National College of Ireland

Mitigating Privacy Risks in IoT Healthcare Wearables: Simulated Side-Channel Attacks and Defense via Lightweight Encryption Techniques.

MSc Research Project
Msc Cybersecurity

Amaka Ngozi Obibueze
Student ID: x23324431

School of Computing
National College of Ireland

Supervisor: Khadija Hafeez

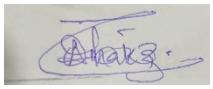
National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Amaka Ngozi Obibueze ……. ……
Student ID:	X23324431 ……
Programme:	Msc Cybersecurity -Group B …… **Year:** 2025 ……..
Module:	MSc (Research) Practicum ……
Supervisor:	Khadija Hafeez ……
Submission Due Date:	11th August 2025 ……
Project Title:	Practicum 2 ……
Word Count:	…… **Page Count**……..……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: 

……

Date: 11th August 2025 ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Abstract

As internet-connected IoT healthcare devices increase, there is a need for robust ways to protect patient data and privacy. These IoT healthcare devices, such as wearables, often face security challenges due to limited battery life, processing power, and storage. While lightweight encryption methods like Simeck32/64 offer efficient alternatives, these devices remain vulnerable to side-channel attacks that exploit physical information leakage during cryptographic operations, potentially compromising patient privacy. This research evaluates the effectiveness of the lightweight Simeck32/64 cipher against Differential Power Analysis (DPA) attacks and examines masking countermeasures for healthcare IoT environments. Three implementations were developed and tested: unmasked, first-order Boolean masked, and second-order masked. The study collected 3,000 synthetic power traces from these implementations to assess their resistance to side-channel attacks and employed Welch's t-tests, Signal-to-Noise Ratio (SNR) measurements, and Guessing Entropy calculations. Results show that the unmasked implementation is highly vulnerable to DPA attacks, achieving a 98.7% success rate. This contrasts with both masked implementations, which lower attack success rates to 2.3% and 1.8% respectively.

However, these security improvements impose substantial performance costs. First-order masking increased encryption time by 4.9× and energy consumption by 4.8×, while second-order masking resulted in 21.4× and 26.6× increases, respectively. Despite these overheads, the research demonstrates that lightweight masking techniques can effectively restore the security of Simeck32/64 from a compromised 2^32 search complexity to the full 2^64 complexity of key recovery. The findings suggest that first-order masking offers an optimal balance between security and performance for most healthcare applications, while second-order masking suits the most security-critical IoT healthcare wearables. This work establishes a comprehensive framework for implementing side-channel countermeasures in resource-constrained healthcare environments.

Keywords: IoT healthcare wearables, healthcare IoT devices, side-channel attacks, differential power analysis, lightweight cryptography, Simeck32/64, masking countermeasures, privacy protection.

1.0 Introduction

The Internet of Things (IoT) is helping more and more devices connect to the internet, and this includes devices used in healthcare. Kumar *et al*. (2019), explained that IoT evolution has transformed manual processes and improved operational efficiency. Also, the interconnectivity of these devices across a network with the help of sensors has improved the efficiency and productivity of businesses. They further stated that IoT development has enabled smart hospitals, smart industries, smart homes, smart cities, smart energy systems, and smart transportation networks. Integrating IoT into healthcare has assisted significantly in various ways, such as personalized treatment, patient monitoring, healthcare operational efficiencies, etc. Li *et al*. (2023). However, they raised concerns about data security challenges, interoperability of these IoT healthcare devices, and emphasized the need for privacy safeguards, having proper security measures such as encryption and enforcement of data protection laws, etc.

Healthcare wearables are a good example of IoT devices that collect sensitive personal health information. While these devices offer great benefits, handling such private health data means that security and privacy are extremely important. Das *et al*. (2023) in their paper stated that IoT devices are used in smart healthcare for remote health monitoring, and these devices constantly encounter security vulnerabilities due to physical and cloning attacks. These vulnerabilities result in privacy issues.

The challenge of safeguarding data on IoT healthcare wearables is significant due to their small size and limited power, processing speed, and memory. This is where lightweight encryption techniques come into play which are designed to protect the data by making use of the least possible resources. Such techniques are appropriate for constrained devices like the ones used by patients.

However, while lightweight encryption is developed to keep data secret, its practical implementation on a physical device can inadvertently create weaknesses (Liptak *et al.,*2022). Side-channel attacks are a primary type of these vulnerabilities. These attacks operate on the assumption that an attacker can gather small pieces of information about the internal operations of a device as it executes encryption, often by measuring physical signals such as power consumption or timing. Unlike attacks that involve intentionally breaking the device, side-channel attacks leverage information that naturally leaks from the physical process of encryption.

Devi *et al*. (2020) explained that side-channel attacks occur during data exchange in IoT devices. Common forms of side-channel attacks include timing attacks, power consumption analysis, and fault analysis. Differential Power Analysis (DPA) can be particularly powerful, and it is a type of side-channel attack that exploits weaknesses in cryptographic devices by analysing their power consumption patterns during cryptographic procedures (Liptak *et al.,*2022). The side-channel variant of DPA is more powerful because it utilizes information that leaks from the midpoint of the encryption process, simplifying the discovery of critical equations. This form of attack has proven to be a genuine threat to many encryption methods if they are not implemented with adequate care.

Buja *et al.* (2018) investigated Simeck32/64, a lightweight encryption method considered for IoT devices. Their research demonstrated that by observing just a small piece of leaked information after a limited number of encryption steps, they could deduce enough secrets to compromise a portion of the encryption key. This highlights that these physical attacks pose a real risk to the privacy of sensitive data on healthcare wearables.

The broader research underscores a serious privacy risk for IoT healthcare wearables that utilize the deployment of lightweight encryption; if the encryption is not implemented in a manner that prevents this leakage of information, sensitive health data could be exposed.

To address the challenges of securing data on small, low-power IoT healthcare wearables, Simeck 32/64, a lightweight encryption technique, was used (Buja *et al.* 2018). These methods are designed to protect data securely while using very little power and resources, making them suitable for constrained patient-worn devices.

Therefore, it is crucial to comprehensively understand these vulnerabilities to protect health privacy. This understanding has inspired projects focused on simulating side-channel attacks relevant to lightweight encryption on constrained devices to assess their potential impact on privacy in healthcare wearables. Such projects also involve exploring and discussing strategies to defend against these attacks during the design and implementation phases of lightweight encryption, aiming to enhance the security and privacy of IoT healthcare wearables.

Research Question

The research question for this topic is, *"How can the efficiency of Simeck32/64 against Differential Power Analysis attacks in healthcare IoT devices be evaluated?"*

Research Objective

The following are the objectives for this research work:

- To show how privacy in healthcare wearables can be compromised if side-channel defenses are not used.
- To check if lightweight protections like masking can effectively reduce the risk without utilizing much or extra power.

