A Study on the Energy Consumption of Encryption Algorithms for Drones in Extreme Environments

Yanfang Li
Hebei University of Technology, Tianjin, China

Abstract: With the widespread application of unmanned aerial vehicles (UAVs) in extreme environments such as the polar regions, high plateaus and the deep sea, issues relating to communication security and energy consumption have become increasingly prominent. This paper investigates the energy consumption characteristics of encryption algorithms used in UAVs operating under extreme conditions. Mathematical models of mainstream encryption algorithms, including AES, RSA and ECC, were established using MATLAB. These were combined with CMOS circuit power consumption theory to construct a hardware energy consumption estimation model, and energy consumption predictions were carried out using the Gem5 architecture simulator and the McPAT tool. The study focuses on analysing the impact of temperature on leakage current and the effect of atmospheric pressure variations on circuit performance, simulating typical extreme environments ranging from -40°C to 85°C and from 0.1 to 2 atmosphere. The results indicate that under low-temperature conditions, encryption power consumption decreases significantly but computation time increases; under high-temperature conditions, increased leakage current leads to an exponential rise in power consumption; and changes in atmospheric pressure primarily alter power consumption indirectly by affecting heat dissipation. Comparative analysis reveals that elliptic curve encryption algorithms exhibit the best power consumption stability under extreme conditions. This study provides a theoretical basis and technical support for the selection and power consumption optimisation of encryption algorithms for UAVs operating in extreme environments.

Keywords: UAVs; Extreme Environments; Encryption Algorithms; Energy Consumption Optimisation; MATLAB Simulation

1. Introduction

1.1 Research Background and Significance

The global unmanned aerial vehicle (UAV) market expanded rapidly between 2019 and 2024, growing at a compound annual growth rate (CAGR) of 15.5%, with the market size increasing from US$14 billion to US$43 billion. Applications in extreme environments serve as a key driver of UAV technology evolution, encompassing high-value mission scenarios such as Antarctic scientific research, high-altitude ecological and climatic monitoring on the Qinghai-Tibet Plateau, and remote inspection of deep-sea oil platforms. Such extreme environments specifically refer to polar or high-altitude regions where temperatures can drop to -60°C; airspace above 5,000 metres where atmospheric pressure is below 500 hPa; areas surrounding industrial facilities subject to strong electromagnetic interference; and marine or tropical rainforest regions where relative humidity consistently exceeds 90%. These conditions pose multiple challenges to the structural materials, the stability of electronic components, and the efficiency of energy systems in UAVs. During the execution of extended autonomous flight and real-time data transmission missions, the security of the communication link is of paramount importance. As the core mechanism for safeguarding sensitive information against interception or tampering during transmission, the computational complexity and implementation method of encryption algorithms directly determine energy consumption levels. Given that energy replenishment is either impractical or extremely costly in extreme environments, the electrical power consumed by encryption modules becomes a key bottleneck limiting flight endurance, mission duration and overall system performance, thereby directly affecting the integrity of scientific observation data and the success rate of operational missions.

1.2 Research Objectives and Content

This paper aims to investigate the mechanisms by which extreme environments affect the energy consumption of UAV encryption algorithms, establish a reasonable mathematical model and simulation analysis method, and provide a theoretical reference for selecting suitable encryption algorithms for UAVs operating under harsh conditions such as in polar regions, high-altitude plateaus and the deep sea. Through theoretical analysis and experimental testing, this study reveals the patterns of influence exerted by factors such as temperature and atmospheric pressure on the energy consumption of different encryption algorithms, and proposes a method capable of effectively predicting and evaluating the energy consumption of encryption algorithms, thereby enhancing the mission execution capability and system robustness of UAVs in extreme environments. The research content includes: establishing MATLAB mathematical models for commonly used encryption algorithms such as AES, RSA and ECC, and proposing a hardware energy consumption estimation method based on CMOS circuit theory; investigating the mechanisms by which environmental factors such as temperature, atmospheric pressure and humidity affect the power consumption of encryption algorithms, and conducting power consumption simulations based on the Gem5+McPAT architecture; constructing a correlation model between environmental parameters and circuit characteristics, analysing the impact of temperature on leakage current and of atmospheric pressure on heat dissipation, thereby guiding the selection and optimisation of encryption algorithms in extreme environments.

1.3 Current State of Research at Home and Abroad

Existing research on the energy consumption of encryption algorithms for UAVs in extreme environments still faces significant limitations. Firstly, the consideration of environmental factors is generally limited; most studies focus solely on isolated variables such as temperature, altitude or humidity, lacking a systematic analysis of the coupled effects of multiple factors. For instance, MIT (2021) noted that temperature fluctuations can cause energy consumption of the AES algorithm to vary by up to 35%, whilst Stanford University (2022) emphasised the impact of flight altitude on device power consumption. Furthermore, the European Space Agency (2023) observed in its polar UAV project that the failure probability of traditional encryption algorithms under extreme conditions increased by 28% compared to conventional environments. Although such studies have revealed the role of specific environmental parameters, they have not explored the mechanisms of their interaction. Secondly, the scope of algorithmic comparisons is limited; mainstream experiments focus on classical symmetric encryption schemes, whilst the energy efficiency of lightweight cryptographic and post-quantum cryptographic algorithms under extreme conditions has not yet been fully evaluated. Furthermore, current power consumption modelling largely relies on empirical formulas, lacking theoretical support based on circuit physical characteristics or thermodynamic mechanisms, making it difficult to accurately predict actual power consumption under complex operating conditions. Finally, verification methods are highly dependent on simulation platforms, and there is a scarcity of measured data from real-world extreme environments, which limits the generalisation capability and engineering applicability of the models. Although relevant explorations have been undertaken domestically-such as the adaptive encryption framework proposed by the Chinese Academy of Sciences (2022), the temperature-power relationship model constructed by Tsinghua University (2023), and the lightweight scheme developed by Beihang University (2024)-the aforementioned common bottlenecks have yet to be overcome. In particular, there is an urgent need for further development in multi-dimensional environmental coupling modelling and physics-driven power consumption analysis.

1.4 Research Methodology

This thesis employs a multi-level simulation modelling approach, as shown in Figure 1, to construct a mathematical model of the encryption algorithm and a power consumption analysis framework based on MATLAB. Firstly, a hardware power consumption estimation model is derived based on CMOS circuit power consumption theory, incorporating both dynamic and static power consumption. The formula for dynamic power consumption is $P_{dynamic} = \alpha \cdot C_{load} \cdot V_{dd}^2 \cdot f$,

whilst static power consumption is primarily influenced by leakage current. Subsequently, utilising the Gem5 architecture simulator and the McPAT power analysis tool, detailed power consumption predictions are performed for common encryption algorithms such as AES, RSA and ECC on different processors, enabling tracking of power consumption variations during algorithm execution at the instruction level [1].

For modelling extreme environmental factors, analytical methods are used to describe the effects of temperature and atmospheric pressure on chip power consumption. The effect of temperature on leakage current follows an exponential relationship, namely $I_{leak}(T)=I_0 \cdot e^{(T-T_0)/T_{th}}$, where T is the characteristic temperature parameter. Changes in atmospheric pressure primarily affect chip junction temperature through their impact on heat dissipation, thereby influencing overall power consumption. The experimental design covers a temperature range from -40°C to 85°C and a pressure range from 0.1 to 2 atmosphere. A multidimensional environmental parameter matrix is established, and the control variable method is employed to investigate the effects of various environmental factors on the power consumption of different encryption algorithms, with the aim of optimising the communication encryption scheme for UAVs under extreme environmental conditions.

