International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Fuzzy-Word Based Cryptosystem

Ashutosh Pandey[1], Vikas Kumar Jain[2], Dharamveer Singh[1], Sunil Kumar Kashyap[3]
[1]Department of Mathematics, Kalinga University, Raipur, Chhattisgarh, India
[2]Department of Chemistry, Govt. Engineering College, Raipur, Chhattisgarh, India
[3]Department of Mathematics, School of Advanced Sciences, Vellore Institute of Technology University, Vellore, Tamil Nadu, India

ABSTRACT

A hard mathematical problem interacts with cryptosystem. As Factorization and Discrete Logarithm based cryptosystems are RSA and ElGamal respectively. This paper presents new hard problem as fuzzy-word computing and then its applies on cryptography.

Keywords: Factorization, Discrete Logarithm, RSA, ElGamal, Cryptosystem

I. INTRODUCTION

Information and mathematics are the two different words. But these two distinct words are adjoined in the year 1948, when C. E. Shannon presented the new idea as "A Mathematical Theory of Communication". This became a landmark of the existed world of electronic communication.

Nature is itself based on the communication by coding. The uniqueness is the leading reason behind this. The modern world is inspired by the nature and its elements. Various electronic devices are based on the natural examples.

This study deals with the security of the information by fuzzy theory. Security is essential in communication by the protocol agreement between sender and receiver. The message sends with any hard mathematical problem via network. The original message is called plaintext. This plaintext represents as the ciphertext by the algebraic operation. Later this ciphertext converts into the plaintext. The conversion depends on the keys. Sender uses the public key of receiver and receiver uses the private key of own. This system is called cryptography.

The information transmits with security by a single reason i.e. system consist the hard mathematical problem. This is one of the important applications of the pure mathematics. Number theory is one of the purest branches of mathematics. Cryptography is one of the great modern applications of pure mathematics. Hence we are presenting a new dimension on cryptology interacted with fuzzy sets and logic. Next section is based on the review of literatures.

II. Literature Review

Zadeh [1] introduced the fuzzy as the new set in 1965. This set fulfils all the basic rules of the classical set theory. The new set theory is established by membership function. This is the set based on the classes. In 1979, he [2] presented the theory of reasoning. This is an approximation over the set. Another fundamental work came in the year 1983 when he [3] proposed some dimensions for the natural languages. The computational aspects for the languages are represented by the fuzzy quantifiers.

In 1972, De Luca et al [4] gave the definition of entropy in fuzzy set theory. A non-probabilistic concept is applied in fuzzy set.

Baruah [5] put another function called reference function in 1999. It is based on fuzzy membership and its subsets. In 2011, he [6] developed a field theory for the fuzzy sets. All the algebraic extension is defined on this theory. In the same year he [7] reviewed the fuzzy set theory via the basic structure of the classical set theory. The belief and realities are demonstrated in this article. This was the fruitful year of research for Baruha, he [8] tried to obtain the roots of the fuzzy polynomials. Its physical presence or absences are studied in this review. The measuring and approximating are applied for this.

In 2011, the entropy of fuzzy set is studied by Dhar [9]. Hwang and Yung's contribution on the roots of fuzzy set are reviewed by him. Next year, he [10] put a note on entropy of fuzzy sets. This was a generalised study of the fuzzy set over the physical study of entropy. In the same year, he [11] proposed a new theory on fuzzy indexing. Its separation and substitution are covered in this theory. In 2012, he [12] turned the fuzzy sets into the fuzzy numbers and its geometrical representations. In the same year, he [13] studied fuzzy sets as the symmetry rather than membership function. The conditions, similarity and comparison for the breaking the symmetry of fuzzy sets is presented in this paper. 2012 was the productive year for Dhar, when he [14] published five papers on fuzzy and its variants. Another work of him came as subsets of the fuzzy set in the same year. He constructed some basic rules for obtaining the fuzzy subsets.

Casasnovas et al [15] introduced the finiteness of fuzzy sets in 2003. They used scalar cardinalities with the t-norms and t-co-norms operation. In 1993, Li [16] presented a contiuum hypothesis on the fuzzy sets and its cardinality. Wygralak [17] approached to fuzzy sets towards the axiomatic relationship with the scalar cardinalities.

In 1985, Dubois et al [18] focused the modelling of fuzzy sets. The cardinality of fuzzy sets and its quantification are studied by them. They [19] evaluated the fuzzy sets over the scalar evaluation in 1990.

