The unique ethno-mathematics of *Al-Qur'an* and *Al-Hadith* for pattern recognition of para-normal attacks

Ahmad Faizul Shamsudin, Najhan Mohammad Ibrahim[1], Azmi Ahmad[2], Fadhil Shoib[3]

Faculty of Management and Information Technology[1], Centre of Language Studies[2], Library [3], Universiti Sultan Azlan Shah, Kuala Kangsar, Perak Darul Ridzuan, Malaysia, afaizuls@usas.edu.my; najhan@usas.edu.my, azmi@usas.edu.my, fadhil@usas.edu.my

Abstract - This search for patterns to depict para-normal attacks is premised on the non- parametric ethno-mathematics of the 'protective' (*Mu'awwidhatain*) nature of the *Al-Quran* and *Al-Hadith*. It creates unique patterns of objects in the substitution block-cipher boxes which may depict para-normal patterns. Strangely, the security strength of the non-parametric objects from the *Al-Qur'an* and *Al-Hadith* characteristics are measured from parametric algebraic attacks. Though it may seem unconventional the objects yield unique patterns. The extracted objects that form the unique patterns however were insufficient to build the 256 bit block-ciphers. The development of expanding objects from other ancient scriptures filled up the differences between these objects and the para-normal objects in a pattern of a 256 bit block-cipher. The remaining voids are to be filled up by random numbers that can be replaced by the ethno mathematics of the mysterious ancient Jawi scripts. It may also increase the security strength of the block cipher pattern, though this may not be critical.

Keywords—cryptographs; ethno-mathematics; block-cipher;

I. INTRODUCTION

Most of the cyber attacks may be culturally 'para-normal' against the personal data and content of millions of individuals as shown by the 'eastern centric' targets (1). Unfortunately, the encryption algorithms (e.g., RSA, ECC) despite being the last layer of the Defense-in-Depth paradigm of current computer security systems could not produce the patterns to recognize such para-normal attacks. On the other hand, culturally based ethno-mathematics for non-parametric encryption paradigms can be conceptually premised to recognize the culturally biased attacks (2), (3), (4).

Personal data secured in block ciphers incorporates a sequence of permutation and substitution operations (6) and later evolved into product ciphers (7). Ethno-mathematics in computing product is a product cipher that operates on an appropriate block size and key-length standards against algebraic and abnormal attacks (8). This paper examines the development of pattern recognition of para-normal attacks from the 8-bit S-Boxes in 256-bit block patterns from a non-parametric ethno-mathematical extraction method of the non-parametric objects of the Al-Quranic Scripts (5). This research may be a new approach in cryptography based on non-parametric component combined with pseudo-random number generator to produce the S-Box that is supposedly resist**a**n**t** against **the algebraic (a parametric)** linear and differential cryptanalysis**.** Although the aim is the production of patterns, the security strength of the 256-bit block cipher is also considered as an added value to pattern recognition.

II. SYMBOLS USED IN PARA-NORMAL ATTACK

Examples of para-normal attacks are carried out by the use of seemingly normal letters such as shown in Figure 1 below.

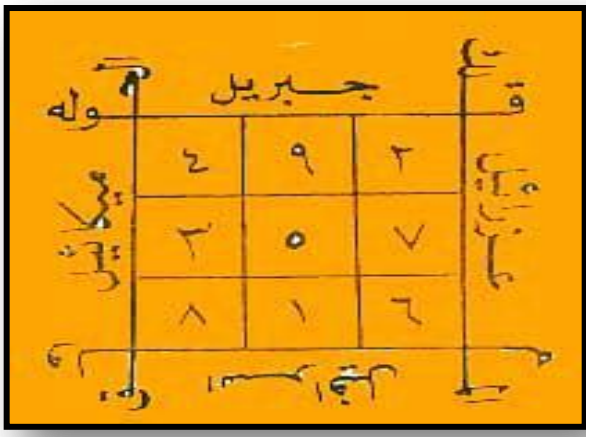


Figure 1:Ancient Scripts embedded with Arabic Letters on a template.
The para-normal object is a Hebrew letter lamed as : (. לi) with Hexadecimal code 05DC. Similarly another example is a seemingly normal series of letters with strange symbols as shown in Figure 2 below;