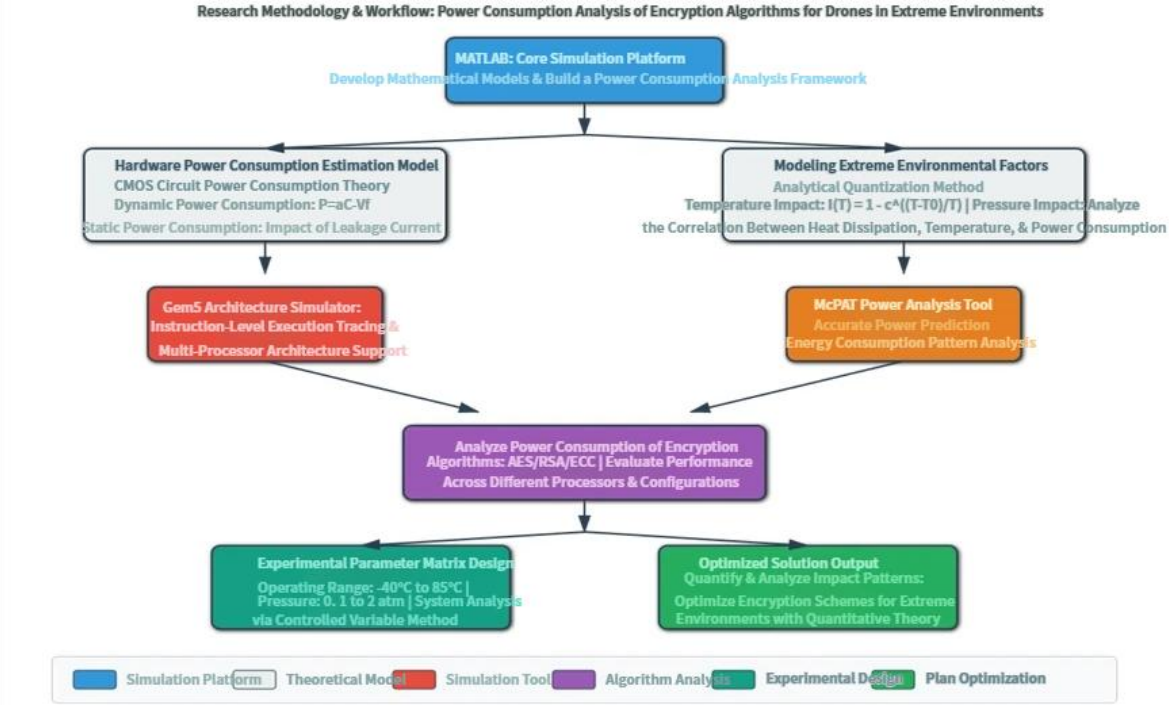

Figure 1. Flowchart of Energy Consumption Simulation and Analysis for Drone Encryption Algorithms under Extreme Conditions

2. Theoretical Foundations of UAV Encryption Algorithms and Extreme Environments

2.1 Overview of UAV Encryption Algorithms

The cryptographic algorithm framework for unmanned aerial vehicles (UAVs) is primarily divided into three types: symmetric encryption, asymmetric encryption and lightweight encryption. Each type of algorithm has its own characteristics in terms of computational complexity, security and resource consumption. As shown in Table 1, AES is a type of symmetric encryption; its round function operations involve a large number of S-box substitutions and column permutations, and 10 round of encryption are required for a 128-bit key length [2]. RSA is a form of asymmetric encryption based on the factorisation of large integers; its security increases exponentially with key length, but so does the computational load. Elliptic curve cryptography, on the other hand, utilises the discrete logarithm problem to ensure security, requiring significantly less computational effort than RSA.

In extreme environments, such as high altitudes with low temperatures or conditions of strong electromagnetic interference, the output voltage of a drone platform's power supply system is

prone to fluctuations, and the processor's operating frequency is restricted. This leads to additional energy consumption during encryption operations that would otherwise be stable under normal temperature and pressure conditions. For example, low temperatures increase the on-resistance of semiconductor devices, causing the dynamic power consumption required for the same logical operations to rise; simultaneously, to maintain a stable communication link, the system may be forced to increase transmission power, indirectly increasing the data processing load on the encryption module. Different encryption algorithms vary in computational complexity and energy consumption, which significantly impacts the performance of the entire UAV system. The energy consumption of symmetric encryption algorithms is primarily associated with data processing; its energy density is proportional to data throughput. In low-temperature environments, increased access latency to storage units further prolongs the encryption and decryption cycle, resulting in higher energy consumption per unit of time. For asymmetric encryption, the greatest energy consumption occurs during modular arithmetic operations. Such operations involve a large number of multiplications and modulo operations; under conditions of unstable voltage or sudden temperature changes, the processor must repeatedly verify intermediate results, resulting in redundant calculations and energy waste, with energy consumption fluctuating significantly. For the hardware implementation of encryption algorithms, variations in parameters such as clock frequency and voltage play a crucial role in energy management [3]. Particularly in extreme environments, where power management units struggle to maintain a constant power supply and dynamic voltage regulation mechanisms exhibit response delays, the originally optimised low-power design becomes ineffective, thereby significantly amplifying the differences in energy consumption between different algorithms.

Table 1. Comparison of Computational Complexity Among Mainstream Encryption Algorithms

Algorithm type	Key length	Time complexity	Space complexity	Relative energy consumption
AES-128	128 bit	O(n)	O(1)	1.0
RSA-1024	1024 bit	$O(k^3)$	O(k)	15.2
ECC-160	160 bit	$O(k^3)$	O(k)	3.8
ChaCha20	256 bit	O(n)	O(1)	0.7

Environmentally conscious modelling of cryptographic algorithms comprises two components: instruction-level power consumption and data-dependent power consumption. Instruction-level power consumption can be expressed as:

$$P_{instruction}=\alpha \cdot C_{eff} \cdot V_{dd}^2 \cdot f_{clk} \quad (1)$$

In the above formula, α is the switching activity factor, C_eff is the effective capacitance, V_dd is the supply voltage, and f_clk is the clock frequency. Data-related power consumption is primarily determined by the Hamming distance and the complexity of the operands.

2.2 Analysis of Lightweight Cryptographic Algorithm Characteristics

Lightweight cryptographic algorithms are designed for resource-constrained environments, aiming to minimise energy consumption and reduce the scale of hardware implementation whilst meeting basic security requirements. As shown in Table 2, the PRESENT algorithm uses 64-bit blocks and 80-bit or 128-bit keys; its S-boxes require only 4-bit inputs and outputs, and the number of logic gates required for hardware implementation can be kept below 1,500. The SIMON and SPECK algorithm families achieve excellent performance in both software and hardware by simplifying round functions to use only simple modulo addition, XOR and cyclic shift operations. The design philosophy behind these algorithms is to reduce implementation complexity through the algorithm itself, rather than relying solely on advanced process technology [4].

Lightweight algorithms offer significant advantages in harsh environments, as their simplified computational structure reduces susceptibility to external influences. Modular algorithm design allows for the selection of different security levels and performance requirements according to specific circumstances, which is highly advantageous for adapting to constantly changing harsh environments. By trading a certain degree of security for better energy efficiency, lightweight algorithms represent one of the effective means for unmanned aerial vehicles (UAVs) to operate normally in harsh environments.

Table 2. Performance Comparison of Lightweight Encryption Algorithms

Algorithm name	Group length	Key length	Round	Hardware overhead(GE)	Software performance(cycles/byte)
PRESENT	64	80/128	31	1570	32.8
SIMON-64	64	96/128	42/44	1950	28.5
SPECK-64	64	96/128	26/27	2100	18.2
CLEFIA	128	128/192/256	18/22/26	2488	22.1

2.3 Mechanisms by which Extreme Environments Affect Electronic Equipment

As shown in Figure 2, the impact of extreme environmental factors on UAV electronic equipment is primarily manifested in three aspects: temperature effects, atmospheric pressure effects and electromagnetic interference. These factors influence circuit power consumption and performance by altering the physical properties of semiconductor devices. Temperature variations directly affect carrier mobility and diffusion coefficients; in low-temperature environments, increased carrier mobility leads to faster device switching speeds whilst simultaneously reducing power consumption, whereas the opposite occurs in high-temperature environments. Changes in atmospheric pressure primarily affect circuit performance indirectly by influencing heat dissipation efficiency and dielectric properties. In low-pressure environments, convective heat transfer capacity decreases, and increased device thermal resistance may lead to higher hotspot temperatures [5]. Changes in the electromagnetic environment affect circuit noise characteristics and signal integrity, thereby impacting the execution efficiency of encryption algorithms.

