Tec Empresarial
P-ISSN: 1659-2395; E-ISSN: 1659-3359

ON CATEGORY MORPHISM-TAKUGI-SUGINO OUTPUT FUNCTION BASED COMPACT CYBER SECURITY PROTOCOL

A J Khan[1], Vinita Dewangan[2], Sunil Kumar Kashyap[3], Romibala[4]
[1]Professor Mathematics, MATS University, Raipur, khanaj@matsuniversity.ac.in

[2]Assistant Professor, MATS University, Raipur, dr.vinitad@matsuniversity.ac.in

[3]Professor Mathematics, MATS University, Raipur, drsunilkk@matsuniversity.ac.in
[4]Research Scholar, MATS University, Raipur, lilly123114@gmail.com

ABSTRACT

This paper proposes the compact protocol for developing cyber security system in context to security and efficiency. The security is achieved through the category morphism over the fuzzy graph. The fuzzy graph coloring is studied in discrete membership function. The permutation based fuzzy graph-categroy morphism based matrix generates the computational chaos, which creates the computational complexity for the attackers, thus its application comprises with the cyber security systems. The chaotic complexity is performed in one way and this characteristic applies to set the digital security system but another way is fast by Takugi-Sugino output function, this provides the efficiency advantage. This compact category morphism-Takugi-Sugino output phenomenon constructs the secure network protocol for developing cyber security system.

Key Words: Category, Morphism, Fuzzy Graph, Takugi-Sugino Output Function.

1. Introduction: In 1965, Zadeh [1] introduced the new thought on the collection of objects through the membership approach. This new idea on set theory is referred as the fuzzy set. Fuzzy set is based on the grading or the classification of objects. Thus, the set is classified in two types majorly, crisp set and fuzzy set. Later this theory became very popular by its significant application in real world problems, viz. automatic washing machine, automatic camera, robotics, surgery, transport, space, industrial machinery etc. In modern research, fuzzy is associated with artificial intelligence, machine learning and automation which left huge impact on scientific and technological societies.

Zadeh [1,4] introduced the discrete thought of fuzzy based on classification of objects through the membership function. This is discrete than the conventional set which is based on just a collection of well defined objects. This is not just a collection of objects but classification of objects through the membership function. Thus, Zadeh gave the new name of this set, fuzzy set. Later, it is generalized into fuzzy logic, fuzzy rule, fuzzy coloring etc. This becomes so popular by its application in real world problems. There exist several applications [2-9], e.g. information theory, automation, diagnosis, artificial intelligence, business and industries, medicine and surgery etc.

Gehrke et al. [10] studied the fuzzy set by piecewise interval decomposition approach. The constant membership function is generalized for obtaining the piecewise membership function. Greenfield et al. [15] extended the preceding result with fuzzy logic in 2016. This is an extension for complex valued function with discrete fuzzy rules. In 2021, Nasir et al. developed a mechanism for curing the disease. This mechanism is based on fuzzy relation and complex fuzzy logic rules. This work is inspired by Chen et al. [17] whose complex fuzzy set and its neurofuzzy architecture. Li [27] developed a data analysis model based on intuitionistic fuzzy sets. This was a discrete approach to redefine fuzzy set. Although, in 2001, De et al. [28] applied the intuitionistic fuzzy set for diagnosis the critical disease. The intuitionistic fuzzy set also used in [29-30] for obtaining the optimum solution.

In 1976, the concept of public key cryptography appeared. Basically this was a key agreement protocol as the application of number theoretic hard problem. The discrete logarithm problem [DLP] based key exchange protocol was introduced by Diffie et al. [31]. In 1985, first real and practical system is developed based on the preceding key agreement protocol. This is an equivalent secure and efficient as RSA, elliptic curve etc [33-36]. Efficiency and security both are key parameters for any security system, ElGamal and RSA both are credited as the real systems but efficiency is not as much as expected. Thus, elliptic curve based system exists for both the challenges. Some examples are [37, 39-45]. There are some discrete security systems based on the corresponding discrete approach, i.e. XTR, Hyper elliptic, Non-Abelian etc. [45-50]. In modern world, there are various new ideas are appearing frequently, e.g. cryptocurrency, digital signature, compact artificial intelligence, transporting models, space crafts, etc.

