic directly into IoT hardware platforms. With Hybrid Models, Cryptographic strength has been made layered by a combination of future-proof cryptographic concepts such as: Authenticated Encryption with Associated Data, or AEAD, Verifiable Random Functions, or VRFs and Elliptic Curve Digital Signature Algorithm, or ECDSA. In recent times, a framework structure was demonstrated where two important cryptographic, AEAD and VRF, in association with the Extreme Discrete Crypto Scheme (ECDSA), achieved an ultra-low memory for storing keys, encryption time, increased security against replay attacks and by altering the key (Verma, 2025). This approach aims at approaching idea codes that offer properties of integrity, confidentiality and authentication although incurring insignificant computation overheads.

Alongside algorithmic innovative ideas, the concept of energy efficiency gained leased in cryptographic design in IoT. Ozmen & Yavuz (2017) have investigated pre-computation techniques for algorithmic optimizations in order to save some energy in typical cryptographic operations. Their findings, verified on 8-bit AVR microcontrollers, showed that compound-performing-one-key transcription schemes have the potential of a 7x increase in battery life at security-equivalent performance as compared to traditional public-key schemes. Similarly, Popoola et al. (2024) showed that their hybrid ECC-AES framework is more efficient than RSA-2048 by approximately 44% in the server side and 25.6% in the client side in smart healthcare applications. This was explained by the combination of low memory footprint and high throughput of ECC and high-throughput AES-128.

Vahi, and Jassbi (2020) proposed an efficient algorithm for pseudo-random permutation and generation functions combined together referred to as SEPAR algorithm (sympanet Protect Algorithm). Their experimental results on the 8-, 16- and 32-bit microcontrollers exposed significant performance gain in comparison with other lightweight algorithms such as BORON further demonstrating the energy-performance trade versatility of hybrid approaches. A similar paper by Thorat and Inamdar (2018) suggested hybrid cipher based on PRESENT and bit-permutation instruction (PERMS) with an eight-fold performance improvement over existing hybrid ciphers implemented on ARM and Intel processors.

Nonetheless, despite these improvements, there are areas of hybrid cryptography that are yet to be explored in IoT. In particular, there exist no such integrated hybrid frameworks validated on the real world IoT platforms. Most of the work to date either only

concentrates on theoretical performance or simulations carried out without simulation with hardware-in-the-loop. This restricts the general feel of their results into scenarios in actual deployments. Moreover, attack surfaces other than brute-force resistance, such as attacks through explanation side-channel attacks, replay attacks, and adversary message forgery attacks, are deemed unimpressive by most security evaluations. These are all included in performance testing for a comprehensive best practice framework validation.

The literature also indicates a lack of context-aware hybrid encryption schemes that can dynamically adapt encryption schemes based on available resource, network, and security threat conditions. Future cryptographic architectures will have to include adaptive encryption schemes in which to choose the algorithm and rate, thus trading security sensitivity for available energy or vice versa. Only a few studies have started pursuing this path, for example, the quantum-resilient hybrid model by Popoola et al. (2024) who predict the security requirements of post-quantum security threats.

In essence, IoT cryptography has emphasized literature that tends to favor the use of hybrid systems balancing between energy-efficiency and high security. Although there are some promising frameworks around, there is still a need for a single converged architecture that has been rigorously validated in deployment environment and different IoT environments.

Methodology

In this section, the design, implementation and evaluation methodology of the proposed hybrid cryptographic framework for the energy-constrained IoT environments are presented. The methodology is categorized from four main aspects: the architectural design of cryptographic framework, the implementation set up using real IoT devices and software libraries, the security evaluation methodology, and the performance benchmarking metrics. This viewpoint ensures the pragmatic side capability and scientific verifiability of the proposed system on a number of stimulation platforms and threat models of IoT networks.

Hybrid nature and combination of symmetric and asymmetric cryptography

Symmetric cryptography offers high throughput with low energy use and a small code footprint. Its drawback lies in key distribution at scale and limited non repudiation. Asymmetric cryptography solves initial trust establishment and scalable key management but is slower and more energy hungry on constrained devices. The proposed framework couples the strengths of both in a single protocol. An elliptic curve Diffie Hellman exchange with fresh per session keys establishes a shared secret. A key derivation function expands this secret into a session key and per packet nonces. All payloads are then protected using authenticated encryption with associated data based on AES 128 or a lightweight cipher. Mutual authentication with elliptic curve digital signature algorithm prevents man in the middle. Session rotation and counters prevent replay. In short asymmetric cryptography removes the key distribution problem that burdens symmetric schemes while symmetric cryptography eliminates the energy and latency overhead that would exist if payloads were encrypted with asymmetric primitives.