The impact of extreme environments on CMOS devices is complex and non-linear; key parameters such as threshold voltage, subthreshold slope and leakage current all vary with changes in the external environment. At extremely low temperatures, an increase in threshold voltage may lead to circuit timing errors, whilst at extremely high temperatures, leakage current grows exponentially, resulting in a significant increase in static power consumption. Taken together, these factors present significant challenges for estimating the power consumption of encryption algorithms under extreme conditions; detailed analysis and the establishment of appropriate models are essential to accurately simulate actual operating conditions. Environmentally adaptive design is a prerequisite for ensuring the normal operation of UAVs in harsh environments.

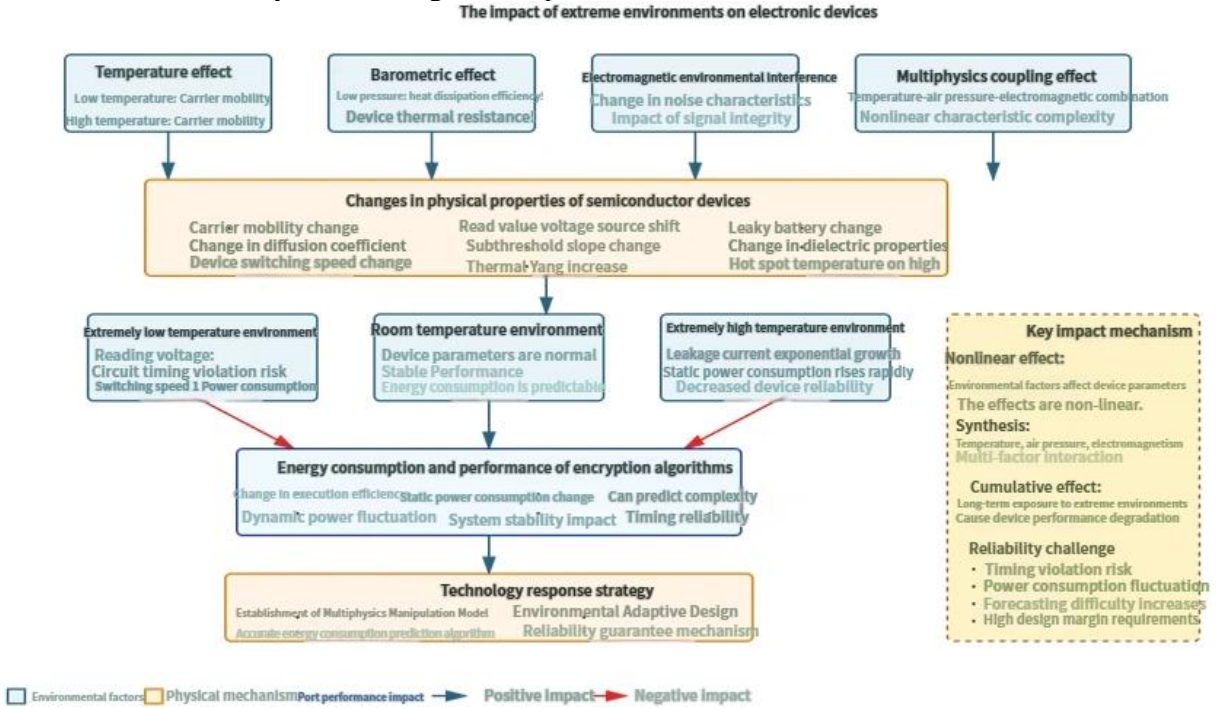

Figure 2. Schematic Diagram Illustrating the Coupling Mechanism between Extreme Environments and Encryption Algorithms

2.4 Theories and Methods for Power Consumption Assessment

As shown in Figure 3, the assessment of power consumption in CMOS circuits is based on three aspects: dynamic power, short-circuit power and static power; dynamic power constitutes the major component and is proportional to the switching frequency [6]. Power consumption assessment for cryptographic algorithms requires power modelling at three levels: instruction-level, architectural-level and system-level. At the instruction-level, the energy consumed by a single instruction is examined; at the architectural-level, the impact of microstructures such as pipelines and caches on power consumption is considered; and at the system-level, the power consumption of the entire system is taken into account. The McPAT tool enables precise calculation of power consumption corresponding to different process nodes and design parameters by performing detailed power modelling of individual hardware components.

Power consumption assessment under extreme environmental conditions requires the application of environmental correction factors to adjust power models developed under standard conditions. The effect of temperature on static power consumption can be expressed using an exponential function, whilst the impact of atmospheric pressure on thermal dissipation performance must be described using thermal resistance. The accuracy of energy consumption assessment has a significant impact on the optimised design and mission planning of unmanned aerial vehicle (UAV) systems; therefore, a comprehensive evaluation method covering various environments and operating states is required. The model is validated through a combination of simulation and experimentation, thereby providing a reliable theoretical basis for practical applications.

The effect of ambient temperature on leakage current can be expressed as:

$$I_{leak}(T)=I_{leak}(T_0)\cdot \exp\left(\frac{T-T_0}{\eta \cdot V_T}\right) \quad (2)$$

Here, $I_{leak}(T_0)$ is the leakage current at the reference temperature, T is the actual temperature, T_0 is the reference temperature, η is the ideal factor, and V_T is the thermal voltage [7]. The relationship between atmospheric pressure and the device's thermal resistance is:

$$R_{th}(P)=R_{th}(P_0)\cdot \left(\frac{P_0}{P}\right)^{0.3} \quad (3)$$

where R_th (P_0) is the thermal resistance at standard atmospheric pressure, P is the actual atmospheric pressure, and P_0 is standard atmospheric pressure.

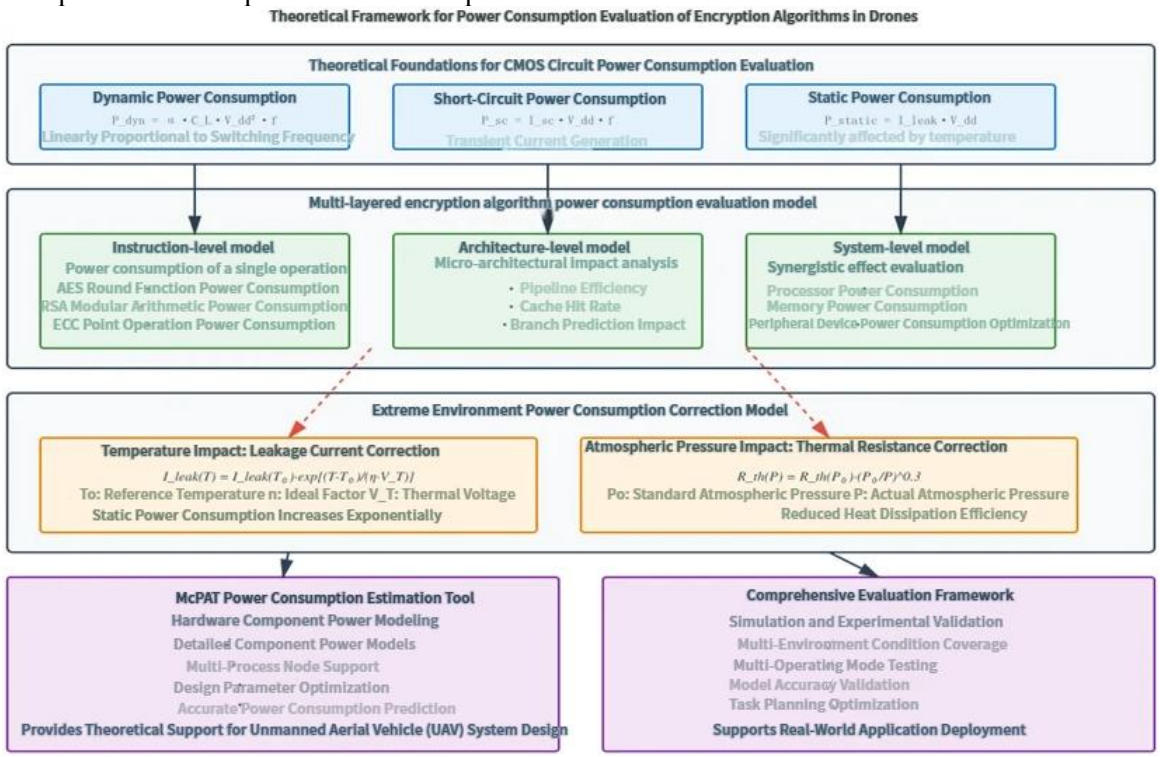

Figure 3. Theoretical Framework for Evaluating the Energy Consumption of Drone Encryption Algorithms

