Abstract

Moustafa Hussein Aly

Improvement of Radio Frequency Identification Security Using New Hybrid Advanced Encryption Standard Substitution Box by Chaotic Maps

Radio Frequency Identification (RFID) technology is widely utilized by businesses, organizations and wireless communication systems. RFID technology is secured using di erent ways of data encryption, e.g., Advanced Encryption Standard (AES). The Substitution Box (S-Box) is the core of AES. In this paper, a new algorithm is proposed to generate a modified S-Box with new keys, specifically a key and plaintext-dependent S-Box using an improved RC4 encryption algorithm with Logistic Chaotic Maps (LCM). The strength of the proposed S-Box is tested throughout the paper, and compared against the state-of-the-art S-Box implementations, namely, the static S-Box, dynamic S-box, KSA and PRGA S-Box, and RC4 S-Boxes with Henon chaotic maps. The comparison between the state-of-the-art S-Boxes and the proposed S-Box demonstrates that the use of the Logistic Chaotic Map increases the security of the S-Box and makes the di erential and linear cryptography more sturdy. In particular, using the strict avalanche test, we demonstrate that the proposed S-Box improves the security by achieving a cipher text bit-flip ratio of 0.4765, which is closer to 0.5 (where half the bits are flipped), while maintaining a minimum elapsed time of 19 milliseconds for encryption and decryption.