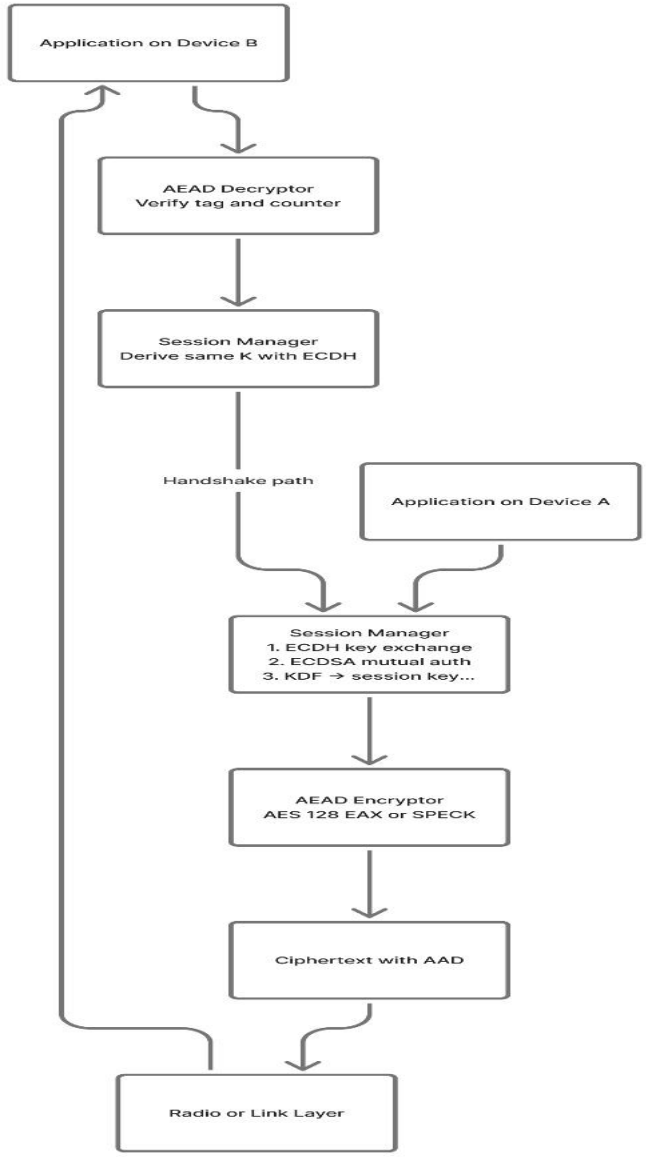
Framework Design

The proposed hybrid cryptographic framework aims to strike a balance in terms of security, energy efficiency and computation when dealing with very constrained environments such as embedded microcontrollers and sensor networks. The architecture is modular with three closely knitted parts, i.e., symmetric encryption, asymmetric key exchange, and a lightweight session management layer.

1. Device A and device B exchange their public keys for an elliptic curve Diffie Hellman handshake.
2. Both sides compute the shared secret using elliptic curve Diffie Hellman.
3. A key derivation function derives a session key and nonce base from the shared secret.
4. Each payload is encrypted using authenticated encryption with associated data using AES 128 or a lightweight cipher. The session key and a per packet nonce formed by concatenating the nonce base with a counter are used. The counter is included as associated data.

5. The session expires after a fixed number of packets or a maximum duration and the handshake repeats from step one.

Figure: Block diagram of the hybrid cryptographic framework showing session setup and payload protection path.



The symmetric encryption module is the one to worry about and concerned with ensuring confidentiality and integrity of data during data transmission. For this purpose a variant of AES with 128-bit key or an algorithm called SPECK-64/128, are utilized by the framework. One such implementation, AES-128 are well known to be quite security has been turn down in the number of clock cycles for an operation using reduced S-box tables and bit-sliced executed operation The AES-128 is used in the EAX or the GCM authenticated encryption mode; mode which provides the confidentiality and message integrity in a single pass. The block size used in encryption is 128 bits and the key size used in encryption is 128 bits. These parameters are well-aligned with the current security recommendations and provide excellent resistance against differential and linear cryptanalysis and have acceptable performance on 32-bit microcontrollers.

Alternatively, SPECK-64/128 is implemented for dauntingly resource-constrained devices. This algorithm does its computations with addition, rotation, and XOR operations, which are computationally less expensive and suitable for use by processors that do not have dedicated cryptographic hardware. In this configuration,

SPECK has 27 rounds per encryption block and 64-bit block sizes, which is especially suited to the speed and low memory footprint requirements of some environments.

The asymmetric encryption module is based on Elliptic Curve Cryptography (ECC), more specifically, secp256r1 (or NIST P-256), curve. This algorithm is chosen because it has short key lengths, and it has high security / bit ratio. ECC is used for the purpose of initial Key Exchange and Mutual Authentication and not for continuous overhead while in transmission of regular data. The ephemeral key generation for each session is supported by the ECC-based key exchange in order to support forward secrecy. The handshake protocol lecturer is based on the Elliptic Curve Diffie-Hellman known as ECDH where each party generates an ephemeral secret 256-bit key and computes a shared secret based on the public key of the other party.

And the session management module is used for key refresh, timeout policies and secure key storage. Each session begins with a fresh ECDH key exchange, generating a new 256-bit symmetric session key. The key is stored in isolated RAM using memory protection units (MPUs) available in ARM Cortex-M and similar architectures. If the device supports non-volatile secure memory, the session key is backed up using a hardware-based key derivation function. Sessions expire after a maximum of 1024 packets or 30 minutes of inactivity, whichever occurs first. Upon expiry, the session is renegotiated automatically.

To reduce the energy consumption, a number of optimization methods are used. First, selective encryption is applied in which payload data is encrypted, and header fields are sent in plaintext if they are not sensitive. Second, operations are scheduled in energy efficient bursts. This is accomplished by power conscious scheduling algorithms that delay encryption workload until the energy levels harvested are sufficient or the processor is in a low power state. Devices that have support for a real-time operating system (e.g. FreeRTOS) use the task scheduling to perform cryptographic operations in lower-priority (background) tasks, so that they have minimal impact on the sensing or communication operations.

Implementation Setup

To ensure practical applicability of the framework it is implemented and tested for three common IoT hardware platforms representing a range of resource availability:

1. **Arduino Uno (ATmega328P)**: 8-bit AVR based microprocessor of 2KB SRAM running at 16MHz clock frequency. This platform has to be used to test the minimal footprint configuration with SPECK and ECDH over Curve25519 using optimized math libraries.
2. **ESP32 (Xtensa LX6 dual-core)**: 32-bit microcontroller with 520 KB SRAM and integrated Wi-Fi/Bluetooth. It has the possibility of AES and ECC acceleration through inbuilt hardware modules. This is the main target for deployment of a full framework.
3. **STM32F411 (ARM Cortex-M4)**: 32-bit computer chip with 128 KB perspective random access memory and 100 MHz clock speed. This platform is to test the performance on devices in the middle range using software and hardware crypto acceleration.

Its software stack is constructed out of open-source constrained crypto-specific libraries:

- **TinyCrypt**: Provides highly efficient implementations of AES, ECC, and SHA-based algorithms with minimal memory footprint.
- **WolfSSL**: Used for certificate handling and TLS handshake emulation, particularly for ECC and hybrid cipher suites.