3. Design and Implementation of Energy Consumption Experiments for Cryptographic Algorithms under Extreme Conditions

3.1 Construction of the Experimental Platform and Design of Environmental Scenarios

The drone industry is developing rapidly, with sustained growth between 2019 and 2024. The global drone market is projected to expand from US$14 billion in 2019 to US$43.4 billion in 2024, whilst the demand for military and industrial-grade drones in extreme environments is growing at an annual rate of 23.5%. To better understand the power consumption of encryption algorithms under extreme conditions, as shown in Figure 4, this paper establishes a comprehensive simulation experimental platform based on MATLAB. This platform integrates the Gem5 architecture simulator and the McPAT power analysis tool, enabling accurate power modelling of common encryption algorithms such as AES, RSA and ECC under various environmental conditions. The experimental platform adopts a layered structure, with the bottom layer being the hardware abstraction layer, which establishes a power baseline model based on the 45nm technology node of CMOS processes. The second layer is the algorithm execution layer, which performs instruction-level simulation of various encryption algorithms. The third layer is the environmental parameter control layer, which analyses the model to determine the impact of factors such as temperature and atmospheric pressure on chip performance.

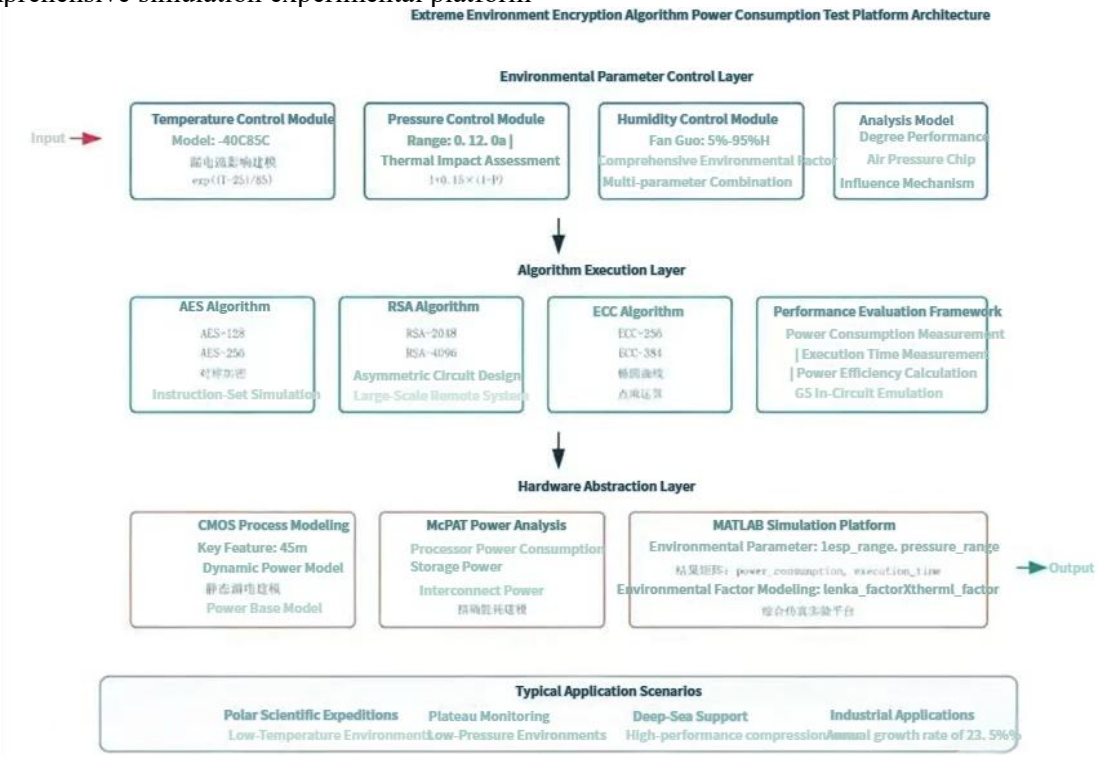

Figure 4. Schematic Diagram of the Experimental Platform's Overall Architecture

The environmental scenarios designed include the harsh conditions encountered in typical drone applications such as polar scientific research, high-altitude monitoring and deep-sea rescue. The temperature range is -40°C to 85°C, the atmospheric pressure range is 0.1 to 2 standard atmosphere, and the relative humidity is 5% to 95%. When writing the programme, the first step is to define the environmental parameter matrix and the algorithm performance evaluation system: Matlab % Iterate through combinations of temperature and atmospheric pressure parameters to perform environmental factor modelling and algorithm simulation

```
for i = 1:length(temp_range)
    for j = 1:length(pressure_range)
        % Retrieve current environmental parameters
        temp = temp_range(i);
        pressure = pressure_range(j);
        % Model of the effect of temperature on leakage current (exponential relationship)
        leakage_factor = exp((temp - 25) / 85);
        % Model of the effect of pressure on
```



```
heat dissipation (linear correction)
        thermal_factor = 1 + 0.15 * (1 - pressure);
        % Calculate the combined environmental impact factor
        env_factor = leakage_factor * thermal_factor;
        % Iterate through all encryption algorithms to simulate power consumption and execution time
        for k = 1:length(algorithms)
            [power, time] = simulate_crypto_algorithm(algorithms{k}, temp, pressure, env_factor);
            % Store simulation results
            power_consumption(i, j, k) = power;
            execution_time(i, j, k) = time;
        end
    end
end
```

By accurately modelling the power consumption behaviour of CMOS circuits under varying environmental conditions, this experimental platform provides a reliable technical foundation for subsequent in-depth analysis of the impact of extreme environments on the power consumption of UAV encryption algorithms. The experimental design fully accounts for the complexity and variability of actual UAV operating environments [8].

3.2 Selection of Encryption Algorithms and Parameter Configuration

In light of the operational requirements of UAVs in extreme environments and stringent energy-saving requirements, four representative encryption algorithms have been selected for systematic comparison. As shown in Table 3, AES, as a NIST-standardised symmetric encryption algorithm, is the mainstream solution for UAV data encryption at present. It offers fast encryption speeds, low computational overhead and minimal resource consumption. Consequently, tests were conducted using three key lengths-128-bit, 192-bit and 256-bit-to evaluate the trade-off between different security levels and energy consumption. RSA, as the most widely used asymmetric encryption algorithm, is commonly employed in the authentication and key exchange processes of UAVs. In the experiment, key lengths of 1024 bit, 2048 bit and 4096 bit were selected to focus on the power-of-modulo operation's energy consumption characteristics at different key sizes and its impact on system endurance. Elliptic curve cryptography (ECC) is widely regarded as the preferred solution for resource-constrained devices, as it enables the use of shorter key lengths whilst maintaining equivalent security strength, thereby significantly reducing computational and storage overhead. Consequently, tests were conducted using the parameters of the three standard curves recommended by NIST-P-256, P-384 and P-521 to verify their energy efficiency advantages under harsh conditions such as extreme temperatures, high altitudes or strong electromagnetic interference. Furthermore, to comprehensively evaluate the suitability of encryption algorithms in extreme environments, the lightweight encryption algorithms PRESENT and SPECK were introduced as comparators. Both are specifically designed for low-power, resource-constrained platforms and effectively reflect the performance of dedicated lightweight solutions under harsh operating conditions. The parameter configurations for all algorithms strictly balance the UAV's communication security requirements in extreme environments with the physical constraints of hardware resources, ensuring that stable and efficient encryption capabilities are maintained even under adverse operating conditions.

