Manuscript number**: IoT-41406-2024**

Title**:** **A Physical Layer Endogenous Security Architecture with Dynamic Slicing Encryption for IoT**

**The paper proposes a novel PHY-ES architecture with a SEK-based DSE scheme that provides endogenous encryption and decryption for IoT sensing data. The overall concept of combining physical layer security with endogenous key generation is interesting and timely; however, the algorithm descriptions and security analysis require further clarification and logical structuring, and there is a need to distinguish the proposed algorithms from conventional recursive functions by avoiding potential notational conflicts. While the idea is promising, several issues need to be addressed to improve the clarity and strength of the work.**

1. Figures: The figures should be provided in SVG format to ensure clarity and scalability.
2. Performance Comparison: The current performance comparison focuses on KGNet and BCFL key generation schemes against DES. It should also include a comparison with similar SEK-based works, particularly those that encrypt on the physical layer.
3. Algorithm Notation: The algorithm naming (E1-E3 and D) currently creates confusion as it seems to imply recursive functions. It is recommended to revise the notation to clearly distinguish sequential steps.
4. Algorithm E3 Clarity: In Algorithm E3, more details are needed on how the i-th row of the generated key K is inserted into the i-th row of X. A step-by-step explanation would be beneficial.
5. Security Analysis: The security evaluation should incorporate discussions on potential attacks. For instance, if a chosen-text attack is applied with a constant one-bit plaintext, the initial SEKs K might become all zeros (in cases where S is odd), making the disarranging easily distinguishable. This raises concerns regarding the overall robustness of the SEK-based DSE scheme.