Design Large Symmetric Algorithm for Securing Big Data

Omar A. Dawood 1st
College of Computer
Sciences and Information Technology
University of Anbar, Iraq
The_lionofclub@yahoo.com
Omar-Abdulrahman@uoanbar.edu.iq
Phone: 009647905884333
orcid.org/0000-0003-3276-602X

Ali M. Sagheer2nd
Al Qalam University College, Iraq
dean@alqalam.edu.iq

Salah Sleibi Al-Rawi3rd
College of Computer
Sciences and Information Technology
University of Anbar, Iraq
dr_salah_rawi@yahoo.com

Abstract— Today several Institutions, organizations, companies and research centers deal with hundreds of gigabytes or terabytes of the massive amount of renewable data every day. This large volume of the data requires an appropriate algorithm to protect the sensitive data that may involve credential data. These important data may contain the username and confidential password, financial accounts numbers, social security numbers, secret one-time passwords of online access or digital certificates. The various types of data need high protection from stealing, hacking or malicious actions. In this paper, we have proposed a large block cipher model by following the principles of contemporary block ciphers criteria and implemented real designing steps of algebraic ideas. The proposed cipher is considered as an extended cipher with a big size of encryption/decryption block of 512-bits and a key length of 128-bits which are expanded to reach 512-bits fit to the state matrix. This cipher is based on Substitution and Permutation Network (SPN) structure with three layers of four iterated stages similar to the Advance Encryption Standard (AES) structure, but with an extended size. A new non-linear S-Box It has adopted, new Shifting technique and a distinct mix column of order eight as well as it uses a new technique in expanding key from 128-bits to 512-bits. The proposed algorithm accepts the key length of 128-bits as the initial input of a secret key and the ciphering key is expanded from 128-bits to 512-bits for the first round and the other expanded rounds. The key scheduling

128, 192 and 256-bits with 10, 12 and 14 rounds respectively according to the NIST demand and conditions. AES cipher has a good efficiency in most software and hardware implementations and it proved a high performance in a wide scope of applications and platforms [2]. The AES cipher consists of four main stages operations that are repeated for each round until the end of an algorithm that can be clarified as follows:

- SubByte Operation: it is a non-linear stage that performs on each entry of the state matrix that consists of three distinct components: start by taking the multiplicative inverse for each byte in the Galois Field GF(2^8). Next, apply non-linear mapping to the entry of each input byte and the outcome bitwise XORed with a hexa-value of 0x63.
- ShiftRow Operation: it is a very simple step and it is a linear stage that works on a shifting each row by a number of placements to gain the high level of diffusion.
- MixColumn Operation: the mixcolumn stage is the multiplication of the state array with constant of MDS matrix.
- AddRoundKey: The key with a certain length is bitwise XORed with state of the array of 128-bit [3].

The outline of the present paper: this paper is organized as follows: Section I explain the main motivation beyond the design idea. Section II submits the proposed large cipher