2. Preliminaries: In this section, fuzzy set and its application is presented.

2.1. **Fuzzy Set:** Let, the space be X, the generic element of $X = x$, A fuzzy set (class) = $A; A \in X$. Then, its characterization is defined by a membership function $= f_A(x)$, Such that, $x \in [0,1]$, the membership; $x \in A$. Hence, $f_A(x) = 1$, the higher grade of the membership: $x \in A$, as the conventional set theory term, $A = \{0,1\}$, over

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

Next, the fuzzy set is explained with an example.

2.2. **Example of Fuzzy Set: Let,** the real number be X, the fuzzy set of real numbers which are much greater than 5, Then, $f_A(x) \in R$, Its functional value might be;

$$f_A(0) = 0;$$
$$f_A(5) = 0;$$
$$f_A(9) = 0.01;$$
$$f_A(106) = 0.3;$$
$$f_A(999) = 0.89;$$
$$f_A(10000) = 1.$$

Next, the definition of graph is presented. The concept of graph is introduced by Euler in 1735.

2.3. **Graph: If** $G(V,E); V = \{v_1,...,v_n\}, E = \{e_1,...,e_n\}$, where V is the set of vertices and E is the set of edges, then $G(V,E)$ is said to be a graph. This can also be noted by crisp graph.

Next, graph coloring is defined through k-coloring of crisp graph.

2.4. **k-Coloring of Crisp Graph:** Let the map be f. If f is defined from V to the set of k-elements $\{1,2,...,k\}$ such that $f(u) \neq f(v); u,v \in E$, then it is called k-coloring of graph $G(V,E)$.

Next, the concept of fuzzy graph is explained. Kaufmann introduced the fuzzy graph $\tilde{G}(V,\tilde{E})$.

2.5. **Fuzzy Graph:** Let $\tilde{G}(V,\tilde{E})$. be a fuzzy graph, where V is the vertex set and $\tilde{E}$ is the fuzzy edge set characterized by the matrix $\mu = \mu(u,v)_{u,v \in V} : \mu(u,v) = \mu_{\tilde{E}}(u,v); u,v \in V; u \neq v, \mu_{\tilde{E}} : V \times V \to I$ is the membership function.

The concept and application of fuzzy graph coloring are presented through a monotone family of sets defined by chromatic number of $\tilde{G}$. .

2.3. Fuzzy Graph Coloring (FGC): If $G(V,E)$ is a fuzzy graph, where $V = \{1,2,...,n\}$ and is a fuzzy number on the set of all the subsets of $V \times V$. Assume $I = A \cup \{0,1\}$, where $A = \{\alpha_1 \leq ... \leq \alpha_k\}$ is the fundamental set of $\tilde{G}$. For each $\alpha_i \in I$, G_{α_i} denotes the crisp graph $G_{\alpha_i}(V, E_{\alpha_i}); E_{\alpha_i} = \{(u,v); \mu(u,v) \geq \alpha_i\}$ and $\chi_{\alpha_i} = G(\chi_{\alpha_i})$ denotes the chromatic number of crisp graph $G(\chi_{\alpha_i})$.

This can be extended for variants of fuzzy graph coloring. The next definition is an important approach of modern algebra, i.e. category.

2.4. Category: A category C consists of a class of objects and sets of morphisms between those objects. Next, some results on FGC are presented.

