Refined Approaches to Evaluating the Robustness of Lightweight Symmetric Ciphers Against Differential-Linear Cryptanalysis

Tsemma Dmytro Oleksandrovych

[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, dmytro.tsemma@nure.ua

Abstract. *The protection of data in devices with limited computational capabilities — such as IoT sensors, embedded controllers, and smart identification systems — relies heavily on lightweight cryptographic algorithms. The emergence of the NIST Lightweight Cryptography standardization initiative has reinforced the importance of developing energy-efficient and secure cryptographic primitives. However, even optimized lightweight ciphers must maintain resilience to complex hybrid attacks like differential-linear cryptanalysis. This study explores modern approaches for assessing the robustness of lightweight symmetric ciphers against such attacks, highlighting structural factors influencing cipher security and presenting strategies for their enhancement. In addition to identifying vulnerabilities, the paper emphasizes the importance of integrating automated analysis tools for evaluating cipher resistance. By combining formal mathematical models with empirical testing on reduced cipher versions, researchers can achieve a more accurate understanding of security margins. The proposed approach not only supports the design of future lightweight algorithms but also provides practical guidance for developers implementing cryptographic protection in real-world IoT ecosystems, where balancing speed and reliability is a critical factor*

Keywords: lightweight encryption; cryptanalysis; hybrid attacks; cipher evaluation; IoT protection; SPN architecture; Ascon cipher.

I. Introduction

The rapid growth of Internet of Things (IoT) ecosystems has led to an urgent demand for cryptographic solutions that combine computational efficiency with strong security guarantees. Lightweight symmetric ciphers address this need by optimizing algorithmic structures to minimize memory and energy consumption. Nevertheless, their simplified architectures may be more vulnerable to cryptanalytic methods, particularly hybrid ones that merge differential and linear techniques [1].

Differential-linear cryptanalysis, introduced in the early 1990s, has evolved into one of the most effective methods for analyzing symmetric-key ciphers [2]. Lightweight encryption schemes — due to reduced complexity and smaller state sizes — represent an appealing target for such attacks. Therefore, evaluating their resistance to these combined methods is a key step in ensuring long-term reliability and trustworthiness.

Modern embedded systems operate in increasingly hostile environments where physical and side-channel attacks are becoming as relevant as classical cryptanalysis. Therefore, assessing resistance to hybrid methods such as differential-linear cryptanalysis should be complemented with implementation-oriented security evaluation. This comprehensive approach ensures that lightweight ciphers remain robust not only in theory but also under practical deployment conditions.

II. Methodology and analysis

1. Overview of Core Cryptanalytic Techniques

To properly estimate cipher resistance, it is necessary to understand the nature of the attacks being tested.

- Differential Analysis. This approach observes how specific differences in input propagate through encryption rounds and affect output pairs. Predictable propagation patterns can help identify the secret key [1].
- Linear Analysis. This method seeks linear correlations between plaintext and ciphertext bits that occur with non-random probability [2].
- Differential-Linear Method. A hybrid approach that combines the two — applying differential analysis in early rounds and linear approximations in later rounds to improve key recovery efficiency [3].

Recent studies have demonstrated that the effectiveness of differential-linear attacks strongly depends on the statistical properties of intermediate state distributions. Even minor imbalances in the probability of differential trails can amplify linear correlations, leading to key leakage. Therefore, a detailed probabilistic analysis of cipher components — especially S-box layers — is essential for predicting potential vulnerabilities. The integration of automated tools for correlation analysis further improves accuracy when testing complex substitution-permutation networks.

2. Criteria for Evaluating Lightweight Ciphers

Testing the robustness of lightweight cryptosystems against differential-linear attacks involves both theoretical modeling and empirical verification.

- Block Structure and Number of Rounds: Lightweight ciphers often utilize smaller block sizes and fewer rounds, which may reduce diffusion and non-linearity. Adjusting these parameters enhances resistance without compromising efficiency.
- S-Boxes and P-Boxes: The substitution-permutation (SPN) framework depends on carefully designed S-Boxes and P-Boxes. Simpler S-Boxes, though beneficial for performance, can introduce linear or differential weaknesses. Optimizing their algebraic structure improves the cipher's robustness.
- Resource Constraints: Since lightweight algorithms must function under limited memory and energy budgets, designers often face trade-offs between performance and security.