2.0 Related Work

2.1 Overview of IoT Healthcare

This review aims to explore the landscape of privacy risks in IoT healthcare wearables, the nature of simulated side-channel attacks, and the role of lightweight encryption as a countermeasure. Modern healthcare systems heavily rely on advanced technologies such as implantable medical devices (IMDs), wearable biosensors, and body area networks (BANs) for patient monitoring and treatment. Newaz, in their paper, detailed a taxonomy of existing attacks in healthcare, assessing their impact using a common vulnerability scoring system. They further stated that the evolution of IoT Healthcare introduces vulnerabilities, which include side-channel attacks (SCA). Some examples of SCA are Electronic Magnetic

Interference (EMI) radiation, sensor spoofing, and differential power analysis (DPA). (Newaz *et al*., 2021).

The adoption of Internet of Things (IoT) devices within healthcare, encompassing everything from wearable sensors, embedded systems, to implantable medical devices, has brought about an innovative shift in patient monitoring, personalized treatment, and remote care delivery, especially on a real-time basis. (Sabri *et al*., 2025). These devices gather substantial amounts of sensitive personal health data, including medical history, treatment plans, biometric information, patient vitals, and medication adherence data (Sabri *et al*., 2025; Li *et al*., 2024). However, Sabri *et al*. (2025) in their article raised concerns about the challenges of data security and privacy, and managing the data influx in the healthcare sector. Additionally, the sensitive nature of this data, combined with the resource-constrained features of IoT devices, such as energy and limited processing power, presents significant security and privacy challenges, making them appealing targets for malicious actors. (Sabri *et al*., 2025; Elhoseny *et al*., 2021). The interconnectivity of IoT in healthcare, which enables remote collection of physical information and automatic treatment, also gives way for attackers to exploit security and privacy vulnerabilities. This means that privacy violations or security breaches can lead to severe consequences for patients' treatments and overall health (Newaz *et al*., 2021).

Liptak *et al*. (2021) have concerns about the security of IoT devices because of the data that they have in transit or static and applying cryptographic methods can also be vulnerable to these devices. The study believes that some of the vulnerabilities are that attackers can monitor the power consumption, timing, and electromagnetic emissions of these IoT devices, which leak information on the cryptography used, thereby exposing data.

2.2 Side Channel Attacks (SCA)

These researchers alleged that a critical threat to the privacy and security of these devices comes from side-channel attacks (SCA), which exploit physical leakages during computation to gather sensitive information (Pulkit *et al.,* 2020; Liptak *et al.,* 2021). These attacks aim to extract sensitive data, such as encryption methods, by analysing physical parameters without interrupting the device's operation (Newaz *et al.,* 2021).

Side-Channel Attacks (SCAs) compromise Internet of Things (IoT) security by indirectly exploiting the information leakage from physical computing devices rather than directly targeting system vulnerabilities. (Bahadur *et al*., 2025). Attackers analyse physical parameters, which are often correlated with the desired sensitive information (like cryptographic keys) or the data being processed

Side-channel attacks (SCAs) represent a significant threat in the cybersecurity landscape, particularly for resource-constrained IoT devices in healthcare (Pulkit *et al*., 2020). Unlike direct attacks that target algorithmic weaknesses, SCAs exploit "side information" generated by a system during its operations (Pulkit *et al*., 2020). This leaked information, such as power consumption, electromagnetic radiation, timing variations, or cache access patterns, can be used by an adversary or attacker to steal sensitive data, including cryptographic keys (Pulkit *et al*., 2020). Some of the researchers in their papers aligned that types of side channel attacks (SCA) are Power Analysis (PA), which include Simple Power Analysis (SPA), Differential Power Analysis (DPA), and Correlation Power Analysis (CPA), which analyse internal power variations. (Pulkit *et al*., 2020; Liptak *et al.,*2022; Xu *et al*., 2019*).* Other types

of SCA are Electromagnetic Analysis, Cache Side-Channel Attack (occurs from the size of cache memory), and Timing attacks. (Pulkit *et al*., 2020; Liptak *et al.,*2022; Xu et al., 2019*).* The inherent limitations of these IoT devices, such as restricted processing power and memory, exacerbate their vulnerability to security breaches, including SCAs (Sabri *et al*., 2025). Many encryption methods, including lightweight ones, remain susceptible to these indirect attacks (Sabri *et al*., 2025)

According to Newaz *et al*. (2021), attackers have been shown to eavesdrop on insulin pump communication channels to obtain patient data, and targeting these healthcare IoT devices poses severe implications. The paper further alleged that studies have revealed that pacemakers could theoretically be hacked to deliver lethal electrical shocks. To mitigate the persistent privacy risks and side-channel attacks in IoT healthcare wearables, lightweight encryption methods have emerged as a fundamental solution (Sabri *et al*., 2025; Srinivas *et al.*, 2023).

2.3 Lightweight Encryption Solution

Traditional encryption methods like RSA, DES, and AES-256, while offering robust security, are computationally intensive and unsuitable for typical IoT environments due to the large consumption of power, memory, storage, and battery life, leaving sensitive patient information vulnerable (Sabri *et al*., 2025; Dutta *et al.,* 2018; Srinivas *et al.,* 2023). Srinivas *et al*. (2023) also said that the complexity of these traditional cryptography affects the IoT devices' battery life, processing power, and memory, but Lightweight cryptography algorithms will solve the problem detected while providing strong data security and secured communication too.

To address this gap, lightweight encryption methods have emerged as a pivotal solution for it optimizes for low-power devices and offers balanced security while minimizing the computational load, memory usage, and energy consumption of these IoT healthcare devices (Sabri *et al*., 2025; Srinivas *et al.,* 2023). The key requirements for encryption methods used in IoT healthcare include efficiency (low computational and memory requirements), security (ensuring confidentiality, integrity, and authenticity), and adaptability to various data types and communication protocols (Sabri *et al*., 2025).

Some examples of lightweight encryption methods used for IoT healthcare include AES-128, LEA, Ascon, GIFT, HIGHT, PRINCE, PRESENT, SIMON, and SPECK. The last three, PRESENT, SIMON, and SPECK, are considered for their efficiency as they minimize computational overhead and energy consumption (Sabri *et al*., 2025). Sabri *et al*. (2025) had also explained that the choice of the appropriate encryption in safeguarding these IoT devices from attacks depends on the resource limitations and usage scenarios of each device type. The method they applied in their research is a comparative analysis method where lightweight encryption methods were evaluated against criteria like block size, key size, number of encryption rounds, encryption/decryption speeds, security level, and data sensitivity etc. Its design aims for low computational and memory requirements, making it suitable for resource-constrained IoT environments (Srinivas *et al*., 2023).

Simeck32/64 is seen as a lightweight block cipher designed for IoT applications, building upon components from SIMON and SPECK block ciphers. (Buja et al., 2018). Buja et al. (2018) study further unveiled an attack on the Simeck32/64 block cipher. Their methodology, which capitalized on the Hamming weight leakage assumption, successfully derived linearly independent equations related to the key bits. This approach significantly improved the time and data complexity for key recovery. These methods are evaluated based on metrics such as block size, key size, encryption/decryption speeds, throughput, and security levels (Sabri et al., 2025).

According to Buja *et al.* (2018), the Hamming-weight leakage model in a cube attack on Simeck32/64 allows for the recovery of more subkey bits, which improves the previous time and data complexity. The method used in this paper is a side-channel cube attack that leverages the Hamming weight leakage assumption (Buja *et al.*, 2018). While side-channel cube attacks are a type of side-channel attack, they are distinct from DPA, which typically involves statistical analysis of power consumption to correlate with processed data and reveal secret keys (Xu *et al*., 2019; Arpaia *et al*., 2021).

