2011 Sixth International Conference on Bio-Inspired Computing: Theories and Applications

Immune systems approaches for cryptographic algorithm

Suriyani Ariffin[1], Ramlan Mahmod, Azmi Jaafar
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
Serdang, Selangor, Malaysia
suriyani@tmsk.uitm.edu.my, ramlan@fsktm.upm.edu.my,
azmi@fsktm.upm.edu.my

Muhammad Rezal Kamel Ariffin
Faculty of Science
Universiti Putra Malaysia
Serdang, Selangor, Malaysia
rezal@math.upm.edu.my

***Abstract*—This paper proposed immune-inspired approaches in designing a new function for cryptographic algorithm named as 3D-AES. The immune systems approaches were selected on the basis of complex features that are desirable for substitution and permutation process to ensure adequate security and confidentiality of the systems in the world of information technology. This paper will identify the correspondences and highlight essential computation elements that can be applied in cryptographic algorithm that satisfies with Shannon's confusion and diffusion properties. The 3D-AES uses components in Advanced Encryption Standard (AES) algorithm and new core components based on immune systems approaches. Cryptographic strength in the context of this paper is related to the ability of the algorithm to produce a random output. The empirical findings are presented and identified that the randomness of the output in the 3D-AES algorithm are comparable with AES algorithm.**

***Keywords*-cryptographic algorithm; block cipher; AES; Artificial Immune System; protein structure; randomness test**

I. Introduction

Artificial Immune Systems (AIS) [1] [2] are computational systems inspired by theoretical immunology and observed immune functions, principles and models, which are applied to complex problem domains. Currently, various relevant processes and concepts of AIS exist with many and diverse applications [3] [4]. Many models had explored based on immune system such as in machine learning [5], negative selection algorithm [6], search method [7] and Clonal Selection Principle [8]. There have been doubts on the necessity of yet another biologically inspired approach, especially given the perceived similarity to computer security. It is based on the CDIS [9] models and the intrusion-detection system [10] [11] and Dasgupta [12] also state that AIS can be possible to apply in developing computer security systems. Taking into considerations of this immunological physiology and the basic technique of cryptographic algorithm in computer security systems, adaption of immune system theory will be explored and customized in this paper.

This paper describes the proposed algorithm called 3D-AES, inspired by the design of the AES [13] and with some innovative designs based on the immune systems. The test suite [14] from NIST was chosen to test sequences generated by proposed new block cipher done by Soto et. al. [15] for five finalists of AES candidates. This statistical tests suitable in the evaluation of random number generators and pseudo-random number generators used in cryptographic applications. This paper is organized as follows: Section 2 describes the cryptographic algorithm, Section 3 describes the new immunology as inspiration, Section 4 describes the key 3D-AES block cipher design concept, Section 5 estimates the empirical analysis of 3D-AES and Section 6 concludes and future works of the paper.

[1]The first author is also affiliated with the Universiti Teknologi MARA, Shah Alam, Malaysia

II. Cryptographic algorithm

In traditionally, the cryptography is a study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge. Historically, cryptography helped ensure secrecy in important communications, such as those of spies, military leaders and diplomats. In simple terms, cryptography is the science concerned with the study of secret communication. With the invention of computers and the internet, the need for this encryption scheme is now universal in the world of information security.

A cryptographic algorithm includes block cipher algorithm that has five ingredients: plaintext and ciphertext, encryption and decryption algorithms and secret keys. In cryptography, a block cipher encryption algorithm fixed bit block of plaintext as input and output a corresponding fixed bit block of ciphertext. AES was chosen by NIST as the Federal Information Processing Standard (FIPS), also known as FIPS197. The AES encryption used by governmental groups, business and individuals around the world to protect private computers and networking systems. In AES, plaintext, ciphertext, subkeys and data blocks are represented by a two-dimensional (2D) 4 x 4 state matrix of bytes for 128, 196, 256 and 512 bits in steps of 32 bits. In this block cipher, complete text diffusion is achieved in 10, 12 and 14 rounds respectively, due to a combination of *ShiftRows* and *MixColumns* over a 4 x 4 state matrix. Key diffusion is depending on the key size. It takes more rounds to guarantee fast diffusion for both text and key bits as the block size increase. Although Nakahara [16] already designed the 3D block cipher operates on

978-0-7695-4514-1/11 $26.00 © 2011 IEEE
DOI 10.1109/BIC-TA.2011.33

512-bit blocks and 512-bit key, however the iteration round increase from 14 to 22 rounds. It will make the speed performance of the block cipher decrease and the result of the randomness test is not presented yet. This fact motivates of the research, leading to three-dimensional (3D) array, with a larger block size (512 bits), 128 bits key and iterates 10 rounds which makes it attractive as a building block in construction of new block cipher.