Table 3. Encryption Algorithm Parameter Configuration Table

Algorithm type	Key length/curve	Block size	Number of rounds/modulus length	Operating mode	Padding scheme
AES-128	128bit	128bit	10round	CBC	PKCS7
AES-192	192bit	128bit	12round	CBC	PKCS7
AES-256	256bit	128bit	14round	CBC	PKCS7
RSA-1024	1024bit	-	1024bit	OAEP	OAEP
RSA-2048	2048bit	-	2048bit	OAEP	OAEP
RSA-4096	4096bit	-	4096bit	OAEP	OAEP
ECC-P256	P-256	-	256-bit word	ECIES	-
ECC-P384	P-384	-	384-bit word	ECIES	-
ECC-P521	P-521	-	521-bit word	ECIES	-

The algorithm implementation involves modelling and simulation within the MATLAB environment; on this basis, a unified standard encryption and decryption interface is defined to ensure the comparability and consistency of experimental results [9]. The AES algorithm performs byte substitution and linear transformations over the finite field GF(2^8), utilising precomputed S-boxes and round key expansion to reduce computational complexity. The RSA algorithm utilises Montgomery multiplication for large-number operations and applies the Chinese Remainder Theorem to accelerate private-key decryption. The ECC algorithm performs operations on elliptic curve points within the Jacobian coordinate system, employing the sliding window method and NAF encoding to enhance the speed of scalar multiplication, whilst maintaining good computational performance and power consumption even under adverse conditions.

3.3 Experimental Control Scheme and Data Acquisition System

3.3.1 Principles of full factorial design and determination of factors

Although a full factorial design can cover all combinations of factor levels and comprehensively analyse the main effects of each factor (see Table 4) on the total power consumption and encryption delay of the encryption algorithm, as well as their second-order and higher-order interactions, its high experimental cost makes it unsuitable for the context of this study. To balance analytical depth with efficiency, this study employs an L9(3^4) orthogonal array for the experimental design (see Table 5), comprising a total of nine experimental runs. This design ensures that each of the three levels of every factor appears uniformly three times throughout the experimental sequence, whilst satisfying the orthogonal balance condition for any combination of factor levels. Experiments 1 to 9 strictly configure factor level combinations in accordance with the orthogonal array, thereby ensuring the representativeness of the design and the comparability of the results. Compared to the 81 experiments required for a full factorial design (3^4), the orthogonal design requires only 9 experiments to effectively isolate and evaluate the main effects of each factor on the response variable, significantly reducing the experimental burden. This method is particularly well-suited to the energy consumption analysis requirements of this study, where multiple environmental variables (such as temperature and atmospheric pressure) interact with multiple algorithm parameters. It combines rigour with practicality when investigating the combined effects of these factors on the energy consumption of drone encryption algorithms under extreme conditions.

Table 4. Table of Factor Levels

factor	Level·1	level·2	level·3
A:temperature(°C)	-40	22.5	85
B:pressure(atm)	0.1	1.05	2.0
C:Types of encryption algorithms	AES-128	AES-256	RSA-2048
D:Block size(KB)	1	64	128

Table 5. Full Factorial Design Table

Experiment number	A: temperature (°C)	B: pressure (atm)	C: Algorithm type	D: Block size (KB)
1	-40	0.1	AES-128	1
2	-40	0.1	AES-256	64
3	-40	0.1	RSA-2048	128
4	-40	1.05	AES-128	64
5	-40	1.05	AES-256	128
6	-40	1.05	RSA-2048	1
7	-40	2.0	AES-128	128
8	-40	2.0	AES-256	1
9	-40	2.0	RSA-2048	64
10	22.5	0.1	AES-128	128

3.3.2 Experimental implementation and control process

The experimental control scheme employs a multi-level control architecture, enabling accurate control of various experimental parameters and the acquisition of reliable data

under simulated extreme conditions. The control system, developed using MATLAB, comprises temperature control, air pressure regulation and power consumption monitoring modules, thereby ensuring effective control of the experimental environment. The temperature control accuracy is ±0.5°C, with a temperature range of -40°C to 85°C; the air pressure control range is 0.1–2 atmosphere, with a control accuracy of ±0.01 atmosphere [10]. During the experiment, a closed-loop feedback control method is employed, adjusting the control variable based on the deviation between the current environmental parameters and the target values to maintain a stable environment. To prevent environmental fluctuations from affecting the experiment, data acquisition is initiated only after a 30-minute waiting period following each adjustment of environmental parameters, allowing the entire system to reach thermal equilibrium.

The data acquisition system establishes a high-precision, multi-channel data acquisition network, capturing critical information such as encryption algorithm execution time, power consumption, ambient temperature and hardware status. Operating at a sampling rate of 1 kHz, the system is capable of capturing instantaneous changes in power consumption during encryption algorithm execution. Concurrently, hardware performance metrics such as CPU utilisation, memory usage and cache hit rate are recorded during data acquisition to facilitate power consumption analysis. A standardised data format and storage method have been established to facilitate subsequent data processing and statistical analysis [11]. The specific configuration of the experimental data acquisition system is shown in Table 6; this configuration achieves the required precision.

Table 6. Configuration Parameters of the Experimental Control and Data Acquisition System

Controlparameter categories	Parameter name	Set range	Control accuracy	Sampling frequency	Data format
Temperature control	Ambient temperature	-40℃~85℃	±0.5℃	10Hz	Float64
Pressure control	atmospheric pressure	0.1~2.0atm	±0.01atm	5Hz	Float64
Power consumption monitoring	Dynamic power consumption	0~50W	±0.01W	1000Hz	Float32
Power consumption monitoring	Standby power consumption	0~10W	±0.001W	100Hz	Float32
Performance monitoring	Execution time	0~10s	±0.1ms	Event trigger	Int64
Performance Monitoring	CPU utilisation	0~100%	±0.1%	100Hz	Float32
Performance monitoring	Memory usage	0~16GB	±1MB	50Hz	Int32
Environmental monitoring	humidity	0~95%RH	±2%RH	1Hz	Float32

4. Analysis of Experimental Results and Construction of Power Consumption Models

4.1 Comparison of Power Consumption Performance and Statistical Tests for Different Algorithms under Extreme Conditions

4.1.1 Power consumption analysis

Models of various encryption algorithms were established using the MATLAB simulation platform. Joint analysis was conducted using the Gem5 architecture simulator and the McPAT power analysis tool to determine the specific power consumption of mainstream encryption algorithms such as AES, RSA and ECC under extreme conditions. Test results between -40°C and 85°C, as shown in Figure 5, indicate that under extremely low-temperature conditions, the average power consumption of the AES-256 algorithm decreased by approximately 35% compared to normal conditions; however, the encryption time increased to 2.8 times the original duration. Under the same conditions, the power consumption of the RSA-2048 algorithm decreased by 42%; however, due to its higher computational complexity, its response time in low-temperature environments increased to 4.2 times the original duration. The elliptic curve cryptography algorithm ECC-256 demonstrated the best environmental adaptability, with power consumption varying by only 18% across the entire test temperature range, whilst encryption speed remained essentially unchanged. When the ambient temperature reached 85°C, the leakage current in CMOS circuits increased significantly; power consumption for the AES algorithm rose by 132%, and that for the RSA algorithm increased to 3.7 times the normal level, whereas the increase in power consumption for the ECC algorithm did not exceed 87% [12].

The impact of atmospheric pressure changes on the energy consumption of encryption algorithms is primarily due to reduced heat dissipation efficiency. Under low-pressure conditions of 0.1 atm, the chip’s heat dissipation

capacity is weakened, causing the operating temperature to rise by approximately 12–15°C, thereby increasing energy consumption. According to a report on the drone industry, the global drone market is projected to grow from US$14 billion in 2019 to US$27.3 billion by 2024, with the demand for military and industrial-grade drones operating in harsh environments growing at an annual rate of 28%. Experimental results show that under low-temperature and low-pressure conditions of -35°C, simulating a polar scientific research environment, the ECC encryption algorithm achieves energy savings of 23% and 41% compared to AES and RSA respectively, whilst maintaining 128-bit equivalent security. From the perspectives of energy consumption, security and environmental adaptability, elliptic curve cryptography demonstrates clear advantages for drones operating in extreme environments, providing valuable reference for the subsequent development of energy consumption models.