3. Results on FGC: The following theorems will be applied to develop the cyber security protocol.

3.1. **Theorem:** Let $G(V,E)$ be a fuzzy graph, where $V = \{v_1,...v_n\}$, and $E = \{e_1....e_n\}$ the membership function of $\tilde{E}$ be

$$\mu = \begin{bmatrix} - & 0 & . & . & \mu(v_1, v_n) \\ 0 & - & 0 & . & . \\ . & 0 & - & 0 & . \\ . & . & 0 & - & 0 \\ . & . & \mu(v_n, v_{n-m}) & 0 & - \end{bmatrix}$$

and

the complement of $\mu(v_{i,} v_j); i, j = 1,2,\ldots,n$ is defined by $\overline{\mu}(v_i, v_j) = 1 - \mu(v_i, v_j)$ represented by matrix

$$\overline{\mu} = \begin{bmatrix} - & 1 & . & . & \overline{\mu}(v_{1,} v_n) \\ 1 & - & 1 & . & . \\ . & 1 & - & 1 & . \\ . & . & 1 & - & 1 \\ . & . & \mu(v_{n,} v_{n-m}) & 1 & - \end{bmatrix},$$

Then, there exists a category C.

Proof: By definition of category,

For every $(\mu, \overline{\mu})$, there exists a set

$$Hom_C(\mu, \overline{\mu})$$

Which is morphisms from $\mu \to \overline{\mu}$, or

$$\begin{vmatrix} - & 0 & . & . & \mu(v_{1,} v_n) \\ 0 & - & 0 & . & . \\ . & 0 & - & 0 & . \\ . & . & 0 & - & 0 \\ . & . & \mu(v_{n,} v_{n-m}) & 0 & - \end{vmatrix} \to \begin{vmatrix} - & 1 & . & . & \overline{\mu}(v_{1,} v_n) \\ 1 & - & 1 & . & . \\ . & 1 & - & 1 & . \\ . & . & 1 & - & 1 \\ . & . & \overline{\mu}(v_{n,} v_{n-m}) & 1 & - \end{vmatrix}.$$

Consider, a membership function $\widetilde{\mu} \in \widetilde{G}$ and its matrix representation will be

$$\mu = \begin{bmatrix} - & 0 & . & . & \widetilde{\mu}(v_1, v_n) \\ 1 & - & 0 & . & . \\ . & 1 & - & 0 & . \\ . & . & 1 & - & 0 \\ . & . & \widetilde{\mu}(v_n, v_{n-m}) & 1 & - \end{bmatrix}.$$

Then, the composition of morphisms is defined by

$Hom_C(\mu, \overline{\mu}) \times Hom_C(\overline{\mu}, \widetilde{\mu}) \to Hom_c(\mu, \widetilde{\mu})$ over the morphisms

$$\begin{bmatrix} - & 1 & . & . & \bar{\mu}(v_1,v_n) \\ 1 & - & 1 & . & . \\ . & 1 & - & 1 & . \\ . & . & 1 & - & 1 \\ . & . & \mu(v_n,v_{n-m}) & 1 & - \end{bmatrix} \rightarrow \begin{bmatrix} - & 0 & . & . & \tilde{\mu}(v_1,v_n) \\ 1 & - & 0 & . & \\ . & 1 & - & 0 & . \\ . & . & 1 & - & 0 \\ . & . & \tilde{\mu}(v_n,v_{n-m}) & 1 & - \end{bmatrix}.$$

There exist the 3 fuzzy graphs, $\tilde{G}_{\mu}(\tilde{V},E),\tilde{G}_{\bar{\mu}}(\tilde{V},\tilde{E}),\tilde{G}_{\tilde{\mu}}(\tilde{V},E)$.

Its matrix representation will be

$$\tilde{G}_{\mu}(V,\tilde{E}) = \begin{bmatrix} - & 0 & . & . & \mu(v_1,\tilde{e}_n) \\ 0 & - & 0 & . & . \\ . & 0 & - & 0 & . \\ . & . & 0 & - & 0 \\ . & . & \mu(v_n,\tilde{e}_{n-m}) & 0 & - \end{bmatrix},$$

$$\tilde{G}_{\bar{\mu}}(V,\bar{E}) = \begin{bmatrix} - & 0 & . & . & \bar{\mu}(v_1,\bar{e}_n) \\ 0 & - & 0 & . & . \\ . & 0 & - & 0 & . \\ . & . & 0 & - & 0 \\ . & . & \bar{\mu}(v_n,\bar{e}_{n-m}) & 0 & - \end{bmatrix},$$

$$\tilde{G}_{\tilde{\mu}}(V,\bar{E}) = \begin{bmatrix} - & 0 & . & . & \tilde{\mu}(v_1,\bar{e}_n) \\ 0 & - & 0 & . & . \\ . & 0 & - & 0 & . \\ . & . & 0 & - & 0 \\ . & . & \tilde{\mu}(v_n,\tilde{e}_{n-m}) & 0 & - \end{bmatrix}.$$