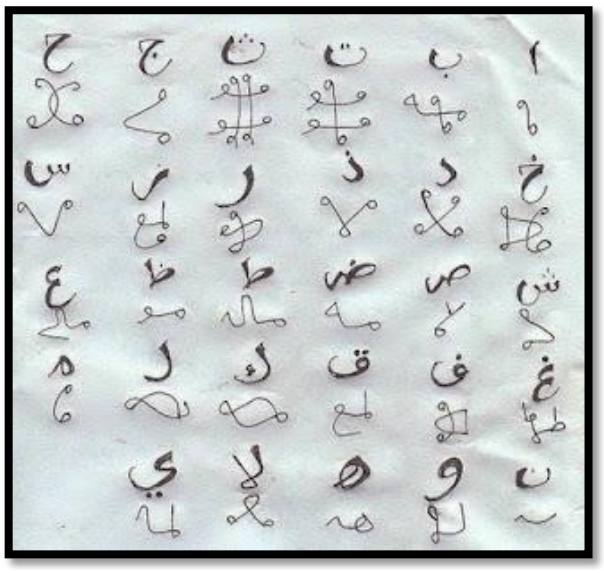


Figure 2: A template engraved with seemingly normal Letters alongside strange objects.

The letter Alif (ا) appeared alongside the Latin letter reversed esh loop with hexadecimal code FE8E as ﺎ

II. ETHNO-MATHEMATICS IN NOVEL S-BOX DESIGNS

The broader concept of ethno-mathematics includes "all culturally identifiable groups with their jargon, codes, symbols, myths, and even specific ways of reasoning and inferring" (9). The International Study Group of Ethno-mathematics (ISGE webpage, July 2009) emphasized the importance of ethno-mathematics in increasing the understanding of cultural diversity in mathematical practices. The philosophical argument, however, is that ethno-mathematics may be against the dominant views that mathematical truth is immutable, monolithic, universal and timeless (10). On the other hand, the epistemological argument for the ethno-mathematics of the Al-Qur'an encompasses a universal and immutable divine truth for mankind.

The special Qur'anic *Al-Muqatta'at* or sometimes known as *Fawatih* or openers such as *Yaasiin, Haamiim, Alif-Laam-Miim, Taa-Sii-Miim,* is that they are mysterious and their true meanings are not known to humans (11). The use of a protective ethno-mathematics of *Mu'awwidhahtain* is rooted from *Auz* which means to protect and fortify as found in Chapters *Al-Ikhlas, Al-Falak, Al-Nas*. Prophet Muhammad (peace and blessings of Allah unto him) recited the *Al-Mu'awwizatain* to form a protective barrier against shaytan and and their evil magics (12). The recitation of Ayatul Qursi is believed to be as safeguard from evil spirits (13). In general all the Qur'anic verses can be used as protector of the believers from all the temptations of the devil and as cure of all sicknesses (14).The epistemological argument for the special Quranic *Al-Muqatta'at* or sometimes known as *Fawatih* or openers such as *Yaasiin, Haamiim, Alif-Laam-Miim, Taa-Sii-Miim,* is that they are mysterious and their true meanings are not known to humans (9). The recitation of *Ayatul Qursi* is believed to be as safeguard from evil spirits (13). In general all the Quranic verses can be used as protector of the believers from all the temptations of the devil and as cure of all sicknesses (14).