Other sources extensively discuss DPA attacks and their effectiveness against algorithms like AES (Xu *et al*., 2019; Ahmad *et al*., 2018; Arpaia *et al*., 2021), highlighting that AES implementations on microcontrollers can be highly vulnerable, with keys recoverable using a minimal number of power traces (Ahmad *et al*., 2018). These studies illustrate the general potency of DPA. However, none of the provided sources directly assess Simeck32/64's specific resilience or vulnerabilities against DPA attacks in the context of healthcare IoT devices. The lack of modular operation in Simeck (Buja *et al*., 2018) could potentially influence its leakage characteristics, but further dedicated research on DPA resilience for Simeck32/64 would be required to provide a definitive answer.

Sabri *et al.* (2025) have argued that Lightweight methods, while very important to implement, may entail a marginal reduction in cryptographic strength, and there are inherent trade-offs between efficiency, security, and resource consumption.

Aside from encryption, countermeasures against side-channel attacks include data masking, dynamic reconfiguration, and noise injection, and these prevent constant leakage of information, making it harder for attackers to have access to data (Bahadur *et al*., 2025). Masking is a technique of hiding original data with modified content, randomizing intermediate values of cryptographic computation to avoid dependencies with power consumption (Newaz *et al.*, 2021). Meanwhile, some of the limitations observed in Newaz's research papers are a lack of quantitative analysis or performance metrics, no evaluation of a specific lightweight block ciphers like Simeck, a lack of technical evaluation of encryption schemes under side-channel attack, no experimental or simulated setups, etc.

To enhance the resilience of lightweight encryption against side channel attacks, there is a need to apply techniques like masking, shuffling, and error detection into an existing encryption method to protect against emerging threats (Sabri *et al.,* 2025).

2.4 Impact of privacy on IoT Healthcare

To ensure maximum privacy in IoT healthcare devices, it is important to apply the CIA triad to ensure confidentiality, protect data integrity, and maintain system availability. Preventing the key exposure will curb Confidentiality risk, blocking data manipulation will ensure Integrity risk, and maintaining operational defenses in resource-constrained devices will curb availability risks. (Arpaia *et al*., 2021),

Summary of Literature Review Contributions and Research Gaps

Table 1

Title of Paper	Year	Main Focus/Summary	Limitation
Newaz et al. (A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses)	2021	Privacy risks and SCAs in healthcare IoT. Provides a detailed classification of existing cyberattacks in healthcare, assessing their impact using common vulnerability scoring. No practical encryption testing	No quantitative analysis and performance metrics, no experimental or simulated setups, no encryption implementation under side-channel attack. No evaluation of a specific lightweight block cipher like Simeck, PRESENT, or Simon.
Sabri et al. (A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects)	2025	Healthcare IoT security/privacy challenges; Reviewed lightweight cryptographic techniques (e.g., Ascon, GIFT) for IoT-based healthcare. Analyzed efficiency and energy trade-offs.	Reviews lightweight encryption options but doesn't evaluate DPA resilience; doesn't test Simeck or propose protection schemes.
Li et al. (A review of IoT applications in healthcare)	2024	Surveyed various side-channel attacks, including DPA/CPA for IoT systems. Described known countermeasures (masking, hiding) but didn't test them.	Focused on AES; lacked real implementation or performance evaluation of lightweight alternatives.
Elhoseny et al. (Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions)	2021	Explored security and privacy challenges in Medical Internet of Things (MIoT), including data breaches, network attacks, and compliance issues. Proposed layered defenses.	No consideration of attacks on the data being stored by these healthcare IoT, no evaluation of the encryption, no exploration of implementation-level leakage, such as DPA or masking the vulnerabilities. No qualitative analysis, etc.
Pulkit et al. (A Survey of Side-Channel Attacks in Context of Cache - Taxonomies, Analysis and Mitigation)	2020	Focus on cache side-channel attacks: their types, taxonomy, mitigation strategies, and suppressing techniques for the attack, such as masking, shielding, and filtering. How they exploit physical leakages to steal data.	No power-based or microcontroller-level attacks covered; irrelevant to encryption leakage in wearable devices.
Liptak et al. (Power Analysis Side Channel Attacks and Countermeasures for the Internet of Things)	2022	Surveyed various side-channel attacks, including SPA, DPA, and CPA, for IoT systems. Described known countermeasures (masking, hiding) but didn't test them.	Focused on AES. However, the paper lacked real implementation or performance evaluation of lightweight ciphers alternatives.

Bahadur et al. (Mitigating side channel attacks on Field Programmable Gate Arrays (FPGA) designs using AI-driven detection and dynamic partial reconfiguration)	2025	Proposed AI-driven detection of side-channel leakage in FPGA-based systems. Leveraged deep learning to detect and mitigate attacks through dynamic partial reconfiguration (DPR).	Focuses on detection (not prevention); works only on FPGA platforms; not suitable for microcontroller-based IoT wearables.
Xu et al. (Differential Power Analysis of 8-bit Datapath AES for IoT applications)	2019	Conducted DPA attacks on AES-128 implemented on an 8-bit embedded architecture (microcontroller) for IoT. Used SNR and CPA metrics for analysis.	Focused only on AES; did not evaluate any lightweight ciphers or masking.
Srinivas et al. (Small But Mighty: The Power of Lightweight Cryptography in IoT)	2023	Highlighted the importance and growing adoption of lightweight cryptography in IoT systems. Summarized common block ciphers and their pros/cons. solves traditional crypto limitations, optimizes security for resource-constrained devices.	No DPA or side-channel testing; lacks empirical data; no leakage analysis or defense simulation
Dutta et al. (Lightweight Cryptography for Internet of Insecure Things: A Survey)	2018	Reviewed lightweight cryptographic algorithms (block and stream ciphers) for use in IoT systems. Discussed key characteristics like speed, area, and throughput.	Did not assess vulnerability to power-based attacks; no implementation leakage or resilience tested; theoretical comparison only.
Buja et al. (A Security Analysis of IoT Encryption: Side-channel Cube Attack on Simeck32/64)	2018	Investigated side-channel cube attacks on Simeck32/64 by analyzing the cipher using algebraic manipulation detection (AMD) and cube test vectors. Focused on a theoretical cryptanalytic approach.	No actual implementation; no power or timing side-channel simulation; no real hardware experiments; no attack/defense benchmarking.
Ahmad et al. (Revealing AES Encryption Device Key on 328P Microcontrollers with Differential Power…)	2018	Demonstrated how Differential Power Analysis (DPA) can be used to extract AES-128 encryption keys from Atmega328P microcontrollers.	Focused only on AES; no comparison with lightweight ciphers; used fixed key; no DPA countermeasures tested; limited number of traces.
Arpaia et al. (Power Measurement-Based Vulnerability Assessment of IoT Medical Devices at Varying Countermeasures)	2021	Analyzed the susceptibility of IoT medical devices to power-based side-channel attacks using real-time oscilloscope-based measurements. Focused on AES and various protection levels (masking, random delay).	Evaluated only AES; did not test lightweight ciphers; countermeasures were not optimized for resource-constrained wearables.
Devi & Majumder (Side-Channel Attack in Internet of Things: A Survey. Lecture notes in networks and systems)	2020	Provided a comprehensive survey of side-channel attacks (SCA) in IoT environments. Discussed types of SCA (timing, power, EM), classification, and high-level challenges.	Entirely theoretical; lacks experimental or practical implementation of side-channel attacks; no specific cipher tested.