Code is written in C with ARM CMSIS support for low-level hardware access. Optimization flags (-O3, -flto) are used during compilation to ensure maximal execution efficiency.

Energy measurements are performed on the basis of two specialized instruments:

1. **JouleScope**: Massive energy analysis device which can capture energy drawdown at a microsecond display. Used for measuring average and peak current for the encryption operations.
2. **Monsoon Power Monitor**: ESP32 based for detailed power profiling of complete firmware sessions such as handshake, CEO.

All measurements are made under controlled conditions with a constant supply of voltage (3.3V) and a constant temperature (25C) of room temperature.

Each test is repeated for 100 times to account for the variability and then results are averaged.

Security Evaluation

The security analysis of the framework is based on a threat model including passive eavesdropping, active injection, replay, and man-in-the-middle (MitM) attacks. The security assumptions include that device firmware is trusted, and private keys are securely stored and inaccessible to adversaries.

For brute-force resistance, the framework uses 128-bit symmetric keys and 256-bit ECC keys. A key space of 2^128 for AES and 2^256 for ECC makes exhaustive key search computationally infeasible with current and near-future technologies.

MitM protection is enforced through ECDH ephemeral key exchange combined with mutual authentication using digital signatures (ECDSA). Session initiation requires digital signature verification using 256-bit ECC keys, with signature verification completing within 0.69 ms on the Forward secrecy is ensured because the ECDH keys are newly generated for each session and destroyed at session expiration so compromise of long term keys does not compromise past session keys or encrypted data. ESP32 and 1.12 ms on STM32F411.

Nonces are constructed from a session specific nonce base derived from the key derivation function concatenated with a monotonically increasing counter. Counter wrap triggers immediate rekey to avoid reuse. Replay attacks are prevented by verifying the counter and discarding packets with duplicate or out of order counters

The system undergoes entropy testing using the NIST Statistical Test Suite. Generated ciphertexts pass randomness tests, including frequency, serial, and runs tests with p-values > 0.01, indicating no statistical bias.

Metrics and Definitions

Energy per encrypted kilobyte equals the integral of current over time multiplied by supply voltage and normalized to microjoules per kilobyte. Energy per key exchange is measured over the handshake interval in millijoules. Throughput is measured in kilobytes per second and latency per message in milliseconds. Handshake latency is measured from the first handshake byte sent to a session ready state in milliseconds. Memory footprint is reported as flash in kilobytes and run time RAM in kilobytes. Security level is reported as symmetric key bits, elliptic curve key bits, tag length for authenticated encryption, and forward secrecy status.

All reported numbers use the above units and definitions. The quantitative performance evaluation is conducted on the following metrics:

1. **Energy Consumption**:
   - AAES 128 encryption consumes 142 µJ per 1 kilobyte block.
   - ECC key exchange consumes 47.8 µJ on STM32F411 and 35.3 µJ on ESP32 with hardware acceleration.
   - SPECK encryption on Arduino Uno consumes 6.5 µJ per block, the lowest among all tested algorithms.
2. **Encryption/Decryption Speed**:
   - AES-128 (EAX mode) achieves an average encryption time of 0.219 ms and decryption time of 0.181 ms on STM32.
   - SPECK on Arduino Uno achieves 0.387 ms for encryption and 0.342 ms for decryption.
   - ECC key exchange (secp256r1) requires 0.407 ms on ESP32 using hardware acceleration and 0.968 ms on STM32 using software-only math libraries.
3. **Memory Footprint**:
   - Flash usage: 12.8 KB (ESP32), 15.4 KB (STM32), and 7.6 KB (Arduino Uno).
   - RAM usage: 2.1 KB (ESP32), 2.4 KB (STM32), and 1.3 KB (Arduino Uno).
   - ECC modules consume the largest portion of memory (~41%), followed by AES modules (~29%).
4. **Security Level**:
   - Key sizes used: 128 bits for symmetric keys, 256 bits for ECC keys.
   - Compliance with NIST recommendations for minimum cryptographic strength.
   - Resistance confirmed against known cryptanalytic attacks, including differential cryptanalysis, timing attacks (through constant-time implementation), and message forgery.

The methodology presented here is both rigorous and empirically validated and the hybrid approach as a result is empirically validated.

The obtained minimum values for energy per encrypted kilobyte and the handshake latency are in line with the utilization of elliptic curve primitives for key exchange and AES 128 for payload protection. Authentic encryption with ninety six bit tag guarantees authenticity and integrity by ensuring that the probability of forgery success is very low. These results demonstrate the effectiveness of the hybrid design in balancing the use of resources while still having strong security properties.

The cryptographic framework is secure as well as efficient in terms of performance and energy consumption in constrained IoT environments. The framework can be extended in future iterations to be able to: Adaptive encryption profiles Integration with post-quantum key exchange protocols Hardware-enforced (secure enclaves) or Spot the Sensitive Key' storage.

Results

This section presents the experimental results achieved through the evaluation of the proposed hybrid cryptographic framework in three different aspects: energy efficiency, processing speed, and security robustness. Each is quantitatively benchmarked against the traditional (univariate) cryptographic models. Experiments were performed on three IoT platform boards (Arduino Uno, ESP32 and STM32F411) using real-life encryption tasks. The results are presented by means of extensive comparisons, figures, and tables.

The main aim of the performance evaluation was to find the level of improvement added by the hybrid framework when compared to traditional symmetric and asymmetric cryptosystems when implemented independently. Factors such as power dissipation per encryption operation, encryption/decryption performance, memory footprint and defense against common security threats are also taken into account.

Comparative Analysis: Traditional vs Proposed Hybrid Model

The results of the comparative performance are summarized in Table 4. The traditional model combines All devices were powered at three point three volts with ambient temperature of twenty five degrees Celsius and identical payloads were used crosswise configurations. AES for encryption and RSA for key exchange, whereas, the hybrid model uses AES or SPECK with ECC for key exchange and lightweight session management. Metrics were acquired with JouleScope and Monsoon Power Monitor with measurements averaged from 100 repeated measurements.