The design of the *ethno-mathematical* Substitution-Box (S-Box) is the most crucial and critical component of the block cipher, especially their vulnerability to non-linear and abnormal attacks (15). Hardware implementations, in particular, necessitate the use of relatively small S-Boxes (16) explained in their work on the possibility of breaking a cryptosystem by defining the specific algorithm using algebraic relation of each of its

component. In AES the simplest algebraic form exists in the SubBytes function that does the substitution operation. AES is a non-Feistel model and can be implemented in software, hardware and firmware.

However, ethno-mathematics of Al-Quran and Al-Hadith, being symbolic and non-parametric would require a new approach as a departure from the traditionally algebraic S-Box designs. Thus the approach is to work on a cryptography with non-parametric combined with pseudo-random number components of S-Boxes. This may be a uniqure class of non-parametric cryptographs. It may seem to be a speculative approach because non-parametrics would avoid mathematical equations to prove whether the S-Box is secured. The motivation however, is the non-parametric nature of the Al-Quran and Al-Hadith that is the main premise of this work. The question is whether it is possible to use a semi-mathematical (ethno-mathematics) approach combined with pseudo-random number generator to provide a crypto system that is still resistant to algebraic attacks?

III. METHODOLOGY OF ETHNO-MATHEMATICAL S-BOX CONSTRUCTION

This unique work adopted the method of constructing perfect non-linear S-Boxes using *Maiorana-McFarland* approach in order for the S-Boxes to be "resistant" against linear cryptanalysis. That is XOR summation is used for extracting Quranic objects. Although there may be no strong evidences of previous studies on this method for the non-parametric Al-Quran, the conventional three methods of XOR summation, modular addition and modular multiplication were investigated. The second method, modular addition was rejected because it showed too many value collision compared to the other two methods. The third method, modular multiplication, was also rejected because the incapability of the computer to hold such a huge multiplication result (e.g., 0x83, 0x87, 0x8A, 0xB9, and 0xB5 to extract value from (گ ه يء ص).

Thus, the construction of semi-mathematical *Ethno-Mathematical* S-Boxes (or E- SBoxes) begins with the extraction of the non-parametric Quranic objects. The extraction process can be described as follows; Qura'nic object Q_i is denoted as the object that will be extracted, consists of k Arabic letters sequence from $q_1, q_2, ..., q_{k-1}, q_k$. The extracted value X_{Qi} is obtained from Q_i through the method below:

$$X_{Qi} = \bigoplus_{N=1}^{K} q_n$$

Where the value of $q_1, q_2, ..., q_k$ is the *least-significant byte* UTF-8 value of each single Arabic character such as 0x81 (ف), 0x88 (و), 0x8A (ي), and 0xA7 (ا) to 0xBA (غ) .

As a brief example, the extracted value from ((الم ا by splitting each of the letter as a single form of arabic character, not as the detail form of each letter (i.e. the character ل not counted as the initial form of لthat appeared in the beginning of a word). Therefore appear as, (a ل ⊕ م (الم ا
⊕ ١ = 0x85 ⊕ 0x84 ⊕ 0xA7 = 0xA6 [5].

,

The disadvantage of such method described above, is the possibility of more than one Quranic objects mapped to the same value, that the result of extraction of two different objects Q1 and Qj would give the same value. Moreover, some words appeared repetitively in other parts of the Holy Quran itself. Thus, based on these unique characteristics of the ApQuran, it is proposed that there will be two variants of *collisions*:

i. Object Collision (OC) is the collision that occur when two or more identical Quranic objects appeared in different components. For instance, the word (ي ا لنـ) is found in the *Al-Mu'awwidzatain* as well in *Ayatul Kursi*.

ii. Value Collision (VC) is the collision 1that occur when two or more different Quranic objects, Qi and Qj give the result

In constructing the 8-Bit Block Cipher, K_r is denoted as the key operated to each of the round of the block cipher as the output from key-scheduling algorithm. K_r is divided into two equal sub-key of K_r, denotes as K_{Lr} and K_{Rr}

$$K_r = K_{Lr} \;//\; K_{Rr}$$

From each of the sub-keys, is produced S_L and S_R as the seeds value for the *Linear Feedback Shift*