In 1980, Gottwald [20] wrote a note on the cardinals of the fuzzy set. Raselsu [21] proposed the fuzzy criteria under the context of cardinality, quantifiers and aggregation. In 2011, Bason [22] et al designed a system of analysis of the fuzzy attributes. This is based on discrete norms of fuzzy sets. Recently Janssene et al [23] measured the fuzzy sets via the transitivity.

The literature of Stavroulakis [24] covers almost all the topics of the information and communication related security. Juels et al [25] drafted an idea towards fuzzy based security systems in 1999. The extension of this work came in the existence in the year 2002, when they [26] modified their scheme.

In 2001, Chang et al [28] proposed the new cryptographic protocol based on the bio-mechanism. Vielhauer et al [29] presented a scheme based on statistical approach with the digital signature scheme.

In 2006, Dodis et al [29] introduced a scheme based on fuzzy extraction. They provided some techniques for developing the strong keys. The biometrics and noisy data are used under this study. Nowadays several works has been initiated based on this method.

Margarov [30] developed a secret sharing protocol based on fuzzy vault in the year 2009. This is also referred as the secure and efficient cryptosystem in the world of security.

In 2004, Savvides et al [31] designed a device by face recognition technique. The biometric filter based system is designed for the upgrading the security. Jain et al [32] presented a new system based on the fingerprint resolution in 2000. This is a system called as filterbank.

A new cryptosystem came in the existence in the year 2004 called biometric cryptosystem. This is invented by Uludag et al [33]. In the same year Lin et al [34] generated a biometric authentication device. Clancy et al [35] proposed an authentication system based on the finger print technique in the year 2003.

In 2004, Uludag et al [36] set a security system based on fuzzy configuration. Fuzzy is generalised in this paper with finger print characterisation.

This study is based on the discrete study of fuzzy sets and its application in cryptography. Fuzzy sets are based on the membership function and this characteristic will be used over the security performances.

III. METHODS AND MATERIAL

Arduino **Fuzzy Analysis:** An analysis of fuzzy set and fuzzy logic is presented here. This will be base for the proposed cryptosystem.

Fuzzy Set Analysis: Although this set is defined by class and membership function but here we study this set over the security aspects.

The crisp set: $X = \{x\}.$

Membership function: $f_A(x) \to [0,1].$

$$f_A(x) = 1 : x \in A,$$
$$or$$
$$f_A(x) = 1 : x \notin A.$$

Hence,

The fuzzy set will be,

An ordered pair: $(X, f_A(x)) : x \in X, or, (X,[0,1]).$

Cryptosystem is a security system under the probable security (Much or more or most). An attack is defined as another cryptosystem which is equivalent to the existed. Let A and B be the two cryptosystems, then it will be said to equal if A = B. By fuzzy it is defined as below:

$$A = B,$$
$$or,$$
$$f_A(x) = f_B(x),$$
$$or,$$
$$f_A = f_B.$$

The complement is defined as;

$$f_{A'} = 1 - f_A.$$

Next, the fuzzy set is reviewed under the context of cryptography in below:

Let,

The set of message be $M = \{m_1,...,m_n\}.$

Or,

The message as string represented by,

$$S = m_1...m_n ; m_i \in 0 \text{ or } 1.$$
$$eg.$$
$$S = 0110100101\ 01.$$

Let the membership function is defined as “secure”. Let the fuzzy set be A, which will be defined as follows:

$$f : secure,$$
$$or,$$
$$f : probability(m_i) > 0,$$
$$or,$$
$$f : 0 < probability(m_i) \le 1,$$

Then the fuzzy set will be represented by,

$$f_A(m_1) = 0,$$
$$f_A(m_2) = 0,$$
$$.$$
$$.$$
$$.$$
$$f_A(m_k) = 0.1,$$
$$.$$
$$.$$
$$.$$
$$f_A(m_l) = 0.3,$$
$$.$$
$$.$$
$$.$$
$$f_A(m_m) = 0.7,$$
$$.$$
$$.$$
$$.$$
$$f_A(m_n) = 1.$$

Hence the fuzzy set will be:

$$A = \{0/m_1...0.7/m_m,..,1/m_n\}.$$

Similarly, the set of message can be represented for the fuzzy membership function defined “insecure” as below:

$$f : insecure,$$
$$or,$$
$$f : probability(m_i) < 1,$$
$$or,$$
$$f : 0 \le probability(m_i) < 1,$$