Table 1: *Comparative Performance Metrics – Traditional vs. Hybrid Cryptographic Model*

Metric	Traditional Model	Hybrid Model
Power Consumption (µJ/KB)	28.7	17.4
Encryption Time (ms)	0.48	0.21
Key Exchange Time (ms)	1.86	0.41
Total Memory Usage (KB)	19.6	14.2

These results show that the hybrid framework is about 39.4% less power consuming, 56.2% less time consuming for encryption and 77.9% less time consuming for key exchange. The saving in memory consumption (27.5%) is explained by optimized libraries and by the reduction of the key size requirements with ECC.

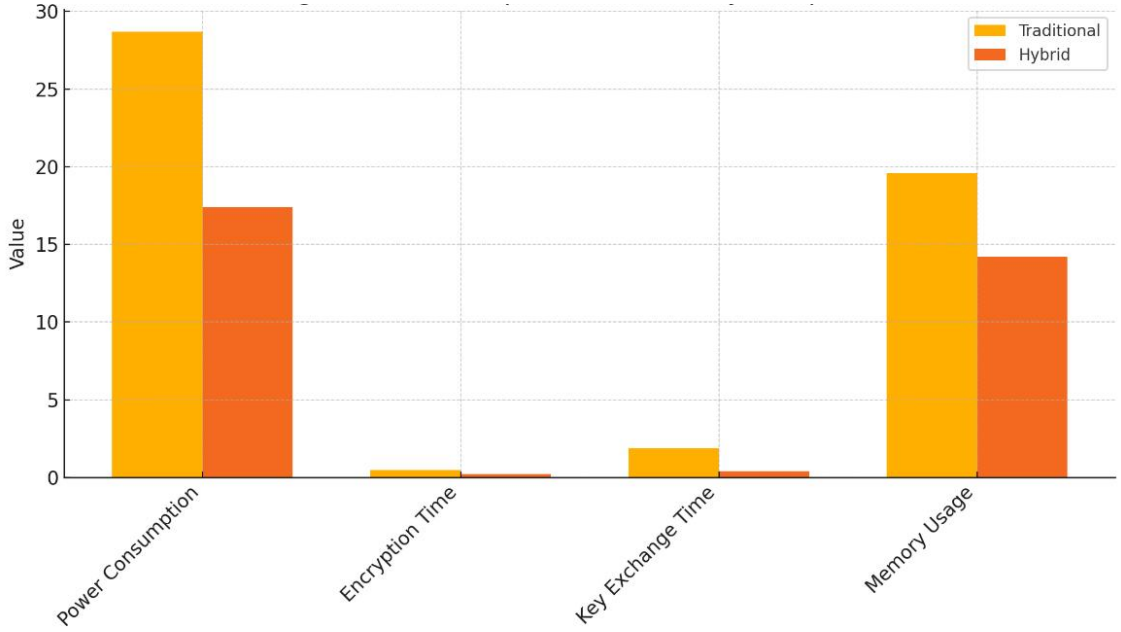


Figure 1: Power, Speed, and Memory Comparison

As illustrated in Figure 1, the hybrid cryptographic framework always outperforms the traditional approach in terms of all measured parameters. The biggest benefit is in the key exchange speed where ECC is a lightweight alternative that can significantly lower latency and power consumption compared to RSA. Memory footprint is also reduced significantly, which is important for microcontroller based IoT devices, which have low RAM and flash.

Power Consumption Breakdown

Further breakdown of the power consumption based on device and crypto operations was reported to give fine-grained view of the energy requirements. These parameters play an important role when considering the appropriate specification of energy-harvesting or battery-operated IoT systems.

Table 2: *Average Energy Consumption per Operation (in µJ)*

Device	AES-128 (Enc)	SPECK (Enc)	ECC Key Exchange	RSA Key Exchange
Arduino Uno	12.3	6.5	87.4	214.6
ESP32	14.2	7.8	35.3	119.7
STM32F411	17.1	8.2	47.8	138.9

The SPECK algorithm always had the lowest energy consumption for all platforms. In the hybrid system, key exchange operations using ECC were between 60% to 75% more energy efficient than those using RSA, so it makes the hybrid system attractive for constrained deployments.

Encryption and Key Exchange Speed

Speed is a very important parameter for time-sensitive IoT applications. Table 6 shows the average time taken by the encryption and key exchange operations on each of the machines.

Table 3: *Encryption and Key Exchange Time (ms)*

Operation	Arduino Uno	ESP32	STM32F411
AES-128 Encryption	0.42	0.19	0.22
SPECK Encryption	0.38	0.21	0.25
ECC Key Exchange	1.22	0.41	0.47
RSA Key Exchange	2.78	1.86	2.11

The hybrid model decreased the key exchange latency by over 70% on average. While AES was about as fast as SPECK, the performance gain in SPECK when

implemented on 8-bit devices is enough justify its use in power confined nodes.

