Enhancing Hierocrypt-3 performance by modifying its S-Box and modes of operations

Wageda I. El Sobky[1], Ahmed R. Mahmoud[1], Ashraf S. Mohra[1], T. El-Garf [2]
[1] Benha Faculty of Engineering, Benha University, Egypt
[2] Higher Technological Institute 10th Ramadan, Egypt
Email: wageda.alsobky@bhit.bu.edu.eg; ahmed.mokhtar@bhit.bu.edu.eg;

Abstract[1] — Human relationships rely on trust, which is the reason that the authentication and related digital signatures are the most complex and confusing areas of cryptography. The Massage Authentication Codes (MACs) could be built from cryptographic hash functions or block cipher modes of operations. Substitution-Box (S-Box) is the unique nonlinear operation in block ciphers, and it determines the cipher performance. The stronger S-Box, the stronger and more secure the algorithm. This paper focuses on the security considerations for MACs using block cipher modes of operations with the Hierocrypt-3 block cipher. the Hierocrypt-3 could be considered as a week cipher. It could be enhanced by changing its S-Box with a new one that has better performance against algebraic attack with using different modes of operations. The mathematical model for the new S-Boxes with its properties is provided. The result of this change appeared in the mirror of Average Strict Avalanche Criterion (SAC) and some other properties. SAC could be improved from 0.80469 to 0.16406. The Hierocrypt-3 could be enhanced for more security.

Index Terms— Hierocrypt, S-Box, Security, Block Cipher, Cryptography, MACs, COVID-19.

I. INTRODUCTION

Nowadays, with the wide spread of the corona virus (COVID-19) and the extremely large growth of online shopping processes, digital data communication and online bank transactions over computer networks, information content security becomes a prime concern in the whole world. Internet itself has many security threats that could be easily used to corrupt the data transferring over the network. Cryptography plays an important role for providing security for digital data transmission over such this insecure network. Cryptographic algorithms scramble data into unreadable text which can be only read or decrypted by those possesses the associated security key. Message authentication codes (MACs) are commonly used in network transactions to maintain information integrity [1]. They confirm that a message is authentic; that it really does come, in other words, from the stated sender, and hasn't undergone any changes during the transaction using digital signatures [2]. A verifier who also possesses the key can use it to identify changes to the content of the message in transaction.

The Substitution box (S-Box) is the unique nonlinear operation in block cipher, and it determines the cipher performance [3]. The stronger S-Box, the stronger and more secure algorithm. By selecting a strong S-Box, the nonlinearity and complexity of these algorithms increases and the overall performance is modified [4]. This change will be seen here on the Hierocrypt-3 [5] as an example of block ciphers.

The S-Box construction is a major issue from initial days in cryptology [6][7][8]. Use of Irreducible Polynomials to construct S-Boxes had already been adopted by crypto community [9].

The Hierocrypt-L1 and Hierocrypt-3 are algorithms of symmetric block ciphers that were submitted to the NESSIE project [10][11], but were not selected. Both algorithms were among the cryptographic strategies prescribed by CRYPTREC for the Japanese government utilize in 2003 [12], however, both algorithms have been dropped to "candidate" by CRYPTREC revision in 2013. The Hierocrypt algorithms were candidate block ciphers for the NESSIE project, where Toshiba corporation started developing it from 2000 to 2002. In September 2001, Toshiba Corporation announced for the Hierocrypt-L1 specifications which was an algorithm that uses 64-bit block iterated cipher using a 128-bit cipher key [11]. In September 2001, Toshiba Corporation also announced for the Hierocrypt-3 specifications which was an iterated 128-bit block cipher algorithm that uses 6.5, 7.5, or 8.5 rounds of encryption, according to the key size 128, 192 or 256, respectively [5]. In October 2001, Toshiba Corporation announced for the Hierocrypt-3 Self Evaluation which mentioned that the Hierocrypt-3 is secured [13]. In January 2004, Rogawski published an article that mentioned that the Hierocrypt-3 is a very flexible algorithm and could be optimized for any purpose like speed, area and memory [14]. In 2016, KUROKAWA et al published an article which mentioned that related key attacks and meet-in-the-middle attacks (including biclique attacks) were evaluated on Hierocrypt-3. In their evaluations [15], no flaws that could be realistic threats were found [16].

In this article, The S-Box principle is deeply analyzed and a new S-Box is provided with its principle. the

[M]anuscript received Month Day, 2020; revised Month Day, 2020.
This work was supported by the Foundation Name under Grant No. XXXXXX.
Corresponding author email: ahmed.mokhtar@bhit.bu.edu.eg.
doi:10.12720/jcm.v.n.p-p