The composition of morphisms is defined by

$$Hom_C(\tilde{G}_{\mu}(V,\tilde{E}),\tilde{G}_{\bar{\mu}}(\tilde{V},\tilde{E}),)\times Hom_C(\tilde{G}_{\bar{\mu}}(V,\tilde{E}),\tilde{G}_{\tilde{\mu}}(\tilde{V},E),)\rightarrow Hom_C(\tilde{G}_{\mu}(\tilde{V},\tilde{E}),\tilde{G}_{\tilde{\mu}}(V,\tilde{E}),).$$

Hence, there exists the category C defined over the fuzzy graphs.

This completes the proof.

Next theorem is based on

Next theorem is based on the application of cosine amplitude method. There are the two finite sets, vertices and edges. These finite sets constitute the fuzzy graph as the function defined by $\tilde{G}(V,\tilde{E})$ with the membership function

$$\mu = \begin{bmatrix} - & 0 & . & . & \mu(v_1, v_n) \\ 0 & - & 0 & . & \\ . & 0 & - & 0 & . \\ . & . & 0 & - & 0 \\ . & . & \mu(v_n, v_{n-m}) & 0 & - \end{bmatrix}.$$

Its discrete representation sets the concept of cosine amplitude. Basically, this method comprises with data samples. Further, these data samples will be applied to develop a security system. These data samples form the data array X,

$$X = \{x_{1,...,} x_n\}.$$

Each element is referred as the vector of length m,

$$x_i = \{x_{i_1} ,...., x_{i_m}\}.$$

This implies a statement, if there is the data sample then there will be the m-dimensional space. It means there is the one to one correspondence as vector to m-coordinate. Then, there exists a relation r_{ij}, compares with the pair of vectors (x_i, x_j), defined by,

$r_{ij} \rightarrow (x_{i}, x_j)$, the membership function under the state of relation R is $\mu_R(x_i, y_j)$ and the corresponding relation matrix will be of order n. Further, the computational method of r_{ij} will be discussed. This approach comprises with fuzzy system theory and rule reduction. Next theorem is based on the formulation for computing r_{ij}.

3.2. Theorem. Let $G(V,E)$ be a fuzzy graph, where $V = \{v_1 ,...., v_n\}$, and $E = \{e_1 ,...., e_n\}$ the membership function of $\widetilde{E}$ be

$$\mu = \begin{bmatrix} - & 0 & . & . & \mu(v_1, v_n) \\ 0 & - & 0 & . & \\ . & 0 & - & 0 & . \\ . & . & 0 & - & 0 \\ . & . & \mu(v_n, v_{n-m}) & 0 & - \end{bmatrix},$$

the relation be,

$$r_{ij} \rightarrow \left(\begin{bmatrix} x_{i_{11}} & & \\ & & \\ & & x_{i_{nn}} \end{bmatrix}, \begin{bmatrix} x_{j_{11}} & & \\ & & \\ & & x_{j_{nn}} \end{bmatrix} \right),$$

And the membership function be,

$$''_{R} \left(\begin{bmatrix} x_{i_{11}} & & \\ & & \\ & & x_{i_{nn}} \end{bmatrix}, \begin{bmatrix} x_{j_{11}} & & \\ & & \\ & & x_{j_{nn}} \end{bmatrix} \right),$$

Then, the computation of r_{ij} is defined by

$$r_{ij} = \begin{bmatrix} ''\left(\dfrac{x_{i_{11}}}{x_{j_{11}}} \right) & & \\ & & \\ & & ..\left(\dfrac{x_{i_{nn}}}{x_{j_{nn}}} \right) \end{bmatrix}.$$