III. Immunology as Inspiration

The immune system is a complex defence mechanism that has evolved to provide an extremely efficient mechanism for ridding the body of foreign substances. The immune system depends on the production of antibodies consists of proteins which bind to specific foreign particles such as bacteria and viruses. There are some possible metaphors models that can be adopted in constructing the cryptographic algorithm that satisfies with Shannon's [17] confusion and diffusion properties.

A. Antigen-antibody interaction

Antigen-antibody interaction [18] is involving different terms as shown in Figure 1. An antibody is the protein molecule or called immunoglobulin that is produced against a specific antigen and may possibly have derived an idea of proteins as stable, independent structures. An antigen is a molecule that binds specifically to an antibody, but the term now also refers to any molecule or molecular fragment that can be bound by a major histocompatibility complex (MHC) [19]. An antigen is anything that is recognized by the body's immune system as foreign.

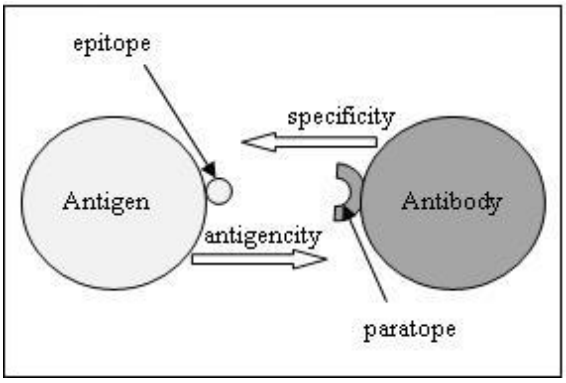

Figure 1. The terms used to describe antigen-antibody interaction

An epitope is the part of an antigen and a paratope is the part of an antibody that recognizes the epitope. Antigenicity or immunogenicity is the capability of an antigen to trigger an immune response and bind to an antibody. Specificity refers to the ability or likelihood of an antibody to bind with an antigen. During the clonal selection immune respond, this theory identified an exponential increase in antigen and antibody produced as shown in Figure 2.

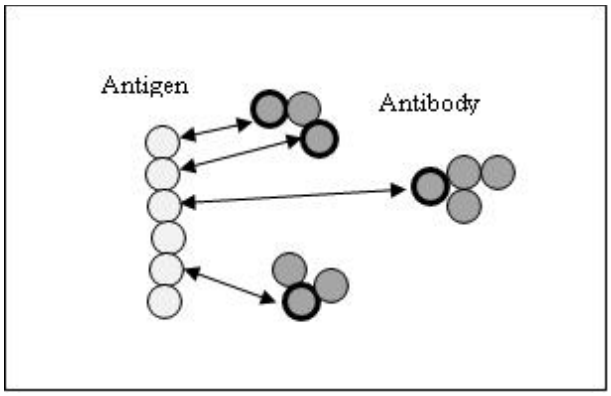

Figure 2. The exponential increase during the diversity of antibodies

B. Somatic Hypermutation Model (SHM)

SHM is a diversity generating, regulated cellular mechanism displayed by the adaptive immune response. It involves a programmed process of mutation affecting the variable regions of immunoglobulin genes (protein). Li et. al. [20] indentified that the mutations of gene are base on substitutions of the cell. This characteristic of SHM is relevant to characteristic of cryptographic algorithm in the confusion [17] properties.

C. Protein structure

Proteins are containing random amino acids sequence structure where each atom in the sequence occupies a unique place in the relative 3D structures. Structure proteins also have the information of the geometry of protein including the distance, angle and dihedral angle between amino acids sequences in the protein structure. The protein folding problem creates a random search problem in searching amino acids sequence. Base on the Levinthal's paradox [21] and problem formulation from Karplus [22] and Dobson et. al. [23], if we take a 100 amino acids or residues protein and each residue can have only 3 positions or conformational states. From this number of residues proteins and positions, it will be generate 3^{100} or about 10^{48} possible states of amino acids sequences. The protein can explore a new state of configuration and each configuration takes about 10 - 11 seconds, there are about 108 seconds in a year or about 10^{25} years which mean this is longer than the age of the universe. In other circumstances, if we drop necklace pearl to the ground for many times, it is impossible to get the same conformational states of the sequence of pearls. All of these procedures and behaviours can be a substantial on random number generator and adapted to generation encryption in cryptographic algorithms. This proposed approach model is mentioned in [24].

