Provably-Secure LED Block Cipher Diffusion and Confusion Based on Chaotic Maps

Hussain M. Al-Saadi[1], Imad S. Alshawi[*2]
Department of Computer Science, College of Computer Science and Information Technology,
University of Basrah, Basrah, Iraq
E-mail: hussain.mk1978@gmail.com[1], emadalshawi@gmail.com[2]

Keywords: lightweight block cipher, LED block cipher, chaos, Lorenz system, security, NIST tests

Received: January 4, 2023

Lightweight cryptography algorithms have concentrated on key generation's randomness, unpredictable nature, and complexity to improve the resistance of ciphers. Therefore, the key is an essential component of every cryptography algorithm since it affects the algorithm's level of security. Light Encryption Device (LED) is a high-performance, lightweight block encryption solution that works on resource-constrained devices and considers a lighter version of AES. It employs a 64-bit block cipher with two significant instances using 64-bit and 128-bit keys, respectively. A lack of key scheduling in LED heightens security risks, such as key-related attacks. Specifically, now that LED has been hacked and is no longer secure. Therefore, LED must achieve a high diffusion and confusion level to withstand known attacks. Chaos-based encryption provides an exceptionally high level of security because of the unique characteristics of chaotic systems, which are defined by various nonlinear deterministic dynamic equations. Merge LED algorithm and the advantages of chaotic maps randomness provide successful confusion and diffusion property to improve the LED algorithm's shortcomings by increasing its security. This paper presents a lightweight approach to construct a robust, sufficiently using 3-D Lorenz system chaotic map to generate a one-time pseudo-random bit key to avoid being predicted by adversaries, resulting in achieving sound confusion and diffusion and withstand known assaults. A NIST test suite found that the performance of the LED based on the 3-D Lorenz chaotic map approach in terms of data secrecy is nearly 0.3003 higher than that of the LED and keeps the trade-off between computation cost and security.

Povzetek: Predstavljena je izgradnja robustnega in izvedbeno ugodnega 3-D Lorenzovega sistema za generiranje psevdo-naključnega ključa.

1 Introduction

Information security protects data against unauthorized access, detection, modification, or destruction with upholding confidentiality, integrity, and availability (CIA) [1]-[2]. Cryptography protects data in transit (either electronically or physically) through networks. Thus, it is necessary to use current cryptography techniques to fend off security risks [1], [2]-[3]. In resource-constrained systems, conventional cryptography algorithms are extremely slow, complex, and energy-intensive [4]-[5]. The use of low-cost computational algorithms is growing in popularity. Symmetric and asymmetric lightweight cryptography algorithms are classified into two categories.

The symmetric encryption algorithm encrypts and decrypts data using the same secret key. While asymmetric key encryption, data is encrypted with a public key and decrypted with a private key. Block cipher and stream cipher are two distinct symmetric key encryption methods. Trivium, Grain, and Salsa20 are examples of stream ciphers, while Present, LED, RECTANGLE, and HIGHT are examples of block ciphers [6]-[7]. In block cipher, encryption and decryption occur concurrently on a block of a defined size (64 bits or more). In contrast, stream cipher continuously processes the input information bit by bit (or word by word). Claude Shannon suggested confusion and diffusion as crucial aspects of any cryptography [8]-[9] to strengthen the cipher. Stream ciphers rely primarily on the confusion property, but block ciphers combine confusion and diffusion more straightforwardly than stream ciphers [7]. Except for LED, most ciphers, like AES, SPECK, TWINE, PRESENT, and SIMON, require key scheduling, in which actions are performed on the initial secret key to improve the cipher's security. Each round produces a unique round key. The round keys can be made outside the cipher and downloaded at runtime, or the cipher can make them before it starts and save them in memory or make them "on the fly." [10]. The LED method has a minimum block size of 64 bits, a low hardware cost, and a greater frequency than the AES block cipher [8]-[11]. Therefore, LED is the optimal choice if any application requires the smallest area and the quickest time for encryption and decryption [11].

LED is no longer as secure as the current cryptanalysis techniques. Biclique attack is a technique of meet-in-the-middle cryptanalysis applied to the most common lightweight block ciphers, LED, Piccolo, and PRESENT [12], resulting in slow and limited diffusion