Proof: Let the finite set of k-tuple objects be $X = \{x_1, ..., x_k\}$. The corresponding set of rules for every element of X is $R = \{r_1, ..., r_k\}$. Then there exists an Intersection Rule Configuration (IRC). IRC is a computational tool for computing the rule based independent values with significant computational time and security. This is represented by the following exponential relation with n number of input values,

$$R = r^n.$$

$$\text{Or, } R = r_i r_{i+1} \cdots$$

This is classified discretely for computing every element with the membership function through the Single Value Decomposition (SVD) method. SVD is based on linear algebra and coordinate transformation. Thus the set of unique transformation exists. This generates the distinct coordinate system. There will be the Takugi-Sugino output function for the inputs represented by

$$Z=(z_1,\ldots,z_n)=\frac{\sum_{i=1}^{R} z_i\prod_{j=1}^{n}\mu_j}{\sum_{i=1}^{R}\prod_{j=1}^{n}\mu_j}.$$

So, the fuzzy graph generalization of the element x_i into $\tilde{G}(\tilde{V},E)$ through Z is computed

by,

$$Z\ \frac{\sum_{i=1}^{R} z_i\prod_{j=1}^{n}\mu_j}{\sum_{i=1}^{R}\prod_{j=1}^{n}\mu_j}=\mu\left(\frac{x_{i_{11}}}{x_{j_{11}}}\right)+\ldots+\mu\left(\frac{x_{i_{m1}}}{x_{j_{m1}}}\right)$$

.This Z establishes the set of rules as follows:

Rule: If $A(x_1)$ and $B(x_2)$ then Z.
This generalizes for the finite set X and the fuzzy graph $\tilde{G}(\tilde{V},E)$ as follows:

$$(\tilde{G}(\tilde{V},E)(x_i,x_j,r_{ij}),\mu_{\tilde{G}}(x_i,x_j,r_{ij}),=\begin{bmatrix}((x_{i_{11}},x_{j_{11}},r_{11}),\mu_{\tilde{G}}(x_{i_{11}},x_{j_{11}},r_{11}))\\ \vdots\\ ((x_{i_{nm}},x_{j_{nm}},r_{nm}),\mu_{\tilde{G}}(x_{i_{nm}},x_{j_{nm}},r_{nm}))\end{bmatrix}.$$

Then, the corresponding relation over fuzzy graph is,

$$(R(x_i,x_j,r_{ij}),\mu_R(x_i,x_j,r_{ij}),=\begin{bmatrix}((x_{i_{11}},x_{j_{11}},r_{11}),\mu_R(x_{i_{11}},x_{j_{11}},r_{11}))\\ \vdots\\ ((x_{i_{nm}},x_{j_{nm}},r_{nm}),\mu_R(x_{i_{nm}},x_{j_{nm}},r_{nm}))\end{bmatrix}.$$

The Takugi-Sugino output function is,

$$(Z(x_i,x_j,r_{ij}),\mu_Z(x_i,x_j,r_{ij}),=\begin{bmatrix}((x_{i_{11}},x_{j_{11}},r_{11}),\mu_Z(x_{i_{11}},x_{j_{11}},r_{11}))\\ \vdots\\ ((x_{i_{nm}},x_{j_{nm}},r_{nm}),\mu_Z(x_{i_{nm}},x_{j_{nm}},r_{nm}))\end{bmatrix}.$$

Hence, the computational matrix of r_{ij} is,

$$r_{ij} = \begin{bmatrix} \cdot\cdot\left(\frac{x_{i_{11}}}{x_{j_{11}}}\right) & & \\ & & \\ & & \cdot\cdot\left(\frac{x_{i_{nn}}}{x_{j_{nn}}}\right) \end{bmatrix}.$$

This completes the proof.