Then the fuzzy set will be represented by,

$$
\begin{array}{l}
f_A(m_1) = 1, \\
f_A(m_2) = 0.7, \\
. \\
. \\
. \\
f_A(m_k) = 0.5, \\
. \\
. \\
. \\
f_A(m_l) = 0, \\
. \\
. \\
. \\
f_A(m_m) = 0, \\
. \\
. \\
. \\
f_A(m_n) = 0.
\end{array}
$$

Hence the fuzzy set will be:

$$A = \{1/m_1 ... 0.7/m_m, .., 0/m_n\}.$$

In above, it is discussed that the fuzzy set considered on the basis of membership function as “secure” and “insecure”. This can be generalised with “much, more and most” for both secure and insecure.

The fuzzy rule is required here because there are existed some conditions. Generally fuzzy rule is used when the linguistic variable needs to convert into the numerals. Here everything is based on the binary process.

Thus the binary fuzzy rule is presenting as per the cryptographic requirements in below:

$$
\begin{array}{l}
If \rightarrow Then, \\
If : probability(message) = 0, \\
Then : cryptosystem(\text{secure}). \\
If : probability(message) \neq 0, \\
Then : cryptosystem(in\text{secure}).
\end{array}
$$

The structure of any cryptosystem as per the fuzzy set will be redefined as below after the conventional cryptosystem:

$$
\begin{array}{l}
Cryptosystem : \\
input \\
\downarrow \\
pla\text{int}\ ext \\
\downarrow \\
encryption \\
\downarrow \\
transmission \\
\downarrow \\
ciphertext \\
\downarrow \\
decryption. \\
\downarrow \\
output
\end{array}
$$

$$
\begin{array}{l}
Fuzzy - Cryptosystem : \\
input \\
\downarrow \\
pla\text{int}\ ext \\
\downarrow \\
fuzzification \\
\downarrow \\
encryption \\
\downarrow \\
transmission \\
\downarrow \\
ciphertext \\
\downarrow \\
decryption. \\
\downarrow \\
defuzzification \\
\downarrow \\
output
\end{array}
$$

Here, the fuzzification and defuzzification will be analysed. These provide the extra security with the same efficiency. The fuzzy encryption is presenting in below:

IV. RESULTS AND DISCUSSION

Fuzz Encryption: The plaintext converts in to the ciphertext by the fuzzification. The process will be discussed in the next para.

4.1. The Plaintext;

Let, The message be *m*. This is also called an original message or plaintext. There is no need to fuzzification to the message.

The message will be used in encryption originally. But another direction on the plaintext will be discussed in this study.

The word will be treated as the number. Hence the problem with number generalises with the problem with message.

4.2. The Hard Mathematical Problem (HMP): This is the base of any cryptography. All cryptosystems are based on any mathematical problem, e.g. factorization, discrete logarithm etc. In this idea, we do not use the HMP but will use the new hard problem based on the fuzzy called the fuzzy hard problem (FHP). The message and the FHP will be performed together by the fuzzy process.

The message and the FHP will be treated as the two distinct sets and the fuzzy as the characterisation tool.
In the next subsection, FHP is given.

4.3. FHP: Although Zadeh [37] introduced the fuzzy based computation in 1996. He suggested the new fuzzy methodology of computation by fuzzy called computation with words. Here we establish this idea as FHP.
Let,
The original message be *m* represented as follows:

$$m = f(A) : A = Alphabet,$$

As we know that, message is the set of words with the rule called grammar.

We define the grammar rule by the binary operation rule. As the number follows the binary rule, the same generalisation will be applied on the words also.
The fuzzy cryptosystem is presented in below:

4.4. Fuzzy Encryption:

The mapping presents as below:
Let a word be,

$$w = f(l) : l = letters.$$

As the string, the word *w* is presented as,
$w = w_1 w_2 ... w_n$.

The mapping of the binary operation with the string of two letters is presented in below:

$$+ \to ab \to a+b$$
$$- \to ba \to b-a$$
$$\times \to aa \to a \times b$$
$$\div \to ac \to c \div a$$

The illustration is given in below:
Let a word be “no”. It is performed as below:

$$\begin{array}{l} no \\ \downarrow \\ n*o \\ \downarrow \\ n+l+m+n+o \end{array}$$

The word i.e. the plaintext “no” became the ciphertext as $"n+l+m+n+o"$.