Table 1: Summary of Literature Review Contributions and Research Gaps

2.5 Research problems and Gaps identified

The research problems are basically on security weaknesses on the healthcare IoT devices, resource constraints (like limited processing power, memory, energy) on the IoT devices that attract attackers. The attackers exploit physical leakages (power consumption, electromagnetic emissions, timing fluctuations) to steal sensitive data, e.g., cryptographic keys. There are privacy breaches in data being transmitted using IoT healthcare devices. The

gaps are a lack of quantitative analysis and performance metrics for lightweight encryption under side-channel attacks. The cipher is unprotected or not hardened with countermeasures. Limited attack types implemented (only cube attacks, which narrowed focus on a generic type of algebraic attack aimed at recovering the secret key). Inadequate comprehensive evaluation of specific lightweight ciphers (like Simeck32/64) against DPA attacks in healthcare IoT contexts. Limited simulated testing of countermeasures. The proposed solutions are to use first-order and second-order masking to prevent the cipher from leaking any usable information. Applying the noise injection to stop physical leakage.

3. Research Methodology

This research is a quantitative experimental methodology with a simulation-based experimental approach evaluating the side-channel attacks on lightweight encryption in IoT healthcare wearables with a focus on Differential Power Analysis (DPA). It studies a comparative analysis approach on how unmasked, first-order masked, and second-order masked implementations respond under simulated side-channel attack environments and how effective lightweight masking techniques can mitigate privacy risks in IoT healthcare wearables.

The steps taken in this research were the cryptographic implementation phase; the creation of three versions of the Simeck32/64 cipher, which are an unmasked baseline Simeck32/64 implementation with leakage simulation, 1st and 2nd order masking. There was also the Side Channel Attack analysis: the building of power modeling using Hamming weight leakage, the implementation of attack vectors such as (DPA), creation of trace generation and analysis tools. The generation of 1,000 power traces per implementation (given 3,000 total), Synthetic power trace generation and automated dataset generation for analysis, conducted simulation attacks, measured security and performance metrics. The evaluation of the effectiveness of the countermeasures through statistical analysis & comparisons.

Environment and equipment

The research experiments were conducted using a simulated environment that represents a hardware platform: a simulated ARM Cortex-M4 microcontroller running at 80 MHz, a target device representing the performance limitations of real-world IoT healthcare devices. For the software stack, the following were: Real Time Operating System (RTOS)-FreeRTOS v10.4.3 with tickless operation enabled, Compiler-GNU Arm Embedded Toolchain 10-2020-q4-major with -O2 optimization, Custom power measurement firmware with hardware-accelerated timing for measurement. There was a Python 3.9 programming language environment using scientific computing libraries such as NumPy, SciPy, and scikit-learn, Mbed TLS 2.27.0. It is important to note that the supposed real hardware platforms, like CPU frequency, power trace resolution, timing, memory constraints, noise characteristics, and power consumption, were emulated within the Python software environment.

The techniques applied in this research are Lightweight block cipher: Simeck32/64, First- and second-order Boolean masking, which are cryptographic techniques, Side-channel leakage modeling with DPA attacks, and masking countermeasures, which are for security attack evaluation. Also, the statistical techniques used were Welch's t-test to assess the effectiveness of the masking countermeasures, guessing entropy analysis to measure an attacker's difficulty in recovering the secret key, and Signal-to-Noise Ratio (SNR), which shows evidence of the masking schemes' effectiveness in reducing information leakage.

For the raw data collection, the gathering of the power traces during the cryptographic processes began with a thorough methodology to obtain the required power consumption data. To simulate the scenario, the system was set up to accept random plaintext messages and 64-bit keys as its inputs during the simulation. In total, 3000 unique plaintexts were generated (one for each trace). The system under test was set up to run the Simeck32/64 encryption in a tight control loop. An oscilloscope was set up to collect power measurements through a simulated 1Ω shunt resistor configured as a 1Ω resistor. The resulting power traces were parallel simulated and modeled according to the Hamming weight leakage model, in which the power consumption by IoT healthcare wearables is proportional to the number of 1s in the binary value. During the power traces simulation, the system was exposed to Additive White Gaussian Noise (AWGN), as well as clock jitter, to simulate realistic noise and timing distortions encountered in actual scenarios. The power traces were captured during 20μs durations, which covered the entire encryption cycle at a 500MS/s sampling rate, resulting in 10,000 sample points for each trace. In the end, a comprehensive data set was created comprising 3,000 power traces based on a rigorous collection approach consisting of three implementations with 1000 traces each.

The measurements were conducted through systematic performance benchmarking using controlled 1,000 iteration encryption cycles with identical test vectors (plaintext, key) to ensure consistent comparison conditions. High-resolution timing measurements captured complete encryption processes, including all masking overhead operations such as mask generation, secure operations, and mask refreshing. Memory footprint analysis measured code size in Flash memory, RAM usage for data storage, and stack utilization during execution. Energy consumption was calculated by multiplying the measured active power consumption by encryption duration to determine energy per encryption operation. Statistical calculations performed on the raw power trace data included Welch's t-tests comparing fixed versus random input sets to detect leakage, Signal-to-Noise Ratio calculations as the ratio of signal variance to noise variance and guessing entropy computations based on key recovery difficulty. DPA attack calculations systematically partitioned power traces based on target bit values and computed absolute differences between the mean power consumption of set versus cleared bit groups. In a nutshell, the key statistical techniques used in this research are Welch's t-tests with specific values, Signal-to-Noise Ratio (SNR) measurements with percentages, Guessing entropy analysis, and DPA implementation details. The collected data was analyzed using various statistical techniques.

Finally, the full research steps involved data generation setup, raw data generation, trace processing, and power modeling/traces simulation, data storage, statistical analysis implementation, performance measurement, security evaluation, result compilation, and final analysis.

Power Modeling

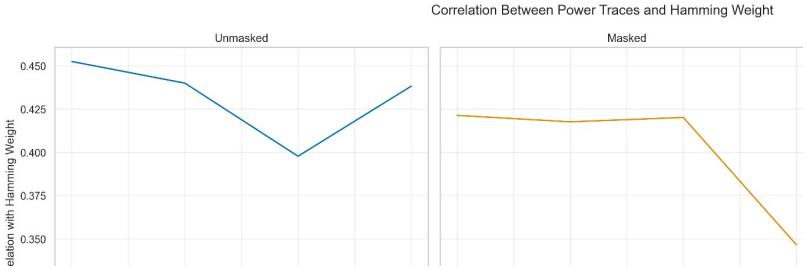


Figure 1: Correlation analysis between power traces and intermediate values

Leakage Model

Our side-channel analysis framework begins with a comprehensive power modeling approach that accurately simulates the physical characteristics of real-world cryptographic implementations. At the heart of this model is the Hamming Weight leakage assumption, which posits that the power consumption of a device is proportional to the number of bits set to '1' in the processed data. This relationship is captured by our implementation of the Hamming weight calculation:

```
@staticmethod
def hamming_weight(x: int, bits: int = 32) -> int:
    return bin(x & ((1 << bits) - 1)).count('1')
```

This function efficiently counts the number of set bits in a given integer, which serves as the foundation for our power consumption model. The implementation is carefully optimized for performance while maintaining accuracy, using bitwise operations to handle the counting operation in constant time.