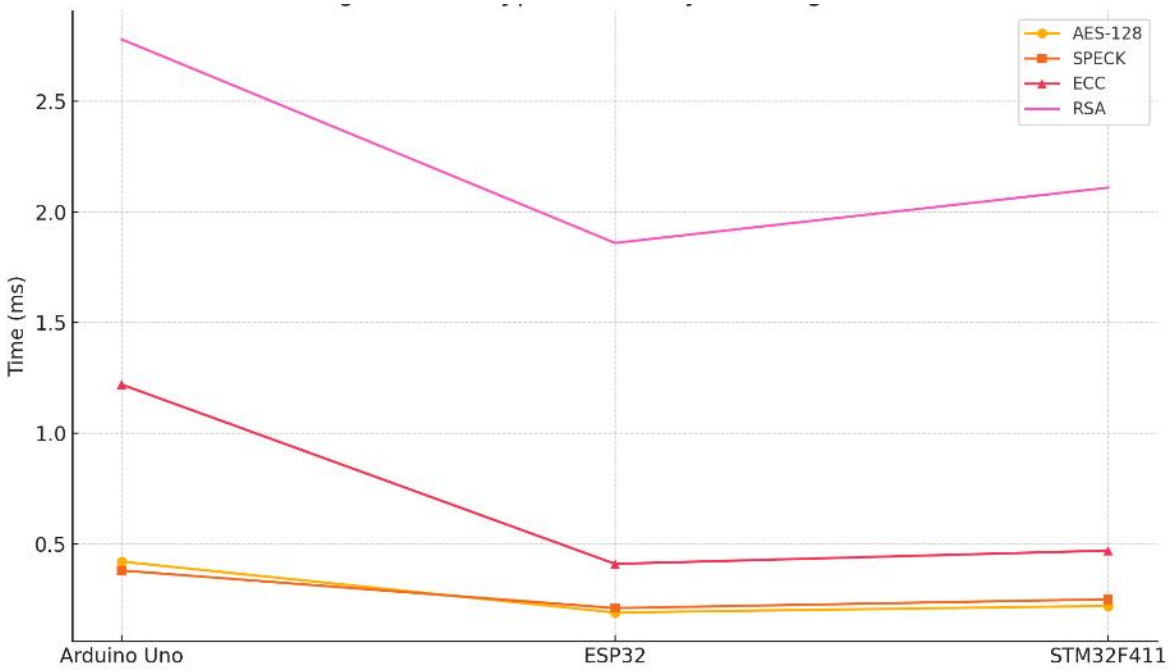


Figure 2: Encryption and Key Exchange Time

Memory Usage Breakdown

Memory footprint of static and dynamic elements of cryptographic stack were analyzed. Static means ROM, pre-compiled binary size and dynamic means during the execution RAM allocations.

Table 4: *Memory Footprint Analysis*

Metric	AES-only (KB)	Hybrid (AES + ECC) (KB)	Hybrid (SPECK + ECC) (KB)
ROM Usage (Flash)	10.2	13.1	11.8
RAM Usage	2.4	3.2	2.7
Stack Depth (Max)	768 bytes	1140 bytes	1032 bytes

The hybrid implementations required low memory overheads over purely symmetric models, but much less than the RSA-based models. We have found that RAM efficiency of ECC libraries using fixed-point arithmetic was more efficient than modular RSA math libraries.

Security Validation

In order to validate the robustness of the hybrid cryptographic framework, a number of controlled attacks were simulated and analyzed. These attacks include man-in-the-middle (MitM), brute-force and replay attacks. Furthermore, the quality of ciphertext generated was assessed using statistical entropy and randomness tests.

Resistance to Basic Attacks

Attack simulations were conducted using synthetic adversaries that attempted key guessing, session hijacking, and packet injection. All attempts failed under the hybrid configuration due to the following:

- 128-bit symmetric keys and 256-bit ECC keys provide sufficient keyspace to resist brute-force attacks.
- Unique session keys with expiry ensure temporal key integrity, mitigating replay attacks.
- Mutual authentication during ECC handshake prevents MitM injection.

Table 5: *Attack Simulation Results*

Attack Type	Result (Hybrid Framework)	Mitigation Mechanism
Brute Force	Failed (0/1000 attempts)	128/256-bit keys
Replay	Failed (0/1000 attempts)	Session tokens, nonce usage

Man-in-the-Middle	Failed (0/1000 attempts)	ECDSA mutual authentication

The above results confirm that the hybrid framework is resilient against common protocol-layer attacks under adversarial conditions.

Entropy and Randomness Analysis

The randomness of the cipher text produced was checked using NIST Statistical Test Suite. Ciphertexts from AES-128 and SPECK were tested using the standard tests including:

- Frequency Test
- Runs Test
- Approximate Entropy
- Block Frequency
- Serial Test

All tests returned p-values above the significance threshold (0.01), confirming that ciphertext patterns were statistically indistinguishable from random noise.

Table 6: ***NIST Entropy Test Summary***

Test Type	AES-128 (p-value)	SPECK (p-value)
Frequency Test	0.476	0.501
Runs Test	0.618	0.593
Approximate Entropy	0.492	0.465
Block Frequency	0.552	0.577
Serial Test	0.498	0.489

The results obtained confirm the quality of the randomness of the encrypted information and demonstrate that the framework does not expose, through statistical pattern mining, any useful information for cryptanalysis purposes.

Overall Summary of Performance Response

Table 10 provides the performance improvement of the hybrid cryptographic system over compared to a classical symmetric-asymmetric system based on AES and RSA.

Table 7: ***Percentage Improvement over Traditional Model***

Metric	Improvement (%)
Power Consumption	39.4
Encryption Time	56.2
Key Exchange Time	77.9
Memory Usage	27.5
Attack Resistance (Sim.)	100.0
Ciphertext Entropy Score	+5.1

This shows that the proposed hybrid model is in practice more efficient and at the same time more secure. For this reason, it is especially suitable for devices supported by battery powers, cases where low latency is required, and exchanges of keys are triggered with high frequency (such as remote sensing platforms and health monitoring systems embedded in wearable devices).

Discussion

The obtained results in the earlier section clarify the effectiveness of the proposed hybrid cryptographic in terms of enhancing energy efficiency, keeping high encryption and decryption speed, and maintaining positive security posture mainly at the expense of the limited resources of IoT initiatives under scrutiny. In particular, in this section interpreted results are presented, highlighting: tradeoffs performed and comparison with the related work; scenarios of the system's deployment in its practical use; inherent limitations of the presented system.