The research will be adopting the process and structure of generating the protein to generating random ciphertext from new block cipher. The elements of protein structure that can be inspired to design the new block cipher are:

- Sequence of amino acids.

- Each protein folds into a unique 3D structure from the combination of amino acid sequence.
- Information of the geometry of protein including distances, angles and dihedral angles in 3D structure.
- Have torsion angles which can rotate freely for every bonds at the sequence of amino acids.

IV. 3D-AES Block Cipher Design Concept

This section will be describe the design model, input and output format and function description of 3D-AES block cipher.

A. Design Model

The design model is adopted from the interaction between antigen and antibody as shown in Figure 3 and 4. Key and plaintext represent as antigen and antibody respectively. The eiptope and paratope as part of antigen and antibody will be define as lookup table which refer tu the combining the key and plaintext to procude the ciphertext. Due to the complexity and security as AES algorithm concept, this process will generated in 10 rounds.

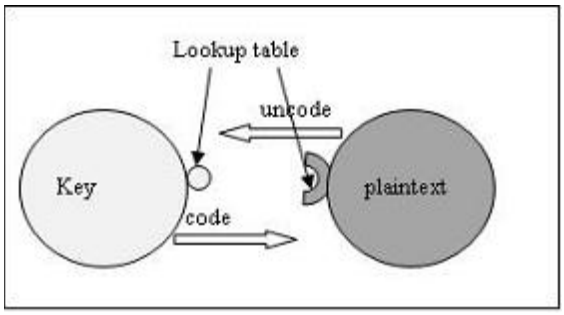

Figure 3. The interaction between key and plaintext

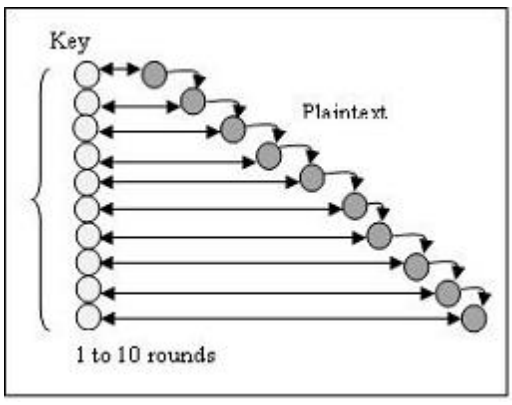

Figure 4. The key-plaintext interaction continued iteration until 10 rounds

B. Input and Output Format

Internally, the 3D-AES algorithm's operations are performed on a 3D array of bytes called *Cube*. The *Cube* is mapped to the 3D structure from the combination of amino acid sequence of protein with finite length of 64 bytes (512 bits). The *Cube* consists of three independent vectors including four lengths, four widths and four depths of bytes, each containing Nb bytes, where Nb is the block length divided by 64 as illustrated in [24] (Figure 5). In the *Cube* array denoted by the symbol A, each individual byte has two indices, with its length number x in the range $0 <= x < 4$, width number y in the range $0 <= y < 4$ and its depth number z in the range $0 <= z < 4$. This allows an individual byte of the state called *Slice* to be referred to as either $A_{x,y,z}$ or $A[x, y, z]$.

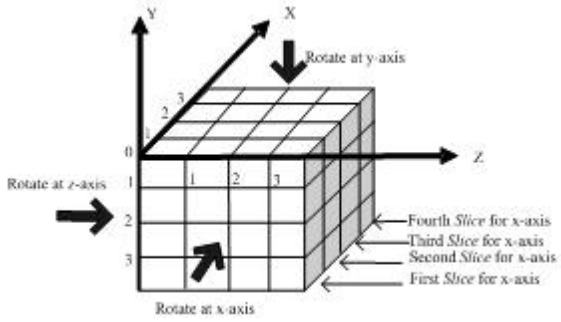

Figure 5. The *Slice* definition and rotation direction for *Cube* array

C. Function description

The components of cipher consists of encryption and decryption scheme as described in Figure 6. The input plaintext at encryption process is copied to the *Cube*. After the initial *AddRoundKey*, the *3D-SliceRotate* and *MixColumns* are transformed by implementing the ten iteration rounds function with the final round differing slightly from the first 9 rounds. This new component is mapped to the type of geometry of protein including distances, angles and dihedral angles in 3D structure. The *3D-SliceRotate* was coded by transformation functions *getSliceCube*, *getRotateSlice*, *SubBytes* and *ShiftRows*. The *SubBytes*, *ShiftRows*, *MixColumns* and *AddRoundKey* modules are the existing module from AES algorithm.