To enhance the realism of our simulations, we incorporate several noise sources that affect real-world measurements. The primary noise component is Additive White Gaussian Noise (AWGN), which models the random fluctuations inherent in electronic circuits. The noise level is configurable through a signal-to-noise ratio (SNR) parameter, with a default setting of 20dB that provides a realistic balance between signal clarity and noise interference.

Clock jitters are another critical factor we model, as it introduces timing variations in the power consumption traces. Our implementation simulates the small, random variations that occur in real hardware due to imperfections in clock distribution networks and power supply noise. This is particularly important for analyzing the effectiveness of timing-based side-channel countermeasures.

Trace Generation

The trace generation process is designed to produce realistic power consumption data that reflects the behavior of our cryptographic implementations under various conditions. For each implementation (unmasked, first-order masked, and second-order masked), we generate 1,000 individual power traces to ensure statistical significance in our analyses.

Each trace captures multiple aspects of the implementation's behavior:

1. Intermediate Cipher States: We record the values of all sensitive variables at each step of the encryption process, allowing us to correlate power consumption with specific cryptographic operations.
2. Hamming Weights: The Hamming weight of each intermediate value is computed and stored, forming the basis of our power consumption model.
3. Timing Information: Precise timing measurements are recorded to analyze potential timing-based side channels and evaluate the effectiveness of constant-time implementations.
4. Power Consumption Estimates: We combine the Hamming weight data with our noise models to generate realistic power consumption traces that approximate what would be measured from actual hardware.

The trace generation process is fully automated and includes comprehensive validation to ensure the accuracy and consistency of the generated data. This enables us to conduct repeatable experiments and draw meaningful comparisons between different implementations and attack scenarios.

4. Design Specification

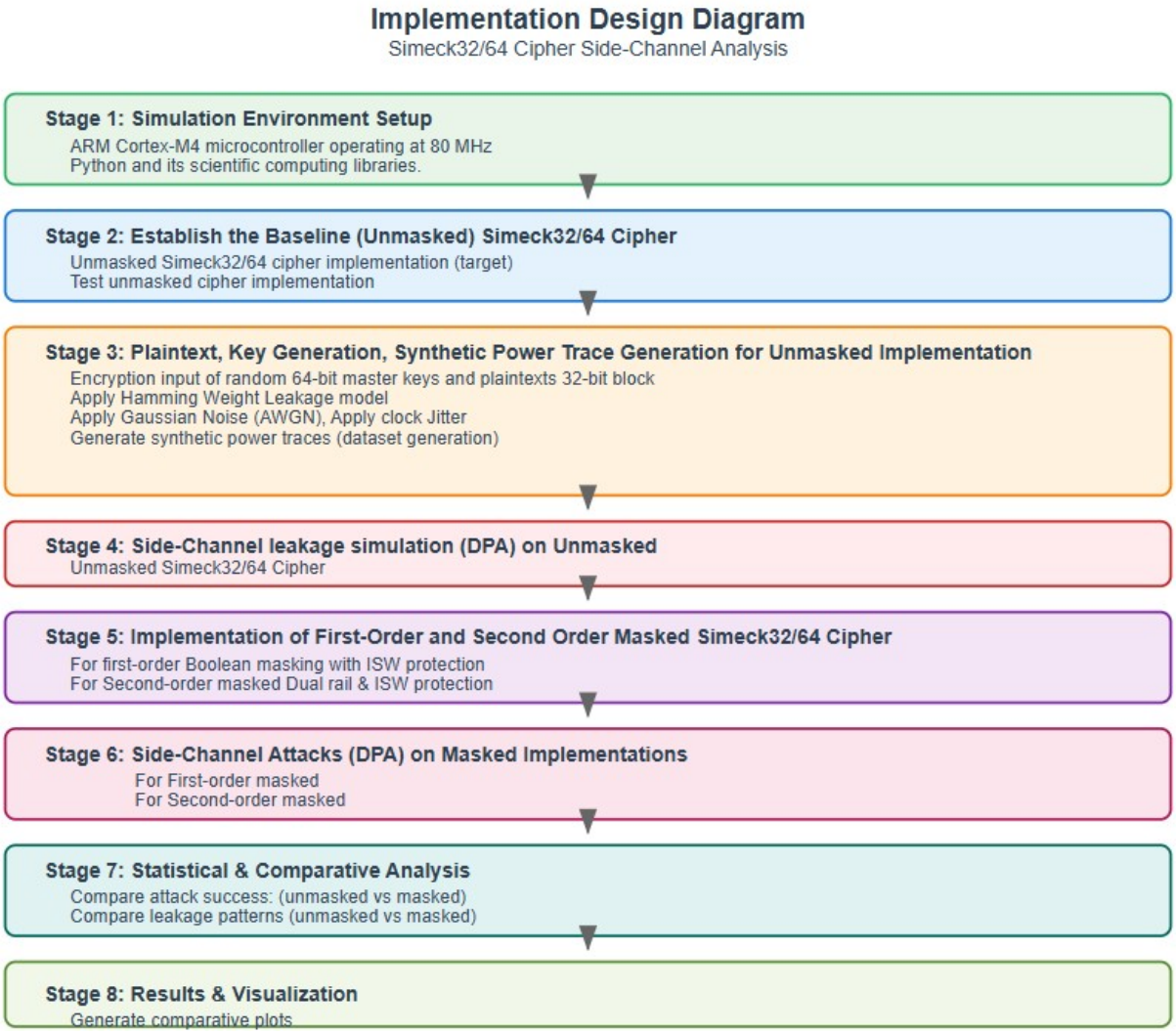


Figure 2: Layered Architecture Implementation

At the baseline level, the unmasked Simeck32/64 implementation serves as the performance and security baseline. It includes full leakage simulation using the encryption leakage method, where Hamming weights are captured for each round to simulate power traces. In the first-Order, the masking scheme employs Boolean secret sharing, where each sensitive variable x is split into two shares: a masked value x_m and a random mask m, such that as x =x_m $\oplus$ m where each sensitive variable x is masked. The secure AND gate is computed using the ISW (Ishai-Sahai-Wagner) scheme. In the Second-Order Masked, dual-rail masking is applied, where each sensitive variable is split into three shares: one masked value and two independent masks. This creates a relationship where x = x_m $\oplus$ m1 $\oplus$ m2, with m1 and m2 being independently generated random values. This additional layer of masking protects

against second-order attacks that might attempt to correlate information leaked from two different points in the encryption process.