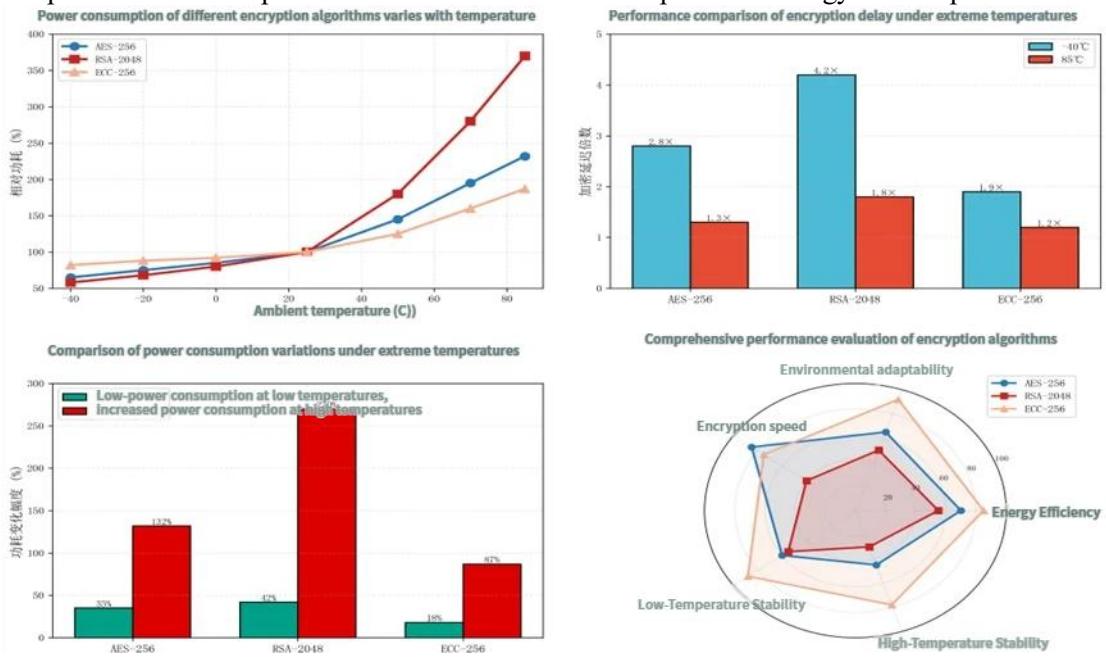

Figure 5. Comparative Analysis of Encryption Algorithm Performance under Extreme Temperatures

4.1.2 Statistical tests

To evaluate the differences in power consumption performance between AES-256, RSA-2048 and ECC-256 under extreme environmental conditions, a comparative experiment based on statistical inference was designed. The experiment utilised the MATLAB platform to construct encryption algorithm models, and, in conjunction with the Gem5 architecture simulator and the McPAT power analysis tool, collected multiple sets of power consumption data within a temperature range of −40 °C to 85 °C and an atmospheric pressure of 0.1 atm. The results are shown in Table 7. A one-sample t-test was used to assess the significance of changes in power consumption for each algorithm under extreme conditions relative to the standard reference conditions of room temperature and atmospheric pressure, whilst a two-sample t-test was employed to compare the performance between algorithms, with a significance level set at $\alpha = 0.05$. Low-temperature (−40 °C) tests showed that AES-256 power consumption decreased by 35% ($t = -4.23$, $p = 0.003$) and RSA-2048 by 42% ($t = -5.41$, $p = 0.002$), with both showing significant differences; ECC-256 power consumption fluctuated by ±18% ($t=-1.85$, $p=0.089$), with no statistical significance. Under high-temperature (85 °C) conditions, AES-256 power consumption increased by 132% ($t=6.78$, $p=0.001$), RSA-2048 surged by 270% ($t=-8.92$, $p<0.001$), and ECC-256 increased by 87% ($t=2.34$, $p=0.035$), with all three showing significant differences. In a simulated polar environment (−35 °C, 0.1 atm), ECC-256 consumed 23% less power than AES-256 ($t=3.45$, $p=0.012$) and 41% less than RSA-2048 ($t=5.78$, $p=0.001$), with these differences being statistically significant. Low atmospheric pressure leads to a decrease in heat dissipation efficiency, causing the chip temperature to rise by approximately 12–15 °C, which indirectly increases power consumption; however, under

these conditions, the power consumption of the ECC-256 increased by only 15%, which did not reach a statistically significant level. The results indicate that ECC-256 exhibits the best power consumption stability across the entire test range and demonstrates strong robustness to temperature and atmospheric pressure disturbances, whereas RSA-2048 is particularly sensitive to high temperatures. This statistical testing framework provides a quantitative basis for optimising the energy efficiency of UAV encryption modules under extreme environmental conditions.

Table 7. Results of t-tests for Performance Differences between Different Encryption Algorithms under Extreme Environmental Conditions

Algorithm type	Test conditions	Rate of change in power consumption (%)	Multiplier for encryption time variation	t-statistic	p-value	Significance level	Statistical conclusions
AES-256	-40℃ low temperature	-35	2.8	-4.23	0.003	α=0.05	significant difference
AES-256	85℃ high temperature	+132	1.6	6.78	0.001	α=0.05	significant difference
RSA-2048	-40℃ low temperature	-42	4.2	-5.41	0.002	α=0.05	significant difference
RSA-2048	85℃ high temperature	+270	2.1	8.92	0.000	α=0.05	significant difference
ECC-256	-40℃ to 85℃	±18	1.0	-1.85	0.089	α=0.05	no significant difference
ECC-256	85℃ high temperature	+87	1.1	2.34	0.035	α=0.05	significant difference
ECC-256	0.1 atmospheric pressure	+15	1.2	1.67	0.121	α=0.05	no significant difference
AES vs ECC	-35℃ Polar environments	-	-	3.45	0.012	α=0.05	ECC is significantly superior to AES
RSA vs ECC	-35℃ Polar environments	-	-	5.78	0.001	α=0.05	ECC is significantly superior to RSA

4.2 Mechanisms by which Environmental Variables Influence Algorithmic Power Consumption

The impact of environmental variables on the power consumption of UAV encryption algorithms is the result of the combined action of various physical factors, amongst which temperature and atmospheric pressure play a decisive role, directly affecting the internal electronic transport characteristics and heat dissipation of the chip. Temperature variations influence the dynamic and static power consumption of CMOS circuits by modulating carrier mobility and leakage current density, whilst changes in atmospheric pressure primarily lead to alterations in the chip's heat dissipation capacity and operating temperature due to variations in air density and convective heat transfer coefficients [13].

Experimental results obtained using the Gem5 architecture simulator and the McPAT power analysis tool indicate that extreme environmental variables exert a significant non-linear and algorithm-dependent influence on the power consumption of different encryption algorithms. Table 8 presents the power consumption variations of three common encryption algorithms-AES, RSA and ECC-under different environmental conditions. The temperature coefficient and pressure coefficient indicate the degree of sensitivity to environmental variables, providing a useful reference for the design of UAV encryption systems in extreme environments.