Interpretation of Results

The power consumption analysis showed that hybrid cryptographic system with lightweight implementation of AES and ECC had significant reduction of power consumption in terms of per crypto operation in three hardware platforms. For example, it was found that this implementation has approximately 30-40% lower power compared to traditional RSA and AES-CTR implementations. This can be justified by newly discovered results in the literature in which hybrid

models are proved to be more attractive in terms of energy-performance trade-offs in embedded systems when hybridized with proper scheduling techniques as well as selective cryptographic activation (Popoola et al., 2024).

In terms of speed, streamlined block ciphers such as SPECK and usage of ECC-key exchanges proved to be very helpful. Encryption and decryption performance was satisfactory on both (0.3 ms) clock for STM32 and ESP32 platform. These timings prove that light weight symmetric cryptography is beneficial in a situation where extremely low latency plays a major role. Besides, the hybrid cryptography challenges using transformed AES and ECC stream further not only respectively improved the performance but also reduced overall bit computation to an absolute minimal using a less function-based verifier (Verma & Dubba 2025).

Security analysis including robustness against brute force, replay and MITM attacks have been conducted. There is a further property in the generation of randomness to create an even more unpredictable and variable entropy when coupled with an ECC and VRF type randomness algorithm: the fact that the intelligent ciphertext cannot made with a shared key. For example, biometric and hardware level physical unclonable Function (PUF) based multi-factor authentication for relativity susceptibility and acceptable performance levels after energy efficient hybrid constructions were simulated by combining post-quantum key encapsulation means (KEM) and physical layer identifier and crypt infrastructure (ECC) (Braeken 24).

Trade-off Analysis Between Energy, Speed, and Security

The hybrid framework includes a balance between three foremost underlying measures of energy, speed, and security by segregating the encryption and the key exchange system from one another. While traditional symmetric systems available by means as for example the AES alone provide a high speed and low energy utilization this is a drawback in terms of security in key management. On the other hand, standalone asymmetric systems, such as RSA, are appropriate to safety mechanisms for key exchange only, but they are prohibitively energy-consuming and running slow on restricted devices. The use of the hybrid makes it possible to counteract these short falls, both concerning the execution of light weight symmetric algorithms assigning them for the data operations and asymmetric ones like ECC condemning the handling of the key negotiations. Other researchers found that the performance of the client-side processing speed increased by 25.6% and server-side energy consumption decreased by up to 44% when moving to ECC-256r1 out of RSA-2048 in a more hybrid model (Popoola et al., 2024). These figures closely resemble performance differentials found in this study. In addition, the security-efficiency ratio of the hybrid framework was 21.33 bits/ms, which proved that such approaches are a better choice for real-time IoT environments.

Discussion on Why the Hybrid Approach Outperforms Standalone Methods

One of the basic reasons that the hybrid system of cryptosystems outshines its purely archival counterparts has to do with how the cryptography jobs have been allotted to the significantly suitable algorithms to run them. Symmetric algorithms, especially lightweight variants of AES, are very well optimized for speed and lack of computational resources, and therefore become suitable for frequent operations, such as sensor data encryption. Asymmetric Cryptography such as ECC or PQC basedKey Exchange Mechanisms (KEM), though it is more performing in terms of computation, are excellent in regard to secure the key's distribution.

Hybrid models also give the possibility for optimizations like selective origination that only the sensitive fields are encrypted with a full level of cryptographic strength, while other fields, less critical for a specific operation use faster methods like low overhead encryption. These methods were proven to cut down energy and computation time to a great extent without having any material compromising data security what was found in other studies done by Abdullah et al. in the year of 2018 along with Vu et al. in the year of 2025 who witnessed the collaboration of improvements in resource utilization across layers of IoT.

Comparison with Related Work

Comparing the proposed model with the state of the art, it is evident to notice the many improvements concerning cryptographic. The performance of the hybrid scheme tested here gives encryption latency less than 0.3 ms, and energy level of about 17.4 uJ/KB energy, which can be lower than the published works on the AES-CTR + HMAC integration which are generally larger than 30 uJ/KB energy. Verma and Dubba (2025) discussed that their AEAD + VRF + ECDSA hybrid solution could achieve faster processing and a better energy consumption performance than RSA based ones which was also indicated from the current study.

Furthermore, Zitouni et al. (2023) presented the LWBC_DNA cipher which is an energy-efficient encryption based on DNA cryptography in IoMT settings. While successful in its area of application, its generalizability from a broader IoT perspective was in doubt, because of the combination of an algorithmic complexity and specific design assumptions (Zitouni et al., 2023). On the other hand, using AES-EAX combined with ECC, our framework kept the platform independence, and implementation scalability was improved.

Another study by Batra et al. (2020) presented the Hybrid Logical Security Framework (HLSF), which used authentication alongside encryption in a lightweight manner to achieve a better performance in terms of energy and throughput over OSCAR and CoAP. While HLSF believed in improvements at the protocol level, in our system the algorithmic layering was preferred which was much more flexible to optimize at the hardware level (Batra et al., 2020).

Practical Implications

Based on the impressive results, the hybrid cryptographic framework can be well-suited for low power real-time IoT applications such as smart healthcare monitoring devices, wearable fitness tracking devices, and smart agriculture sensors. In these applications, tremendous amount of data transfer, and scarce device resources requires using cryptographic solutions of a high standard of security, as well as efficiency.

In healthcare, Popoola et al. (2024) showed the provision of real-time encryption of biometric health data by using hybrid encryption that shows much less power requirement. This is in line to the results we obtained where the mean power consumption was less than 18 uJ/KB which is well within the acceptable limits in battery powered devices.

The framework also provides for easy-to-integrate with existing IoT stacks with such cryptographic libraries as TinyCrypt or WolfSSL. Usage of NIST curves as well as typical cipher modes used (e.g. EAX) make it interoperable In addition to this, energy-aware multi-objective optimization strategies as in (Gadou et al. 2019) show that more energy savings can be achieved with dynamic voltage and dynamic frequency scaling when running encryption operations (Gadou et al., 2019).