Next, the digital security system is presented based on the above results. The security of this system interacts with the computational difficulty of r_{ij}. There is the compact key based on the fuzzy graph, fuzzy graph coloring and the category morphism. Hence its permutation forms the unique structure for developing the digital security system. This protocol becomes the foundation to propose the discrete and distinct cyber security systems.

4. The Protocol for Developing Cyber Security System:

4.1. Input:

$$\tilde{G}(V,\tilde{E}), \mu, \bar{\mu}, C, r_{ij}.$$

4.2. Permutation:

4.2.1. $Hom_C(\mu,\bar{\mu}) \times Hom_C(\bar{\mu},\tilde{\mu}) \rightarrow Hom_C(\mu,\tilde{\mu})$.

4.2.2. $\tilde{G}_\mu(V,\tilde{E}), \tilde{G}_{\bar{\mu}}(V,\tilde{E}), \tilde{G}_{\tilde{\mu}}(V,\tilde{E})$.

4.2.3. $Hom_C(\tilde{G}_\mu(V,\tilde{E}), \tilde{G}_{\bar{\mu}}(V,\tilde{E}),) \times Hom_C(\tilde{G}_{\bar{\mu}}(V,\tilde{E}), \tilde{G}_{\tilde{\mu}}(V,\tilde{E}),) \rightarrow Hom_C(\tilde{G}_\mu(V,\tilde{E}), \tilde{G}_{\tilde{\mu}}(V,\tilde{E}),)$.

4.3. Network:

4.3.1. $Z = \dfrac{\sum_{i=1}^{n} z_i \prod_{j=1}^{n} \mu_j}{\sum_{i=1} \prod_{j=1} \mu_j} = \mu\left(\dfrac{x_{i_{11}}}{x_{j_{11}}}\right) + \ldots + \mu\left(\dfrac{x_{i_{m1}}}{x_{j_{m1}}}\right)$

4.3.2. $$r_{ij} = \begin{bmatrix} \left(\frac{x_{i_{11}}}{x_{j_{11}}}\right) & & \\ & & \\ & & \cdots\left(\frac{x_{i_{nn}}}{x_{j_{nn}}}\right) \end{bmatrix}.$$

4.4. **Output:** The Takugi-Sugino function:

$$(Z(x_i, x_j, r_{ij}), \mu_Z(x_i, x_j, r_{ij}), = \begin{bmatrix} ((x_{i_{11}}, x_{j_{11}}, r_{11}), \mu_Z(x_{i_{11}}, x_{j_{11}}, r_{11})) & \\ & \\ & ((x_{i_{nn}}, x_{j_{nn}}, r_{nn}), \mu_Z(x_{i_{nn}}, x_{j_{nn}}, r_{nn})) \end{bmatrix}.$$

5. Conclusion: There are two key parameters for testing any cyber security protocol, security and efficiency. Sometimes, the system satisfies the probable security protocol but its computational complexity takes more time by the applied hard mathematical representation. Thus the system is referred secure but inefficient. The proposed cyber security protocol fulfills both the standards, security and efficiency. The category morphism mechanism transforms the chaotic fuzzy graph coloring into feasible finite matrix. This provides the probable security advantage. The Takugi-Sugino output function sets the faster operation over the fuzzy graph. Hence, this dual approach develops a secure network protocol and respective applications.

References

1. Zadeh, L.A., "Fuzzy sets", Information and Control, Volume 8, issue 3, June 1965, pages 338-353.

2. Klir, G.J.; Folger, T.A. Fuzzy Sets, Uncertainty, and Information; Prentice Hall: Englewood Cliffs, NJ, USA, 1988.

3. Mendel, J.M. Fuzzy logic systems for engineering: A tutorial. Proc. IEEE 1995, 83, 345–377. [CrossRef]

4. Zadeh, L.A. The concept of a linguistic variable and its application to approximate reasoning—I. Inf. Sci. 1975, 8, 199–249. [CrossRef]

5. Bustince, H.; Burillo, P. Mathematical analysis of interval-valued fuzzy relations: Application to approximate reasoning. Fuzzy Sets Syst. 2000, 113, 205–219. [CrossRef]

