Improved Salsa20 Stream Cipher Diffusion Based on Random Chaotic Maps

Lamia A. Muhalhal[1], Imad S. Alshawi[*2]
Email: allalemyaa@gmail.com[1], emad.alshawi@uobasrah.edu.iq[2]

[*]Imad S. Alshawi
Department of Computer Science, College of Computer Science and Information Technology,
University of Basrah, Basrah, IRAQ

Keywords: NIST statistical test suite, lightweight stream cipher, salsa20 stream cipher, chaotic map, security

Received: July 8, 2022

To enhance stream ciphers, numerous studies have concentrated on the randomness, unpredictable nature, and complexity of keystream. Numerous stream algorithms have been put forth. Most of them require a significant amount of computational power. Salsa20 is a high-performance stream encryption solution that works on computers with fewer resources and uses a secure method that is faster than AES. They suggest Salsa20 for encryption in common cryptographic applications. Users who value speed over certainty should utilize the Salsa20 family of reduced-round ciphers, such as the (8,12) round cipher. It uses a 256-bit key and a hash algorithm. A successful fusion makes use of both the Salsa20 algorithm's and the random maps' advantages to improve the Salsa20 algorithm's shortcomings by increasing its unpredictability. Particularly now that Salsa20/7 has been hacked and Salsa20/12 is no longer as secure as it previously was. As a result, Salsa20 needs to achieve a high level of diffusion to withstand known attacks. Right now, salsa20 and its shortened versions rank among the fastest ciphers. This study presents a novel lightweight approach to construct a strong keystream that is sufficiently random to avoid being predicted by adversaries, achieve good diffusion, and withstand known assaults. A NIST test found that the performance of the (Salsa20-chaotic maps) approach in terms of data integrity and secrecy is nearly 0.3131 higher than that of the Salsa20.

Povzetek: Predlagan je algoritem generiranja varnih gesel za kriptirni algoritem Salsa20, s čemer se odpravi nedavno odkrite probleme.

1 Introduction

The protection of data from unauthorized access, disclosure, alteration, or destruction while upholding confidentiality, integrity, and availability is known as information security (CIA) [1]–[3]. Cryptography is used to protect data while it is in transit (either electronically or physically) through networks. It is necessary to use current cryptography techniques [1], [3], [4] . The selection of a suitable crypto algorithm will have a dynamic effect on a device's lifetime and performance in terms of battery life, hardware memory, calculation time, and communication bandwidth [4].

Conventional cryptography algorithms are slow, complicated, and energy-intensive when used with resource-constrained systems [5], [6]. The use of simple algorithms is growing in popularity. Symmetric and asymmetric algorithms for lightweight cryptography are separated into two groups. The symmetric encryption method uses the same secret key for both encrypting and decrypting operations. Data is encrypted using a public key and decrypted using a private key in asymmetric key encryption (public-key encryption). Two further symmetric key encryption techniques are block cipher and stream cipher. Trivium, Grain, and Salsa 20/12 are stream ciphers, whereas PRESENT, RECTANGLE, SIMON, and SPECK are block ciphers [2]–[4], [7].

This project is part of the Cryptographic Stream Project (ECRYPT), which was founded in 2005 [4], [7]. This project provides solutions that are both efficient and secure, as well as popular and widely used [4], [7]. Salsa20 was among the winners. A more secure and quicker variant of AES is called Salsa20 (20 rounds). Due to its low hardware requirements and simple structure, Salsa20 is an effective stream cipher for data encryption [4], [7]–[9]. One of the quickest stream ciphers currently accessible is Salsa20, as well as its condensed variants. Salsa20/12 is no longer as secure as it previously was, whereas Salsa20/7 has been broken. To achieve good dissemination and withstand known attacks, Salsa20 must therefore address this issue [10], [11]. A chaotic system or computational intelligence (CI) is therefore the ideal answer. Several techniques for chaotic systems have been devised [12]–[16]. The application of chaos theory, a kind of nonlinear system, in cryptography has recently been made to address issues with existing encryption techniques, which are losing their ability to provide quick and secure encryption for large amounts of data simultaneously [15]. Because of their unique properties and high sensitivity to their beginning conditions, chaotic systems are incredibly unpredictable over the long term. Chaotic systems are extremely sensitive to changes in beginning conditions