International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 1, February 2023, pp. 833~841
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i1.pp833-841

A hybrid modified lightweight algorithm for achieving data integrity and confidentiality

Lamia A. Muhalha, Imad S. Alshawi
Department of Computer Science, College of Computer Science and Information Technology University of Basrah, Basrah, Iraq

Article Info

Article history:

Received Apr 2, 2022
Revised Jul 18, 2022
Accepted Aug 19, 2022

Keywords:

Hash function
Keystream generator Salsa20
NIST statistical test suite
Salsa20 algorithm
Speck algorithm

ABSTRACT

Encryption algorithms aim to make data secure enough to be decrypted by an attacker. This paper combines the Speck and the Salsa20 to make it difficult for an attacker to exploit any weaknesses in these two algorithms and create a new lightweight hybrid algorithm called Speck-Salsa20 algorithm for data integrity and confidentiality (SSDIC). SSDIC uses less energy and has an efficient throughput. It works well in both hardware and software and can handle a variety of explicit plaintext and key sizes. SSDIC solves the difficulties of the Speck algorithm. The sequence generated by Speck is not random and fails to meet an acceptable success rate when tested in statistical tests. It is processed by generating a random key using the Salsa20 algorithm. Salsa20 is a high-speed secure algorithm that is faster than advanced encryption standard (AES) and can be used on devices with low resources. It uses a 256-bit key hash function. The recovery of the right half of the original key of the Speck algorithm is also handled by modifying the Speck round function and the key schedule. Simulation results show, according to a National Institute of Standards and Technology (NIST) test, the performance achieved by the SSDIC is increased by nearly 66% more than that achieved from the Speck in terms of data integrity and confidentiality.

Corresponding Author:

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

1. INTRODUCTION

The protection of data from unauthorized access, disclosure, alteration, or destruction while ensuring confidentiality, integrity, and availability is very important to information security [1]. As there are unknown risks, threats, and vulnerabilities, there is no 100% guaranteed security [1]–[4]. Cryptography is used to keep data secure while it is in transit (electronic or physical). The increasing demand for the confidentiality of information necessitates the creation of new encryption techniques and algorithms [1], [2], [5], [6]. According to William Stalling, the security of encrypted data is entirely dependent on two factors: the strength of the cryptographic technology and the secrecy of the key [7]. These algorithms must be fast and secure enough to prevent wasting resources in low constrain devices.

Modern encryption algorithms are essential in data transmission systems. Choosing an appropriate encryption algorithm will have an impact on device longevity and performance in terms of battery life, device memory, processing lag, and connection bandwidth [8], [9]. Conventional encryption techniques are slow, complex, and very energy-intensive when dealing with resource-constrained systems [9], [10]. Solutions for resource-limited hardware lightweight algorithms are becoming more common and used [9], [10]. The face of lightweight cryptography has been a popular research topic for decades. The lightweight