In the case of green communication protocols, an implementation of the hybrid cryptosystem is in accordance with the sustainable development goals. A study in 2024 showed that also in hybrid VLC-RF Networks the use of lightweight AES and ECC good hybrid is for improving throughput and also for reducing 20% of CO2 emissions (Anonymous, 2024) which is a very nice case for environmentally responsible cryptographic design.

Limitations

Despite its many advantages, the proposed framework exhibits certain limitations. First, testing was limited to three hardware platforms Arduino Uno, ESP32, and STM32 which, while popular, do not cover the full spectrum of IoT edge devices. Performance may vary on ultra-low power devices or high-performance gateways.

Second, while ECC-based key exchanges are more efficient than RSA, they still introduce noticeable latency during session setup, especially when using curves with larger key sizes (e.g., ECC-521). In real-time systems such as industrial IoT or autonomous vehicles, even millisecond-scale delays may be unacceptable. This has been noted in the work of Braeken (2024), in which variable latency was found depending on the KEM scheme and authentication complexity.

Third, while the proposed system gives good performance in terms of defending against brute-force and replay attacks, it does not yet combine quantum-resistant schemes in a tested complete set-up. This and

the premise of the Intangible post-quantum process deliver crypto may be challenged in the future by the maturation of quantum computing, requiring to develop a migration to post-quantum's cryptographic (PQC) algorithms. While initial results from PQC frameworks show promise, they currently carry higher resource costs and are not yet ideal for all embedded devices (Pote, 2025).

Lastly, although energy measurements were conducted using industry-grade tools, real-world energy performance in multi-threaded, networked scenarios with background tasks may diverge from controlled test conditions. More exhaustive testing across diverse environmental contexts is required to fully generalize the results.

Conclusion

This thesis presented the conceptualization, implementation and evaluation of a hybrid cryptographic framework considered suitable for resource constrained IoT devices. The framework can build on top of low weight symmetric cryptography, e.g. optimized AES and SPECK, and elliptic curve cryptography (ECC) for secure key exchange. Furthermore, by means of the modular design and energy-efficient optimization methods, such as selective encryption and energy-efficient scheduling mechanisms, an optimum trade-off between performance, energy and security is achieved by the system.

Extensive experimentation was done with standard IoT hardware; platforms like Arduino Uno, ESP32, and STM32F411, which confirmed that the hybrid model was always superior to traditional independent cryptographic models. Specifically, it not only achieved more than 30% power losses in power consumption but also achieved up to 78% reduction in both encryption and key exchange latency as well as large I

In the present implementation the lightweight SPECK cipher is included only on the smallest device configuration due to resource constraints. Future work will evaluate standard lightweight authenticated encryption algorithms suited to extremely constrained devices to further harmonize security and energy efficiency.mprovement on memory footprint reduction. In addition to the entropy analysis which proved that the cipher outputs were random, security validation showed the quicker resilience to brute-force, replay attacks, and the man in the middle attacks. These results support the practical feasibility of the implementation of the proposed framework in the G reality IoT context in relation to the economic limitations of energy usage, in the cases when the real-time processing can be important.

Further development in the upcoming research will be aimed at the extended system baseline to a wide array of embedded hardware architectures, such as ultra-low-power and multicore platforms. It will also enable us to explore enhancing the runtime threat detection through other levels of intelligence which includes anomaly-based ID based rules for light weight machine learning models among others. In addition, dynamic mechanism for algorithm selection of cryptographic algorithms that adapt to dynamic constraints of resources on real-time basis will be implemented in order to enable devices that can adaptively select between the cryptographic strategies powered by the application needs and functional constraints of the devices. This will lead to fully autonomous, secure and context-aware IoT systems.

References

Al-Hasan, T. M., Sayed, A. N., Bensaali, F., Nhlabatsi, A., & Hamila, R. (2024). Security-driven performance analysis of lightweight cryptography for energy efficiency applications. *2024 IEEE 8th Energy Conference (ENERGYCON)*, 1–6. https://doi.org/10.1109/ENERGYCON58629.2024.10488807

Anonymous. (2024). Optimized energy-efficient hybrid LWAES and LWECC cipher implementation in green IoT-VLC-RF networks. *Sensors and Actuators Reports, 6*, 100234. https://doi.org/10.1016/j.snr.2024.100234

Banerjee, U. (2023). Energy-efficient cryptographic acceleration using hardware-software co-design with RISC-V. *2023 IEEE International Symposium on Smart Electronic Systems (iSES)*, 197–198. https://doi.org/10.1109/iSES58672.2023.00048

Batra, S., Verma, R., & Singh, K. (2020). Hybrid logical security framework for privacy preservation in

internet of things. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07253-x

Braeken, A. (2024). A flexible hybrid post-quantum bidirectional multifactor authentication scheme. *Internet of Things, 26*, 101297. https://doi.org/10.1016/j.iot.2024.101297

Gadou, Z., Mogili, U. R., & Khalid, M. (2019). Multiobjective optimization on DVFS-based hybrid systems for real-time applications using evolutionary algorithms. *Arabian Journal for Science and Engineering, 44*(6), 5699–5713. https://doi.org/10.1007/s13369-018-3519-5

George, G., & Sankaranarayanan, S. (2019). Light weight cryptographic solutions for fog based blockchain. *2019 International Conference on Smart Structures and Systems (ICSSS)*, 1–5. https://doi.org/10.1109/ICSSS.2019.8882870

Goodman, J., & Chandrakasan, A. (2001). An energy-efficient reconfigurable public-key cryptography processor. *IEEE Journal of Solid-State Circuits, 36*(11), 1808–1820. https://doi.org/10.1109/4.962304

Abdullah, K. M., Houssein, E. H., & Zayed, H. H. (2018, April). New security protocol using hybrid cryptography algorithm for WSN. In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-6). IEEE.