The additional term is $l+m+n.$
Now, apply the fuzzy principle as:
The membership function: “+”.
The fuzzy set: $(\{n,o\}, n+l+m+n+o).$

There will be unique $"l+m+n"$ for the word “no”.

How we decrypt the ciphertext, the next subsection lies with this:

4.5. Fuzzy Decryption:

The received message or the ciphertext is,

$$"n+l+m+n+o".$$

The applied algebraic operation will be shifted by the fuzzy operation as below:
Let A be the applied membership function as:

$$A : n*o.$$

B is another membership function as:

$$B : l+m+n.$$

The fuzzy operation for these two membership functions is denoted as:

$$f_{AB} = f_A . f_B .$$

$$f_{A+B} = f_A + f_B$$

.

$$f_{A-B} = f_A - f_B$$

$$f_{A/B} = f_A / f_B .$$

Hence the fuzzy decryption will be proceeded as the inverse fuzzy operation of addition i.e. subtraction.
The ciphertext holds the following condition:

The original message = $f_B - f_A$.

V. CONCLUSION

Although cryptography started for the security of the message only in ancient but now it has generalised the digital society. Message transformation has become a science today. Recently biological aspect of the cryptography has launched. The natural secret also lies with this domain.

Hence the current work will be directed the future plan towards the security. This study is presented as the application of the fuzzy set and cryptography both. Zadeh's contribution was the landmark in the development of real mathematical application but today this has been applied in almost every field of the society.

VI. REFERENCES

[1]. L. A. Zadeh, "Fuzzy Sets", Inform. and Control, vol. 8, (1965), pp. 338-353.

[2]. L. A. Zadeh, "A theory of approximate reasoning", Machine Intelligence, vol. 9, (1979), pp. 149-194.

[3]. L. A. Zazeh, "A computational approach to fuzzy quantifiers in Natural Languages", Computation and Mathematics, vol. 9, (1983), pp. 149-184.

[4]. A. De Luca and S. Termini, "A definition of non probabilistic entropy in the settings of fuzzy set theory", Information and Control, vol. 20, (1972), pp. 301-312.

[5]. H. K. Baruah, "Fuzzy Membership with respect to a Reference Function", Journal of the Assam Science Society, vol. 40, no. 3, (1999), pp. 65-73.

[6]. H. K. Baruah, "Towards Forming a Field of Fuzzy Sets", International Journal of Energy Information and Communications, vol. 2, no. 1, (2011), pp. 16 - 20.

[7]. H. K. Baruah, "Theory of Fuzzy sets Beliefs and Realities", International Journal of Energy, Information and Communications, vol. 2, no. 2, (2011), pp. 1-22.

[8]. H. K. Baruah, "In Search of the Root of Fuzziness: The Measure Theoretic Meaning of Partial Presence", Annals of Fuzzy Mathematics and Informatics, vol. 2, no. 1, (2011), pp. 57 - 68.

[9]. M. Dhar, "On Hwang and Yang's definition of Entropy of Fuzzy sets", International Journal of Latest Trend Computing, vol. 2, no. 4, (2011), pp. 496-497.

[10]. M. Dhar, "A Note on existing Definition of Fuzzy Entropy", International Journal of Energy Information and Communications, vol. 3, no. 1, (2012), pp. 17-21.

[11]. M. Dhar, "On Separation Index of Fuzzy Sets", International Journal of Mathematical Archives, vol. 3, no. 3, (2012), pp. 932-934.

[12]. M. Dhar, "On Geometrical Representation of Fuzzy Numbers", International Journal of Energy Information and Communications, vol. 3, no. 2, (2012), pp. 29-34.

[13]. M. Dhar, "On Fuzzy Measures of Symmetry Breaking of Conditions, Similarity and Comparisons: Non Statistical Information for the Single Patient", International Journal of Mathematical Archives, vol. 3, no. 7, (2012), pp. 2516-2519.

[14]. M. Dhar, "A Note on Subsethood measure of fuzzy sets", International Journal of Energy, Information and Communications, vol. 3, no. 3, (2012), pp. 55-61.