Register (LFSR) operation using 8-bit XOR-summation on each of the sub-keys.

$$S_L = \bigoplus_{n=1}^{8} K_{Lr(n)} = K_{Lr(1)} \oplus K_{Lr(2)} \oplus \ldots \oplus K_{Lr(8)}$$

$$S_R = \bigoplus_{n=1}^{8} K_{Rr(n)} = K_{Rr(1)} \oplus K_{Rr(2)} \oplus \ldots \oplus K_{Rr(8)}$$

S_R will be used to generate 22-bit LFSR output, that will split into A = 4 *bits*, B = 5 *bits*, C = 5 *bits*, and D = 8 *bits*. Later, the value of *A, B, C, D* will be used to generate random sequence number using another *LFSR* on each of the component (*A* → *Al-Muqatta'at*, *B* → *Al-Mua'wwidzatain*, *C* → *Ayatul Kursi*, and *D* → *Un-appeared Values*) to determine which of the extracted value that will be put inside the S-box. Whereas S_L will be used to generate 256 sequences, $E = i_1, i_2, \ldots, i_{256}$, of number that will determine the distribution of value from *Al-Muqatta'at*, *Al-Mu'awwidhatain*, *Ayatul Qursi*, and the *Unappeared Value* in order to distribute the extracted value from each component randomly on the S-boxes. Therefore, the output of LFSR (SL) will be neglected because of the unappeared values.

$LFSR_8(S_R) \rightarrow A \;//\; B \;//\; C \;//\; D$

$LFSR_8(S_L) = i_1, i_2, i_3, \ldots, i_{256}$

A, B, C and D will be processed as follows;

i. A is the seed of 4-bit LFSR that produces 13 numbers of random sequence, a1, a2, a3, ..., a13, used to determine which of the extracted value from *Al-Muqatta'at* component that will be put inside S-box randomly. The value of 14 and 15 are ignored.

ii. B is the seed of 5-bit LFSR that produces 19 numbers of random sequence, b1, b2, b3, ..., b19, used to determine which of the extracted value from *Al-Mu'awwidzatain* component that will be put inside S-box randomly. The value from 20 until 31 are ignored.

iii. C is the seed of 5-bit LFSR that produces 17 numbers of random sequence, c1, c2, c3, ..., c17, used to determine which of the extracted value from *Ayatul Kursi* component that will be put inside S-box randomly. The value from 18 until 31 are ignored.

iv. D is the seed of 8-bit LFSR that produces 207 numbers of random sequence, d1, d2, d3, ..., d207, used to determine which of the extracted value from *Unappeared Value* component that will be put inside S-box randomly. The value from 208 until 255 are ignored.

$LFSR_4(A) = a_1, a_2, a_3, \ldots, a_{13}$
$LFSR_5(B) = b_1, b_2, b_3, \ldots, b_{19}$
$LFSR_5(C) = c_1, c_2, c_3, \ldots, c_{17}$
$LFSR_8(D) = d_1, d_2, d_3, \ldots, d_{207}$

Finally, the S-box, denotes as S, is constructed using the random sequence , E = i1, i2, i3, ..., i256 as the index of the S-box S, and each of Si will be assigned by the value taken from *Al-Muqatta'at*, *Al-Mu'awwidzatain*, *AyatulKursi*, and *Unappeared Value* orderly by component but randomly by the value of each component.

$Siw = Aam\ (1 \le w \le 13)\ (1 \le m \le 13)$

$Six = Bbn\ (14 \le x \le 32)\ (1 \le n \le 19)$

$Siy = Cco\ (33 \le y \le 49)\ (1 \le o \le 17)$

$Siz = Ddp\ (50 \le z \le 256)\ (1 \le p \le 207)$

Whereas S_L will be used to generate 256 sequences, $E = i_1, i_2, \ldots, i_{256}$, of number that will determine the distribution of value from *Al-Muqatta'at*, *Al-Mu'awwidhatain*, *Ayatul Qursi*, and the *Unappeared Value* in order to distribute the extracted value from each component randomly on the S-boxes.