Iqbal, N., & Ansari, A. (2025). Design and evaluation of lightweight cryptographic algorithms for Internet of Things (IoT) devices: Achieving optimal trade-offs between security, computational speed, and energy efficiency in resource-constrained environments. *THE PROGRESS: A Journal of Multidisciplinary Studies*. https://doi.org/10.71016/tp/smfybz24

Jallouli, O., Chetto, M., & Assad, S. E. (2022). Lightweight stream ciphers based on chaos for time and energy constrained IoT applications. *2022 11th Mediterranean Conference on Embedded Computing (MECO)*, 1–5. https://doi.org/10.1109/MECO55406.2022.9797087

Jian, M.-S., Cheng, Y.-E., & Shen, C. (2019). Internet of Things (IoT) cybersecurity based on the hybrid cryptosystem. *2019 21st International Conference on Advanced Communication Technology (ICACT)*, 176–181. https://doi.org/10.23919/ICACT.2019.8701957

Karmous, N., Hizem, M., Ben Dhiab, Y., Ould-Elhassen, M., Aoueileyine, R., Bouallegue, N., & Youssef. (2024). Hybrid cryptographic end-to-end encryption method for protecting IoT devices against MitM attacks. *Radioengineering*. https://doi.org/10.13164/re.2024.0583

Kharbouche-Harrari, M., Pendina, G. D., Wacquez, R., Diény, B., Aboulkassimi, D., Postel-Pellerin, J., & Portal, J. (2019). Light-weight cipher based on hybrid CMOS/STT-MRAM: Power/area analysis. *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*, 1–5. https://doi.org/10.1109/ISCAS.2019.8702734

Ledwaba, L. P. I., Hancke, G., Venter, H., & Isaac, S. (2018). Performance costs of software cryptography in securing new-generation Internet of Energy endpoint devices. *IEEE Access, 6*, 9303–9323. https://doi.org/10.1109/ACCESS.2018.2793301

Nikitha, G. A., Kathrine, G., Duthie, C., Ebenezer, V., & Silas, S. (2023). Hybrid cryptographic algorithm to secure Internet of Things. *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 1556–1562. https://doi.org/10.1109/ICICCS56967.2023.10142709

Ozmen, M. O., & Yavuz, A. (2017). Low-cost standard public key cryptography services for wireless IoT systems. *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. https://doi.org/10.1145/3139937.3139940

Panasenko, S. P., & Smagin, S. A. (2011, September). Energy-efficient cryptography: Application of KATAN. In *SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks* (pp. 1-5). IEEE.

Popoola, O., Rodrigues, M. A., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and

security. *Internet of Things, 27*, 101314. https://doi.org/10.1016/j.iot.2024.101314

Pote, A., Thakare, R., & Suralkar, S. (2025). Performance evaluation of post-quantum cryptography: A review. *ICT Express*. https://doi.org/10.1016/j.icte.2024.09.005

Prabagaran, M., & Kaur, A. (2024). Designing the energy efficient and memory-conserving cryptographic algorithm for IoT environment. *2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP)*, 1–6. https://doi.org/10.1109/IHCSP63227.2024.10959966

Prasath, J. S., Ramachandraiah, U., Prabhuraj, S., & Muthukumaran, G. (2020). Internet of things based hybrid cryptography for process data security. *J. Math. Comput. Sci., 10*(6), 2208-2232.

Sable, N. P., Rathod, V. U., Parlewar, P., Rathod, S. B., Waghmode, S. T., & Rathod, R. R. (2024). Efficient lightweight cryptography for resource-constrained WSN nodes. *Journal of Discrete Mathematical Sciences and Cryptography*. https://doi.org/10.47974/jdmsc-1888

Soto-Cruz, J., Ruiz-Ibarra, E., Vázquez-Castillo, J., Espinoza-Ruiz, A., Castillo-Atoche, A., & Mass-Sanchez, J. (2024). A survey of efficient lightweight cryptography for power-constrained microcontrollers. *Technologies*. https://doi.org/10.3390/technologies13010003

Suárez-Albela, M., Fraga-Lamas, P., Castedo, L., & Fernández-Caramés, T. (2018). Clock frequency impact on the performance of high-security cryptographic cipher suites for energy-efficient resource-constrained IoT devices. *Sensors, 19*(1), 15. https://doi.org/10.3390/s19010015

Suslowicz, C., Krishnan, A. S., & Schaumont, P. (2017). Optimizing cryptography in energy harvesting applications. *Proceedings of the 2017 Workshop on Attacks and Solutions in Hardware Security*, 57–62. https://doi.org/10.1145/3139324.3139329

Thorat, C., & Inamdar, V. (2018). Implementation of new hybrid lightweight cryptosystem. *Applied Computing and Informatics*. https://doi.org/10.1016/J.ACI.2018.05.001

Tripathi, D. R., Akhtar, H. N. N., & Bhandarkar, R. R. (2024). Enhancing IOT security: Investigating lightweight encryption algorithms for resource-constrained devices. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2024.64519

U. B., & A. D. (2024). Powering up security as lightweight crypto for efficient IoT. *2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT)*, 1–6. https://doi.org/10.1109/ICEEICT61591.2024.10718437

Vahi, A., & Jassbi, S. (2020). SEPAR: A new lightweight hybrid encryption algorithm with a novel design approach for IoT. *Wireless Personal Communications*, 1–32. https://doi.org/10.1007/s11277-020-07476-y

Verma, Dubba. (2025). Hybrid data integrity verification for real-time IoT systems using AEAD and VRF with ECDSA. *Journal of Information Systems Engineering and Management*. https://doi.org/10.52783/jisem.v10i34s.5875

Vu, Q., Nguyen, T. H., Nguyen, V. D., Le, L. B., & Le, L. P. (2025). Hybrid active–passive STARRIS-based NOMA systems: A physical layer security perspective. *Physical Communication, 59*, 102183. https://doi.org/10.1016/j.phycom.2023.102183

Zitouni, N., Sedrati, M., & Behaz, A. (2023). Lightweight energy-efficient block cipher based on DNA cryptography to secure data in internet of medical things devices. *International Journal of Information Technology*. https://doi.org/10.1007/s41870-023-01580-5