D. Rotation and Dihedral Angel of 3D-SliceRotate

The *3D-SliceRotate* is a permutation process of 4 x 4 x 4 state of bytes includes rotation at x-axis, y-axis and z-axis. The state for every *Slice* for a 64-byte data block show in Figure 7. The set $(a_{000}, a_{001}, a_{002}, a_{003}, ..., a_{033})$ represents the front *Slice* or the first vertical slice, the set $(a_{100}, a_{101}, a_{102}, a_{103}, ..., a_{133})$ represents the second vertical slice and so on. In this paper we only discuss the implementation experiment results for the rotation at x-axis only.

Every *Slice* of the *Cube* module will be rotate at *3D-SliceRotate* module implementation in 4 types of angel, there is no rotation slice for the first slice or 0^0, second will be rotate in 90^0, third slice will be rotate in 180^0 and fourth slice will be rotate in 270^0 as shown in Figure 8- 10 respectively.

V. Empirical Results

Security was the most important factor in the evaluation and encompassed features such as resistance of the algorithm to cryptanalysis, soundness of its mathematical

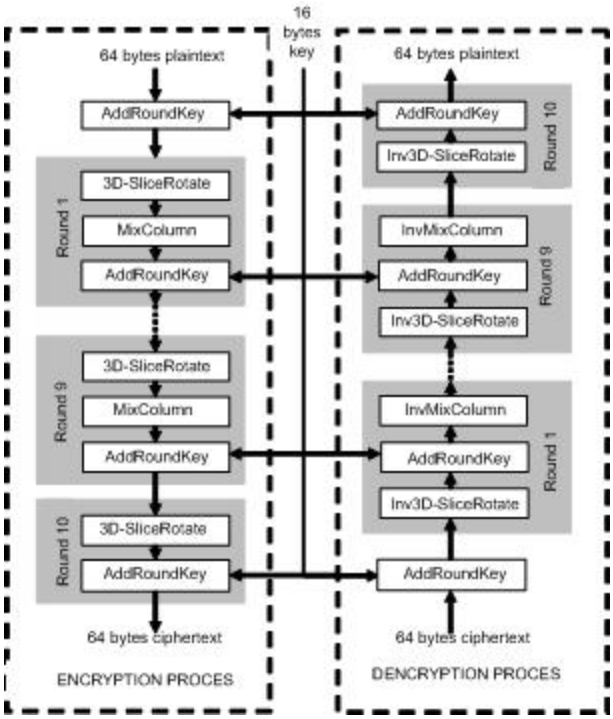

Figure 6. The components of 3D-AES block cipher

First Slice	Second Slice
$a_{000}\ a_{001}\ a_{002}\ a_{003}$	$a_{100}\ a_{101}\ a_{102}\ a_{103}$
$a_{010}\ a_{011}\ a_{012}\ a_{013}$	$a_{110}\ a_{111}\ a_{112}\ a_{113}$
$a_{020}\ a_{021}\ a_{022}\ a_{023}$	$a_{120}\ a_{121}\ a_{122}\ a_{123}$
$a_{030}\ a_{031}\ a_{032}\ a_{033}$	$a_{130}\ a_{131}\ a_{132}\ a_{133}$
Third Slice	**Fourth Slice**
$a_{200}\ a_{201}\ a_{202}\ a_{203}$	$a_{300}\ a_{301}\ a_{302}\ a_{303}$
$a_{210}\ a_{211}\ a_{212}\ a_{213}$	$a_{310}\ a_{311}\ a_{312}\ a_{313}$
$a_{220}\ a_{221}\ a_{222}\ a_{223}$	$a_{320}\ a_{321}\ a_{322}\ a_{323}$
$a_{230}\ a_{231}\ a_{232}\ a_{233}$	$a_{330}\ a_{331}\ a_{332}\ a_{333}$

Figure 7. The state for every *Slice*

basis, randomness of the algorithm output and relative security compared with other algorithm. In this paper the comparison randomness tests of the algorithm output between AES and 3D-AES were made using NIST Test Suite [14]. It is a statistical package consisting of sixteen tests that were developed to test the randomness of arbitrarily long binary sequences produced by either hardware or software based cryptographic random number generator. These tests focus on a variety of different types of non-randomness that could exist in a sequence. The analysis used a significance level $\propto$ = 0.01 of statistical tests. If a *p-value* for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A *p-value* of zero indicates that the sequence appears to be completely non random.