Finally, the S-box, denotes as *S*, is constructed using the random sequence $E = i_1, i_2, i_3, \ldots, i_{256}$ as the index of the M S-box, and each of S_i will be assigned by the value taken from *Al-Muqatta'at*, *Al-Mu'awwidhatain*, *Ayatul Qursi*, and *Unappeared Value* orderly by component but randomly by the value of each component.

The Ethno-Mathematical S-Box (or E-SBox) although for pattern recognition purposes may also

possess the low differential uniformity that will make the block cipher 'pattern' to resist against the differential cryptanalysis. Thus, this E-SBox 'pattern' with a non-linear step in the round faction will determine the block-cipher's resistance against linear cryptanalysis, as required by AES (Advanced Encryption Standard) [17]. Nevertheless, modern block-cipher designs, with increasing number of rounds can reduce the differential probabilities of the S-Boxes and make the cryptanalysis more difficult [18].

IV. RESULTS

A.Ethno-Mathematical E- SBoxes

The main components of the E-S Box are from *Al-Muqatta'at, Al-Muawwidhah, Ayatul Qursy* and Random Variables. As stated previously, *Al-Muqatta'at* (also known as *Fawatih*) shows the mysterious meaning and their true meanings are still not known. *Mu'awwidhatain* (rooted from *Auz*) is to protect and it is recited to protect against evil. The *Ayatul Qursi* is the protector of the devil and as cure of all sicknesses. In order to fill up the 256 bits the empty S-boxes need to be filled up after the previous 3 types of objects are used. These random variables are called the Un-appeared Values. There are characteristics that need to be fulfilled by the random objects which are termed collisions. The object used must be free from Object Collision (OC) which is when two identical Qur'anic objects appear in two different components.

The object must also be free from Value Collision (VC), which occur when objects give the same extraction value, thus it will be mapped in the same value. Currently, there are 13 *Al-Muqatta'at* objects, 19 *Al-Muawwidhah* objects and 17 *Ayatul Qursi* objects.

In a series of 207 value objects are from various Qur'anic sources [5]. The values that were successfully extracted to fulfill the remaining bits were using several phenomenon such as *Isra – Mi'raj, Asmaul Husna, Lailatul Qadr, Ummul Al-Qur'an (Al-Fatihah)* and *Juz 'Amma.*

13	84	88	12	81	81	80	83	80	81	86	82	85	80	15	06
14	04	13	05	82	09	04	83	80	82	80	81	05	85	80	94
87	00	81	87	07	80	80	12	87	09	85	90	05	80	83	81
81	03	03	85	10	86	80	80	81	81	85	87	83	81	81	87
80	08	81	86	02	81	02	81	01	85	14	03	84	00	90	86
80	06	80	81	87	05	81	13	04	00	80	84	81	83	80	13
81	80	81	02	04	04	85	84	03	81	80	80	83	02	00	02
80	05	91	90	86	80	12	01	81	02	91	01	81	80	08	81
08	04	81	80	00	83	81	07	85	81	90	83	01	05	06	80
01	00	81	01	81	80	81	81	86	81	08	81	08	80	84	86
05	80	04	04	80	04	80	80	00	02	07	87	85	80	80	04
80	81	00	80	04	80	81	85	82	82	80	80	02	81	00	91
05	81	10	03	05	07	03	80	01	08	81	84	04	14	82	81
80	03	84	87	80	81	81	81	14	81	81	80	82	81	80	87
81	02	03	08	00	82	04	05	80	07	01	81	08	02	12	84
06	81	10	14	08	81	00	10	00	03	82	80	80	94	82	07