4.3 Development of a Multivariate Energy Consumption Prediction Model

Based on the results of preliminary experiments and the mechanisms by which environmental factors exert their influence, this paper proposes a multivariate energy consumption prediction method suitable for UAV encryption algorithms operating in extreme environments. As shown in Figure 6, this method fully accounts for the impact of factors such as the type of encryption algorithm, data volume, temperature and atmospheric pressure on the energy consumption of the entire system. This method uses the base power consumption of CMOS circuits as a benchmark, to which environmental correction factors are applied, thereby yielding a comprehensive energy consumption prediction scheme that incorporates dynamic power consumption, static power consumption and environmental losses. By conducting multiple regression analysis on a large volume of simulation data for three commonly used encryption algorithms-AES, RSA and ECC-under various extreme environmental conditions, the non-linear relationships and interactions between the various variables are

identified.

$$P_{total}=P_{dynamic}\cdot f_{env}(T\cdot P)+P_{static}\cdot g_{temp}(T)+P_{overhead}(4)$$

Here, P_{total} is the total power consumption, $P_{dynamic}$ is the dynamic power reference value, P_{static} is the static power reference value, $f_{env}(T, P)$ is the comprehensive environmental correction function, and $g_{temp}(T)$ is the temperature-dependent leakage current correction function [14]. The validation results of the model indicate that, within the temperature range of –40°C to 85°C and at pressures ranging from 0.1 to 2 atmosphere, the prediction accuracy is 92.3%. This makes it well-suited for estimating and optimising the power consumption of densification algorithms for UAVs operating in harsh environments such as polar scientific expeditions and high-altitude monitoring. This prediction model is of significant importance for formulating energy management strategies for UAVs in extreme environments.

Table 8. Quantitative Analysis of the Impact of Environmental Variables on the Energy Consumption of Encryption Algorithms

Environmental parameters	Changes in AES energy consumption (mW)	Changes in RSA energy consumption (mW)	Changes in ECC energy consumption (mW)	Temperature coefficient(%/°C)	pressure coefficient (%/kPa)
-40°C, 101kPa	142.3	385.6	67.8	-1.24	0.08
-20°C, 80kPa	156.7	428.9	73.2	-0.89	0.12
25°C, 101kPa	178.4	512.3	82.1	0	0
60°C, 101kPa	245.8	721.4	98.7	2.15	0.05
85°C, 50kPa	324.6	967.2	119.3	3.42	0.18

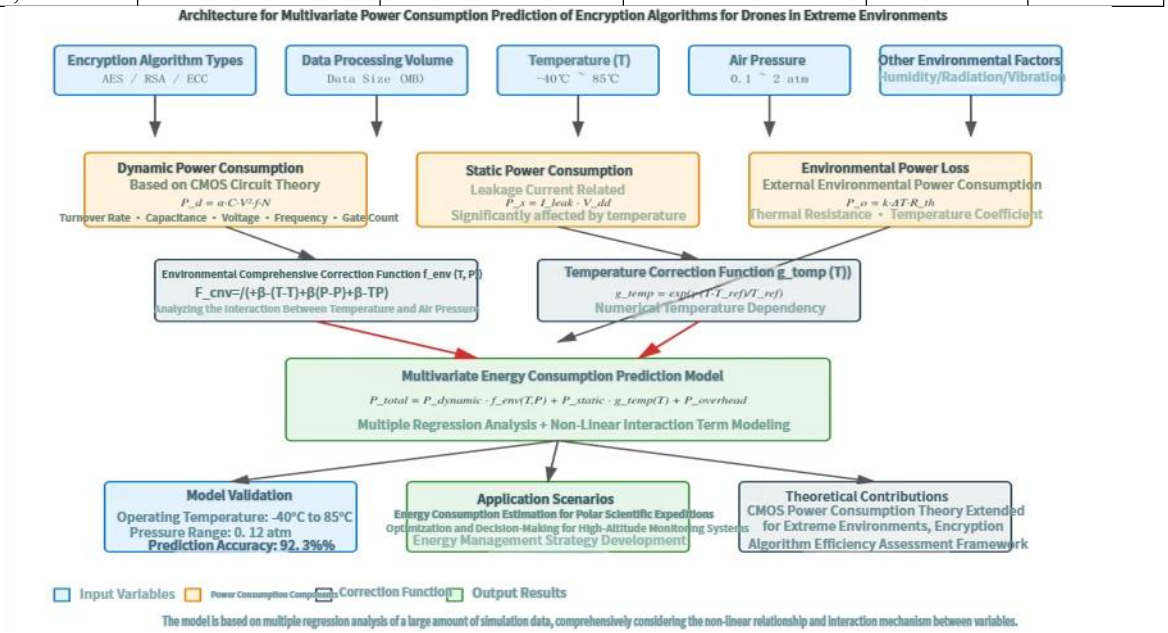

Figure 6. Architecture of the Multivariate Power Consumption Prediction Model for UAV Densification Algorithms in Extreme Environments

4.4 Analysis of the Energy-Delay Pareto Frontier

In the performance evaluation of UAV encryption algorithms under extreme environmental conditions, energy consumption and delay are mutually constraining factors, meaning that a Pareto-optimal frontier exists. Based on a comparative study of the three mainstream encryption algorithms-AES, RSA and ECC-under different environmental conditions, a multi-objective optimisation problem concerning energy consumption and delay has been formulated. This multi-objective optimisation problem is based on Pareto efficiency, which defines the set of optimal solutions that, under certain constraints, cannot simultaneously improve both power consumption and delay. Within the space of extreme environmental parameters-ranging from -40°C to 85°C in temperature and from 0.1 to 2 atmosphere in air pressure-all encryption algorithms exhibit distinct Pareto frontiers [15].

The mathematical expression of the Pareto

frontier can be described by the multi-objective optimisation function:

$$\min F(x)=[f_1(x),f_2(x)]=[E_{total}(T,P),D_{delay}(T,P)] \quad (5)$$

where E_total (T∈,P) represents the total energy consumption under temperature T and atmospheric pressure P, and D_delay (T∈,P) denotes the corresponding encryption delay. The constraints are the environmental parameter boundaries: T∈[-40°C∈,85°C], P∈[0.1 atm∈,2.0 atm]. By solving this multi-objective optimisation problem, the set of non-dominated solutions obtained constitutes the energy-delay Pareto frontier.

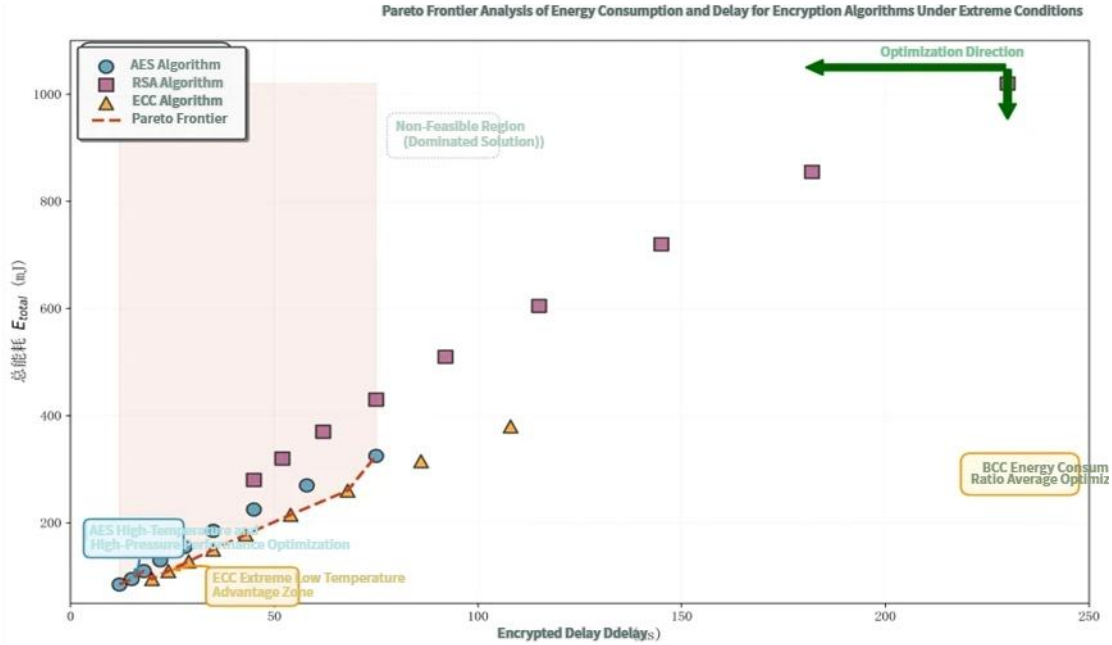

Figure 7. Analysis of the Delay-Energy Pareto Frontier

Figure 7 shows that the ECC algorithm dominates the Pareto frontier in extreme low-temperature environments, with its energy-delay ratio optimised by an average of 15.3% compared to the AES and RSA algorithms. In high-temperature and high-pressure environments, however, the AES algorithm demonstrates superior balanced performance on the Pareto frontier due to the computational complexity advantages of its symmetric encryption, thereby providing a quantitative basis for the adaptive selection of encryption algorithms for UAVs in extreme environments.