6. Goguen, J.A., Jr. Concept representation in natural and artificial languages: Axioms, extensions and applications for fuzzy sets. Int. J. Man-Mach. Stud. 1974, 6, 513–561. [CrossRef]

7. Zywica, P. Modelling medical uncertainties with use of fuzzy sets and their extensions. In Proceedings of the International ˙ Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems, Cádiz, Spain, 18 May 2018; Springer: Cham, Germany, 2018; pp. 369–380. [CrossRef]

8. Román-Flores, H.; Barros, L.C.; Bassanezi, R.C. A note on Zadeh's extensions. Fuzzy Sets Syst. 2001, 117, 327–331. [CrossRef]

9. Dubois, D.; Prade, H. Gradualness, uncertainty and bipolarity: Making sense of fuzzy sets. Fuzzy Sets Syst. 2012, 192, 3–24. [CrossRef]

10. Gehrke, M.; Walker, C.; Walker, E. Some comments on interval valued fuzzy sets! Structure 1996, 1, 2. [CrossRef]

11. Bustince, H. Indicator of inclusion grade for interval-valued fuzzy sets. Application to approximate reasoning based on interval-valued fuzzy sets. Int. J. Approx. Reason. 2000, 23, 137–209. [CrossRef] Appl. Sci. 2021, 11, 7668 31 of 31

12. Turksen, I.B. Interval-valued fuzzy sets and 'compensatory AND'. Fuzzy Sets Syst. 1992, 51, 295–307. [CrossRef]

13. Ramot, D.; Milo, R.; Friedman, M.; Kandel, A. Complex fuzzy sets. IEEE Trans. Fuzzy Syst. 2002, 10, 171–186. [CrossRef]

14. Ramot, D.; Friedman, M.; Langholz, G.; Kandel, A. Complex fuzzy logic. IEEE Trans. Fuzzy Syst. 2003, 11, 450–461. [CrossRef]

15. Greenfield, S.; Chiclana, F.; Dick, S. Interval-valued complex fuzzy logic. In Proceedings of the 2016 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Vancouver, BC, Canada, 24–29 July 2016; pp. 2014–2019.

16. Nasir, A.; Jan, N.; Gumaei, A.; Khan, S.U. Medical diagnosis and life span of sufferer using interval valued complex fuzzy relations. IEEE Access 2021, 9, 93764–93780. [CrossRef]

17. Chen, Z.; Aghakhani, S.; Man, J.; Dick, S. ANCFIS: A neurofuzzy architecture employing complex fuzzy sets. IEEE Trans. Fuzzy Syst. 2010, 19, 305–322. [CrossRef]

18. Yazdanbakhsh, O.; Dick, S. A systematic review of complex fuzzy sets and logic. Fuzzy Sets Syst. 2018, 338, 1–22. [CrossRef]

19. Tamir, D.E.; Rishe, N.D.; Kandel, A. Complex fuzzy sets and complex fuzzy logic an overview of theory and applications. Fifty Years Fuzzy Log. Its Appl. 2015, 326, 661– 681.

20. Dai, S.; Bi, L.; Hu, B. Distance measures between the interval-valued complex fuzzy sets. Mathematics 2019, 7, 549. [CrossRef]

21. Greenfield, S.; Chiclana, F.; Dick, S. Join and meet operations for interval-valued complex fuzzy logic. In Proceedings of the 2016 Annual Conference of the North American Fuzzy Information Processing Society (NAFIPS), El Paso, TX, USA, 31 October–4 November 2016; pp. 1–5.

22. Atanassov, K.T. Intuitionistic fuzzy sets. Fuzzy Sets Syst. 1986, 20, 87–96. [CrossRef]

23. Burillo, P.; Bustince, H. Intuitionistic fuzzy relations (Part I). Mathw. Soft Comput. 2016, 2, 5–38.

24. Atanassov, K.T. Interval valued intuitionistic fuzzy sets. In Intuitionistic Fuzzy Sets; Physica: Heidelberg, Germany, 1999; pp. 139–177.