After development of new block cipher using Java in order to generate 1000 sequences of bits with the length of the bit string is 100 bits ciphertext files. From the results

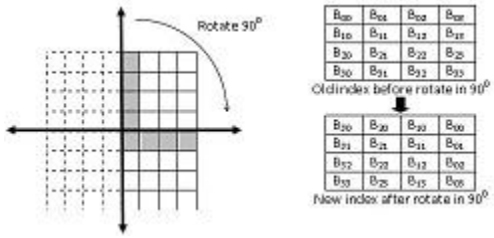

Figure 8. The *Slice* rotation of 90^0

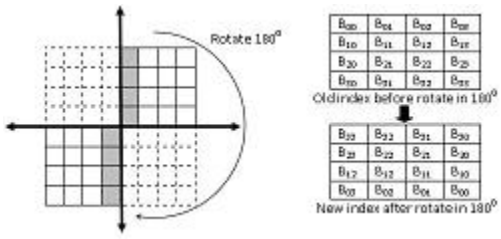

Figure 9. The *Slice* rotation of 180^0

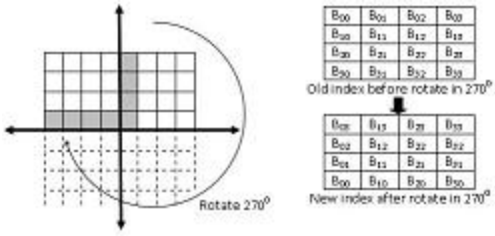

Figure 10. The *Slice* rotation of 270^0

of the frequency test for 3D-AES, it reported that 982 of 1000 sequences have the *p-value* $\geq$ 0.01, which means that 3D-AES passed the randomness on the frequency test. To examine the randomness of the output, 1,280,000

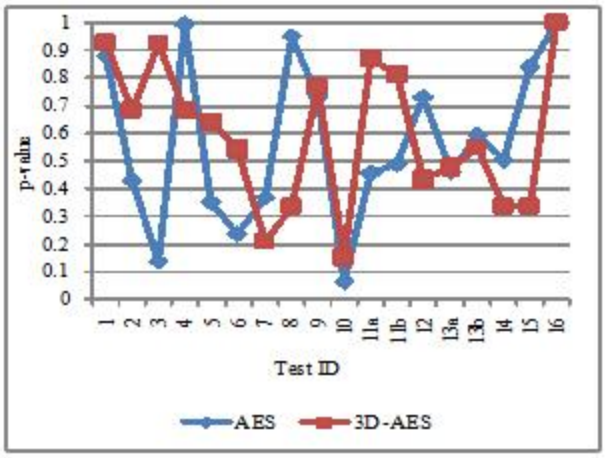

Figure 11. The chart for the *p-values* between 1,280,000 bits generated using AES and 3D-AES

bits were generated by AES and 3D-AES. For each of output files, all of sixteen statistical tests (denoted as test ID) were applied and recorded in Figure 11. The figure shows the *p-value* $\geq$ 0.01 for all the sixteen tests. It can be concluded that bits generated by proposed 3D-

AES block cipher algorithm is successfully passed all the randomness tests as same as AES block cipher. The scatter chart in Figure 11 doesn't indicates that 3D-AES is more efficient compare to AES but it do indicate that 3D-AES is comparable with AES of randomly generated outputs whereby one of the evaluation criteria in security measurement of cryptographic algorithm.

VI. Conclusions And Future Work

The results shown in the experimental design those immune systems can be successfully applied to design competitive block ciphers. In this line, the *3D-RotateSlice* function as the core components in 3D-AES can be thought as an instance of a family of designs that can be explored with this paradigm. Perhaps the most relevant aspect in this scheme is the appropriate selection of the AIS algorithms and concepts. The generated block cipher has successfully passed of very demanding statistical tests. One of the significant findings to emerge from this paper is that the one of the security evaluation of the 3D-AES block cipher is comparable with AES block cipher. Although this does not ensures a certain security level for 3D-AES block cipher, it guarantees that neither trivial weaknesses nor implementation bugs exist. Future work should include deeper analysis of the cipher, particularly against basic attacks, such as linear, differential or related-key cryptanalysis.