In addition, the implementation platform has a considerable influence on cipher resistance. Hardware-optimized versions

often exhibit different diffusion dynamics compared to their software counterparts, which may affect the success rate of certain attacks. Thus, resistance evaluation must consider both hardware and software implementations under various power and clock conditions. Furthermore, lightweight ciphers designed for sensor networks should undergo dedicated fault-injection testing to ensure that low-cost optimizations do not inadvertently introduce exploitable weaknesses.

3. Case Study: Ascon Cipher

Ascon – the winner of the NIST Lightweight Cryptography competition – provides a balanced model for resource-efficient yet secure encryption [4]. Experimental analysis of Ascon's structure revealed:

- its S-Box design and diffusion layers exhibit high resistance to combined differential-linear attacks;
- the standard number of rounds offers an optimal compromise between speed and cryptanalytic strength;
- despite minimal hardware footprint, Ascon demonstrates a well-balanced security-performance profile, suitable for constrained IoT environments.To properly estimate cipher resistance, it is necessary to understand the nature of the attacks being tested.

The obtained results suggest that design principles used in Ascon can serve as a baseline for next-generation lightweight cryptographic standards. Further analysis of its round function and permutation layers under truncated differential-linear models indicates high diffusion strength even in reduced-round configurations. These findings can be leveraged to improve the design of future ciphers by adopting similar nonlinear components and permutation strategies while tailoring them for specific embedded platforms.

III. Conclusions and Future Perspectives

Ensuring the resistance of lightweight symmetric encryption algorithms to differential-linear cryptanalysis remains an essential challenge [1]. This research underlines the importance of parameters such as the size of cipher blocks, non-linear substitution layers, and round configurations [5]. Although Ascon demonstrates strong security properties, the continuous evolution of attack methods necessitates further refinement of design strategies [3].

Prospective directions of study include:

- development of adaptive cryptographic frameworks that dynamically adjust their structure based on detected threats [3];
- design of optimized S-Boxes offering stronger non-linearity with minimal implementation cost.[5];
- application of machine learning to automate vulnerability detection and improve cipher testing efficiency;
- exploration of quantum-resistant lightweight encryption techniques capable of maintaining robustness in post-quantum environments [4].

Beyond algorithmic analysis, there is a growing need to establish standardized evaluation frameworks for lightweight cryptography. Such frameworks could define unified criteria for measuring resistance to mixed attacks, making it easier to compare different cipher designs. Additionally, collaboration between academia and industry can facilitate large-scale experimental testing using realistic IoT datasets, thus validating theoretical assumptions. Introducing these practices would help bridge the gap between academic research and practical implementation of secure, lightweight encryption schemes.

Lightweight cryptography will continue to play a pivotal role in the protection of modern distributed systems, provided that resistance to advanced hybrid attacks remains a design priority.

REFERENCES

[1]. Biryukov A., Dunkelman O., Keller N. (2017). Differential-Linear Cryptanalysis of Serpent. Journal of Cryptographic Engineering, 7(1), 15–22. Springer.

[2]. Mendel F., Nad T., Schläffer M. (2019). Differential-Linear Cryptanalysis of Reduced-Round PRESENT. Fast Software Encryption, 10392, 228–245. Springer.

[3]. Stallings W. (2020). Cryptography and Network Security: Principles and Practice. Pearson.

[4]. NIST (2023). Finalists of the Lightweight Cryptography Standardization Process. National Institute of Standards and Technology.

[5]. Beierle C., Kranz T., Leander G., Moradi A. (2021). Comprehensive Analysis of AES S-Box Resistance Against Differential Attacks. IEEE Transactions on Information Forensics and Security, 16, 2132–2147.

[6]. Dunkelman O., Keller N., Shamir A. (2018). Improved Cryptanalysis of Reduced-Round DES. Journal of Cryptology, 31(2), 366–394.