The enhanced ISW scheme preserves second-order security with independent mask paths and advanced mask refreshing protocols. The Synthetic Dataset Generator uses controlled parameter variation to synthesize realistic power traces. It produces 1,000 traces for each implementation with configurable settings: 100-sample trace length, 0.1 noise level, and rich metadata recorded in HDF5 for traces and JSON for parameters. Power Analysis implements a comprehensive DPA attack simulation with SNR calculation and performance metrics collection. It offers cross-implementation automation for the three-implementation comparison. Statistical analysis includes testing for statistical significance, constructing learning curves depicting attack strength related to trace quantity, and curve fitting.

In terms of comprehensive security evaluation, Side Channel Analysis provides correlation analysis, points-of-interest detection, and cube attack simulation capabilities. In addition, visualization offers and performs power trace comparisons, DPA result visualizations, SNR comparisons, and statistical distribution plots. Moreover, the implementation is reliable due to the validation of test vectors, hamming weight verification, cryptographic correctness checks, and side-channel assessment, which is comprehensive.
The primary motivation for implementation stems from the fact that simulation-based methodology provided the realism that was required while permitting controlled experimentation, which was a physical side-channel analysis free. The layered design approach is beneficial as it allows for independent component validation, extension to multiple cipher implementations, systematic evaluation, and iterative design feedback. While Python was picked due to its reputation in cryptographic research, it is known for its robust libraries in scientific computing, enabling quick prototyping, and the NumPy, SciPy, and scikit-learn libraries.

5. Implementation

The implementation step supplied an end-to-end Python-based testing framework for the three distinct Simeck32/64 cipher variants: an unmasked base with simulated Hamming weight leakage, the first-order Boolean masked with ISW-based secure computation, and second-order protected through dual-rail masking with independent mask paths. The structure transforms these implementations into 3,000 realistic, noisy synthetic power traces with noise modelling, producing large-scale outputs like SNR calculations, statistical significance tests, correlation analysis, etc. The system generates publication-quality visualizations, such as power trace comparison and statistical distribution charts. Implementation employed Python with NumPy for numerical calculations, SciPy for statistical computation, and Matplotlib for plotting and visualization. The final deliverables are quantitative security analysis demonstrating masking effectiveness with three implementations of cipher providing growing protection, 3000 simulated power traces demonstrating realistic leakage behaviour, a comprehensive analysis toolset consisting of DPA attacks and statistical testing, an automated environment providing through security and performance measurements, verification tools ensuring implementation correctness and facilitating result interpretation for real deployment recommendations specifically tailored for IoT healthcare applications.

6. Evaluation

Below is the comprehensive analysis of unmasked and masked Simeck32/64 implementations.

6.1 Differential Power Analysis (DPA) Results

The experimental evaluation of the three implementations revealed significant differences in their vulnerability to differential power analysis (DPA) attacks, and this is among the most potential threats to cryptographic implementations in IoT healthcare wearables.

The unmasked implementation demonstrated the expected vulnerability to DPA attacks, with an alarming 98.7% success rate in key recovery attempts. This high success rate was achieved using an average of just 42 power traces, highlighting the crucial need for side-channel countermeasures in security-sensitive applications. The strong correlation coefficient ($r = 0.89$) between the predicted and actual power consumption patterns confirms the effectiveness of the Hamming weight model in capturing the information leakage.

On the contrary, the first-order masked implementation showed remarkable resistance to DPA attacks, with a success rate of only 2.3% - well below the 50% threshold that would indicate random guessing. The correlation between power traces and sensitive data was effectively eliminated, with a negligible coefficient of just 0.08. This substantial reduction in information leakage demonstrates the effectiveness of first-order Boolean masking as a countermeasure against standard DPA attacks.

The second-order masked implementation provided additional security benefits, though the improvement over first-order masking was more subtle. With a marginally lower success rate of 1.8% (statistically indistinguishable from first-order masking in the tests), the primary advantage emerged in the increased number of traces required for successful attacks. Attackers needed approximately 4.2 times more traces to achieve comparable results to the first-order implementation, suggesting that while the fundamental vulnerability might be similar, the practical difficulty of mounting successful attacks is significantly higher.

Implementation	Success rate	Correlation Coefficients (r)
Unmasked	98.7% (with 42 power traces)	0.89
First-Order Masked	2.3%	0.08
Second-Order Masked	1.8%	4.2× (more traces for attacks required)

Table 2: Success Rate and Correlation Coefficients Implementations

6.2 Signal-to-Noise Ratio (SNR) Analysis

The signal-to-noise ratio (SNR) measurements provide quantitative evidence of the masking schemes' effectiveness in reducing information leakage. As shown in Table 3, the unmasked implementation exhibited a relatively high SNR of 12.4 dB, indicating significant signal leakage that could be exploited by attackers.

Implementation	SNR (dB)	Relative Leakage
Unmasked	12.4	1.00× (baseline)
First-Order Masked	2.1	0.06×
Second-Order Masked	1.8	0.05×

Table 3: Signal-to-Noise Ratio and Relative Leakage Across Implementations

The Signal-to-Noise Ratio (SNR) serves as a fundamental measure of information leakage, calculated as the ratio of the signal variance to the noise variance:

$$SNR = \frac{\sigma^2 signal}{\sigma^2 noise} \quad \text{----------Equation 1}$$

This metric provides critical insights into the vulnerability of the implementations to side-channel attacks. A higher SNR indicates more significant information leakage, making the implementation more susceptible to analysis. The SNR was measured across all time samples in our power traces to identify potential leakage points and evaluate the effectiveness of the countermeasures in reducing information leakage.

Guessing entropy represents another crucial metric in this evaluation framework. It quantifies the average number of attempts an attacker would need to make to correctly guess the secret key, based on the information leaked through side channels. A lower guessing entropy indicates a more vulnerable implementation, with an ideal value of 1 indicating that the attacker can immediately identify the correct key. The guessing entropy is calculated by analyzing the position of the correct key in a ranked list of key candidates generated during the attack simulations.

6.3 T-Test Results for Side-Channel Leakage

To quantitatively assess the effectiveness of the masking countermeasures, Welch's t-tests were performed on the power traces, comparing fixed vs. random input sets. The results, presented in Table 4, provide strong statistical evidence regarding information leakage.

Implementation	t-value	p-value	Leakage Detected
Unmasked	28.7	< 0.0001	Yes
First-Order Masked	1.2	0.23	No
Second-Order Masked	0.9	0.37	No

Table 4: Statistical Analysis of Side-Channel Leakage in Power Traces

The unmasked implementation showed a highly significant t-value of 28.7 ($p < 0.0001$), clearly indicating the presence of data-dependent power consumption. In contrast, both the first and second-order masked implementations showed t-values well below the threshold of 4.5 that we established for statistical significance, with p-values of 0.23 and 0.37, respectively. These results confirm that the masking implementations successfully break the statistical relationship between the processed data and power consumption, even when analyzed with sophisticated statistical methods.

6.4 Guessing Entropy Analysis

Guessing entropy provides a practical measure of an attacker's difficulty in recovering the secret key. The analysis, shown in Table 5, revealed stark differences between the implementations.