[15]. J. Casasnovas and J. Torrens, "Scalar cardinalities of finite fuzzy sets for t-norms and t-conorms", Int. J. Uncertain. Fuzziness Knowl. -Based System, vol. 11, no. 5, (2003), pp. 599-614.

[16]. H. x. Li, "The cardinality of fuzzy sets and the continum hypothesis", Fuzy Sets and Systems, vol. 55, (1993), pp. 61-78.

[17]. M. Wygralak, "An axiomatic approach to scalar cardinalities of fuzzy sets", Fuzzy sets and Systems, vol. 110, no. 2, (2000), pp. 175-179.

[18]. D. Dubois and H. Prade, "Fuzzy cardinality and Modelling of impresice quantification", Fuzy sets and System, vol. 16, (1985), pp. 199-230.

[19]. D. Dubois and H. Prade, "Scalar evaluation of Fuzzy sets", Appl. Math. Lett., vol. 3, no. 2, (1990), pp. 37-42.

[20]. S. Gottwald, "A note on fuzzy cardinals", Kybernetika, vol. 16, (1980), pp. 156-158.

[21]. D. Raselsu, "Cardinality, quantifiers and the aggregation of fuzzy criteria", Fuzzy Sets and Systems, vol. 69, (1995), pp. 355-365.

[22]. Y. Bason, D. Neagu and M. J. Ridley, "Fuzzy Set Theoretic Approach for Comparing Objects with Fuzzy Attributes", 11th International Conference on Intelligent Systems, Design and Applications, (2011), pp. 754- 759.

[23]. S. Janssens, B. de Baets and H. de Meyer, "Transitivity of Comparision Measures", Fuzzy Systems, (2002), pp. 1369-1372. International Journal of Energy, Information and Communications Vol. 4, Issue 1, February, 2013.

[24]. Peter Stavroulakis, Mark Stamp: Handbook of Information and Communication Security. Springer 2010, ISBN 978-3-642-04116-7

[25]. A. Juels, M. Wallenberg: A Fuzzy Commitment Scheme, Proc. 6th ACM Conference on Computer and Communications Security, Singapore (1999) pp. 28-36

[26]. A. Juels, M. Sudan: A Fuzzy Vault Scheme, Proc. IEEE Int. Symposium on Information Theory, Lau-sanne (2002) p. 408

[27]. Y. J. Chang, W. Zhang, T. Chen: Biometrics Based Cryptographic Key Generation, Proc. IEEE Conference on Multimedia and Expo, Taipei, Vol. 3 (2001) pp. 2203-2206

[28]. C. Vielhauer, R. Stcinmctz, A. Maycrhofcr: Biomctric Hash Based on Statistical Features of Online Signatures, Proc. 16th Int. Conference on Pattern Recognition, Quebec, Vol. 1 (2002) pp. 123-126

[29]. Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, Technical Report 235, Cryptology ePrint Archive (February 2006)

[30]. G Margarov, M Tolba, Biometrics based secret sharing using fuzzy vault. 7th IntConf on Computer Science and Information Technologies (CSIT'09) (2009), Singapore.

[31]. M. Savvides, B.V.K. Vijaya Kumar, and P.K. Khosla, "Cancelable biometric filters for face recognition", ICPR, 23- 26 Aug. 2004, pp. 922-925 Vol.3.

[32]. A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based Fingerprint Matching", IEEE Trans. Image Process., 2000, 846-859.

[33]. U. Uludag, S. Pankanti, S. Prabhakar, and A.K Jain, "Biometric cryptosystems: issues and challenges", Proceedings of the IEEE, Volume 92, Issue 6, June 2004, pp. 948 - 960.

[34]. C. H. Lin, and Y.-Y. Lai, "A flexible biometrics remote user authentication scheme", Computer Standards & Interfaces, Volume 27, no. 1, Nov. 2004, pp. 19-23.

[35]. T. C. Clancy, N. Kiyavash, and D.J. Lin, "Secure smartcard-based fingerprint authentication", ACM Workshop on Biometrics: Methods and Applications, Nov. 2003, pp. 45-52.

[36]. U. Uludag, A. Jain, "Fuzzy Fingerprint Vault", Proc. Workshop: Biometrics: Challenges Arising from Theory to Practice, pp.1316, Aug 2004.

[37]. L. A. Zadeh, Fuzzy Logic = Computing with words, IEEE Transactions on Fuzzy Systems, 4(2), 1996.