Fig. 2. A 256 bit *Al-Mu'awwidhah* Product Cipher

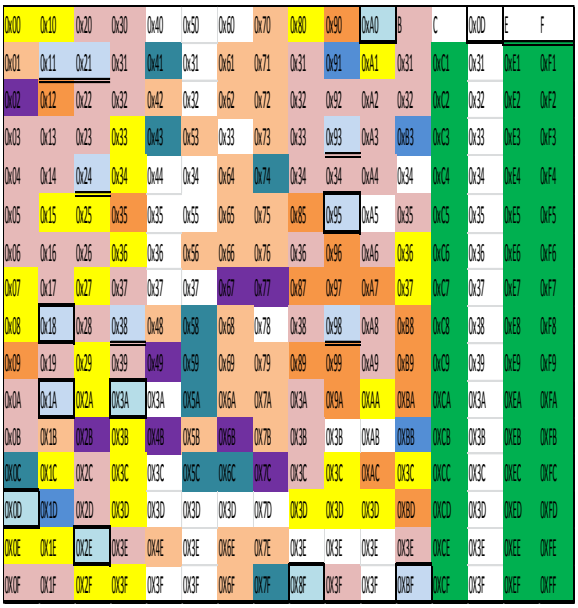
Arabic Unicode object extractions only reach hexadecimal 0x00 until 0x3f and 0x80 until 0Xbf. Several phenomena were tried to derive other When 128 bits of objects were achieved, attempts were made to extract other objects from several Unicode systems such as Indian, Hebrew and Turkey. Indian objects were successfully extracted and reached the values of hexadecimal 0xC0 until 0xCF. The Hebrew Unicode gives hexadecimal 0xE0 to 0xEF. Turkey Unicode gives hexadecimal value from 0xF0 until 0Xff.

At this point there were already about 176 bits of objects. In order to fulfill the rest of the objects, we try to extract more object values from alphabetic character through more *Surah* and selected *Hadith*. The generated object values scattered from 0x40 until 0x7F. Inclusive of alphabetic extractions about 216 bit S-Box were filled up by these objects.

The balance of 40 bits are from Random Variable object with two different stages of implementation to differentiate the objects extracted to produce a 256 bit product cipher.

B.Normal attack test pattern

The 256 bit product cipher becomes the eventual test pattern recognition for para-normal is shown below in Figure 3.



M S-Boxes tested 504,553 showing Non-Linearity (NL) and Differential Uniformity (DU) values.

The Green colored objects are extracted from the *Al-Quran* and *Al-Hadith*. The other colored objects are extracted from normal scripts. The white colored spaces are filled with random numbers and may be objects of para-normal attacks. However, to validate this, ancient Jawi Scripts are proposed to fill up the voids. Any other objects extracted from unknown scripts may presumably indicate the para-normal attack.

V. DISCUSSIONS

A. Expansion to Jawi Scripts

It is possible that new objects from Jawi Scripts are used since the early days of Malay Islamic civilization which can be used to fill up the unknown 40-bit M S-Boxes. The Hex values of those objects from the ancient Aramaic and Syriac languages do not fall in the Value Collision (VC) and Random Variable (RV) tables. Thus the objects from Jawi Scripts need to be expanded and used in RV table in the future in order to enhance the *Ethno-Maths* S-Boxes or E-SBoxes. Based on the 207 objects from RV and the rest are come from AMi, AMr and AMs total objects for 256 bit Block-Cipher are achieved though with a low security strength against algebraic attacks.

The potentials of extracting ethno-mathematical objects from the Jawi scripts are shown by their elusive and mysterious insignia in manuscripts and stone tables in the Malay World that extended to Champa, Jawa and Patani [12].