25. Alkouri, A.S.; Salleh, A.R. Complex intuitionistic fuzzy sets. AIP Conf. Proc. 2012, 1482, 464. 26. Garg, H.; Rani, D. Complex interval-valued intuitionistic fuzzy sets and their aggregation operators. Fundam. Inform. 2019, 164, 61–101. [CrossRef]

27. Li, D.F. Multiattribute decision making models and methods using intuitionistic fuzzy sets. J. Comput. Syst. Sci. 2005, 70, 73–85. [CrossRef]

28. De, S.K.; Biswas, R.; Roy, A.R. An application of intuitionistic fuzzy sets in medical diagnosis. Fuzzy Sets Syst. 2001, 117, 209–213. [CrossRef]

29. Vlachos, I.K.; Sergiadis, G.D. Intuitionistic fuzzy information–applications to pattern recognition. Pattern Recognit. Lett. 2007, 28, 197–206. [CrossRef]

30. Lee, K.M.; LEE, K.M.; CIOS, K.J. Comparison of interval-valued fuzzy sets, intuitionistic fuzzy sets, and bipolar-valued fuzzy sets. In Computing and Information Technologies: Exploring Emerging Technologies; World Scientific: Hackensack, NJ, USA, 2001; pp. 433–439. [CrossRef]

31. W Diffie, M E Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 22, 1976, 644-654.

32. ElGamal, T., A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31, 1985, 469-472.

33. Goodman, R., Mcauley, A., New Trapdoor-Knapsack public key, IEEE Transaction on Information Theory, 132 (6), 1985, 56 – 65.

34. Koblitz, N., Elliptic curve cryptosystems, Mathematics of Computation, 48, 1987, 203-209.

35. Koblitz, N., Hyperelliptic cryptosystems, Journal of Cryptology, 1, 1989, 139-150.

36. Rivest, R.L., Shamir A., Adleman, L., A method for obtaining digital signatures and public key cryptosystems, Communication of the ACM, 21, 1978, 120-126.

37. Satoh, T., The canonical lift of an ordinary elliptic curve over a prime field and its point counting, Journal of the Ramanujan Mathematical Society, 15, 2000, 247-270.

38. Schirokauer, O., Discrete logarithms and local units, Philosophical Transactions of the Royal Society of London, Series A, 345, 1993, 409-423.

39. Schoof, R., Elliptic curves over finite fields and the computation of square roots mod p, Mathematics of Computation, 44, 1985, 483-494.

40. Schoof, R., Nonsingular plane cubic curves, Journal of Combinatorial Theory, Series A, 46, 1987, 183-211.

41. Semaev, I., Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, Mathematics of Computation, 67, 1998, 353-356.

42. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Computing, 26, 1997, 1484-1509.

43. Silverman, J., The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.

44. Silverman, J., The xedni calculus and the elliptic curve discrete logarithm problem, Designs, Codes and Cryptography, 20, 2000, 5-40.

45. Smart, N., The discrete logarithm problem on elliptic curves of trace one, Journal of Cryptology, 12, 1999, 193-196.

46. Stinson, D.R., Cryptography: Theory and Practice, CRC Press, Boca Raton, Florida, 1995.

47. Teske, E., Speeding up Pollard's rho method for computing discrete logarithms, Algorithmic Number Theory: Third International Symposium, Lecture Notes in Computer Science, Springer-Verlag, 1423, 1998, 541-554.

48. Thferiault, N., Index calculus attack for hyperelliptic curves of small genus, Advances in Cryptology — ASIACRYPT 2003, Lecture Notes in Computer Science, Springer-Verlag, 2894, 2003, 75-92.

49. Tobias, C., Design and analysis of cryptographic building blocks on non-abelian groups, Mitt.-Math.-Sem.-Giessen., Volume No. 253, 2004, 122.

50. E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, Advances in Cryptology — EUROCRYPT 2001, Lecture Notes in Computer Science, Springer-Verlag, 2045, 2001, 195210.

51. Washington, L., Elliptic Curves: Number Theory and Cryptography, CRC Press, 2003.