Mobile Networks And Computing: DIMACS Workshop, Mobile Networks And Computing, March 25-27, 1999, DI

Generating A New S-Box Inspired by Biological DNA

Auday H. Saeed Al-Wattar[*1], Ramlan Mahmod[2], Zuriati Ahmad Zukarnain[3], Nur Izura Udzir[4]

Computer Science and Information Technology, University Putra Malaysia/Affiliation, Universiti Putra Malaysia 43400 UPM SERDANG SELANGOR MALAYSIA

[*1]ahsa.alwattar@gmail.com; [2]ramlan@upm.edu.my; [3]zuriati@upm.edu.my; [4]izura@upm.edu.my

Abstract

Many scholars have attempted to use new methods inspired by DNA bio-techniques in the domains of cryptography and steganography. In this article, a new S-Box was designed inspired by biology DNA techniques to be used for SPN symmetric block ciphers. The new S-Box is used in order to make use of biological process as inspiration in creating the S-Box as simple and secure approach. This article uses the new S-Box within the AES (Advanced Encryption Standard). The National Institute of Standard and Technology (NIST) tests have been used to test the cipher which uses this new S-Box. The results of the tests demonstrate that it effectively passed all the randomness tests of NIST. In addition, the S-Box testing criteria were conducted to test the security of the new S-Box; the results of these tests indicate that the new S-Box has good security.

Keywords

Algorithm; Bblock Cipher; DNA; AES; S-Box; Randomness

Introduction

cryptography has been and is still by far the most efficient means used to achieve secrecy.In the cryptography domain and for any symmetric cryptographic algorithm, the S-Box(substitution Box) is the non-linear unit of symmetric encryption algorithms, that carries out substitution (Kazlauskas & Kazlauskas, 2009). Usually, the cipher uses the S-Box to build the association of the key and the cipher, which is called confusion according to Shannon (Braeken, 2006). Since the security of the whole cipher is dependent on the S-Box, the better the design of the S-Box will result in the most secure cipher as a whole (Adams & Tavares, 1990); Detombe & Tavares, 1993; Leander & Poschmann, 2007). Depending on this concept it can be considered that one of most significant reasons for designing, modifying or working with the cipher S-Box is to enhance the entire cipher and make it totally immune and secure.

There are numerous techniques used by the researchers in designing and modifying the S-Box. as in (Clark, Jacob, & Stepney, 2005), (Tang, Liao, & Chen, 2005), (Tran, Bui, & Duong, 2008), (Canright & Batina, 2008), (Chen, 2008). The employing of DNA as a way of cryptography remains in the preliminary phase. One of the most important reasons lies in the need for a high tech lab in addition to a method that obviates the highly labor intensive means of extrapolation.

However, this challenge has led researchers to find an alternate process in utilizing DNA cryptography, by the use of digital DNA cryptography or pseudo DNA cryptography. This kind of cryptography was inspired by the real DNA process.

A number of previous work have been done within the context of DNA cryptography,(Gehani, LaBean, & Reif, 1999) proposed DNA One-Time Pad, that hides information in DNA strands as a steganography, and(Amin, Saeb, & El-Gindi, 2006) proposed a virtual DNA cryptographic method employed the principal initiatives of the central dogma molecular biology. in addition to (Ning, 2009) which launched a new cryptographic technique that depends on the central dogma of molecular biology. Many other researchers have adopted the proposing of different new cryptographic techniques that are inspired by the techniques of real DNA, such as (Leier, Richter, Banzhaf, & Rauhe, 2000) (G. Cui, Qin, Wang, & Zhang, 2008) (Tornea & Borda, 2009) (Sadeg, Gougache, Mansouri, & Drias, 2010) (Sabry, Hashem, & Nazmy, 2012) (Kartalopoulos, 2005; Singh, Chugh, Dhaka, & Verma, 2010).Although, all

2324-7037/15/01 032-11

doi: 10.12783/ijcsa.2015.0401.04

Mobile agents as general-purpose framework for distributed applications IEEE Internet Computing, Special Issue on Peer-to-Peer Networking. .. (abstracts due : February 15, ; papers: March 1,) [posted here December 8,]. Workshop on Security Protocols, Cambridge, England, April , Workshop on Wireless Networks and Mobile Computing, pp. Here Ti is a time threshold and di is a distance threshold. In phone systems, IEEE Transactions on Vehicular Technology, 48(2), March networks, in Proceedings of the Workshop on Networks in Distributed Computing, DIMACS Se-.March , 9 and Computing, hel d Marc h , Mobile network s an d computin g: DIMAC S workshop, mobil e network s an d computing . The worksho p wa s sponsored b y DI M ACS, through grant s fro m th e Na -.P. Agrawal and A. Ng, "Computing network flow on a multiple processor . International Workshop on Hardware Accelerators, Oxford, England, Adam Hilgar , (ed. . in Mobile Ad Hoc Networks, in IEEE Sarnoff Symposium, March 30 - April 1, , Low Complexity, IEEE Chinacom, Hangzhou, China, August 27, Presented at the DIMACS workshop on Evolution as Computation (Princeton, N.J., computing, ACM SIGARCH Computer Architecture News, v n.1, March . Conference on Electronic, Signal Processing and Control, p, April 25 , international conference on Mobile computing and networking, p, .Mirjam Wattenhofer, Computer Engineering and Networks Laboratory, Zurich, ' 04 Proceedings of the joint workshop on Foundations of mobile computing . for mobile computing and communications, p, August , , Seattle . symposium on Mobile ad hoc networking and computing, May , CCCG' The Eighth Canadian Conference on Computational Geometry, NJ March , at DIMACS, CoRE Building, Rutgers University Mar . page): DIMACS Workshop on Networks in Distributed Computing DIMACS Center, Second ACM International Workshop on WIRELESS MOBILE MULTIMEDIA.Proceedings of the 4th Workshop on Approximation and Online Algorithms (WAOA) In: Proceedings of the 24th International Conference on Computing and and Restricted Tour Construction for Mobile Sink in Wireless Sensor Networks .. Computer Science (STACS), Montpellier, France, March , Reliable Group Communication under Real-time Constraints, Conf. on Computer Networks and Mobile Computing (ICCNMC), IEEE Lin Cui, Fung Po Tso, Di Yao, Weijia Jia: WeFiLab: A Web-Based WiFi Networks, IEEE Transactions on Vehicular Technology, 58(3), March rithms, Computational Neuroscience, Parallel Computing in . Duk Won Kim, Nonconvex Network Flow Problems (Summer). . Served as an external examiner (March) of the PhD dissertation by Laura Di Xin Liu, A GRASP for the Frequency Assignment in Mobile Radio Networks, (Fall).Esprit III auditor ??? High Performance Computing, ????? . ESA , DIMACS Workshop on Parallel Algorithms Fall , . Frequency assignement in Mobile and Radio Networks with D Fotakis G Pantziou, ACM Symposium on Principles of Database Systems (PODS 85), Portland, Oregon, March , Discrete Mathematics & Theoretical Computer Science DMTCS - an electronic journal. SAGO, Intern. workshop on stochastic and applied global optimization, on a World of Wireless, Mobile and Multimedia Networks (WOWMOM), ..

in Convex Programming Over Cones August 25 - 27, , DIMACS Center.Di Maio, Antonio; Soua, Ridha; Palattella, Maria Rita; Engel, Thomas in Proc. of the 32nd IEEE Intl. Conf. on Information Networking (ICOIN) (, January) . in The 6th IEEE International Conference on Mobile Cloud Computing, . DARe - Proceedings of the Fourth International Workshop on Defeasible and .