Fig. 3. Terengganu stone dated 702 H (1303 AD)

For example, the Terengganu Stone (shown in Figure 3 above) was 'hidden' under the footsteps of an ancient mosque in Ulu Terengganu. It was later accidently discovered to be a stone tablet written fully in Jawi Script. It is believed to be the oldest Jawi inscriptions found in the Malay World. An interpretation of the inscriptions indicates the proclamation of the 10 basic Islamic tenets for the Muslims to uphold. The true 'coded' meanings behind the Jawi scripts, however remain a mystery up to today. It may hold the "Da Vinci code" of the Malay world for the unbreakable information security and the secret link that kept the Malay world well communicated. Possibly, other similar stone tablets in other parts of the Malay world may fit in the jig-saw puzzle.

An evidence is in the Risalah of Sheikh Yusuf: *Al-Tuhfat al-Sailliyya, Hubbul-Ward, Tuhfat Al-Labib* –'studied' from 7 'wali' of Gunung Bawakaraeng. The other is the 'Rajang' system similar to Hindu Nakshatras and Arabic Anwa: Haribulan 21 – arang, arang, harang, harang . The Chinese 'images' in Syair Rajang, Syair Rakis, Silsilah Raja-Raja Berunai, Shaer Yang Di-Pertuan. In essence the knowledge of '*Firasat*' in *Hikayat Hang Tuah, Taj-al-Salatin, Bustan al-Salatin, Naqlin Bustanul al-Arifin, Tajul Muluk: Firasat Qiafat*: "dahi sempit-kurang budi dan bicara; tubuh warna merah lagi halus-pemalu" [19].

B.Comparisons with other methods.

TABLE 1. ALGEBRAIC ATTACK TEST RESULTS OF M S-BOXES

Differential Uniformity (DU) →

	NL ↓	DU	0	2	4	6	8
	0		**7**	**1**			
	2		**9**	**30**	**2**		
	4		**23**	**05**	**7**	**0**	
	6		**309**	**803**	**62**	**4**	**6**
	8		**040**	**1574**	**443**	**16**	**9**
	0		**1330**	**7900**	**325**	**74**	**0**
	2		**5426**	**3446**	**1247**	**18**	
	4		**3729**	**1227**	**2987**	**84**	
	6		**1722**	**2**	**299**		
	8		**66**	**9048**	**4**		
				33			

[4]M S-Boxes tested 504,553 showing Non-Linearity (NL) and Differential Uniformity (DU) values.

The resistance of non-parametric Ethno-Mathematical SBoxes (E-SBoxes) against linear and differential algebraic (parametric) attacks as shown in Table 1 above with values of DU = 8 and NL= 92-96 are in a better position with S-Boxes Khazad (DU = 8, NL =96) and that of Anubis (DU = 8, NL = 96) although both use parametric design methods. The higher order AES S-Boxes using finite field design method has DU = 4 and NL = 112 [18]. Perhaps if the total 13,734,236 E-SBoxes were tested their resistance values against differential and linear algebraic attacks (cryptanalysis) may be improved.

Nevertheless the existence of 40 Bit non-character
but random S-Boxes may also be the contributing factor to its low resistance values compared to AES Block-Ciphers. Despite the non-parametric design of the *Muawwidhah* block cipher, its resistence is still being evaluated by the differential and linear cryptanalysis. The deviations in the M S-Boxes differentials can be minimized by increasing the number of rounds.

VI. CONCLUSION

An unconventional technique of producing AES equivalent 256 bit S-Box construction is now possible with the non-parametric *Al-Quran, Al-Hadith* and other ancient script objects. However, in this study the ethno-maths are applicable to discrete objects from the Al-Qur'an, Al-Hadith and known Scripts. In practice though, the mysterious para-normal scripts in manuscripts and stone tablets are in continuous calligraphic forms. The challenge now will be the further development of the pattern recognition software that may be enhanced through extractions of more objects from the 'hidden' Jawi manuscripts and tablets.

REFERENCES

[1] Thomas, F. Budinger & Miriam D. Budinger *Ethics of emerging technologies-scientific facts - Moral challenges*, John Wiley & Sons, Inc. New Jersey, 2006.