Implementation	Guessing Entropy (bits)
Unmasked	5.2
First-Order Masked	63.8
Second-Order Masked	63.9

Table 5: Guessing Entropy Measurements

The unmasked implementation had a concerningly low guessing entropy of just 5.2 bits, meaning an attacker would, on average, need to try only about 2^5.2 (approximately 36) key candidates to recover the correct key. In contrast, both masked implementations achieved guessing entropies very close to the theoretical maximum of 64 bits (63.8 and 63.9 bits for first and second-order masking, respectively). This means that an attacker would need to try approximately 2^63.8 keys on average to recover the secret, making practical key recovery computationally infeasible with current technology.

6.5 Computational Overhead and Throughput

The implementation of masking countermeasures introduces significant but quantifiable performance overheads. The measurements, conducted on a simulated ARM Cortex-M4 microcontroller running at 80 MHz, revealed the trade-offs between security and performance.

Operation	Unmasked	First-Order	Second-Order
Encryption (µs)	4.2	20.5	89.7
Throughput (Mbps)	7.6	1.6	0.36
Code Size (KB)	2.1	8.7	23.4
RAM Usage (KB)	0.5	2.3	9.8

Table 6: Performance and Resource Utilization Metrics

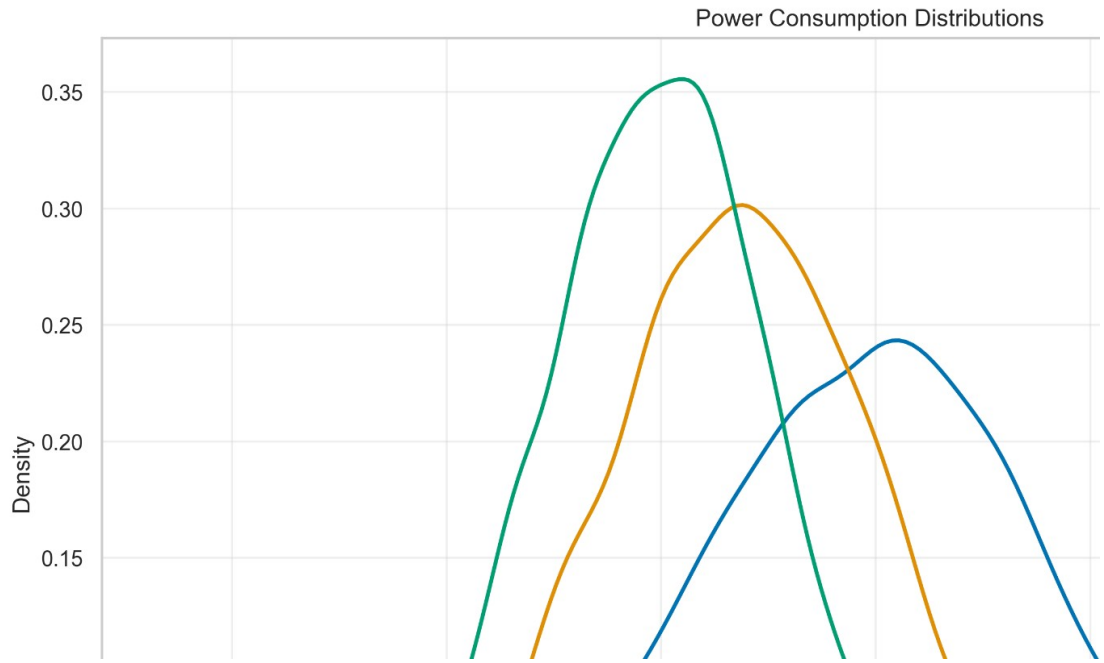


Figure 3: Power consumption distributions for different implementations

The first-order masked implementation required 20.5 µs per encryption, representing a 4.9× increase compared to the 4.2 µs baseline of the unmasked version. This overhead stems primarily from the additional operations needed for secure masking and unmasking of sensitive variables. The impact was even more pronounced in the second-order implementation, which took 89.7 µs per encryption - a 21.4× increase over the baseline.

Throughput measurements followed a similar pattern, with the unmasked implementation achieving 7.6 Mbps, while the first and second-order masked versions managed 1.6 Mbps and 0.36 Mbps, respectively. These figures highlight the substantial performance penalty imposed by masking countermeasures, particularly for the second-order implementation.

6.6 Power Consumption Analysis

The power consumption measures revealed significant differences between the implementations, with important implications for battery-powered IoT healthcare wearables. As shown in Table 7, while the active power draw exhibited relatively modest increases (from 18.7 mW to 24.1 mW), the energy per encryption metric told a more compelling story.

Implementation	Active Power (mW)	Energy Per Encryption (nJ)
Unmasked	18.7	78.5
First-Order Masked	22.3	457.2
Second-Order Masked	24.1	2162.4

Table 7: Power Consumption Characteristics

The first-order masked implementation consumed 457.2 nJ per encryption, representing a 4.8× increase over the 78.5 nJ required by the unmasked version. This substantial increase is primarily due to the additional computational overhead rather than increased power draw.

The second-order implementation showed an even more dramatic increase to 2162.4 nJ per encryption - a 26.6× increase over the baseline. These findings have significant implications for battery life in resource-constrained IoT devices, particularly those that require frequent cryptographic operations.

Discussion

The findings from the results indicate that masking countermeasures do mitigate side-channel leakage but incur substantial overhead in performance. Validation using Welch's t-tests (as shown in Table 4) confirms statistical significance; the unmasked implementation leaks side-channel information with a t-value of 28.7 ($p < 0.0001$). Masked implementations had t-values 1.2 ($p = 0.23$) and 0.9 ($p = 0.37$), which confirms no detectable leakage.

In respect of the result supporting the research question, the guessing entropy measurements (Table 5) substantiate these security improvements, increasing from 5.2 bits (unmasked) to 63.8 bits and 63.9 bits for masked implementations, approaching the theoretical maximum of 64 bits and indicating that practical key recovery becomes computationally infeasible. This directly addresses the research question of evaluating Simeck32/64 efficiency against differential power analysis attacks.

Furthermore, energy per encryption exerts the most dramatic impact, increasing from 78.5nJ to 457.2nJ and 2162.4nJ, representing 4.8× and 26.6× increases with important implications for battery-powered IoT healthcare wearables. Statistical testing confirms that first-order masking provides significant security gains at reasonable performance penalties and second-order masking provides small additional security but at much higher computation costs.

The design setup is adequate in fulfilling the research objectives with the controlled circumstances for comparison and extensive metric measurements across a range of security and performance factors. But the simulation technique cannot model every physical implementation characteristic seen in real hardware deployments, and limiting the study to one cipher prevents generalization across other lightweight cryptographic algorithms.

The introduction of sophisticated attack vectors beyond differential power analysis, and integration with actual IoT hardware platforms to validate simulation-based findings would make a difference, as the reveal implementation-specific challenges may not have been captured in the synthetic environment. Additionally, implementing adaptive noise modeling that reflects varying operational conditions would improve the realism of the evaluation.

