Indonesian Journal of Electrical Engineering and Computer Science
Vol. 31, No. 2, August 2023, pp. 1032~1040
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v31.i2.pp1032-1040

Efficient and secure hybrid chaotic key generation for light encryption device block cipher

Hussain M. Al-Saadi, Imad S. Alshawi
Department of Computer, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received Jan 26, 2023
Revised Mar 15, 2023
Accepted Mar 24, 2023

Keywords:

Chaos
Henon map
LED block cipher
Lightweight cryptography
Lorenz map
NIST tests
Security

ABSTRACT

Lightweight cryptographic algorithms must develop to ensure the confidentiality and integrity of the data in resource-constrained devices. Keys are vital to every cryptography algorithm because they provide randomness, complexity, unexpected nature, and robustness. A light encryption device (LED) is considered a lighter version of advanced encryption standard (AES), but it is vulnerable to related key attacks due to using the same key during the whole encryption process. This paper presents a hybrid chaotic key generator (HCKG) based on 3D Lorenz, and 2D Henon maps to generate a highly randomized key that combines with the LED to provide a high level of secure encryption on resource-constrained devices. We modified the HCKG every four rounds via simple operations to get the subkeys and XORed it with the state to increase the complexity of the ciphertext. Moreover, the HCKG with subkeys allows us to decrease the total number of LED rounds from 32 to 24 to minimize the calculation cost while maintaining a high level of security. National Institute of Science and Technology (NIST) test suite proves that the proposed LED-HCKG demonstrates a high-performance increase by nearly 0.3283 higher than LED concerning data integrity and secrecy.

Corresponding Author:

Imad S. Alshawi
Department of Computer, College of Computer Science and Information Technology
University of Basrah
Basrah, Iraq
Email: emadalshawi@gmail.com, emad.alshawi@uobasrah.edu.iq

1. INTRODUCTION

Current primary research in information security focuses on the following topics: encryption algorithms, key management, authentication protocol, secure routing, denial of service (DoS) attacks, intrusion detection, and access control. Encryption algorithms have been intensively explored for years due to their increasing significance [1]-[3]. As a result, chaos-based cryptography has been a notable trend in literature during the past two decades. The primary features of chaotic systems are sensitive to initial parameters, periodic mixing properties, easy analytic description, and highly complicated behavior. Therefore, make them a prime candidate for developing novel cryptosystems as indicated by chaotic block ciphers, chaotic stream ciphers, and chaotic key encryptions [4], [5]. Conventional cryptography techniques are exceedingly slow, complex, and energy-intensive in systems with limited resources. So, the prevalence of low-cost computational algorithms is expanding. Cryptographic systems can generally be categorized as utilizing either symmetric or asymmetric keys [6]. In resource-constrained systems, conventional cryptography algorithms are quite complex, slow, and energy-intensive [7]. There are primarily four types of lightweight cryptography available for use: lightweight stream ciphers (LWSCs), lightweight block ciphers (LWBCs), elliptic curve cryptography (ECC), and lightweight hash functions (LWHFs). Lightweight block ciphers and stream ciphers are symmetric