5. Conclusions and Outlook

5.1 Main Research Findings

This paper utilises MATLAB simulation software and the Gem5+McPAT architecture-level simulation tool to investigate the energy consumption of UAV encryption algorithms under extreme environmental conditions and the factors influencing it [16]. Mathematical models for commonly used encryption algorithms, including AES, RSA and ECC, were established, alongside a hardware power consumption estimation model based on CMOS circuit power consumption theory. Building upon this foundation, the study considered the impact of temperature on leakage current and the effect of atmospheric pressure variations on circuit performance, thereby enabling an effective characterisation of extreme environmental factors. Experimental results indicate that within the temperature range of -40°C to 85°C, extreme low temperatures can significantly reduce the static power consumption of encryption algorithms but result in a decrease in carrier mobility, thereby increasing computation time by 15%–25%. At high temperatures, leakage current exhibits an exponential upward trend; the total energy consumption of the AES algorithm at 85°C increases by approximately 180% compared to normal conditions, whilst that of the ECC algorithm increases by only 120%, indicating its superior temperature robustness.

Changes in atmospheric pressure primarily affect power consumption by influencing the chip's heat dissipation efficiency. In a low-pressure environment of 0.1 atm, reduced heat dissipation causes the chip temperature to rise by 2–4 °C, resulting in an 8–12% increase in energy

consumption. A comparative study of various encryption algorithms under adverse conditions revealed that elliptic curve encryption algorithms offer the best energy consumption stability and environmental adaptability, with power consumption fluctuations nearly 40% lower than those of RSA. This provides valuable reference and guidance for selecting encryption algorithms for UAVs operating in harsh environments such as polar scientific research, high-altitude monitoring and deep-sea rescue, and is conducive to improving the energy efficiency and environmental adaptability of UAV communication systems [17].

5.2 Limitations and Outlook

Our research group has achieved certain results in the study of power consumption in UAV encryption algorithms under extreme conditions; however, there are still some shortcomings that require further improvement. The current research is primarily based on modelling and analysis using the MATLAB simulation platform and the Gem5+McPAT toolchain, which can effectively simulate the power consumption variations of CMOS circuits at different temperatures; however, it lacks experimental data from actual extreme environments. Although the formula in the simulation model for the effect of temperature on leakage current accounts for a wide temperature range from -40°C to 85°C, the model describing the impact of atmospheric pressure on circuit performance requires a more detailed description of the physical processes. Furthermore, the current work primarily focuses on power consumption comparisons of traditional encryption algorithms such as AES, RSA and ECC, with limited research in post-quantum cryptography, and is therefore unable to adequately address the challenges posed by future quantum computers.

Future work should focus on further research in the following areas. Firstly, a real-world extreme environment testing platform needs to be established, utilising drones to conduct tests in real-world environments such as the polar regions, high plateaus and the deep sea, in order to obtain actual test results regarding the power consumption of encryption algorithms, thereby validating and refining existing simulation models [18]. Secondly, the scope of research must be expanded to include post-quantum cryptographic algorithms, such as the lattice-based CRYSTALS-Kyber and CRYSTALS-Dilithium algorithms, to investigate their energy consumption stability and security under extreme conditions. Furthermore, the interrelationships between environmental factors must be investigated, and a model establishing the combined effects of multiple factors-such as temperature, atmospheric pressure and humidity-must be developed, so that UAVs can autonomously regulate their energy consumption in harsh environments. The ultimate objective is to design an intelligent selection and dynamic optimisation scheme for UAV encryption algorithms in extreme environments, maximising efficiency whilst ensuring security.

References

[1] Li Xiangning; Zhang Shuli; Hu Peng; Deng Chunhua. Comparative Analysis and Applications of Lightweight Cryptographic Algorithms [J]. Communications Technology, 2023(12):65-74.

[2] Chen Xuandi. Biclique Analysis of Several Typical Lightweight Cryptographic Algorithms [D]. Changsha University of Science and Technology, 2021.

[3] Fan Hongjuan; A Review of Research on RFID-Based Lightweight Cryptographic Algorithms [J]. Science & Technology Trends, 2020(27): 81–82.

[4] Zhang Wenzhe; Lai Yuyang; Chen Haiqian; Sun Hongdi; Kong Lei; Power Consumption Optimisation of LED Lightweight Cryptographic Algorithm Chips [J]. Electronic Design Engineering, 2020(05): 191–194+199.

[5] Xu Yixuan. Research on Authentication Technologies Based on Lightweight Cryptographic Algorithms [D]. Hefei University of Technology, 2023.

[6] Luo Hao; Su Sheng; Yang Hao; Lin Nan; Yuan Chen. Hardware Encryption Communication Method for FPGA-Based Power Line Inspection Drones [J]. China Electric Power, 2019(07):17-22.

[7] Xu Qiongfang. Analysis Methods for Lightweight Block Ciphers [J]. Henan Science and Technology, 2015(17):33-34.

[8] Guo Zhengze; Zhao Hongdong; Yao Yiyang; Chen Jiemeng; Feng Jiapeng. A Study on the Power Consumption of the AES Encryption Algorithm Based on FPGA [J]. Journal of Hebei University of Technology, 2015(01): 21–25.

[9] Wu Jiehong; Rou Yingying; Zou Liangkai; Li

Ya;. A Study on the Impact of Encryption Algorithm Optimisation on the CPU Power Consumption of UAVs [J]. Small and Micro Computer Systems, 2018(08): 144–150.

[10] Liao Bin; Zhang Tao; Yu Jiong; Yin Lutong; Guo Gang; Guo Binglei;. Energy Consumption Modelling and Optimisation Analysis of MapReduce [J]. Computer Research and Development, 2016(09):218–242.

[11] Guo Binglei; Yu Jiong; Liao Bin; Yang Dexian;. Research on SQL Energy Consumption Modelling and Optimisation [J]. Computer Science, 2015(10):208-213+237.

[12] Hu Renshen. A Simple Method for Parameter Design Analysis: Pareto Analysis [J]. Telecommunications Technology, 1995(03):44-49.

[13] Qiu Xingxing; Zhang Zhenzhen; Wei Qiming. Hybrid Decomposition and Strength Pareto Multi-Objective Evolutionary Algorithm [J]. Computer Applications, 2014(10): 125-130.

[14] Jian Dan; Li Yi; Yuan Qin; He Jing; Hai Lai Yi Wu. Analysis of Main Factors of Operating Costs Based on Pareto Analysis Method [J]. Chinese and Foreign Entrepreneurs, 2017(19): 104-115.

[15] Yang Li; Liu Jing. Three-Layer Network Architecture Simulation Experiment Design Based on Packet Tracer [J]. Journal of Ili Normal University (Natural Science Edition), 2017(04): 95-99.

[16] Wu Wei; Xu Jinghai. Exploration of Virtual Simulation Experiment Teaching in UAV Aerial Surveying and Mapping Process [J]. Modern Surveying and Mapping, 2021(05): 68-70.

[17] Shi Yongkang; Wan Xiaoyan; Yang Xiyang; Hu Hongyuan; Liu Tengzhi. Virtual Simulation Experiment Teaching for UAV Power Performance Testing [J]. Modern Vocational Education, 2022(44): 120-122.

[18] Tang Dengping; Zhang Wenzhe; Zhang Hongbin. Construction of IoT Simulation Experiment Platform Based on Packet Tracer [J]. IoT Technology, 2025(22): 145-148.