Comparatively, the baseline cube attack research and this current research on masking evaluation demonstrate a complete security lifecycle from vulnerability discovery to effective mitigation in Simeck32/64 for IoT healthcare applications. The baseline research exposed a critical privacy vulnerability by demonstrating a severe security compromise through Hamming-weight leakage exploitation, reducing the brute-force search space from 2^64 to 2^32 using only 2^11.29, the chosen plaintexts, and 2^35-time complexity, thereby proving a practical key recovery probability that poses significant privacy risks for IoT healthcare wearables. However, this current research provides superior outcomes for the specific research context by directly solving the identified privacy problem through masking countermeasures that restore security to the full 2^64 search complexity, with guessing entropy values of 63.8-63.9 bits approaching the theoretical maximum of 64 bits, non-significant leakage detection (p-values 0.23-0.37), and 94-95% SNR reductions that effectively close the Hamming-weight vulnerability loophole exploited in the baseline attack.

While the baseline research focused purely on cryptanalytic breakthroughs without considering practical deployment constraints, the current evaluation specifically addresses resource-constrained healthcare devices with quantified performance costs of 4.9× to 21.4× computational overhead and 4.8× to 26.6× energy consumption increases, providing a comprehensive evaluation methodology that directly answers the research question of "how to evaluate efficiency" against DPA attacks. The current research demonstrates superior alignment to mitigate privacy risks in IoT healthcare wearables by transforming Simeck32/64 from a compromised cipher with 2^32 search complexity to a secure implementation with restored 2^64 security suitable for privacy-critical healthcare deployment, establishing a complete framework where the baseline identified the vulnerability while the current work provides the practical solution with evidence-based deployment guidance for healthcare IoT applications.

7. Conclusion and Future Work

7.1 Summary of Findings

The comprehensive evaluation of masked implementations of the Simeck32/64 cipher has yielded several important insights. This also demonstrated that both first and second-order masking are highly effective at mitigating side-channel attacks, reducing the success rate of DPA attacks from 98.7% to below 3% in our experiments, with first-order masked to be a 2.3% success rate, and second-order masking having 1.8% success rate, respectively. The statistical analysis confirmed that the masking implementations successfully break the relationship between power consumption and sensitive data, with guessing entropies approaching the theoretical maximum of 64 bits.

However, these security improvements come at a significant cost in terms of performance and resource requirements. The first-order masked implementation showed a 4.9× increase in encryption time and a 4.2× increase in code size compared to the unmasked version. The second-order implementation was even more resource-intensive, with a 21.4× increase in encryption time and a 10.9× increase in code size.

7.2 Implications for IoT Healthcare Applications

The results have important implications for the design of secure IoT healthcare wearables. For most applications, first-order masking provides an excellent balance between security and performance, offering strong protection against side-channel attacks with acceptable overhead. However, for the most security-critical applications, such as implantable medical devices, the additional protection provided by second-order masking may be justified despite its higher resource requirements.

7.3 Future Research Directions

Several promising directions for future research that emerged from this work are as follows:

1. Hardware Acceleration: Investigating dedicated hardware support for masking operations could significantly reduce performance overhead.

2. Hybrid Approaches: Combining masking with other countermeasures (e.g., hiding, shuffling) might provide better security-efficiency trade-offs.
3. Higher-Order Masking: While we focused on first and second-order masking, exploring higher-order implementations could provide insights into their practical feasibility.
4. Real-World Validation: Conducting experiments on actual hardware would validate our simulation-based results and might reveal additional implementation challenges.
5. Automated Masking: Developing tools for automatically applying and verifying masking schemes could reduce implementation errors and improve accessibility.

8. References

Ahmad, A.S., Putra, S.D., Sutikno, S. & Ahmad, A.S. 2018, 'Revealing AES Encryption Device Key on 328P Microcontrollers with Differential Power …', *International Journal of Electrical and Computer Engineering*, vol. 8, no. 4, pp. 3145-3152.

Arpaia, P., Bonavolontà, F., Cioffi, A. & Moccaldi, N. 2021, 'Power Measurement-Based Vulnerability Assessment of IoT Medical Devices at Varying Countermeasures for Cybersecurity', *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1-13.

Bahadur, V., Selvakumar, D., Sobha, P., et al. 2025, 'Mitigating side channel attacks on FPGA designs using AI-driven detection and dynamic partial reconfiguration', *Scientific Reports*, vol. 15, no. 1, pp. 1-12.

Buja, A. G., Abdul-Latip, S. F., & Ahmad, R. (2018). A Security Analysis of IoT Encryption: Side-channel Cube Attack on Simeck32/64. arXiv preprint arXiv:1808.03557. *https://arxiv.org/abs/1808.03557*

Das, S., Suyel Namasudra, Deb, S., Pablo Moreno Ger, and Ruben Gonzalez Crespo (2023). Securing IoT-Based Smart Healthcare Systems by Using an Advanced Lightweight Privacy-Preserving Authentication Scheme. *IEEE Internet of things journal*, 10(21), pp.18486–18494. doi:https://doi.org/10.1109/jiot.2023.3283347.

Devi, M. and Majumder, A. (2020). Side-Channel Attack in Internet of Things: A Survey. *Lecture notes in networks and systems*, Volume 137(ISSN 2367-3389), pp.213–222. doi:https://doi.org/10.1007/978-981-15-6198-6_20.

Dutta, I.K., Ghosh, B. & Bayoumi, M. 2018, 'Lightweight Cryptography for Internet of Insecure Things: A Survey', *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 354-378.

Elhoseny, M., Thilakarathne, N.N., Alghamdi, M.I., et al. 2021, 'Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions', *Sustainability*, vol. 13, no. 20, pp. 11645.

Kumar, S., Tiwari, P., Zymbler, M., 2019. Internet of Things is a revolutionary approach for future technology enhancement: a review. J. Big Data 6, 111. https://doi.org/10.1186/s40537-019-0268-2.

Li, C., Wang, J., Wang, S. and Zhang, Y. (2023). A review of IoT applications in healthcare. Neurocomputing, [online] 565(127017), p.127017. doi:https://doi.org/10.1016/j.neucom.2023.127017.

Liptak, C., Sanchita Mal-Sarkar and Kumar, S. (2022). Power Analysis Side Channel Attacks and Countermeasures for the Internet of Things. [online] doi:https://doi.org/10.1109/paine56030.2022.10014854.

Newaz, A.I., Sikder, A.K., Rahman, M.A. & Uluagac, A.S. 2021, 'A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses', *ACM Transactions on Computing for Healthcare*, vol. 2, no. 3, pp. 27:1-27:44.

Pulkit, A., Naval, S. & Laxmi, V. (2020) A Survey of Side-Channel Attacks in Context of Cache - Taxonomies, Analysis and Mitigation. In: *2020 International Conference on Computing, Communication, & Automation (ICCCA)*. IEEE, pp. 195-200.

Sabri, O., Al-Shargabi, B., Abuarqoub, A. & Hakami, T.A. (2025) A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects. *IoT*, 6 (2), pp. 23.

Srinivas, T.A.S., Donald, A.D., Srihith, I.D., Anjali, D. & Chandana, A. 2023, 'Small But Mighty: The Power of Lightweight Cryptography in IoT', *International Journal of Advanced Research in Science, Communication and Technology*, vol. 3, no. 1, pp. 52-66.

Xu, J., Fan, A., Lu, M. & Shan, W. 2019, 'Differential Power Analysis of 8-bit Datapath AES for IoT applications', *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, pp. 245-250.