[2] Savage-Smith, Emile, ed. (2004). *Magic and Divination in Early Islam. The Formation of the Classical Islamic World*, vol. 42, Ashgate Publishing, 2004.

[3] Ibn Mayor, Shem Tov (Late 14th Century A.D.).*Ha Ma'or ha-Gadol*, Ms. Oxford, Bodl, 228, fol. 103a. (In Dov Schwartz. Astronomy in Ancient Judaism.The Encyclopedia of Judaism. 2nd Ed. Jacob Neusner, Alan J. Avery-Peck & William Scott Green, Vol. I, A-E. Brill Leiden, Boston, 2005).

[4] Douglas R. Stinson, *Cryptography Theory and Practice*, third ed., Chapman & Hall/CRC, 2006.

[5] A.Faizul Shamsudin, Rusydi Hasan Makarim, Abi Dzar Jaafar, Mardiana Muhammad Taufick. *Substitution-Box in Unique Class Encryption Al - Muqatta'at, Al-Mu'awwidhazatain and Ayatul Qursi*.(Technical Report), Research Management Centre, IIUM, Sept. 7, 2009.

[6] Jacques Patarin, *Generic Attacks on Feistel Schemes*, International Association for Cryptologic Research ePrint Archive. 2008.

[7] Jacques Patarin and Valerie Nachef and Come Berbain, *Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions*, International Association for Cryptologic Research ePrint Archive. 2007.

[8] National Institute of Standards and Technology, *Federal Information Processing Standards Publication 197*, Advanced Encryption Standards (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf). 26 November 2001.

[9] D'Ambrosio,U. . Ethnomathematics and its address in the history and pedagogy ofmathematics. InPowell,A.B. and Frankenstein,M., editors, Ethnomathematics. Challenging Eurocentrism in Mathematics Eucation, pages 13-24, State University of New York Press, Albany NY, 1997.

[10] Gerdes,P., .Ethno-mathematics as a new research field, illustraties by studies of mathematical ideas in African history. In Saldana, J.J., editor, Science and Cultural Diversity.Filling a Gap in the History of Science, pages 11-36, Cuardernos de Quipu, Mexico., 2001.

[11] Abdallah Yusuf Ali . *The Holy Quran-Text and Translation*, Kuala Lumpur: Islamic Book Trust ; *Al-Ikhlas*, *Al-Falaq*, *Al-Nas*, Pg. 634-635, 1994.

[12] *Sahih Al-Bukhari: Kitab al-Tibb, Bab Ruqyah al-Nabiyy.*Narration by 'Aisha on the superiority of the *Al-Muawwizah*

[13] *Al-Baqarah*; v.255, Pg. 37.

[14] *Al-Isra'*; v. 82, Pg. 268.

[15] Jacques Patarin, Generic Attacks on Feistel Schemes, International Association for Cryptologic Research ePrint Archive, 2008.

[16] Jacques Patarin,Valerie Nachef and Come Berbain , Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions, International Association for Cryptologic Research ePrint Archive, 2007.

[17] National Institute of Standards and Technology, Federal Information Processing Standards Publication 197, Advanced Encryption Standards (http://csrc.nist.gov/publications/fips/fips197/fpf-2001).

[18] Jonathan Katz & Yehuda Lindell (2015), *Introduction to modern cryptography*, (2nd Ed.), A Chapman & Hall Book.

[19]Testing Report submitted by MIMOS, 4 Sept. 2009.

[20] A.Faizul Shamsudin, Jamil Hashim, Wan Sabri Wan Yusof, Abd Rahman Najib (2016), The potential of Jawi ethno-mathematics in Al-Muawizzah (Protective) computing against paranormal attacks, *Proceedings Seminar Tulisan Jawi dan Teknologi*, Universiti Malaysia Pahang, Gambang Pahang, Malaysia.